

Trabajo final de Grado Ingeniería en Sistemas – IUA

Tema:

**Estudio comparativo de entornos virtuales
aplicado a la toma de decisión de Pymes y
grandes empresas**



Alumno: Matías Oscar Sarmiento

Tutor: Eduardo Casanovas

Contenido

CAPÍTULO 1 –INTRODUCCION	4
1.1 Introducción	5
1.2 Situación Problemática	5
1.3 Problema	5
1.4 Objeto de Estudio.....	5
1.5 Campo de Acción.....	6
1.6 Objetivos	6
1.6.1 Objetivo general.....	6
1.6.2 Objetivos específicos	6
1.7 Idea a Defender / Propuesta a Justificar / Solución a Comprobar	6
1.8 Delimitación del Proyecto.....	6
1.9 Aporte Práctico	7
1.10 Aporte Teórico	7
1.11 Factibilidad.....	7
1.11.1 Factibilidad Técnica:.....	7
1.11.2 Factibilidad Operativa:.....	7
1.11.3 Factibilidad Económica:	7
1.12 Métodos de Investigación	7
1.13 Marco Teórico.....	8
CAPÍTULO 2: MARCO CONTEXTUAL	9
2.1 Conceptos básicos	10
2.1.1. Introducción de virtualización	10
2.1.2 Virtualización en las organizaciones TI.....	11
2.1.3 Tipos de virtualización.....	12
2.1.4 Beneficios de la Virtualización	14
2.2 Entornos del objeto de estudio	15
2.3 Relación tesista y objeto de estudio	15
2.4 Análisis de los problemas observados	15
CAPÍTULO 3: MARCO TEÓRICO.....	17
3.1 Características principales de Citrix Xen Server	18
3.2 Características principales de Windows Hyper-V 2012	25
3.3 Características principales de VmWare Vsphere 5.X.....	35
CAPITULO IV - Preparación de hardware Y Entornos de Prueba	42
4.1 Preparación de Hardware	43
4.2 Instalaciones y experiencia de usuario de Hyper-V-2012	47

4.3 Instalaciones y experiencia de usuario de Xen Server	55
4.4 Instalaciones y experiencia de usuario de ESXi 5.X	65
CAPITULO V - ESTUDIO COMPARATIVO DE HERRAMIENTAS.....	73
5.1 Estudio comparativo: Vsphere 5.x, Xen Server 6.X y Hyper v 2012 R2	74
5.1.1. Instalación del producto, Consola de administración y Experiencia de Usuario:.....	74
5.1.2. Posición en el Mercado:	74
5.1.3 Costos de Licencia y Soporte:.....	75
5.1.4 Costos de Herramientas de Gestión y Gestión Centralizada:	76
5.1.5 Gestión de Hosts Físicos:.....	76
5.1.6 Funcionalidad de Integración de RBAC (Role-based access control) con AD (Active Directory) Control de acceso basado en roles integrado con Active Directory	77
5.1.7 Funcionalidad de Gestión multiplataforma de virtualización	80
5.1.8 Funcionalidad de Gestión por navegador web (sin cliente e independiente).....	80
5.1.9 Funcionalidad de Gestión avanzada de operaciones	81
5.1.10 Funcionalidad de Actualizaciones del Hypervisor.....	82
5.1.11 Funcionalidad de Actualizaciones de Máquinas virtuales	83
5.1.12 Funcionalidad de Snapshot en Vivo.....	84
5.1.13 Funcionalidad de Backups Integrado	84
5.1.14 Funcionalidad de Pool de recursos.....	87
5.1.15 Funcionalidades de Seguridad	88
5.1.16 Funcionalidades de Alta disponibilidad	92
5.1.17 Funcionalidades de Migración de máquinas virtuales en vivo:	94
5.1.18 Funcionalidades de Migración automática de máquinas virtuales y gestión de energía.....	95
5.1.19 Capacidades de Configuración de Nodos / Hosts Físicos.....	97
5.1.20 Pruebas de Performance	98
CAPITULO VI – RESULTADOS y CONCLUSION	101
6.1. Resultados Obtenidos.....	102
6.2 Conclusiones	103
Bibliografía	104
Glosario.....	107
Datos Personales del Alumno	107
Datos Personales del Asesor	107

CAPÍTULO 1 –INTRODUCCION

1.1 Introducción

La virtualización está de moda, antes era una tecnología al alcance solamente de las grandes compañías, ahora cualquier empresa pequeña o mediana puede obtener los beneficios de la virtualización, pero ¿qué es y para qué sirve?

La reducción de precios en el hardware y la presencia de productos software de virtualización cada vez más asequibles ha democratizado esta tecnología, que bien utilizada, puede poner a nuestra disposición más opciones de sistemas operativos, costes menores y un mayor control sobre nuestra estructura.

Dentro de la estructura informática de una empresa hemos visto que los servidores pueden desempeñar un papel importante para centralizar recursos y utilizar herramientas específicas que incrementan la productividad a través de la mejora de los procesos de producción, planificación o comunicación. La tecnología nos ofrece la posibilidad de disponer de varios servidores con características muy distintas pero instalando físicamente una sola máquina. Este sistema se llama virtualización. A través de esta tecnología es posible hacer que los recursos de un ordenador, en este caso un servidor, puedan ser compartidos por una o más máquinas virtuales que se comportarán, a su vez como servidores reales.

1.2 Situación Problemática

Actualmente no hay mucha información confiable sobre las herramientas de virtualización a nivel sistema operativo. En el momento de elegir una herramienta de virtualización sobre servidores, la información disponible suele encontrarse orientada hacia la empresa dueña de la herramienta, no encontrándose muchos documentos precisos en la ayuda de la toma de decisiones.

La problemática surgió desde Intel Argentina en el momento que se decidió cambiar de herramienta de virtualización por los costos que esta misma implicaba y a la hora de intentar plantear alguna alternativa nos dimos cuenta que no había mucha información conjunta sobre las herramientas de virtualización para la toma de decisión y que deberíamos realizar un estudio de **investigación**.

1.3 Problema

Falta de información confiable sin orientación comercial para la toma de decisiones para elegir una herramienta de virtualización a nivel sistema operativo

1.4 Objeto de Estudio

El objeto de estudio serán las 3 soluciones de virtualización a nivel sistema operativo más importantes que están disponible en el mercado, la herramienta que nos propone VMWare: Vsphere 5.x, la solución que nos propone Citrix: Xen Server 6.x y opción que nos presenta Microsoft: Hyper-V 2012. El objetivo es investigar las diferentes soluciones y luego elaborar un documento para la toma de decisión que pueda ser utilizado en pymes y en grandes empresas, las cuales poseen distintas características tanto de presupuesto como de estructura jerárquica.

1.5 Campo de Acción

El campo de acción va a estar delimitado por el análisis comparativo a nivel técnico y económico de la herramienta de virtualización de VmWare: Vsphere 5.x, la herramienta de virtualización de Citrix: Xen Server 6.x y la herramienta de virtualización que nos ofrece Microsoft: Hyper-V 2012 sobre un hardware HP enclosure y Blades GX de última generación.

1.6 Objetivos

1.6.1 Objetivo general

Elaborar un documento comparativo que permita a las empresas tanto medianas como grandes, poder tomar una decisión con cierto grado de eficacia a la hora de tener que elegir por algún método de virtualización.

1.6.2 Objetivos específicos

- Investigar las tecnologías VmWare: Vsphere 5.x, Citrix: Xen Server 6.x y Microsoft: Hyper-V 2012
- Realizar análisis de viabilidad técnica de la implementación de las herramientas sobre el hardware disponible.
- Realizar un estudio comparativo de las mismas sobre un mismo requerimiento de hardware en este caso: un hardware HP enclosure y Blades Gx de última generación
- Crear un documento para la toma de decisión.

1.7 Idea a Defender / Propuesta a Justificar / Solución a Comprobar

Lo que se va a realizar es un documento para la toma de decisión con interés educativo y de investigación para la toma de decisión para la virtualización de sistemas operativos y sin intereses comerciales, lo que justificaría el proyecto.

1.8 Delimitación del Proyecto

- Se hará un estudio técnico y económico de las tecnologías VmWare: Vsphere 5.1, Citrix: Xen Server 6 y Microsoft: Hyper-V 2012
- El estudio técnico se realizara sobre un hardware BL380 Gx sobre cajones (enclosures) HP
- El estudio se realizara con máquinas virtuales: Windows 7, Windows 2008, Windows 2012 y Linux

1.9 Aporte Práctico

Cualquier empresa sea una Pymes o una gran empresa se beneficiará del documento realizado en este proyecto, ya que obtendrán un documento sin interés comercial y de gran utilidad a la hora de implementar o intentar cambiar la tecnología de virtualización.

1.10 Aporte Teórico

Al tratarse de tecnologías de virtualización de última generación, al poseer hardware de última generación y al no tener orientación comercial, el estudio que realizamos puede ser muy interesante para cualquier empresa internacional o nacional que necesite empezar en el mundo de la virtualización o que simplemente quiera analizar un cambio de tecnología.

1.11 Factibilidad

1.11.1 Factibilidad Técnica:

Se dispone de un laboratorio en la empresa Intel Argentina y de los permisos necesarios para su uso a los efectos de realizar las pruebas para este trabajo. También se poseen los conocimientos básicos de IT para poder realizar el trabajo.

1.11.2 Factibilidad Operativa:

Esta el interés de Intel para analizar si la herramienta de virtualización que se está utilizada es la correcta o puede ser beneficioso un cambio.

1.11.3 Factibilidad Económica:

Es económicamente factible ya que poseemos el hardware necesario y el software junto con sus respectivas licencias para la investigación, por lo tanto no será necesario ningún tipo de inversión/gasto adicional.

1.12 Métodos de Investigación

El método de investigación utilizado en el proyecto será el método empírico investigación, que permite efectuar el análisis preliminar de la información, así como verificar y comprobar las concepciones teóricas. El fundamento radica en la percepción directa del objeto de investigación y del problema. Su aporte al proceso de investigación es resultado fundamentalmente de la experiencia. Estos métodos posibilitan revelar las relaciones esenciales y las características fundamentales del objeto de estudio a través de procedimientos prácticos con el objeto y diversos medios de estudio.

1.13 Marco Teórico

El propósito de la teoría es definir y explicar el funcionamiento junto con las ventajas y desventajas de las diferentes tecnologías existentes en el mercado con respecto a la virtualización. Otro de los propósitos es explicar los beneficios de la implementación del proyecto y los beneficiados con el mismo. Para la recopilación de dicha bibliografía se utilizarán diferentes medios de consulta (Libros, Newsletters, Internet, Revistas de tecnología).

CAPÍTULO 2: MARCO CONTEXTUAL

2.1 Conceptos básicos

Antes de introducirnos dentro del desarrollo de la investigación, es importante mencionar algunos conceptos básicos que permitirán al lector seguir este documento sin problemas.

2.1.1. Introducción de virtualización

La tarea de reducir los costos operativos y mejorar la agilidad operativa es una tarea de la cual están bajo presión constante los responsables de Tecnologías de Información (IT) como también de con la necesaria gestión de la seguridad, el cumplimiento de normativas legales y ofrecer niveles de servicio cada vez más eficientes manteniendo los máximos niveles de satisfacción del usuario.

La presión por reducir estos costos operativos es más complicada debido al crecimiento exponencial que estamos experimentando gracias al avance de la tecnología y al procesamiento de información masiva que se produce en las organizaciones en la actualidad.

Los precios del hardware se reducen y con ellos la compra o difusión indiscriminada de servidores y estaciones de trabajo, factor que añade nuevos problemas como un sobre exceso de capacidad instalada, problemas de sobrecalentamiento de los centros de datos y aislamiento de distintos tipos de información en instalaciones con grandes cantidades de servidores y puestos de trabajo. Asimismo para el software, la frecuencia y la complejidad creciente que presentan los procesos de distribución de aplicaciones están poniendo a prueba la capacidad de los departamentos de IT. Una encuesta reciente de Gartner muestra que, a nivel mundial, las organizaciones dedican el 70 por ciento de su presupuesto de IT a mantener lo que tienen, y solo el 30 por ciento a nuevas iniciativas. El hallar la manera de reducir el creciente costo de mantenimiento de las aplicaciones y sistemas existentes se ha convertido en el reto de un departamento de IT. Si bien las tendencias de hardware y software están dando lugar a una nueva era en el acceso a la información también significan un reto para poder administrar tantos servidores, estaciones de trabajo y aplicaciones a un costo bajo y de una manera eficiente. La virtualización es una herramienta que nos ayuda a afrontar todos estos inconvenientes actuales que tienen los departamentos de IT.

La Virtualización es la abstracción de los recursos de una computadora, a través de un elemento llamada Hypervisor o VMM (Virtual Machine Monitor) que crea una capa de abstracción entre el hardware de la máquina física (host) y el sistema operativo de la máquina virtual (virtual machine, guest), siendo un medio para crear una versión virtual de un dispositivo o recurso, como un servidor, un dispositivo de almacenamiento, una red o incluso un sistema operativo, donde se divide el recurso en uno o más entornos de ejecución según los entornos que estemos virtualizando. Esta capa de software (VMM) maneja, gestiona y arbitra los cuatro recursos principales de una computadora (CPU, Memoria, Red, Almacenamiento) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. De modo que nos permite tener varios ordenadores virtuales ejecutándose sobre el mismo ordenador físico.

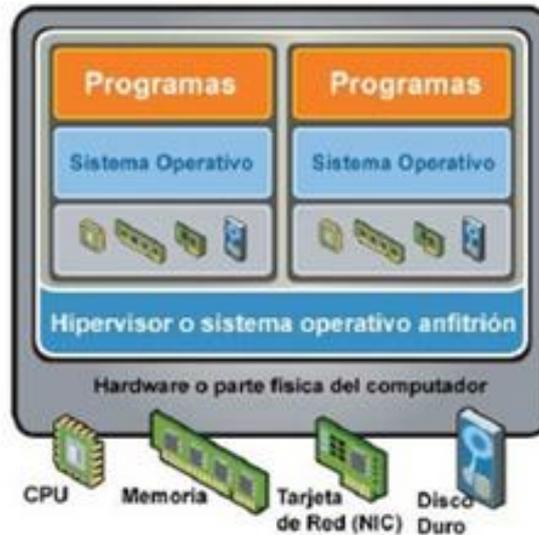


Figura 2.1: modelo de virtualización según VmWare

2.1.2 Virtualización en las organizaciones TI

En las organizaciones de TI en todo el mundo se enfrentan a retos verdaderamente complejos y situaciones extremas que deben superar tanto dentro como fuera de la empresa si desean mantener su competitividad en el mercado y llegar a ser una empresa modelo que quede en la mente de sus consumidores. Algunos de esos retos son:

- Oleadas continuas de amenazas a la seguridad (y dentro de ellas, la creciente importancia que tienen las vulnerabilidades del sistema y los intentos de robo de información).
- Los costes cada vez más elevados de las actividades propias del ciclo de vida de aplicaciones, como la distribución e implantación, las actualizaciones o el soporte.
- Las exigencias de los clientes (internos y externos) de servicios de IT de mayor calidad y una puesta en marcha de los servicios más ágil.
- La proliferación de máquinas (servidores y puestos de trabajo), que dan como resultado infraestructuras de data center y desktop enormemente complejas, masivas y difíciles de gestionar.

La virtualización al momento de reducir costos:

- Disminuye dramáticamente el número de servidores físicos (generando rápidos ahorros en energía, enfriamiento y espacio) ¿Cómo se logra? Convierte los servidores actuales en máquinas virtuales que son hospedadas en servidores físicos logrando una consolidación. En práctica se puede consolidar varias máquinas virtuales por servidor físico.
- Mejora el rendimiento de las inversiones en equipo y la utilización del hardware (antes de la virtualización es común encontrar que los servidores se encuentran trabajando entre un 5 y 10%, y después de la virtualización se aprovecha mejor el hardware asegurando un 70-80% de utilización). En otras palabras antes de virtualizar los servidores por cada dólar invertido en hardware, sólo se utilizan \$10centavos en el mejor de los casos y \$90 centavos están desperdiciados.

- Incrementa la productividad de los usuarios, pues en un ambiente virtual, si un servidor físico se descompone o requiere mantenimiento, no hay downtime ya que es posible apagar los servidores físicos y las máquinas virtuales que se hospedan ahí se viajan (prendidas y con usuarios conectados) hacia otro servidor.
- Reduce el tiempo y costo de provisionar nuevos servidores de semanas/meses a minutos/horas, es decir, si nos piden tener listo 5 servidores nuevos, el tiempo en que nos lo entregan, se instalan los drivers, sistemas operativos, aplicaciones y se unen a la red tardaríamos semanas o meses, pero en un ambiente virtual solo tardaríamos minutos.

Las organizaciones que están adoptando este modelo se encuentran alargando la vida útil de las máquinas actuales hasta por 5 o 7 años más. También es posible generar ahorros de energía si se adoptan clientes ligeros, que no es más que una caja con conectores USB (para conectar teclado, mouse, monitor, impresoras). Los clientes ligeros se encargarán de prender y conectarse a nuestra máquina virtual. En empresas que utilizan clientes ligeros, además de generar ahorros de energía, se olvidan de reemplazar memorias y discos duros por 10 años. Y por si fuera poco, si en una sucursal un cliente ligero llegara a fallar, los niveles de servicio dependerían de lo que la mensajería se tarda en entregar un cliente ligero (pues al llegar, sólo es necesario conectar a la red y automáticamente trae nuestros escritorios con sistemas operativos, aplicaciones, nuestra configuración y archivos, y hasta nuestro fondo de pantalla preferido).

2.1.3 Tipos de virtualización

La virtualización puede ser clasificada por los siguientes tipos: Virtualización por clientes, virtualización por sistemas operativos, virtualización de aplicaciones, emulación de hardware y paravirtualización.

Virtualización por Clientes: Primeramente entendemos que clientes son aquellos computadores de escritorio, portátiles o terminales brutas que se conectan a uno o varios servidores para hacer el trabajo que necesitan, esta idea es muy popular en las compañías, este concepto se basa en la arquitectura o concepto de cliente servidor. Entonces este tipo de virtualización de clientes se produce en máquinas que se conectan a los servidores para realizar su trabajo, como es el caso de teletrabajo.

Virtualización por Sistemas Operativos: Este tipo de virtualización se da cuando primero tenemos un sistema operativo (SO) base o anfitrión en el cual instalamos un programa de virtualización que nos permite instalar a su vez otros sistemas operativos (invitados) que trabajan encima del sistema operativo principal, esto gracias a la capa de virtualización puesta por un software que nos permite esta opción de virtualizar, capa que llamamos en la definición anterior como Hypervisor.

Los sistemas operativos invitados funcionan de forma tal que no se dan cuenta que están siendo virtualizados sobre otro sistema operativo anfitrión. Por otra parte las aplicaciones que trabajan dentro de los invitados lo hacen como si estuviesen funcionando en un computador dedicado para ellos. Esta forma de virtualizar también es conocida como virtualización en contenedores pues los SO invitados están contenidos en una especie de caja que le permita trabajar de forma casi independiente, claro todo esto basado en la disponibilidad del SO anfitrión quien por obvias razones debe estar funcionando bien primero para permitir el funcionamiento de los invitados. Esta forma de virtualizar es eficiente e ideal cuando se requieren máquinas virtuales con un mismo sistema operativo, también reduce los costos de licencias pues con un solo sistema

operativo se pueden montar el anfitrión y todas sus máquinas virtuales. Un ejemplo de virtualización por Sistema operativo es VmWare Workstation que podemos instalarlo en un ordenador común y correr ahí mismo una máquina virtual.

Virtualización de aplicaciones: Este tipo de virtualización presenta la idea de poder tener en un sistema Operativo anfitrión o invitado un programa de aplicación (como por ejemplo un procesador de textos) que pueda ser ejecutado en memoria, sin la necesidad de tener que instalarlo en este Sistema operativo, su utilidad radica sobretodo en el problema que se genera cuando se instalan varios programas, lo que genera que el registro de Windows se rellene de entradas hacia estos programas, que no está mal, el problema en si es que cuando deseemos desinstalar estos programas dejan entradas vacías o cruzadas en este registro de Windows lo cual interfiere o atrasa el rendimiento de nuestro servidor de aplicaciones que estemos ofreciendo a nuestros clientes. Un ejemplo de virtualización de aplicaciones es Citrix XenApp.

Emulación de hardware Este tipo de virtualización presenta la emulación de hardware, es la instalación de software de virtualización (hypervisor) antes de la instalación de cualquier otro Sistema operativo invitado, este hypervisor presenta el hardware del computador a todos los sistemas operativos instalados emulando los recursos que este tiene. El hypervisor también coordina el acceso a los recursos del computador que se da por parte de los sistemas operativos instalados haciendo las veces de guarda de tránsito que decide quien va primero y quien tiene que esperar para usar los recursos. Esta forma de virtualizar tiene muchas ventajas, pues las máquinas virtuales instaladas pueden ser completamente movidas de un computador físico a otro, incluso sin tener que apagarlas, esto claro si se cuenta con el software apropiado como VmWare Vmotion. También es ideal cuando se requieren diferentes sistemas operativos corriendo en un solo PC físico, como por ejemplo Linux, Windows, Solaris o cualquier otro sistema operativo, un ejemplo de emulación de hardware es Windows 2012 Hyper-v.

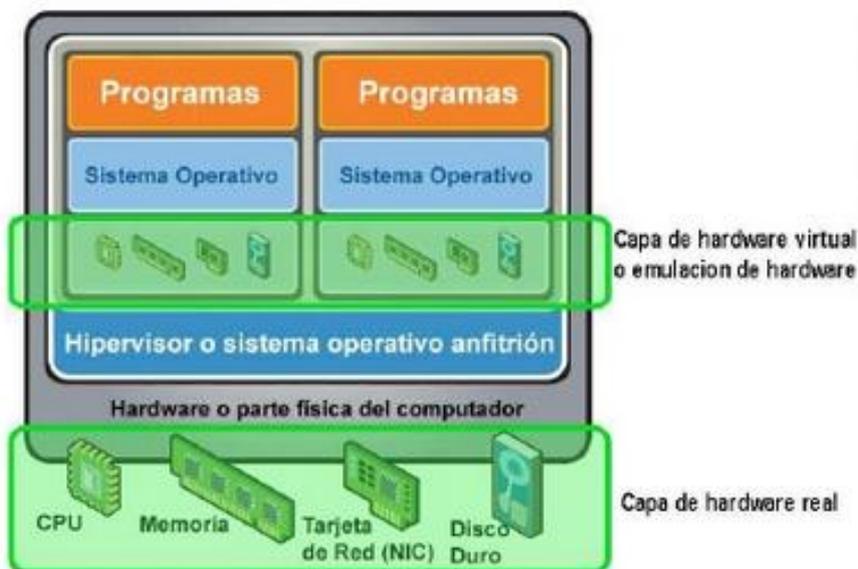


Figura 2.2: modelo de virtualización y tipos de capas según VmWare

Paravirtualización: Esta forma de virtualizar servidores no se genera ninguna emulación de hardware, por el contrario el hypervisor coordina el acceso de los sistemas operativos invitados a los recursos del computador físico, mejor dicho la paravirtualización no es enteramente virtualización como en los otros casos, pues los anfitriones interactúan de manera indirecta con los

recursos físicos del computador como cuando se tiene un computador dedicado. Esta forma de virtualizar es más bien una forma de compartir los recursos por tiempos cortos o a quien los necesite, dándole procesador o memoria o tarjeta de red al anfitrión que lo pide e intercalando el uso de estos entre los anfitriones. Este sistema tiene varias ventajas, entre ellas la poca carga que le da al procesador al no tener que tener una capa completa de virtualización que se encarga de administrar los recursos y virtualizarlos. Otra de las ventajas, es que los sistemas invitados no tienen que limitarse a los accesorios de hardware que sean soportados por el hypervisor, pues al invitado actuar directamente con la parte física es posible manejar todos los accesorios que maneja el sistema operativo montado en el invitado



Figura 2.3: modelo de Para virtualización

2.1.4 Beneficios de la Virtualización

Uso/costo menor energía

La electricidad requerida para que funcionen los centros de datos de clase empresarial ya no está disponible en suministros ilimitados, y el costo está en una espiral ascendente. Por cada dólar gastado en un servidor hardware, un dólar adicional es gastado en energía (incluyendo el costo de los servidores en función y los enfriadores). Utilizando virtualización para consolidar hace posible cortar el consumo total de energía y ahorrar dinero de una manera significativa.

Índices de utilización más altos

Antes de la virtualización, los índices de utilización del servidor y almacenamiento en los centros de datos de la empresa rondaban menos del 50% (de hecho, del 10% al 15% de los índices de utilización fueron los más comunes). A través de la virtualización, las cargas de trabajo pueden ser encapsuladas y transferidas a los sistemas inactivos o sin uso, lo cual significa que los sistemas existentes pueden ser consolidados, así que las compras de capacidad adicional del servidor pueden ser retrasadas o evitadas.

Ahorros de espacio

La extensión del servidor permanece como un serio problema en la mayoría de los centros de datos empresariales, pero la expansión del centro de datos no es siempre una opción, con los costos de construcción promediando miles de dólares por pie cuadrado.

La virtualización puede aliviar la tensión mediante la consolidación de muchos sistemas virtuales en menos sistemas físicos.

Restauraciones rápidas

En el caso de realizar una restauración de nuestro equipo, la copia de seguridad ante un desastre es rápida y sencilla, en cualquier sistema virtualizado.

Lo cual nos asegura que ante un fallo importante, podremos recuperarnos en un plazo bastante más reducido que con un sistema normal.

2.2 Entornos del objeto de estudio

El objeto de estudio a lo largo del desarrollo de este proyecto será el estudio comparativo de los entornos virtuales a nivel sistema operativo utilizado luego para la toma de decisiones de pymes y grandes empresas. La necesidad surge de una decisión que debe tomar Intel en cuanto a su sistema de virtualización. Intel es una empresa multinacional dispersa por todo el mundo en la cual tiene su sede principal internacional en Santa Clara, California y posee sedes en varias partes del mundo, actualmente tiene 82.500 empleados dispersos en todo el planeta del cual el 55 % de los empleados reside en EE. UU. Actualmente el CEO de la empresa es Brian M. Krzanich, el presidente es Renée J. James, y posee unos Ingresos netos de aproximadamente USD53, 3 mil millones.

Intel en Argentina está ubicada en Córdoba por medio de su centro de desarrollo de software y en Buenos Aires el cual es un centro dedicado a la comercialización.

Nuestro proyecto está enfocado a satisfacer la necesidad de Intel Córdoba y su centro de desarrollo de software en la cual tiene un entorno de virtualización con VmWare.

2.3 Relación tesista y objeto de estudio

El origen de este proyecto surge fundamentalmente de la necesidad de Intel de cambiar de tecnología de virtualización y de las pocas alternativas de información confiables con respecto a los distintos tipos de virtualización ofrecidas con sus respectivos beneficios para luego realizar la toma de decisiones.

Al darnos cuenta de esta falta de información en la red global, nos pareció interesante trabajar sobre un documento comparativo de herramientas de virtualización para contribuir con las empresas que lo puedan llegar a necesitar, así como con Intel.

2.4 Análisis de los problemas observados

Uno de los principales problemas que se nos planteó fue la poca información en español que hay sobre virtualización la cual solucionamos con más horas de búsqueda y traduciendo personalmente algunos documentos.

Otra de las dificultades que nos encontramos fue conseguir la forma y/o herramienta a utilizar para realizar las comparaciones de performance, La cual lo pudimos solucionar invirtiendo horas de investigación sobre las diferentes herramientas del mercado.

CAPÍTULO 3: MARCO TEÓRICO

3.1 Características principales de Citrix Xen Server

Citrix XenServer

Citrix XenServer Server es desde la versión 6.2, una plataforma de virtualización de nube, servidores y escritorios, Open Source y gratuita, desarrollada en conjunto por una amplia comunidad (proyecto Xen) y por Citrix. En esta versión están disponibles de manera gratuita, todas las funcionalidades que anteriormente solo estaban presentes en las versiones de pago más avanzadas. De esta manera las empresas de cualquier tamaño tienen a su disposición esta potentísima solución a su alcance. Además cuenta con certificaciones de compatibilidad (Hardware CompatibilityList: <http://hcl.xensource.com/>) y ciclos de vida, pues sí es producto comercial en el sentido de que se puede contratar un soporte con Citrix (Citrix Premier Support 24 x 7), y esto permite también la instalación de las actualizaciones y upgrades que pueda publicar dicha empresa.

El proyecto Xen desarrolla el HypervisorXen, open source. Tiene 10 años de desarrollo, lo que brinda una gran solidez. Es parte de la Linux Foundation y tiene licencia GPLv2. Utiliza el potente proyecto Open-sourceHypervisorXen. Es desarrollado y gestionado por Linux Foundation. Este hypervisor es utilizado por XenServer como el núcleo de su arquitectura, a la que Citrix añade otros componentes propios y XenCenter, la consola de administración.

El soporte para esta versión de Citrix XenServer se vende por socket. Es el equivalente a la anterior licencia Platinum, además de otras ventajas.

Arquitectura y características

Arquitectura

Una infraestructura básica de XenServer se compone, al igual que los demás entornos de virtualización corporativa más importantes (VMWare vSphere y Microsoft Hyper-V), de unos hosts físicos con el hypervisor instalado (XenServer), en los que se encuentran alojadas las máquinas virtuales, y una interfaz de administración (XenCenter, principalmente, o los comandos xe).

XenCenter:

Consola de administración instalada en un PC para gestionar el entorno XenServer

Servidores XenServer:

Servidores host físicos que proporcionan mediante el hipervisor los recursos hardware en los que se ejecutan las máquinas virtuales.

Shared Storage:

Almacenamiento compartido por los servidores XenServer donde se ubican las máquinas virtuales.

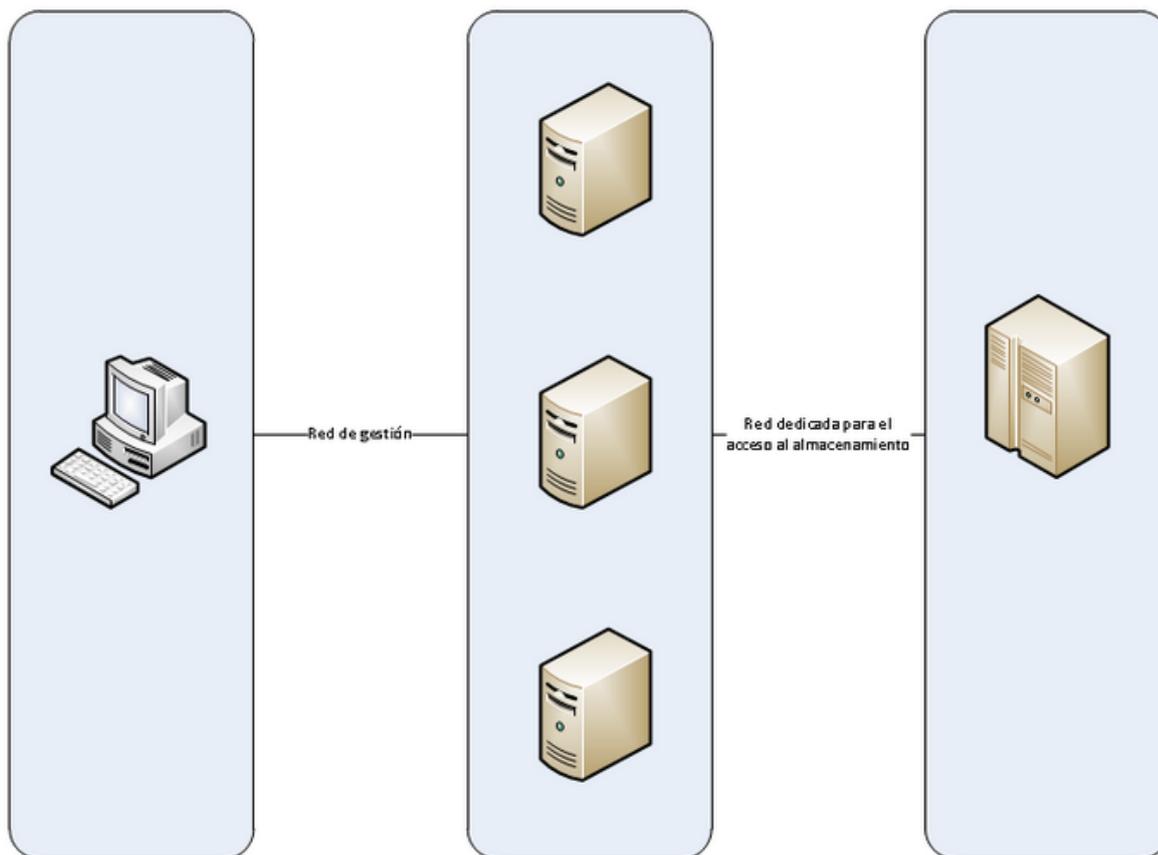


Figura 3.1: arquitectura de XenServer

Hypervisor

El hypervisor XenServer abstrae el hardware físico de los hosts y se lo presenta a medida a las máquinas virtuales. Para realizar esta abstracción, XenCenter utiliza una máquina virtual privilegiada y securizada llamada dom0 (también llama Control Domain o domain0), que ejecuta xapi, el conjunto de herramientas que gestionan XenServer. Además, xapi también ejecuta los drivers de los dispositivos físicos de almacenamiento, hardware, etc.

Storage Repositories

Las máquinas virtuales, físicamente, son ficheros almacenados en un recurso en disco. Estos recursos son denominados storage repository o SR en la jerga XenServer. Pueden ser locales (discos internos en los hosts), o remotos. Un SR remoto se puede crear sobre distintos tipos de almacenamiento:

- NFS VHD
- Software iSCSI
- Hardware HBA
- Fibre Channel
- Fibre Channel over Ethernet (FCOE)

Resource Pools

Si se dispone de más de un host XenServer es recomendable hacer uso de los resource pools. Un Resource Pool es un agrupamiento lógico de servidores que permite su administración conjunta, así como la posibilidad de hacer uso de XenMotion para la migración de máquinas virtuales en ejecución entre los distintos hosts del agrupamiento. En un resource pool puede haber hasta 16 servidores, de similares características, versiones y nivel de parcheado. Si los hosts contenidos en un resource pool son de características idénticas, se denomina pool homogéneo. Si por el contrario existen pequeñas diferencias, se denomina pool heterogéneo. Los resource pools presentan una arquitectura replicada con modelo maestro – esclavo. Uno de los hosts es el master (maestro), a través del cual se administra el pool. La información de la configuración del pool está repartida, por lo que cualquiera de los otros hosts se puede convertir en master sin ninguna pérdida de funcionalidad o configuración. Si un pool tiene configurado un shared storage (un espacio de almacenamiento compartido entre los hosts del pool donde ubicar las máquinas virtuales), las máquinas virtuales dentro de los hosts podrán ser iniciadas en cualquiera de los hosts del pool, si el pool tiene suficiente memoria, y las máquinas virtuales se podrán mover en vivo entre los hosts (XenMotion). Además, si un host falla, sus máquinas virtuales se podrán ejecutar en otro.

XenMotion y High Availability

XenMotion permite mover las máquinas virtuales en ejecución entre distintos hosts sin que las aplicaciones se vean afectadas. De esta manera se pueden realizar tareas de mantenimiento en los hosts físicos de manera transparente a los usuarios. Mover una máquina virtual manualmente es tan sencillo como hacer clic con el botón derecho del ratón en ella y seleccionar “Migrate to Server”, seleccionando el servidor destino. También puede realizarse con comandos xe. No siempre se puede realizar esta migración de manera controlada. Por ejemplo, cuando un host con máquinas virtuales en ejecución sufre un fallo inesperado de hardware y queda fuera de línea, será necesario que la funcionalidad de High Availability esté habilitada para que las máquinas virtuales que se encontraban en ejecución en el host caído sean iniciadas automáticamente en otro host del pool. Además, si el host que falla es el master del pool, High Availability se encargará de promover otro host a master del pool. El reinicio automático de máquinas virtuales permite tenerlas siempre disponibles ante un fallo a nivel de host, máquina virtual o hypervisor.

El agrupamiento de interfaces de red, otra posibilidad disponible con XenServer, también proporciona redundancia de red, y un mayor ancho de banda si es necesario.

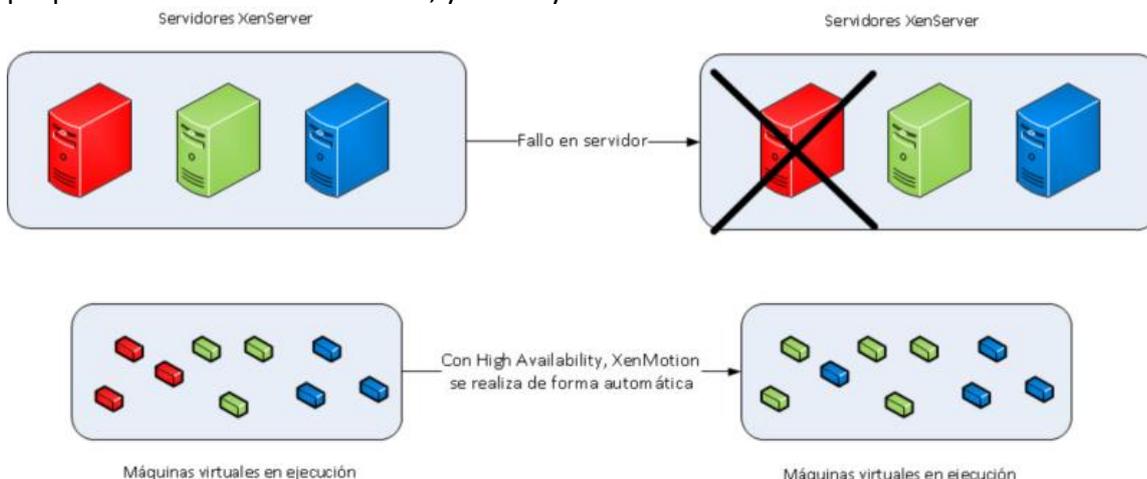


Figura 3.2: ejemplo de utilización de XenMotion High Availability

Shared Storage

Para que se puedan mover máquinas virtuales de un host a otro con XenMotion, es necesario que ambos puedan acceder al recurso de almacenamiento donde están ubicadas las máquinas virtuales. Es por tanto necesario, cuando se crea un resource pool, configurar un Shared Storage, o almacenamiento compartido, accesible por todos los hosts del resource pool, en el que se alojarán las máquinas virtuales. Un shared storage es un storage repository remoto. Es recomendable crear una red separada para conectar con los shared storage.

Xen Storage Motion

Xen Storage Motion es una extensión de XenMotion. Elimina la restricción de que las máquinas virtuales deban moverse entre hosts de un mismo resource pool y permite mover los discos de las máquinas virtuales en funcionamiento (junto con su entorno de ejecución) entre distintos resource pools, storage Repositories o incluso a un almacenamiento local. Mueve los discos antes de ejecutar XenMotion.

XenServer Tools

A las máquinas virtuales que se ejecuten dentro de XenServer se les deben instalar las XenServer Tools. Estas proporcionan los drivers necesarios para el correcto funcionamiento del sistema operativo y un agente de gestión. El soporte para máquinas virtuales en lo referente al sistema operativo invitado se ha extendido a:

- Microsoft Windows 8 y anteriores.
- Microsoft Windows Server 2012 y anteriores.
- SUSE Linux Enterprise Server (SLES) 11 SP2 (32/64-bit)
- Red Hat Enterprise Linux (RHEL) 5.8, 5.9, 6.3, 6.4 (32/64-bit)
- Oracle Enterprise Linux (OEL) 5.8, 5.9, 6.3, 6.4 (32/64-bit)
- CentOS 5.8, 5.9, 6.3, 6.4 (32/64-bit)
- Debian Wheezy (32/64-bit)

Templates

Si es necesario crear una nueva máquina virtual, se puede hacer clic con el botón derecho en uno de los hosts disponibles y elegir “New VM...”, y completar el asistente. Sin embargo, para agilizar el despliegue de las nuevas máquinas virtuales o cuando se quieren crear varias máquinas virtuales con la misma configuración inicial, se debe hacer uso de las templates (plantillas). En las máquinas con sistema operativo Windows, además se debe ejecutar la utilidad de Windows sysprep antes de convertir la máquina en plantilla. Una plantilla se puede crear desde un VM o desde un snapshot de una VM.

Snapshots

Si sobre una máquina virtual vamos a aplicar una actualización de sistema operativo o de una aplicación, y queremos tener la posibilidad de dar marcha atrás en el caso de que el resultado no sea satisfactorio, se puede crear, como en otras soluciones de virtualización,

un snapshot (instantánea) de la máquina virtual. Un snapshot guarda el almacenamiento, la configuración y la información de red de la máquina virtual, por lo que es muy útil para hacer un backup de la misma.

Site Recovery

Se puede configurar y mantener un plan de recuperación sitio a sitio, chequearlo frecuentemente para comprobar que sigue siendo válido.

Gestión del consumo de los hosts

Posibilidad de que dinámicamente las máquinas virtuales se muevan al menor número de hosts posibles, apagando los que no se encuentran en uso.

Optimización de memoria

Se comparte memoria de host sin utilizar entre las máquinas virtuales, para optimizar el rendimiento y el coste. La memoria no utilizada por las máquinas virtuales se comparte entre las que están en ejecución en cada host.

Intellicache

Espacio en disco local en el servidor utilizado por las máquinas de los escritorios virtuales de Xen Desktop para un mayor rendimiento.

Administración basada en roles

Se obtiene un acceso de seguridad por capas a los distintos objetos, como VMs. Permite mejorar la seguridad y delegar el uso y gestión de XenServer, al proporcionar una seguridad basada en niveles de permisos.

Alertas e informes de rendimiento

Para detectar fallos y realizar diagnósticos de rendimiento. El XenServer 6.x Performance and Monitoring Supplemental Pack ha sido integrado en XenServer 6.x. y extendido. Proporciona métricas del rendimiento de CPU, memoria, disco, red, almacenamiento entre otras.

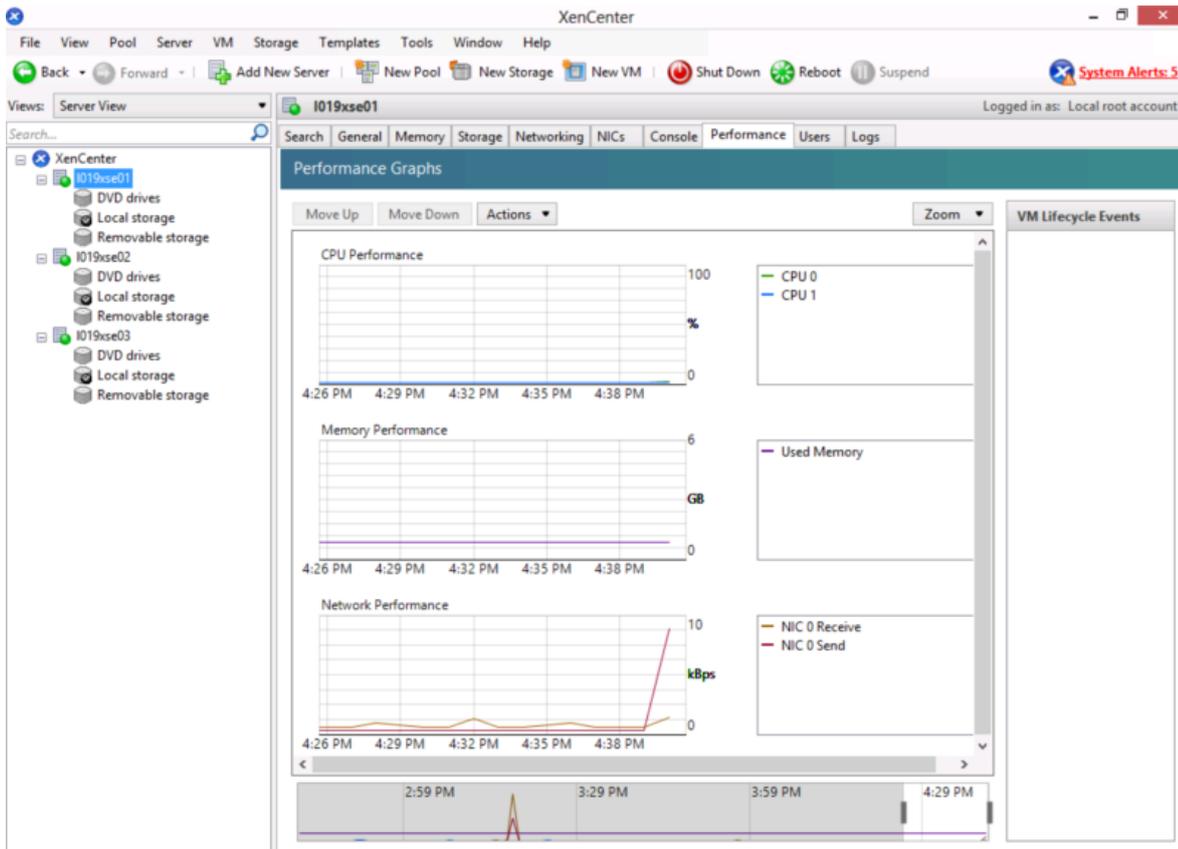


Figura 3.3: ejemplo un informe de rendimiento en XenServer

XenServer Conversión Manager

Permite transformar máquinas virtuales de VMware a XenServer.

Administración: XenCenter y Cli

La consola de administración XenCenter permite una gestión centralizada de hosts, máquinas virtuales, red, almacenamiento y demás funciones de XenDesktop. Comparte la gestión y configuración entre todos los hosts sin necesidad de mantener una base de datos externa. Proporciona acceso a las tareas de creación y administración de las máquinas virtuales y demás elementos como resource pools, storage repositories y permite monitorizar toda la infraestructura de hosts y máquinas virtuales.

Los comandos xe, disponibles en la interfaz local de cada servidor (o por ssh), dan acceso a todas las tareas que puedan hacerse desde XenCenter y más

```

[root@l019xse01 /]# xe sr-list
uuid ( RO) : f517241e-2462-b07c-8cb0-f1ecc6833a35
  name-label ( RW) : DVD drives
  name-description ( RW) : Physical DVD drives
  host ( RO) : l019xse01
  type ( RO) : udev
  content-type ( RO) : iso

uuid ( RO) : d941d7d3-51ec-217c-ba73-ab9588a07957
  name-label ( RW) : Local storage
  name-description ( RW) :
  host ( RO) : l019xse01
  type ( RO) : ext
  content-type ( RO) : user

uuid ( RO) : 3d2b1866-29ed-d84d-c4ba-e871fd789fd3
  name-label ( RW) : Removable storage
  name-description ( RW) :
  host ( RO) : l019xse01
  type ( RO) : udev
  content-type ( RO) : disk

uuid ( RO) : d34ffa70-7291-b9af-56cc-9cc13a7f0cc9
  name-label ( RW) : XenServer Tools
  name-description ( RW) : XenServer Tools ISOs
  host ( RO) : l019xse01
  type ( RO) : iso
  content-type ( RO) : iso

```

Figura 3.4: ejemplo de utilización de comandos CLI

Límites de Xenserver

Límites de los hosts:

- Procesadores lógicos: 160
- vCPUs por host: 3250
- Máquinas virtuales Windows concurrentes por host: 500
- Máquinas virtuales Linux concurrentes por host: 650
- RAM por Host: 1 TB
- NICS físicas: 16
- NICS virtuales: 512
- VLANS por host: 800
- Discos virtuales concurrentes: 512
- GPus por host: 8

Límites de las máquinas virtuales:

- CPUs virtuales por VM: 16
- RAM por VM: 128 GB
- Tamaño disco duro virtual: 2 TB
- Discos por VM: 7
- NICs por VM: 7

Límites de Resource pool:

- Hosts: 16
- VLANS: 800
- Paths a LUN: 8
- Multipathed LUNS por host (usados por SRs): 75
- Hosts por controlador de vswitch: 64

3.2 Características principales de Windows Hyper-V 2012

Windows Hyper-V Server 2012

Windows Hyper-V Server 2012 es la última herramienta de virtualización con la que Microsoft salió a competir en el mercado.

Históricamente Microsoft tenía un producto llamado Virtual-PC y otro llamado Virtual Server que dentro del mercado no podían competir con los productos de VmWare, el número uno en el mundo de la virtualización. Sin embargo, en la versión de Windows Server 2008 R2 incluyó la tecnología Hyper-V para virtualización que lo empezó a acercar lentamente y poder empezar a entrar al mercado de virtualización. Esta tecnología supuso la madurez de tecnología por parte de Microsoft, siendo un software robusto y sencillo de utilizar y con una clara ventaja, la que no tengamos que adquirir software adicional y que por ejemplo podamos instalar dos Windows Server 2012 adicionales (con su licencia) en nuestro servidor.

Esto es, si adquirimos Windows 2012 Server Edición Standard, podemos virtualizar dos servidores más totalmente legales. Por lo que tendríamos de partida una potente estructura para desplegar en nuestra empresa. Con la versión de Windows Datacenter, podremos virtualizar todos los Windows Server 2012 que necesitemos ilimitadamente.

Arquitectura y características

Arquitectura

Una infraestructura básica de Windows 2012 Hyper-V se compone, al igual que los demás entornos de virtualización corporativa más importantes (VMWare vSphere y Citrix XenDesktop), de unos hosts físicos con el hypervisor instalado (Hyper-V), en los que se encuentran alojadas las máquinas virtuales, y una interfaz de administración

Descripción del rol y la tecnología

El rol Hyper-V permite crear y administrar un entorno informático virtualizado mediante la tecnología de virtualización integrada en Windows Server 2012. Al instalar el rol Hyper-V, se instalan los componentes necesarios y, si lo desea, las herramientas de administración. Los componentes necesarios incluyen el hypervisor de Windows, el servicio Administración de máquinas virtuales de Hyper-V, el proveedor de WMI de virtualización y otros componentes de virtualización, como el bus de máquina virtual (VMbus), el proveedor de servicios de virtualización (VSP) y el controlador de infraestructura virtual (VID).

Las herramientas de administración del rol Hyper-V se componen de lo siguiente:

- Herramientas de administración basadas en GUI: Administrador de Hyper-V, un complemento Microsoft Management Console (MMC) y Conexión a máquina virtual, que da acceso a la salida de vídeo de una máquina virtual para poder interactuar con esa máquina.
- Cmdlets específicos de Hyper-V para Windows PowerShell. Windows Server 2012 incluye un módulo de Hyper-V que proporciona acceso de línea de comandos a toda la funcionalidad disponible en la GUI, así como también a la funcionalidad no disponible en ella. Para obtener más información acerca del módulo de Hyper-V, vea el tema sobre el Módulo de Hyper-V para Windows PowerShell. La tecnología Hyper-V virtualiza el hardware para proporcionar un entorno en el que sea posible ejecutar varios sistemas operativos al mismo tiempo en un equipo físico. Hyper-V permite crear y administrar máquinas virtuales y sus recursos. Cada máquina virtual es un equipo virtualizado y

aislado que puede ejecutar su propio sistema operativo. Un sistema operativo que se ejecuta dentro de una máquina virtual se denomina sistema operativo invitado.

Ciente Hyper-V

La tecnología Hyper-V ahora está disponible en una versión de sistema operativo de escritorio de Windows, lo cual permite usar Hyper-V sin instalar un sistema operativo de servidor.

Memoria dinámica

Entre las mejoras de la memoria dinámica se incluyen la posibilidad de configurar memoria mínima y la paginación inteligente, que es una técnica de administración de la memoria que proporciona una experiencia de reinicio confiable en las máquinas virtuales configuradas con menos memoria mínima que la memoria de inicio, lo cual permite mejorar la utilización del hardware, ya que facilitan que puedan ejecutarse más máquinas virtuales en un solo equipo físico al mismo tiempo.

Los recursos de memoria se pueden asignar más eficazmente a las máquinas virtuales, porque se puede configurar una máquina virtual con menos memoria mínima que la memoria de inicio, sin necesidad de prever que haya suficiente memoria disponible para reiniciar la máquina virtual.

Modulo de Hyper-V para Windows PowerShell

El Módulo de Hyper-V para Windows PowerShell incluye más de 160 cmdlets con los que administrar Hyper-V, máquinas virtuales y discos duros virtuales.

La disponibilidad de cmdlets para Hyper-V integrados permite automatizar más operaciones de las que era posible en versiones anteriores de Hyper-V. Los usuarios que ya conocen Windows PowerShell encontrarán tremendamente fácil aprender a usar los nuevos cmdlets debido a la semejanza con los de PowerShell.

Réplica de Hyper-V

Esta característica permite replicar máquinas virtuales entre sistemas de almacenamiento, clústeres y centros de datos ubicados en dos sitios para ofrecer continuidad empresarial y recuperación ante desastres.

Gracias a esta característica, ahora es más sencillo y menos costoso planear e implementar soluciones de cara a la continuidad empresarial y la recuperación ante desastres de las máquinas virtuales. Puede usar una solución integrada para configurar las máquinas virtuales de modo que se repliquen en un segundo servidor que ejecute Hyper-V.

Importación de máquinas virtuales

El proceso de importación se ha actualizado para que resulte más fácil resolver problemas de configuración que de otro modo impedirían importar una máquina virtual. También puede importar una máquina virtual después de copiar los archivos manualmente, en lugar de exportar primero la máquina virtual.

Ahora, el proceso de importación tiene un nuevo diseño que detecta ciertos problemas de configuración y le ayuda a corregirlos.

Migración en vivo

Ahora es posible ejecutar una migración en vivo en un entorno no organizado en clústeres, así como ejecutar más de una migración en vivo al mismo tiempo y usar mayores anchos de banda de red.

Estas mejoras reportan una mayor flexibilidad a la hora de mover una máquina virtual en ejecución, ya que las migraciones en vivo son más fáciles y rápidas de realizar.

Ahora puede ejecutar una migración en vivo sin configurar clústeres de conmutación por error ni volúmenes compartidos de clúster. La migración en vivo en un entorno no organizado en clústeres se admite tanto si el almacenamiento se conserva en un recurso compartido SMB central como si es local. Puede completar las migraciones más rápidamente mediante mayores anchos de banda de red (de hasta 10 gigabits). También puede ejecutar más de una migración en vivo al mismo tiempo para mover rápidamente muchas máquinas virtuales.

Medición de recursos

Ahora es posible recopilar y realizar un seguimiento de datos acerca del procesador físico, la memoria, el almacenamiento y la red que usan determinadas máquinas virtuales.

Puede conocer el uso de recursos de máquinas virtuales específicas. Puede usar estos datos para planear la capacidad, supervisar el consumo de diferentes unidades de negocio o clientes, o capturar los datos que se necesitan para redistribuir los costos derivados de ejecutar una carga de trabajo.

Escala significativamente mayor y resistencia mejorada

Esta versión de Hyper-V ofrece recursos de cálculo y almacenamiento significativamente más grandes que antes, y mejora el tratamiento de los errores de hardware.

Estas características sirven para garantizar que se pueden configurar máquinas virtuales grandes y de alto rendimiento que admitan cargas de trabajo que podrían necesitar escalarse verticalmente de manera significativa.

El equipo que ejecuta Hyper-V en Windows Server 2012 puede configurarse con hasta 320 procesadores lógicos y 4 terabytes (TB) de memoria. Las máquinas virtuales pueden configurarse con 64 procesadores virtuales y 1 TB de memoria. Un control mejorado de los errores de hardware aumenta la resistencia y la estabilidad del entorno de virtualización.

Autorización simplificada

Se incluye el grupo Administradores de Hyper-V, que se implementa como un grupo de seguridad local.

Este grupo puede reducir el número de usuarios que pertenecen al grupo local Administradores, al tiempo que provee a los usuarios de acceso a Hyper-V.

SR-IOV

Esta nueva característica permite asignar un adaptador de red que admite la virtualización de E/S de raíz única (SR-IOV) directamente a una máquina virtual.

El uso de SR-IOV dispara el rendimiento de la red y reduce su latencia, así como la sobrecarga de CPU necesaria para procesar el tráfico de la red.

Puede proporcionar una máquina virtual con conectividad directa a un adaptador de red físico.

Migración de almacenamiento

Mueva los discos duros virtuales que usa una máquina virtual a un almacenamiento físico diferente mientras la máquina virtual sigue ejecutándose.

Esta nueva característica facilita la administración de los subsistemas de almacenamiento físico que usan las máquinas virtuales.

Almacenamiento en recursos compartidos de archivos SMB 3.0

Hyper-V admite ahora el uso de recursos compartidos de archivos SMB 3.0 para proporcionar almacenamiento para las máquinas virtuales.

Esta nueva característica constituye un nuevo modo de proporcionar almacenamiento compartido a máquinas virtuales, sin usar una red de área de almacenamiento (SAN).

Canal de fibra virtual

Esta nueva característica permite establecer una conexión directa con el almacenamiento de canal de fibra desde el sistema operativo invitado que se ejecuta en una máquina virtual.

Esta característica permite virtualizar las cargas de trabajo y aplicaciones que requieren acceso directo al almacenamiento basado en canal de fibra. También permite configurar un clúster directamente en el sistema operativo invitado (denominado a veces clúster invitado).

Con esta característica, los puertos de adaptador de bus host (HBA) estarán disponibles en el sistema operativo invitado.

Formato del disco duro virtual

Este nuevo formato se ha incorporado para satisfacer los requisitos en constante evolución y aprovechar las ventajas de las novedades introducidas en hardware de almacenamiento.

El nuevo formato aumenta el tamaño de almacenamiento máximo por disco duro virtual; además, mejora la estabilidad y eficacia de esos discos.

El nuevo formato del disco duro virtual (VHDX) admite hasta 64 terabytes de almacenamiento. También ofrece protección integrada frente a los daños provocados por errores de alimentación e impide que disminuya el rendimiento de algunos discos físicos de gran sector.

Instantáneas de máquinas virtuales

Ahora, cuando una instantánea de máquina virtual se elimina, el espacio de almacenamiento que esta consumía antes de eliminarse se recupera y vuelve a estar disponible mientras la máquina virtual se ejecuta.

Ya no es necesario apagar ni desactivar la máquina virtual (ni ponerla en estado guardado) para recuperar el espacio de almacenamiento.

Ahora, las operaciones que mantienen sincronizadas a la máquina virtual y a cualquier instantánea que quede tras eliminar una instantánea tienen lugar mientras la máquina virtual se ejecuta. Cuando estas operaciones finalizan, los archivos que contenían las instantáneas (archivos .avhd) se eliminan. Antes, esas operaciones no ocurrían mientras la máquina virtual estaba en funcionamiento o en pausa.

NUMA virtual

Las máquinas virtuales ponen una topología NUMA virtual a disposición del sistema operativo invitado.

Los sistemas operativos más nuevos y las aplicaciones de alto rendimiento, como SQL Server, incluyen optimizaciones que reconocen la topología NUMA de un equipo y la tienen en cuenta al programar subprocesos o asignar memoria, lo que hace que el rendimiento sea mayor. La característica de NUMA virtual permite que el sistema operativo invitado y las aplicaciones con reconocimiento de NUMA que se ejecutan en la máquina virtual (como SQL Server) aprovechen esas optimizaciones del rendimiento.

Se pone una topología NUMA virtual a disposición del sistema operativo invitado. La topología NUMA virtual predeterminada se optimiza de modo tal de que coincida con la topología NUMA del equipo físico.

Conmutador virtual

La arquitectura del conmutador virtual se ha actualizado para proporcionar un marco abierto que permita a terceros agregar nuevas funcionalidades al conmutador virtual.

Este cambio permite a los asociados de Microsoft ampliar el conmutador virtual aprovisionando nuevas funcionalidades como la supervisión, el reenvío y el filtrado en el conmutador virtual.

Requisitos de hardware

Hyper-V requiere un procesador de 64 bits que incluya lo siguiente:

- Virtualización asistida por hardware. Disponible en procesadores que incluyen una opción de virtualización, concretamente, los procesadores con Intel Virtualization Technology (Intel VT) o AMD Virtualization (AMD-V).
- La prevención de ejecución de datos aplicada por hardware (DEP) debe estar disponible y habilitada. Concretamente, debe habilitar el bit XD de Intel (bit ejecutar deshabilitado) o el bit NX de AMD (bit no ejecutar).

Requisitos de software para los sistemas operativos invitados admitidos

Hyper-V incluye un paquete de software para los sistemas operativos invitados admitidos que mejora la integración entre el equipo físico y la máquina virtual. Este paquete se conoce como servicios de integración. En general, este paquete se instala en el sistema operativo invitado como un procedimiento independiente después de configurar el sistema operativo en la máquina virtual. Sin embargo, algunos sistemas operativos ya incluyen los sistemas de integración y no requieren una instalación por separado.

Versiones y requisitos

Windows Server 2012 tiene 4 versiones (pasamos a 4 respecto a las 5 existentes en Windows server 2008):



Figura 3.5: ejemplo de tipos de versiones disponibles en Windows Server 2012

Las verdaderamente profesionales son la "Standard" y la "DataCenter". Ha desaparecido la versión intermedia, llamada "Enterprise". Sin embargo aparecen ahora dos de menor valor que la "standard": las llamadas "Foundation" y "Essentials".

Veamos a quienes van dirigidas estas versiones:

- Windows Server Datacenter. La más compleja y para entornos "en la nube" con un uso intensivo de la virtualización. Permite ejecutar un número ilimitado de máquinas virtuales.
- Windows Server Standard. Cuenta con todas las funciones de Windows Server, permitiendo la virtualización de dos servidores más.
- Windows Server Essentials. Para empresas con hasta 25 usuarios. Los servidores no pueden tener más de dos procesadores. No permite virtualización
- Windows Server Foundation. La versión más sencilla. Para pequeñas empresas con hasta 15 usuarios. Soporta un único procesador. Tampoco permite virtualización.

Las dos versiones que nos interesan son, por tanto la Standard y la DataCenter que soportan hasta 64 procesadores físicos y 4 Tb de memoria física.

- La versión Standard incluye dos instancias de Windows Server 2012
- Windows Server Datacenter permite virtualizar instancias ilimitadas

Para escenarios complejos debemos instalar la versión Datacenter ya que la Standard sólo permite dos máquina virtual adicionales de Windows Server 2012. El modelo de licencias se ha simplificado para la versión Datacenter. Las licencias se adquieren con incrementos de dos procesadores físicos. Por tanto, para un sistema de ocho procesadores físicos, necesitaremos 4 licencias

Los requisitos de virtualización son grandes. Necesitaremos tanta memoria y procesador como le otorgaríamos a las máquinas físicas. Además, los servidores deben permitir la virtualización por hardware. Es algo que debemos tener en cuenta a la hora de adquirir uno, ya sea Intel o AMD. Estas son las especificaciones de hardware:

- IntelVT o tecnología de virtualización para Intel
- AMD-V o virtualización AMD para este tipo de procesadores.
- DEP o prevención de ejecución de datos

Los límites de hardware son los siguientes:

- Hasta 64 procesadores por servidor
- Hasta 320 núcleos por servidor
- Hasta 4 TB de memoria física por servidor.

Esto en cuanto a las capacidades máximas del servidor físico. Y en cuanto a lo que podemos asignar a un servidor virtual:

- Hasta 64 procesadores virtuales por máquina virtual. 2048 procesadores en un servidor físico
- 1 Tb de memoria física por servidor
- 1024 máquinas virtuales activas ejecutándose por servidor.

Por tanto debemos afinar bien a la hora de decidir cuantas máquinas virtuales debemos ejecutar en cada servidor. Por ejemplo, servidores de pocos requisitos como un servidor de ficheros tienen suficiente con dos procesadores y 4 Gb de memoria. Sin embargo para un SQL Server o programas de muchos requisitos tendremos que poner 4 procesadores y 12 Gb para obtener un rendimiento óptimo.

Redes

El diseño de red en la virtualización es un tema importante. Nuestro rendimiento se puede ver afectado seriamente si no configuramos bien la parte de redes. Las recomendaciones son que tengamos dos tarjetas físicas de red:

- Una tarjeta para comunicar nuestro servidor físico y virtuales con el resto de la red de producción
- Una tarjeta dedicada a la administración de los servidores Hyper-V y conectados a una red dedicada a la plataforma de administración del sistema.

En principio no necesitamos más tarjetas, pero podríamos añadir más para servicios que vayamos añadiendo y así independizamos la parte de producción con la parte de gestión. Por ejemplo, la utilización de iSCSI necesitará un adaptador dedicado para hacer uso masivo de la comunicación con el almacenamiento de datos. También será necesaria una tarjeta adicional si establecemos una configuración de clúster por conmutación de redes o el uso de equipos de redes, donde configuráramos varias tarjetas para funcionar como una sola.

Definiremos switches virtuales para la conexión de nuestros servidores. Estos switches pueden trabajar de varias formas:

- Privados. Permiten a las máquinas virtuales comunicarse entre ellas pero no pueden salir del servidor físico que las contiene. No están enlazadas con una tarjeta física de red, por tanto no pueden salir al exterior
- Interna. Permiten comunicarse entre ellas y con el servidor físico. Este tipo de switch tampoco tiene enlace con la tarjeta física, por tanto tampoco tiene conexión con la red externa al equipo físico
- Externa. En este caso, sí que hay un enlace con la tarjeta de red externa. Por tanto tienen total comunicación entre ellas y con el exterior. En este tipo de switch caben tres posibilidades de conexión
 - Utilizando un puerto que representa a una sola tarjeta física
 - Utilizando un puerto que representa un grupo de tarjetas físicas
 - Utilizando varios puertos que representan una sola tarjeta física

En Windows Server 2012 se han añadido dos funcionalidades que antes las proporcionaban fabricantes externos. Se trata de extensiones de los switches que utilizan dos tipos de controladores:

- Controlador de filtro NDIS. Realiza inspección y filtrado de paquetes.
- Controlador WFP. Proporciona funcionalidades de cortafuegos virtuales, monitorización de las conexiones y filtro de red utilizando IPSec.

Si necesitamos otras funcionalidades debemos ir a buscarlas con proveedores de servicios.

Almacenamiento

Tenemos a nuestra disposición varias tecnologías de almacenamiento. Veamos las que debemos utilizar:

- DAS o almacenamiento directo. El almacenamiento está directamente vinculado al sistema operativo. Es decir, se trata de los discos físicos de siempre con sus distintas tecnologías:

- Discos SATA
 - Discos externos eSATA
 - Discos de rendimiento SCSI
 - SCSI serie o SAS
 - Tecnología de almacenamiento avanzada paralela PATA
 - USB
 - FireWire
- Red de almacenamiento SAN (Storage Área Network). Las soluciones SAN aportan grupos de almacenamiento con diversos sistemas de protección como los sistemas RAID. Se conectan con nuestros servidores de varias formas:
 - Fibra óptica
 - iSCSI
 - SAS
 - Servidor de almacenamiento. SMB 3.0 es el protocolo de ficheros de Microsoft. Windows Server 2012 permite configurar servidores con disponibilidad continua y escalable para CSV. (grupos de servidores con conmutación de error o clúster.)

Los sistemas NAS (Network Attached Storage), que son más económicos y que se configuran directamente en las redes locales de forma independiente a los servidores no se pueden utilizar para la virtualización. Un sistema NAS sólo es un sistema que proporciona almacenamiento para nuestra red local:

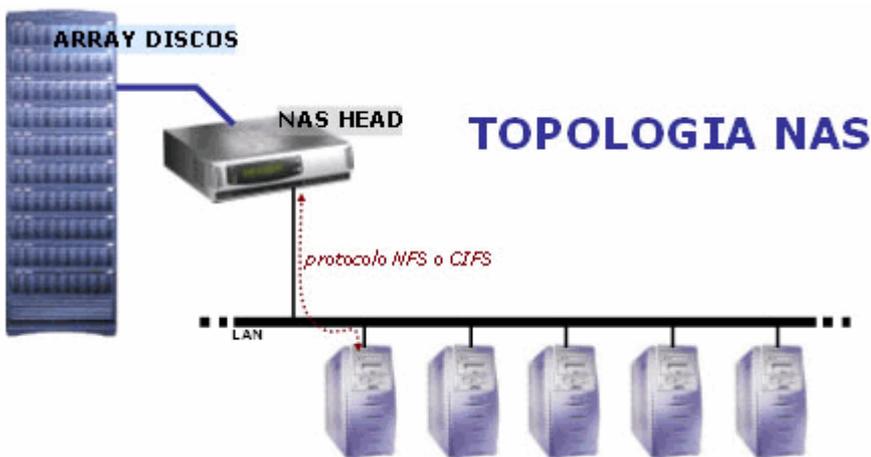


Figura 3.6: ejemplo de topología NAS

Todos los equipos de nuestra red pueden acceder al NAS, ya que se trata de un equipo más. En cambio en las SAN:

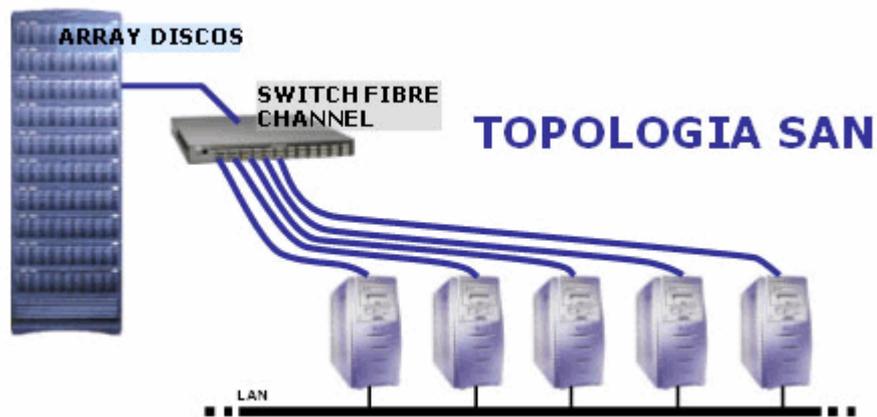


Figura 3.7: ejemplo de topología SAN

Tenemos una red de alta velocidad privada para los servidores. Los equipos de la red no ven esa SAN. Los servidores suelen tener varias tarjetas de red para dedicar una o más para esta conexión con las cabinas de discos.

Las ventajas de las SAN respecto a los discos físicos son muchas. Las SAN permiten publicar varios grupos de almacenamiento para distintos servidores, esto las hace tremendamente flexibles. Además centralizamos la gestión en un sólo sistema en lugar de tener que mantener los distintos DAS de los servidores. Las desventajas son el precio y, al tener que proporcionar tanta flexibilidad, el tiempo de latencia puede ser menor que los discos directos.

Administración

La administración de Hyper-V la realizaremos con dos herramientas:

- Consola de administración de Hyper-V
- Windows PowerShell (consola de comandos avanzada)

Si disponemos de una gran estructura el sistema perfecto es la utilización de System Center 2012 que permite controlar desde una consola todos los servidores de nuestra infraestructura.

Seguridad

La seguridad también es un factor importante a tener en cuenta en nuestro despliegue de esta infraestructura. Las recomendaciones en este caso son:

- Si vamos a desplegar un buen número de servidores, elegir la versión Core de Windows. Sin interfaz gráfica o GUI será más complicado el acceso a los servidores. Siempre podremos utilizar las herramientas administrativas o PowerShell. Windows 8 incorpora las herramientas de administración necesarias para estas versiones Core.
- No instalar roles adicionales en los servidor de Hyper-V. Dejaremos que se dedique completamente a este rol ya que será de uso intensivo con distintos sistema de almacenamiento, switches virtuales y otras tecnologías que no debemos mezclar con otros roles.

Escalabilidad, movilidad y disponibilidad

Escalabilidad es la capacidad de expandirse y ajustar la configuración a las necesidades del momento. Es habitual que un servidor virtual ejecute más roles y necesitemos más memoria o más procesadores. Esta capacidad será vital en la flexibilidad de nuestra instalación.

La disponibilidad es el tiempo en el que está operativos. Debemos minimizar las paradas de servicio. La conmutación por error (failover) es el sistema por el que proporcionaremos redundancia a nuestro entorno y así aumentar la disponibilidad, o mejor dicho, minimizar las caídas.

Los nodos que conforman el clúster están conectados físicamente y se comunican continuamente para saber el estado de cada uno. Los clúster pueden tener hasta 64 nodos con 4.000 máquinas virtuales en ejecución por clúster y hasta 1024 máquinas virtuales por nodo.

La tercera característica importante es la movilidad. Esto permite la migración de máquinas virtuales en ejecución de un nodo a otro en el clúster. Así garantizamos la continuidad del servicio. Las "migraciones en vivo" son las que permitirán esta importante funcionalidad.

- Estos movimientos se pueden hacer de forma concurrente. De esta forma, si un nodo necesita pararse por mantenimiento, podemos pasar todas sus máquinas virtuales a otros.
- Se pueden realizar aunque no pertenezcan a un clúster mediante el almacenamiento compartido
- La "migración de almacenamiento" permite mover el almacenamiento de un sitio a otro sin paradas.

Recuperación ante desastres

Siempre tendremos a Murphy en la nómina de nuestra empresa. Así que debemos estar preparados por si, a pesar de todo, tenemos algún desastre o falta de servicio. Por ejemplo, tenemos las máquinas virtuales en una flamante SAN de última generación pero tiene un fallo en un latiguillo de fibra óptica o en su fuente de alimentación redundante.

La recuperación ante desastres es la capacidad de crear y restaurar máquinas virtuales. Debemos hacer copia de seguridad de:

- Sistema operativo de gestión de Hyper-V
- Configuración discos virtuales, instantáneas y los demás ficheros asociados

Podemos utilizar la copia de volúmenes del software de copia de seguridad de Windows. VSS es el servicio de copia de seguridad de segundo plano de volúmenes que permite:

- Utilizar por consola gráfica o PowerShell el programa de copias de seguridad de Windows
- Realizar copias de segundo plano (Shadow) de carpetas compartidas. Así podemos ver carpetas en distintos puntos de tiempo para restaurar un punto determinado

System Center DPM es un software independiente de Microsoft que permite gestionar el salvado de los servidores. Su nombre es "Data Protection Manager" y se trata de un software avanzado de salvado. Bastante más potente que el programa local.

Además del software y una buena política de copias de seguridad tenemos una nueva funcionalidad que es la "réplica" de Hyper-V. En sí no es un sistema de backup sino de prevención. Permite mantener una réplica de una máquina virtual en funcionamiento sin tener que montar una compleja estructura de clúster. Microsoft Exchange utiliza estos sistemas de réplica proporcionando redundancia en los datos de una forma sencilla.

3.3 Características principales de VmWare Vsphere 5.X

VMWARE VSPHERE 5

VmWare vSphere es una de las plataformas de virtualización líder del sector para construir infraestructuras de cloud, la cual permite a los usuarios ejecutar aplicaciones críticas para el negocio con confianza y responder con mayor rapidez a las necesidades empresariales.

VSphere acelera el cambio hacia el cloud computing para los centros de datos existentes, además de sustentar las ofertas de cloud pública, de tal forma que constituye la base para el único modelo de cloud híbrida del sector. Con más de 250 000 clientes en todo el mundo y la compatibilidad con más de 2500 aplicaciones de más de 1400 partners ISV, VmWare vSphere es la plataforma de confianza para cualquier aplicación.

Beneficios de Vsphere

- **Consolidar y optimizar el hardware de TI:** Permite consolidar 15 máquinas virtuales o más en un solo servidor físico sin sacrificar el rendimiento ni la producción.
- **Mejorar la continuidad del negocio:** Ayuda a las organizaciones a reducir el coste y la complejidad de la continuidad del negocio y la recuperación ante desastres con funciones de TI siempre disponible y protección en capas contra interrupciones del servicio y pérdida de datos.
- **Simplificar las operaciones de TI:** Reduce la sobrecarga operativa y simplifica de manera drástica la gestión de entornos de TI de desarrollo, certificación de la calidad y producción, grandes y geográficamente distribuidos.
- **Proporcionar TI como servicio:** Ofrece a los clientes la facultad de disfrutar de los beneficios del cloud computing, sin renunciar por ello a la seguridad, al cumplimiento con normativas y a un control completo de los activos empresariales.

VmWare ESXi es una plataforma de virtualización a nivel de centro de datos producido por VMware y es el componente de su producto VmWare Infraestructure que se encuentra al nivel inferior de la capa de virtualización, el hypervisor, aunque posee herramientas y servicios de gestión autónomos e independientes.

Está compuesto de un sistema operativo autónomo que proporciona el entorno de gestión, administración y ejecución al software hypervisor, y los servicios y servidores que permiten la interacción con el software de gestión y administración y las máquinas virtuales.

Arquitectura y características

Arquitectura

VMware ESX es un hypervisor del tipo "bare metal", el cual no se ejecuta sobre un sistema operativo externo sino que está embebido en el núcleo del mismo. Para su ejecución, ESX se apoya en un sistema Linux basado en Red Hat Enterprise Linux modificado para la ejecución del hypervisor y los componentes de virtualización de VMware. Hasta la versión 3.5u4 se basa en código ejecutable de 32 bits, pero a partir de la versión 4 (vSphere) su código ejecutable pasa a ser de 64 bits por lo que sus requerimientos pasan a ser mayores ofreciendo a su vez un rendimiento superior.

El arranque de la máquina anfitriona se produce a través de la ejecución de un núcleo Linux el cual proporciona servicios de consola y hardware a nivel del anillo 04 en colaboración con el hypervisor funcionando en modo "Supervisor". A partir de la versión vSphere (versión 4.0), el hypervisor aplica los teoremas de la paravirtualización y sustituye al núcleo Linux por sus propias interfaces, creando un nivel de anillo -1, y pasando a ejecutar el entorno operativo como una máquina virtual.

El vmkernel está programado y configurado siguiendo la arquitectura de microkernel y tiene las siguientes interfaces con el exterior:

- hardware
- sistema invitado
- consola de servicio (Console OS, Service Console)

El vmkernel administra CPU y memoria de manera directa utilizando Scan-Before-Execution (SBE) para priorizar instrucciones e interrupciones especiales y privilegiadas

El acceso al resto del hardware (almacenamiento, red, HID) se realiza por medio de módulos, algunos de ellos similares a los implementados en el núcleo Linux. Para el acceso a alguno de ellos se establece un interfaz de comunicación a través del módulo adicional vmkernel.

El núcleo vmkernel ofrece un interfaz al sistema alojado en la máquina virtual el cual simula una plataforma hardware adaptada a dicho sistema. Esto se lleva a cabo de tal manera que dicho se puede ejecutar sin modificar a través del hypervisor. Como el uso de controladores sin modificaciones en el sistema alojado consume recursos del sistema, el hypervisor ofrece controladores especializados para diferentes sistemas operativos para aumentar el rendimiento. Estos controladores mejorados forman parte de los paquetes VMTTools, compuesto a su vez por diferentes paquetes de utilidades y secuencias de comandos. Tanto los controladores mejorados que permiten un mayor aprovechamiento de la infraestructura física por parte del sistema alojado como las utilidades que ofrecen servicios como el control de la máquina virtual y sus recursos por parte del hypervisor, la comunicación entre máquinas virtuales, los servicios de sincronización horaria y de arranque y parada personalizables. Cada familia de sistemas tiene versiones propias.

Consola de Servicio

Proporciona acceso de bajo nivel a todos los servicios y configuraciones del servidor ESX. Supone una interfaz de gestión alternativa al cliente gráfico y a la RCLI remotos. Tanto la consola como la RCLI pasan a ser servicios considerados obsoletos por parte de VMware orientando su administración al cliente gráfico y los sistemas embebidos monolíticos al estilo del ESXi Server.

Principales funciones y componentes de vSphere

Servicios de infraestructura

- **La arquitectura de VmWare vSphere Hypervisor** proporciona una sólida capa de virtualización acreditada para entornos de producción y de alto rendimiento. Permite que varias máquinas virtuales compartan recursos de hardware con un rendimiento que puede igualar (y, en ocasiones, superar) al nativo.
- **VmWare vSphere Virtual Symmetric Multiprocessing** permite utilizar máquinas virtuales ultra potentes con hasta 128 CPU virtuales.
- **VmWare vSphere Virtual Machine File System (VMFS)** permite que las máquinas virtuales accedan a los dispositivos de almacenamiento compartido (Fibre Channel, iSCSI, etc.). Constituye una tecnología esencial para otros componentes de vSphere, como VmWare vSphere Storage vMotion.
- **Las API de VmWare vSphere Storage** permiten la integración con soluciones de protección de datos, multipathing y matrices de discos de terceros.
- **VSphere Distributed Resource Schedule (DRS)** proporciona balanceo de carga dinámico independiente del hardware y asignación de recursos para máquinas virtuales en clúster. Utiliza la automatización basada en políticas para reducir la complejidad de gestión y reforzar la compatibilidad con los acuerdos de nivel de servicio (SLA).
- **VmWare Distributed Power Management (DPM)**, que se incluye con VmWare vSphere DRS, automatiza el consumo eficiente de la energía en los clústeres de VMware DRS optimizando continuamente el consumo eléctrico de los servidores dentro de cada clúster.
- **VSphere Network Distributed Switch** simplifica y optimiza la red de máquinas virtuales en entornos de vSphere. Además, permite usar switches virtuales distribuidos de terceros, como Cisco Nexus 1000V, en entornos de VmWare vSphere.
- **VSphere vStorage Thin Provisioning** proporciona asignación dinámica de la capacidad de almacenamiento compartido. De este modo, el departamento de TI puede implementar una estrategia de almacenamiento por niveles y reducir al mismo tiempo el gasto en almacenamiento hasta un 50%.
- **VSphere Storage I/O Control** establece las prioridades de calidad de servicio del almacenamiento para garantizar el acceso a los recursos de almacenamiento.
- **VSphere Storage DRS** automatiza el balanceo de la carga y utiliza funciones de almacenamiento para determinar la mejor ubicación para que residan los datos de una máquina virtual concreta cuando se crea y cuando se utiliza a lo largo del tiempo.
- **VSphere Profile-Driven Storage** reduce los pasos para la selección de los recursos de almacenamiento agrupándolos conforme a una política definida por el usuario.
- **VMware Network I/O Control** establece prioridades de calidad de servicio de red para garantizar el acceso a los recursos de red.

Servicios de aplicaciones

- **VmWare vSphere vMotion** permite la migración en caliente de máquinas virtuales entre servidores sin interrupción alguna para los usuarios ni pérdidas de servicio. De esta forma se elimina la necesidad de programar tiempo de inactividad de las aplicaciones para el mantenimiento de servidores.
- **VSphere Storage vMotion** permite la migración en caliente de discos de máquinas virtuales sin interrupción alguna para el usuario. De esta forma se elimina la necesidad de programar tiempo de inactividad de las aplicaciones para realizar el mantenimiento programado o las migraciones del almacenamiento.
- **VMware High Availability (HA)** es la solución automatizada más rentable para el reinicio de todas las aplicaciones en cuestión de minutos en caso de un fallo de hardware o del sistema operativo.
- **VSphere Fault Tolerance (FT)** proporciona disponibilidad continua de todas las aplicaciones en caso de fallo de hardware, sin pérdida de datos ni tiempo de inactividad.
- **VSphere Data Recovery** ofrece unas funciones de backup y recuperación sencillas, rentables y sin agentes de máquinas virtuales para entornos más pequeños.
- **VSphere vShield Zones** simplifica la seguridad de las aplicaciones al aplicar las políticas de seguridad corporativas en el nivel de aplicación en un entorno compartido, manteniendo la fiabilidad y la segmentación de la red de los usuarios y de los datos confidenciales.
- **Las vSphere VMsafe API** posibilitan el uso de productos de seguridad que funcionan con la capa de virtualización para proporcionar a las máquinas virtuales niveles de protección mayores incluso que los de los servidores físicos.
- **La adición en caliente** permite incorporar CPU y memoria a las máquinas virtuales según las necesidades sin interrupciones ni paradas.
- **La conexión en caliente** permite conectar o desconectar dispositivos virtuales de almacenamiento o de red de las máquinas virtuales sin interrupciones ni tiempo de inactividad.
- **La ampliación en caliente de discos virtuales** permite añadir almacenamiento virtual a las máquinas virtuales sin interrupciones ni tiempo de inactividad.

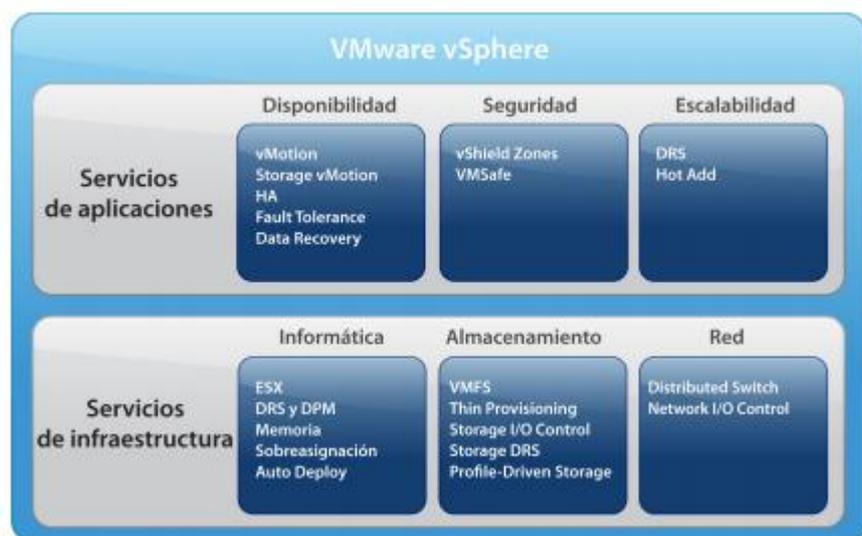


Figura 3.8: conjunto integral de servicios de aplicaciones e infraestructura.

Servicios de gestión

- **VMware vCenter Agent** conecta los hosts vSphere a vCenter Server para la gestión centralizada de todos los hosts y máquinas virtuales.
- **Host Profiles** ayuda a los administradores de TI a simplificar la implementación de hosts y el cumplimiento, gracias a la creación de máquinas virtuales a partir de plantillas de configuración.
- **Virtual Serial Port Concentrator** habilita las conexiones de red mediante el concentrador de puertos serie a la consola de puertos serie de cualquier servidor.
- **vSphere Update Manager** automatiza el seguimiento, la aplicación de parches y la actualización de los hosts vSphere, las aplicaciones y los sistemas operativos que se ejecutan en las máquinas virtuales de VMware.
- **VMware vCenter Converter** permite a los administradores de TI convertir rápidamente servidores físicos y máquinas virtuales de terceros en máquinas virtuales de VMware.
- **vSphere Web Client** permite a los administradores de TI gestionar las funciones esenciales de vSphere desde cualquier navegador, en cualquier lugar del mundo.

Requisitos de Hardware

Procesador de 64 bits

- ESXi 5.0 se instala y se ejecuta sólo en servidores con procesadores x86-64.
- ESXi 5.0 requiere un equipo host con al menos dos núcleos.
- ESXi 5.0 solo admite instrucciones de CPU tipo LAHF y SAHF.
- Procesadores de 64 bits conocidos:
 - Todos los procesadores AMD Opteron

- Todos los procesadores Intel Xeon 3000/3200, 3100/3300, 5100/5300, 5200/5400, 5500/5600, 7100/7300, 7200/7400 y 7500

RAM

- Mínimo 2GB de RAM.

Adaptadores de red

Uno o más controladores Ethernet Gigabit o de 10Gb.

Adaptador de SCSI, adaptador para canal de fibra o controlador RAID interno

Cualquier combinación de uno o más de los controladores que se mencionan a continuación:

Controladores básicos SCSI. Adaptec Ultra-160 o Ultra-320, LSI LogicFusion-MPT, o la mayoría de SCSI NCR/Symbios.

Controladores RAID. Controladores Dell PERC (Adaptec RAID o LSI MegaRAID), HP Smart Array RAID o IBM (Adaptec) ServeRAID.

Instalación y almacenamiento

Disco SCSI o un RAID LUN local sin red con espacio no particionado para las máquinas virtuales.

Para Serial ATA (SATA), se conecta un disco a través de los controladores SAS compatibles o de los controladores SATA incorporados compatibles. Los discos SATA se consideran remotos, no locales. Dichos discos no se utilizarán como partición desde cero por defecto dado que se consideran remotos.

ESXi 5.0 admite la instalación y el arranque desde los siguientes sistemas de almacenamiento:

Unidades de disco SATA. Unidades de disco SATA conectadas en la parte posterior de los controladores SAS compatibles o de los controladores incorporados compatibles.

Controladores SATA. Entre los controladores SAS compatibles se incluyen:

LSI1068E (LSISAS3442E)

LSI1068 (SAS 5)

Controlador IBM ServeRAID 8K SAS

Controlador Smart Array P400/256

Controlador Dell PERC 5.0.1

Entre los SATA incorporados compatibles se incluyen:

Intel ICH9

NVIDIA MCP55

Server Works HT1000

Unidades de disco Serial Attached SCSI (SAS). Se admite para la instalación de ESXi 5.0 y para el almacenamiento de las máquinas virtuales en las particiones VMFS.

Disco dedicado SAN sobre Canal de Fibra o iSCSI

Dispositivos USB. Se admite para la instalación de ESXi 5.0. Para obtener una lista de dispositivos USB compatibles, consulte la VMware Compatibility Guide.

Versiones

Ediciones de VMware vSphere

VMware vSphere Enterprise

La edición VMware vSphere Enterprise incluye funcionalidades como High Availability, Data Recovery, VMware vSphere vMotion, Hot Add, VMware vSphere vShield Zones, Fault Tolerance, VMware vSphere Storage vMotion, VMware vShield DRS, VMware vSphere DPM, Virtual Serial Port Concentrator y VMware vSphere Storage API para integración de arrays y multipathing.

VMware vSphere Enterprise Plus

VMware vSphere Enterprise Plus incluye todas las funcionalidades de vSphere Enterprise, así como asignación de derechos de memoria ampliada, VMware vSphere Virtual SMP de 32 vías, VMware vSphere Distributed Switch, VMware Host Profiles, VMware vSphere Auto-Deploy, VMware vSphere Storage I/O Control, VMware vSphere Network I/O Control, VMware vSphere Profile-Driven Storage y VMware vSphere Storage DRS.

CAPITULO IV - Preparación de hardware Y Entornos de Prueba

4.1 Preparación de Hardware

Para la realización de nuestra prueba utilizamos un cajón HP BladeSystem c7000 nombrado como middleearth01.

Información complementaria sobre el cajón HP

middleearth01

Status Information Virtual Buttons Component Firmware

Enclosure Status OK
Active OA Status OK
Standby OA Status Absent
Power Mode Power Supply Redundant

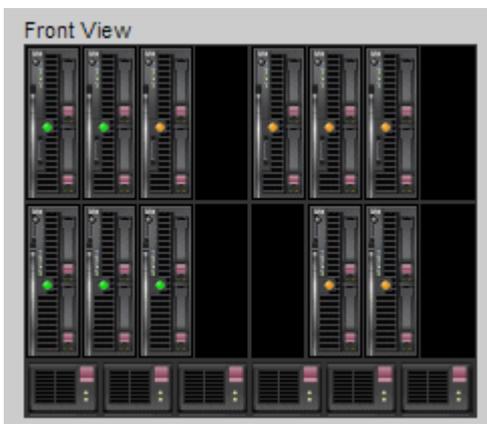
Diagnostics Information
Device Identification Data OK

Enclosure Status Overview

Subsystems and Devices	Status
Device Bay Overview	OK
Interconnect Bay Overview	OK
Power Subsystem	OK
Thermal Subsystem	OK

Part	Model	Manufacturer	Serial Number	Part Number	Spare Part Number
Enclosure	BladeSystem c7000 Enclosure	HP	USE846HR75	412152-B21	N/A
Enclosure Midplane	N/A	HP	N/A	N/A	414050-001
Onboard Administrator Tray	BladeSystem c7000 Onboard Administrator Tray	HP	0185MIP1691	N/A	416000-001
Power Input Module	HP AC Module, Single Phase	HP	N/A	N/A	413494-001

Vista frontal del cajón HP sacado del “Onboard Administrator”



Vista trasera del cajón HP sacado del "Onboard Administrator".

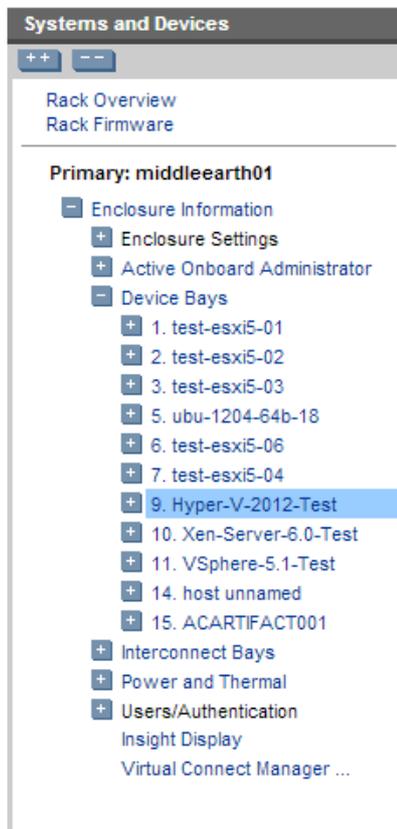


Enclosure Component Firmware Information

Bay	Device Model	Current Firmware Version	Available Firmware Version
-	BladeSystem c7000 Onboard Administrator Tray	1.7	1.7
-	BladeSystem c7000 Insight Display	2.2.2	2.2.2
1	Active Cool 200 Fan	2.9.4	2.9.4
2	Active Cool 200 Fan	2.9.4	2.9.4
3	Active Cool 200 Fan	2.9.4	2.9.4
4	Active Cool 200 Fan	2.9.4	2.9.4
5	Active Cool 200 Fan	2.9.4	2.9.4
6	Active Cool 200 Fan	2.9.4	2.9.4
7	Active Cool 200 Fan	2.9.4	2.9.4
8	Active Cool 200 Fan	2.9.4	2.9.4
9	Active Cool 200 Fan	2.9.4	2.9.4
10	Active Cool 200 Fan	2.9.4	2.9.4

Blades utilizados para las pruebas

Para las pruebas se utilizaron 3 Blades de prueba ubicados en las bahías 9 (servidor de Hyper-v), bahía 10 (servidor xen Server) y bahía 11 (servidor ESX) todos servidores ProLiant BL460c G6 con 32Gb de RAM



Información sobre servidor físico Hyper-V

Device Bay Information - ProLiant BL460c G6 (Bay 9)

Status	Information	Virtual Devices	Boot Options	IML Log
Device Information				
Blade Type	Server Blade			
Manufacturer	HP			
Product Name	ProLiant BL460c G6			
Part Number	507864-B21			
System Board Spare Part Number	595046-001			
Serial Number	USE0494LA3			
UUID	38373035-3436-5355-4530-3439344C4133			
BIOS Asset Tag				
Server Name	Hyper-V-2012-Test			
ROM Version	I24 12/02/2011			
Server NIC Information				
Device ID				
Flex-10 Embedded Ethernet				
NIC 1	68:85:99:C0:DF:08			
NIC 2	68:85:99:C0:DF:0C			
iSCSI 1	68:85:99:C0:DF:09			
iSCSI 2	68:85:99:C0:DF:0D			
Management Processor				
ILO	00:25:B3:A5:F5:08			
Mezzanine Card Information				
Mezzanine Slot	Mezzanine Device	Mezzanine Device Port	Device ID	
1	Emulex LPe1105-HP 4Gb FC HBA for HP c-Class BladeSystem	Port 1	10:00:00:00:c9:a6:82:f4	
		Port 2	10:00:00:00:c9:a6:82:f5	
CPU and Memory Information				
CPU 1	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz (6 Cores)			
CPU 2	Intel(R) Xeon(R) CPU X5670 @ 2.93GHz (6 Cores)			
Memory	32768 MB			

Información sobre servidor físico XenServer

Device Bay Information - ProLiant BL460c G6 (Bay 10)

Status	Information	Virtual Devices	Boot Options	IML Log
Device Information				
Blade Type	Server Blade			
Manufacturer	HP			
Product Name	ProLiant BL460c G6			
Part Number	507864-B21			
System Board Spare Part Number	595046-001			
Serial Number	USE0221XL5			
UUID	38373035-3436-5355-4530-323231584C35			
BIOS Asset Tag				
Server Name	Xen-Server-6.0-Test			
ROM Version	I24 03/30/2010			
Server NIC Information				
Device ID				
Flex-10 Embedded Ethernet				
NIC 1	78:E7:D1:5D:F6:40			
NIC 2	78:E7:D1:5D:F6:44			
iSCSI 1	78:E7:D1:5D:F6:41			
iSCSI 2	78:E7:D1:5D:F6:45			
Management Processor				
ILO	D0:D3:85:E6:F4:68			
Mezzanine Card Information				
Mezzanine Slot	Mezzanine Device	Mezzanine Device Port	Device ID	
1	QLogic QMH2462 4Gb FC HBA for HP c-Class BladeSystem	Port 1	50:01:43:80:04:c1:96:38	
		Port 2	50:01:43:80:04:c1:96:3a	
2	NC354m Quad Port 1Gb NIC for c-Class BladeSystem	Port 1	00:25:b3:b0:f2:40	
		Port 2	00:25:b3:b0:f2:41	
		Port 3	00:25:b3:b0:f2:42	
		Port 4	00:25:b3:b0:f2:43	
CPU and Memory Information				
CPU 1	Intel(R) Xeon(R) CPU X5570 @ 2.93GHz (4 Cores)			
CPU 2	Intel(R) Xeon(R) CPU X5570 @ 2.93GHz (4 Cores)			
Memory	32768 MB			

Información sobre servidor físico ESX

Device Bay Information - ProLiant BL460c G6 (Bay 11)				
Status	Information	Virtual Devices	Boot Options	IML Log
Device Information				
Blade Type	Server Blade			
Manufacturer	HP			
Product Name	ProLiant BL460c G6			
Part Number	507864-B21			
System Board Spare Part Number	595046-001			
Serial Number	USE0293LDM			
UUID	38373035-3436-5355-4530-3239334C444D			
BIOS Asset Tag				
Server Name	VSphere-5.1-Test			
ROM Version	i24.12/02/2011			
Server I/O Information				
Flex-IO Embedded Ethernet	Device ID			
NIC 1	78:E7:D1:64:0A:C0			
NIC 2	78:E7:D1:64:0A:C4			
iSCSI 1	78:E7:D1:64:0A:C1			
iSCSI 2	78:E7:D1:64:0A:C5			
Management Processor				
iLO	78:E7:D1:62:CD:14			
Mezzanine Card Information				
Mezzanine Slot	Mezzanine Device	Mezzanine Device Port	Device ID	
The server does not contain any mezzanine cards				
CPU and Memory Information				
CPU 1	Intel(R) Xeon(R) CPU X5570 @ 2.93GHz (4 Cores)			
CPU 2	Intel(R) Xeon(R) CPU X5570 @ 2.93GHz (4 Cores)			
Memory	32768 MB			

Configuraciones sobre servidores, se configuraron las siguientes IP para los respectivos host y sobre el cajón:

Host IP: 10.230.46.36 – Nombre: host hyperv
 Host IP: 10.230.46.42 – Nombre: host citrix – xentest1
 Host IP: 10.230.46.43 – Nombre: host esx
 Cajón IP: 10.230.46.11

Y las siguientes IP sobre las máquinas virtuales de prueba:

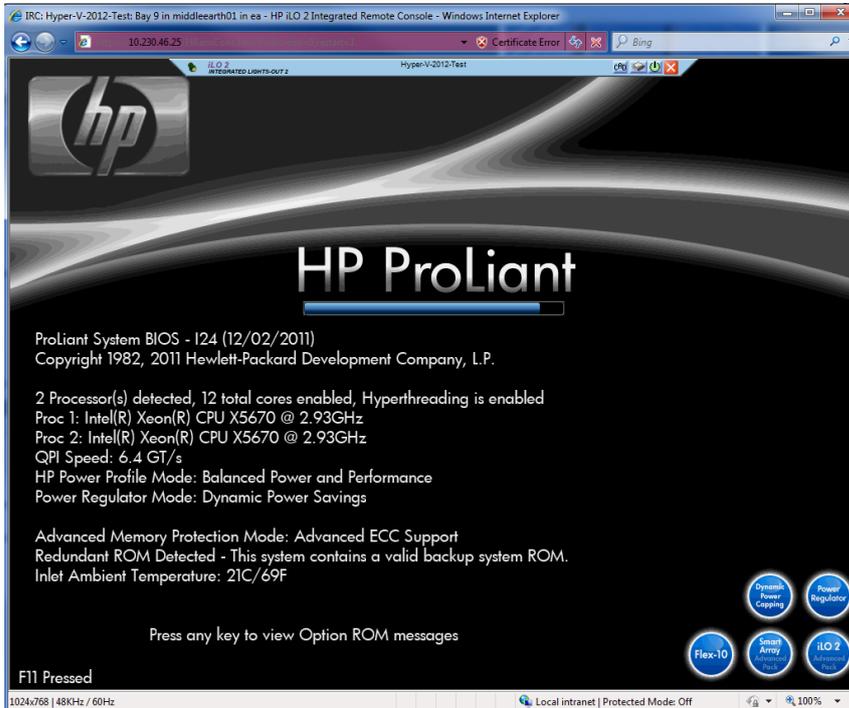
IP: 10.230.61.20, Nombre: Windows2008-esx-test, Usuario: msarmi1x,
 IP: 10.230.61.21, Nombre: Ubuntu12-esx-test, Usuario: msarmi1x,
 IP: 10.230.61.22, Nombre: Windows2008-xen-test, Usuario: msarmi1x,
 IP: 10.230.61.23, Nombre: Ubuntu12-xen-test, Usuario: msarmi1x,
 IP: 10.230.61.24, Nombre: Windows2008-Hyperv-test, Usuario: msarmi1x,
 IP: 10.230.61.25, Nombre: Ubuntu12-hyperv-test, Usuario: msarmi1x,

Máquinas Virtuales

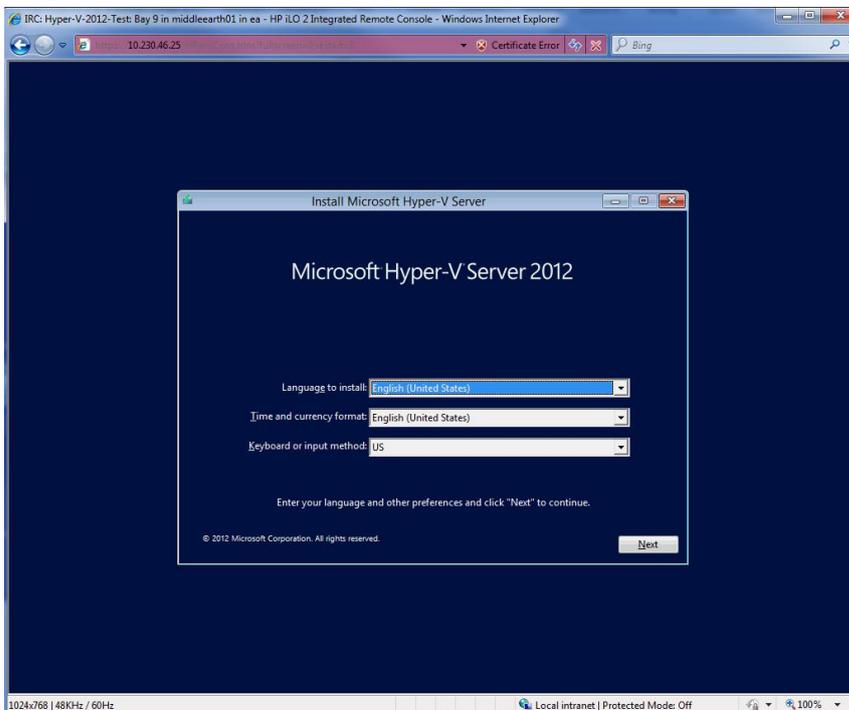
Windows: 40Gb de disco, 4Gb RAM, 1 Core
 Ubuntu: 16Gb de disco, 2Gb RAM, 1 Core

4.2 Instalaciones y experiencia de usuario de Hyper-V-2012

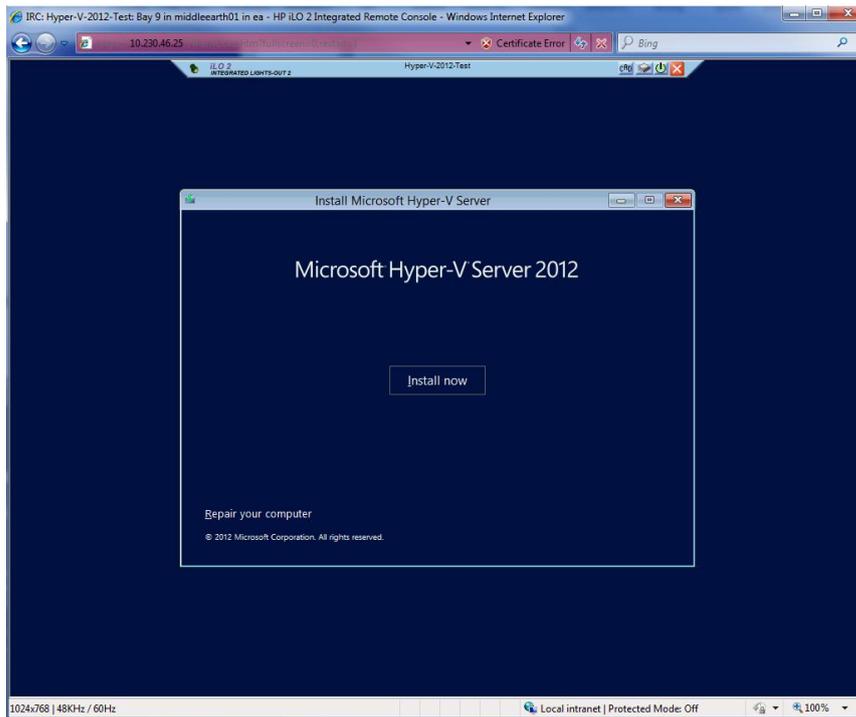
- Encendemos el Blade desde el OnboardAdministrator



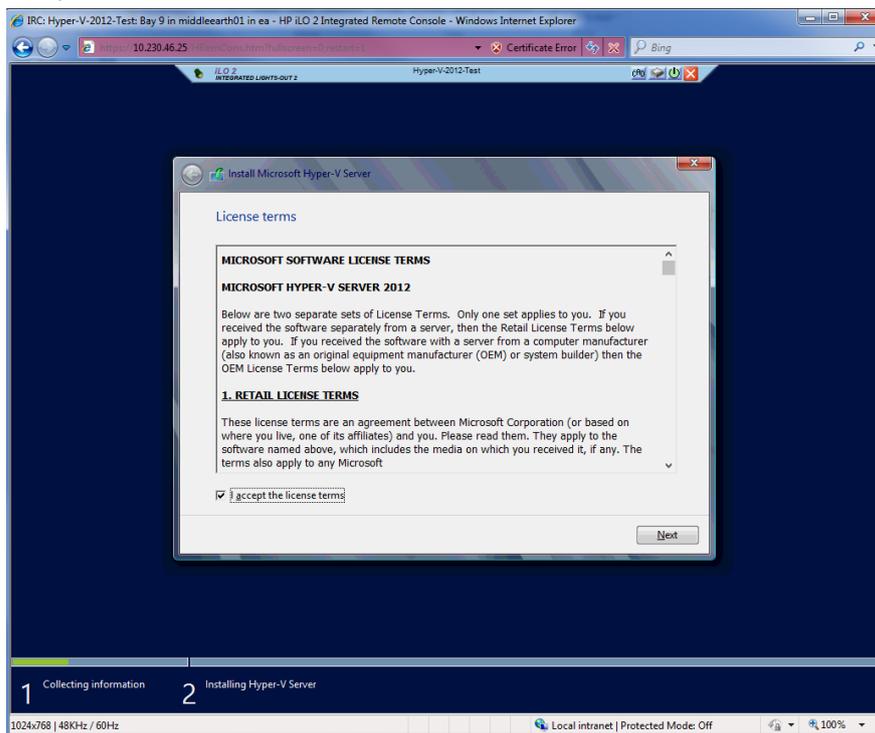
- 1) Elegir el idioma del sistema operativo



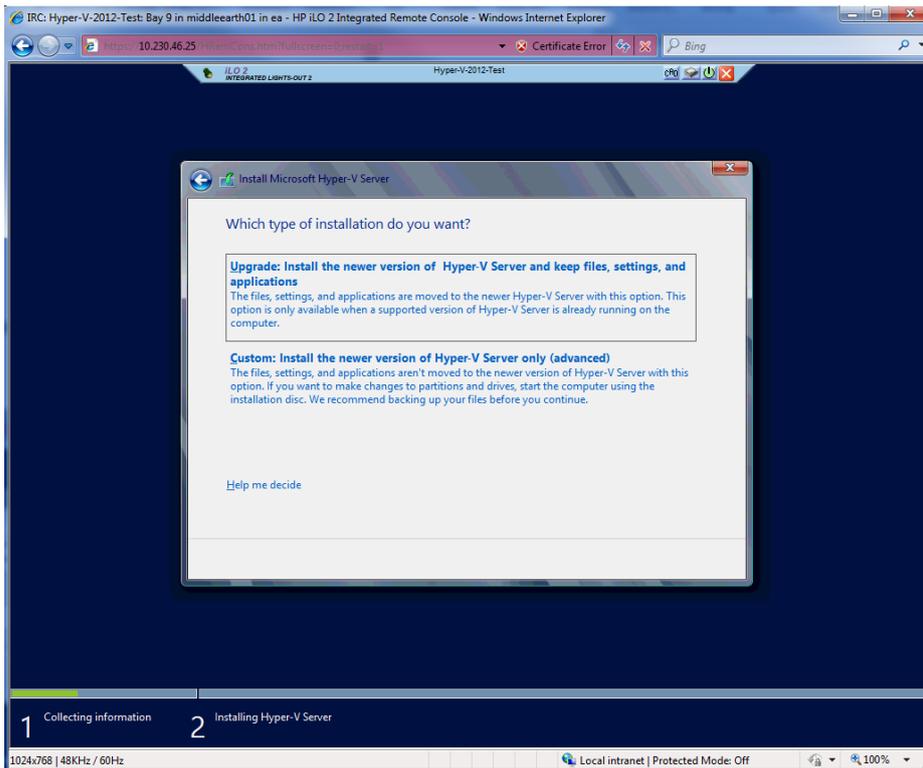
2) Apretamos sobre el botón instalar



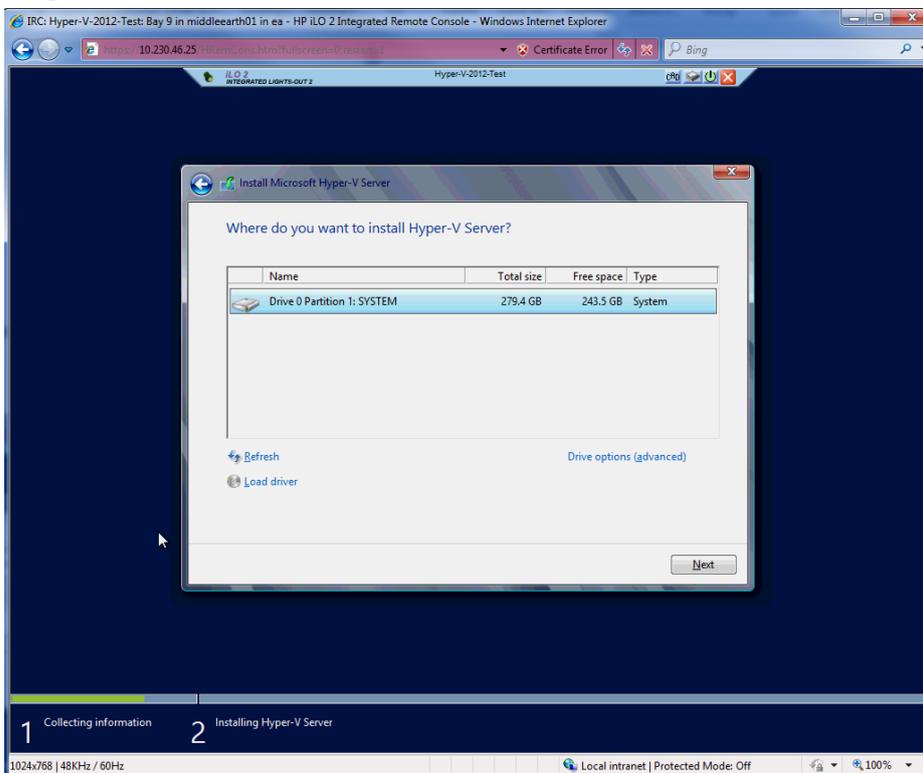
3) Aceptamos los términos de licencia



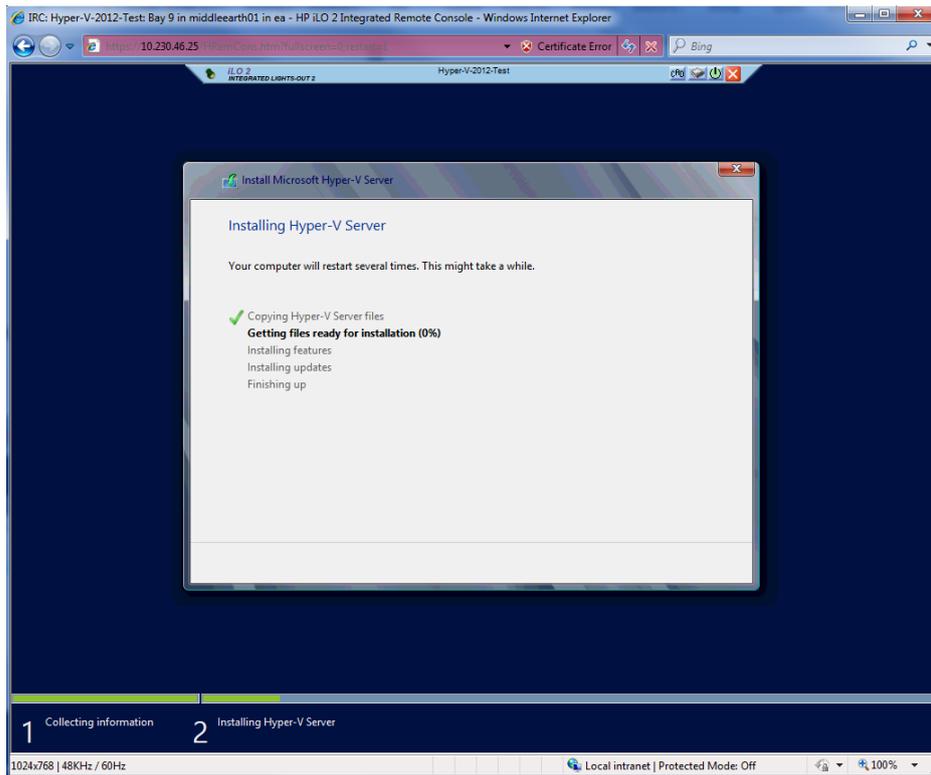
4) Seleccionamos Custom si es que queremos realizar una instalación desde el comienzo



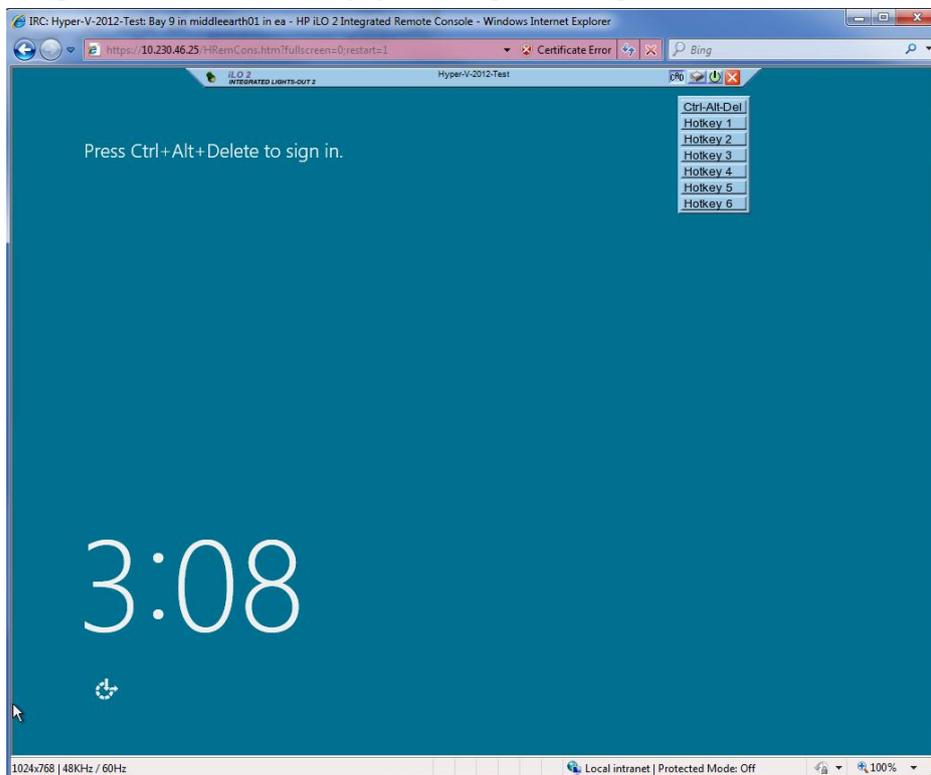
5) Elegimos Disco/Partición donde va a ser instalado



6) Comienza la instalación que dura aproximadamente 10 minutos.



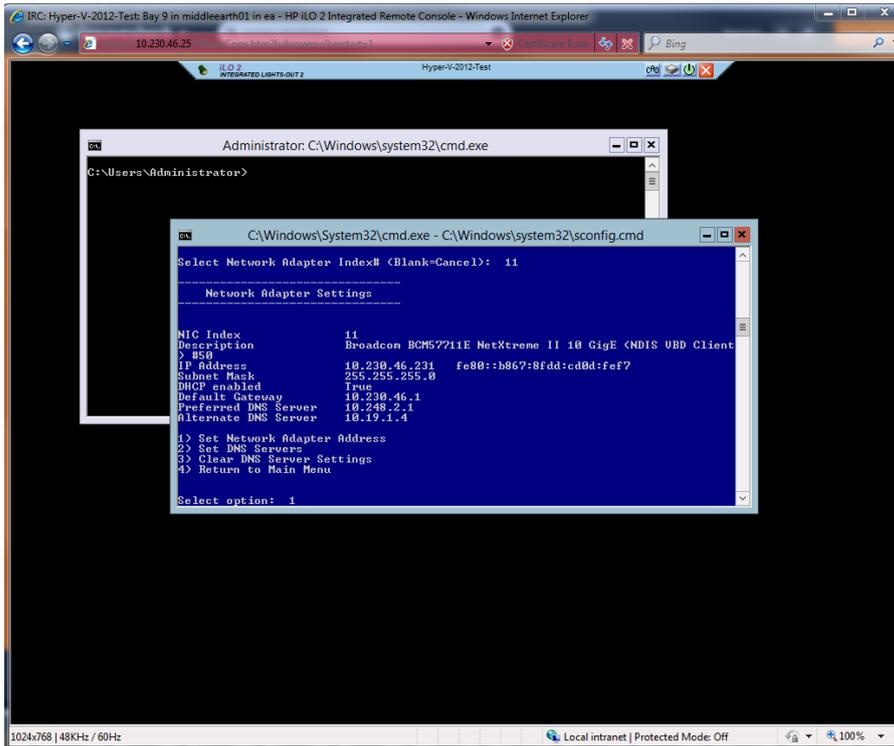
7) Luego de la instalación hay que configurarlo ingresando con Ctrl+Alt+Delete



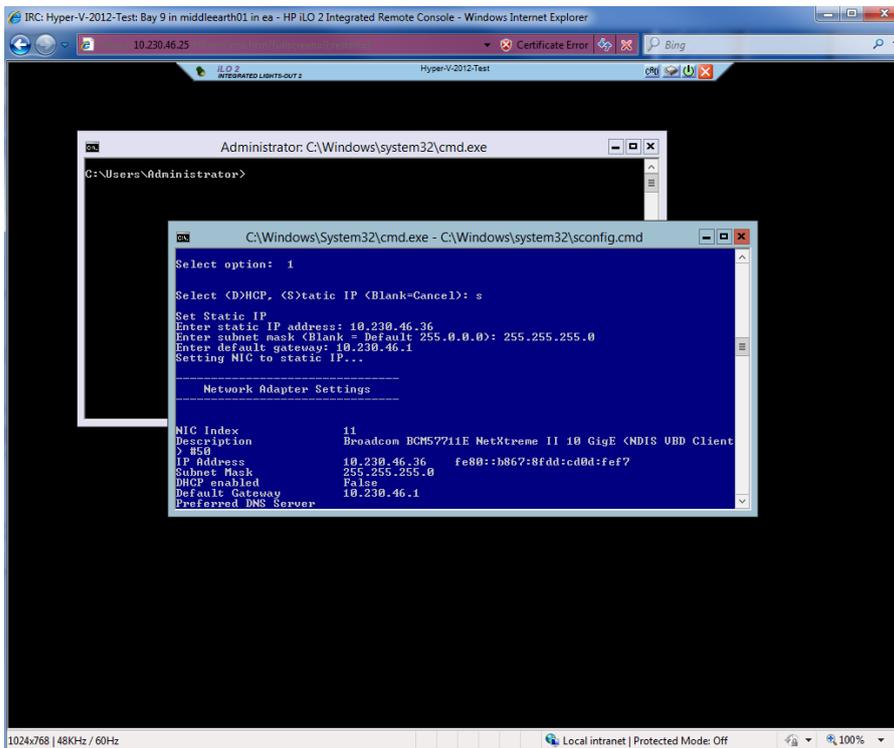
8) Configuramos el nombre a HyperTest2 a través de la Opcion2

9) Luego con la Opción 8 entramos para configurar las características de red

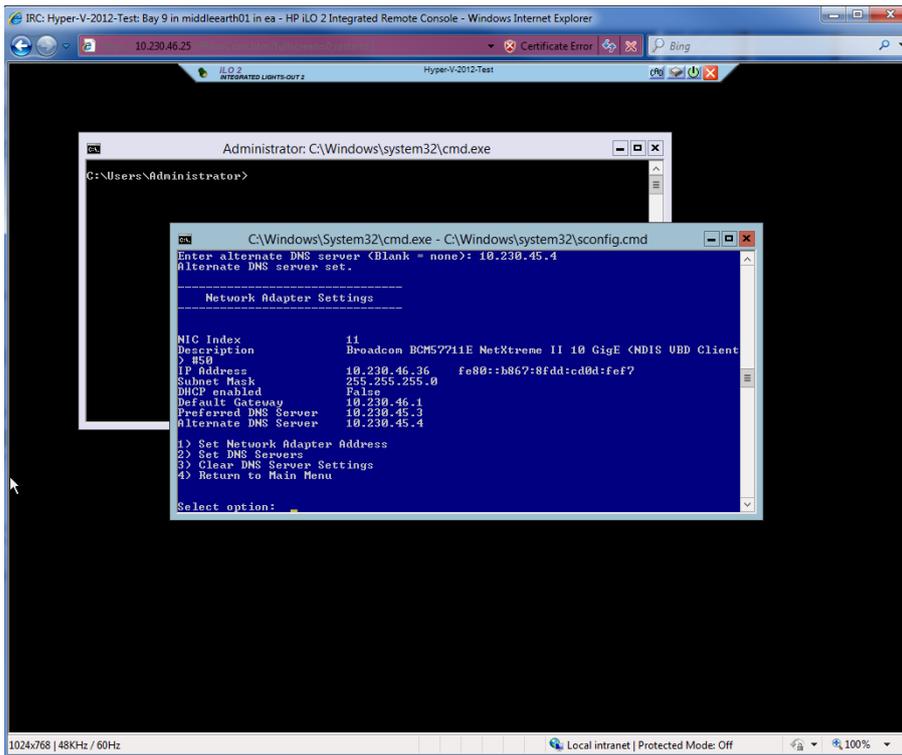
10) Elegimos la NIC a través del NIC Index, en este caso es el numero 11



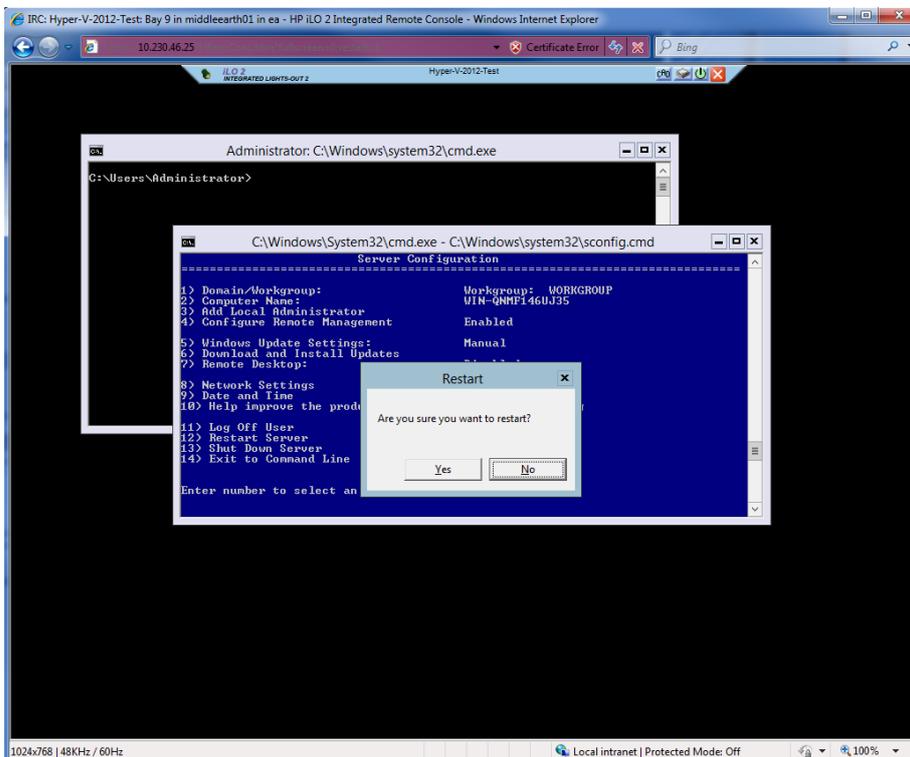
11) Con la Opción 1 configuramos el IP, mascara, Gateway y desactivamos el dhcp.



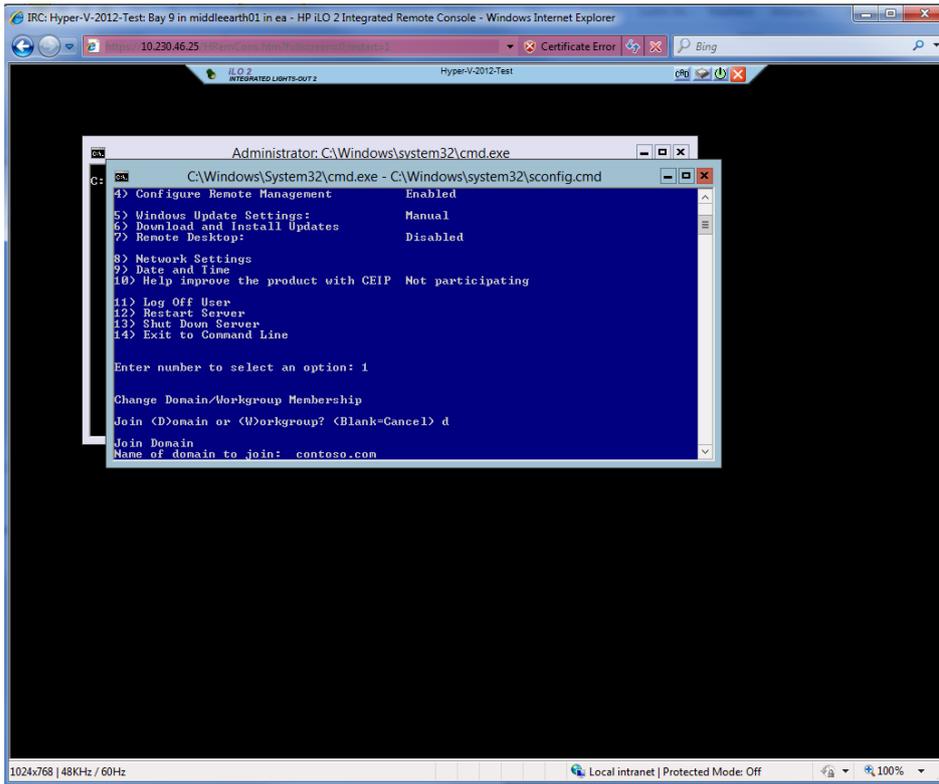
12) Con la Opción 2 luego configuramos el DNS



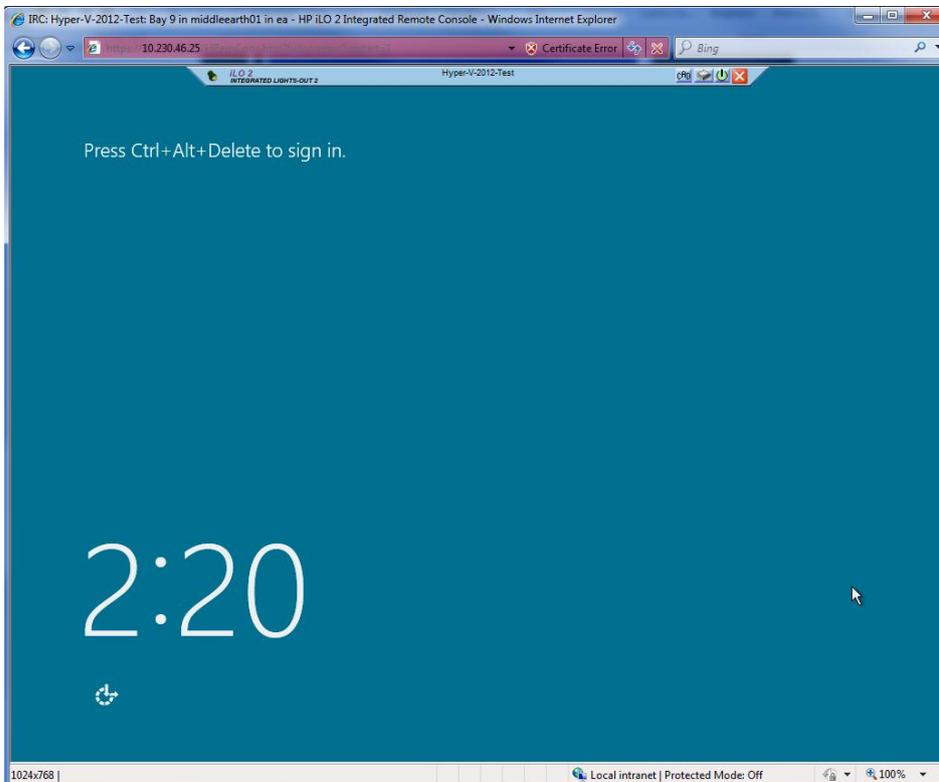
13) Reiniciamos la maquina luego de configurar las opciones de red y nombre



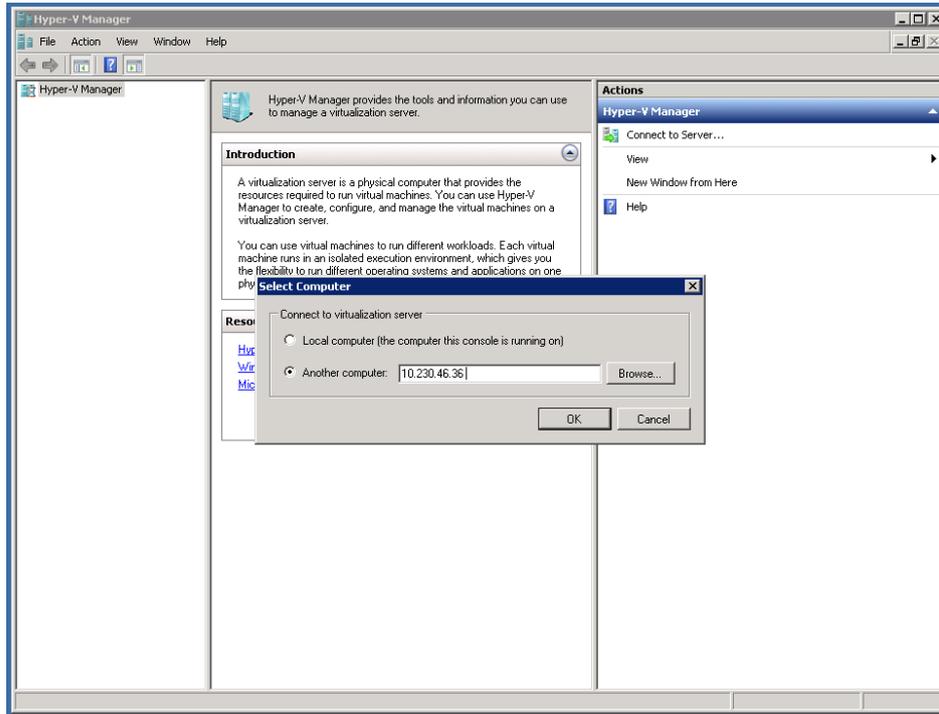
14) Con la opción 1 unimos la maquina al dominio.



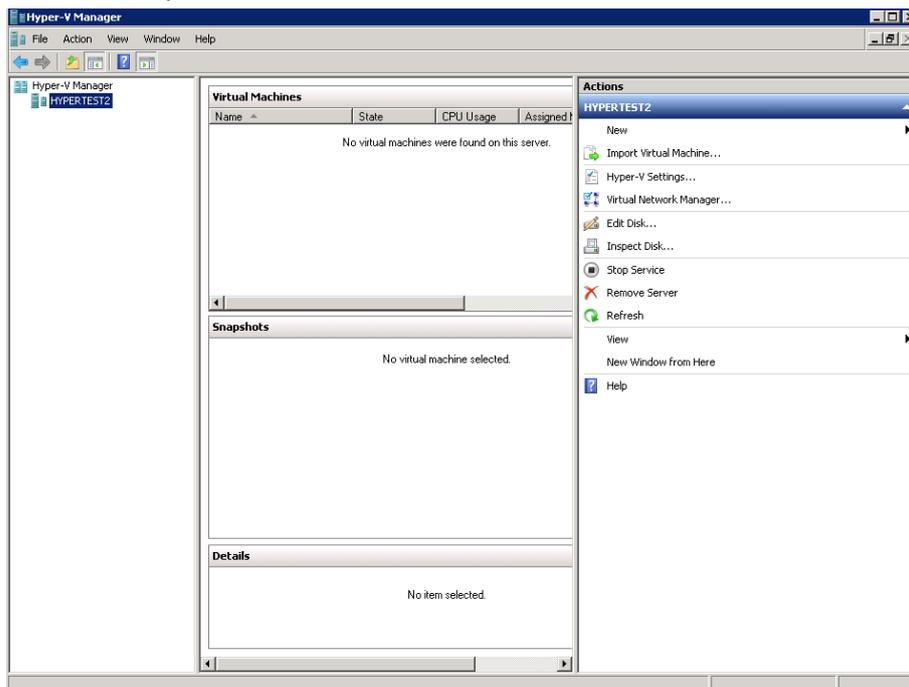
15) Luego de unirla al dominio, el servidor queda listo para ser accedido por una máquina de Administración



- La instalación fue bastante sencilla, la configuración fue sencilla también siempre y cuando el servidor sea unido al dominio, de otra forma la configuración es mucho más difícil y se requiere un nivel alto para su configuración.
- Luego de la instalación del servidor es necesario accederlo desde una máquina de Administración de servidores de Hyper-V
- Luego se agrega al host dentro del Hyper-V Manager (consola de Administración)

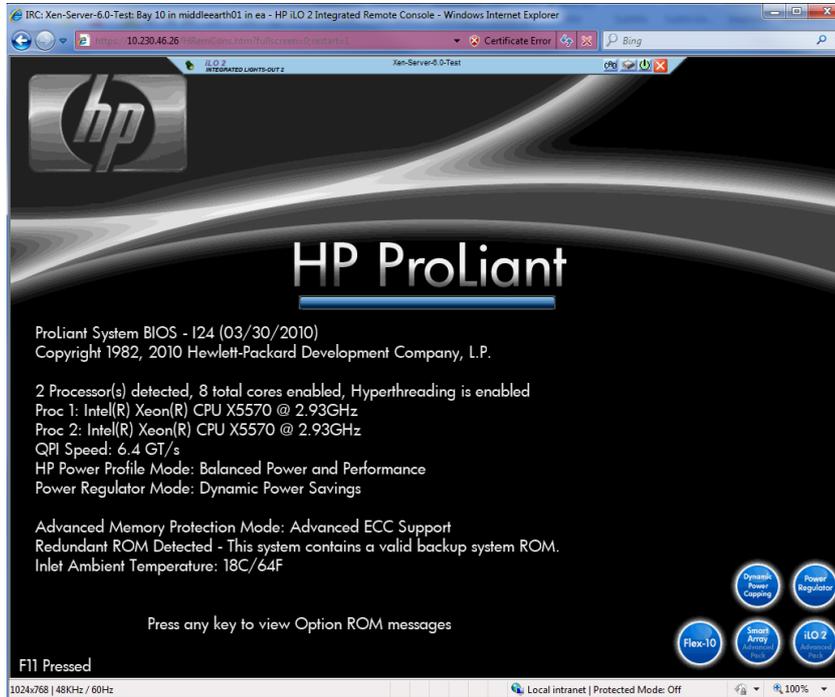


- Queda listo para ser usado.

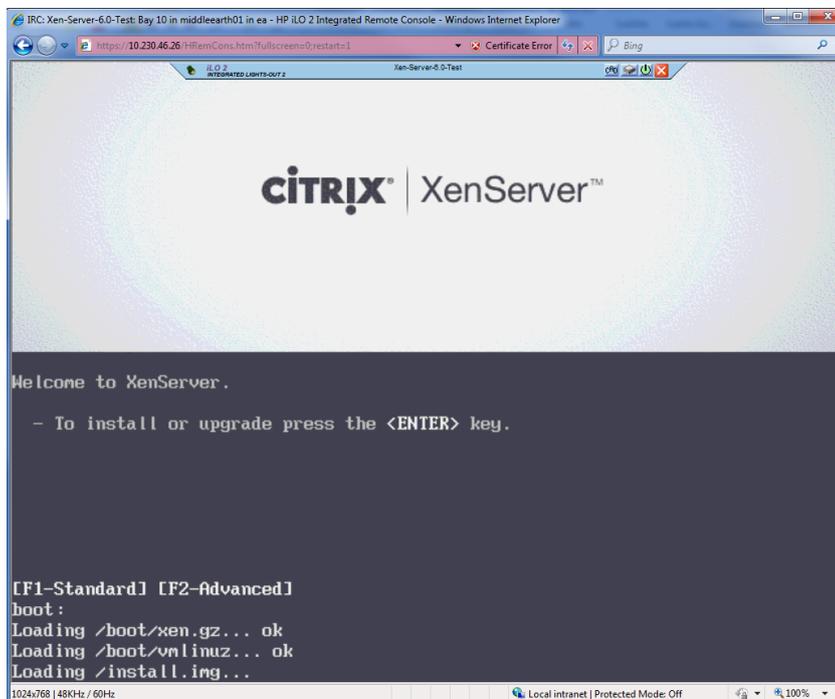


4.3 Instalaciones y experiencia de usuario de Xen Server

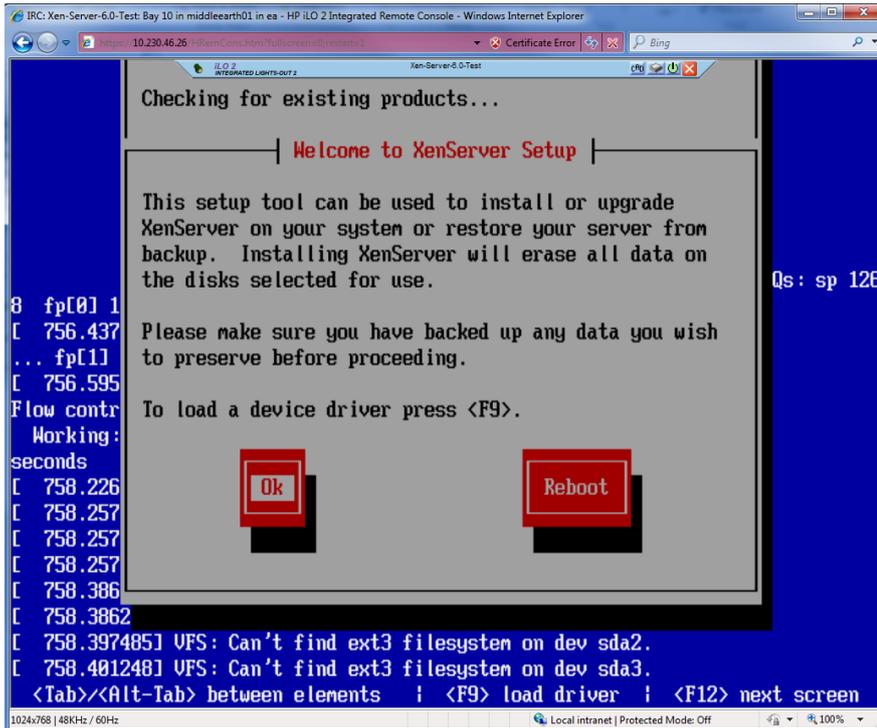
1) Ingresamos al Blade por el OnboardAdministrator



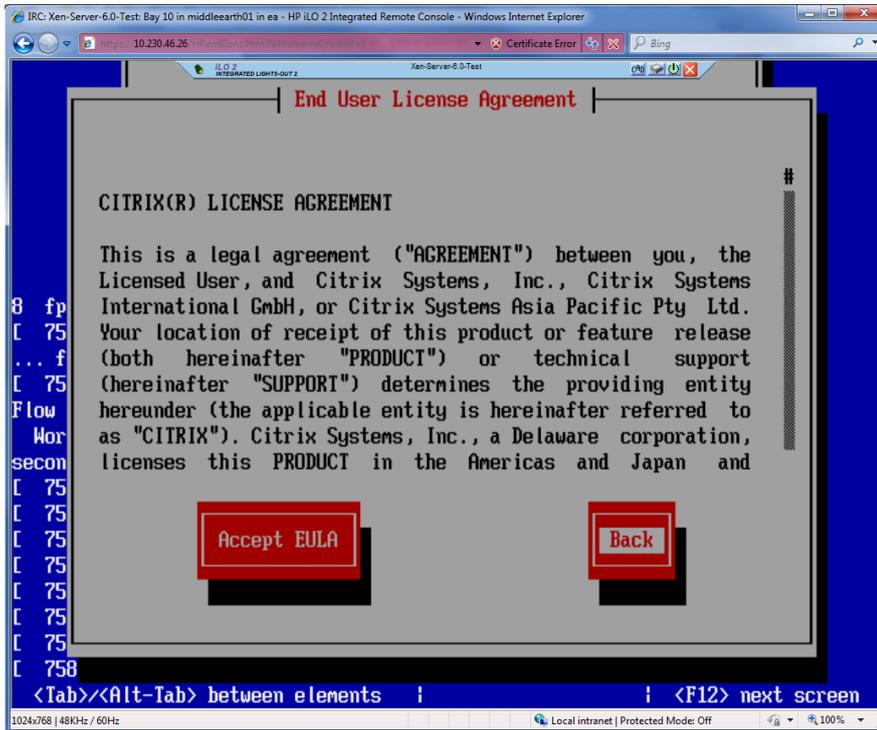
2) Comenzamos con la instalación



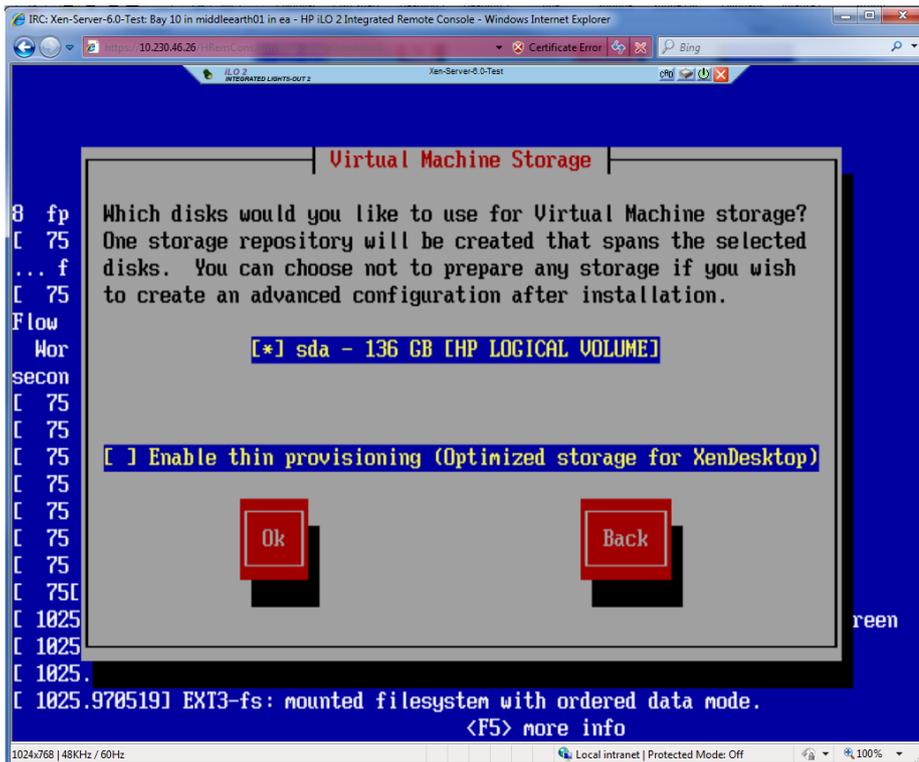
3) Ponemos continuar, para borrar si hubiese algo y comenzar con la instalación



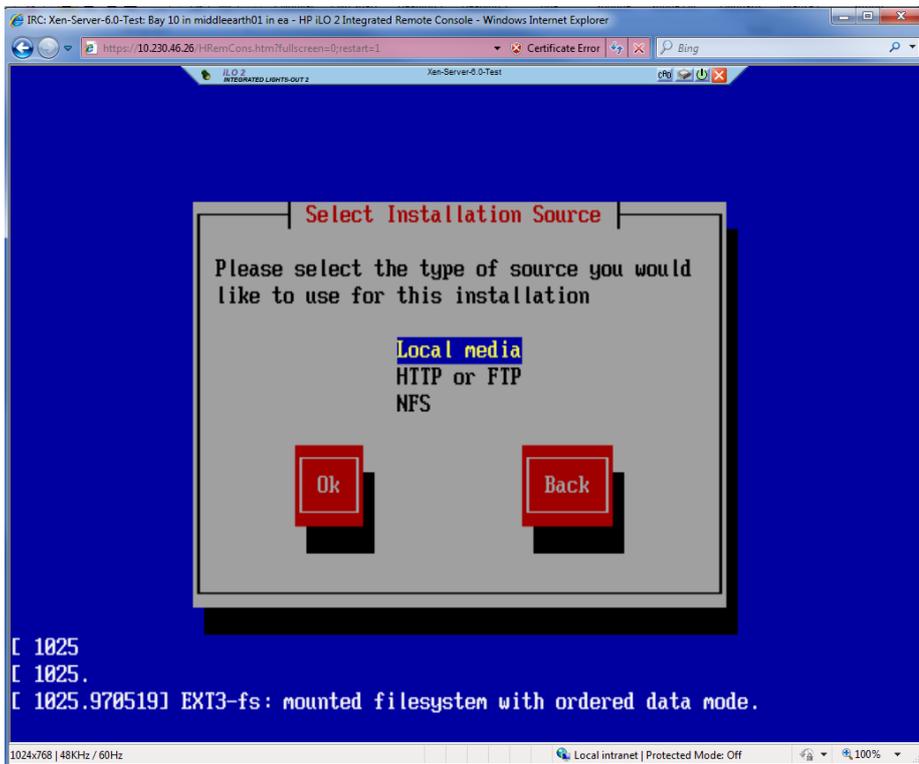
4) Aceptamos el acuerdo de licenciamiento



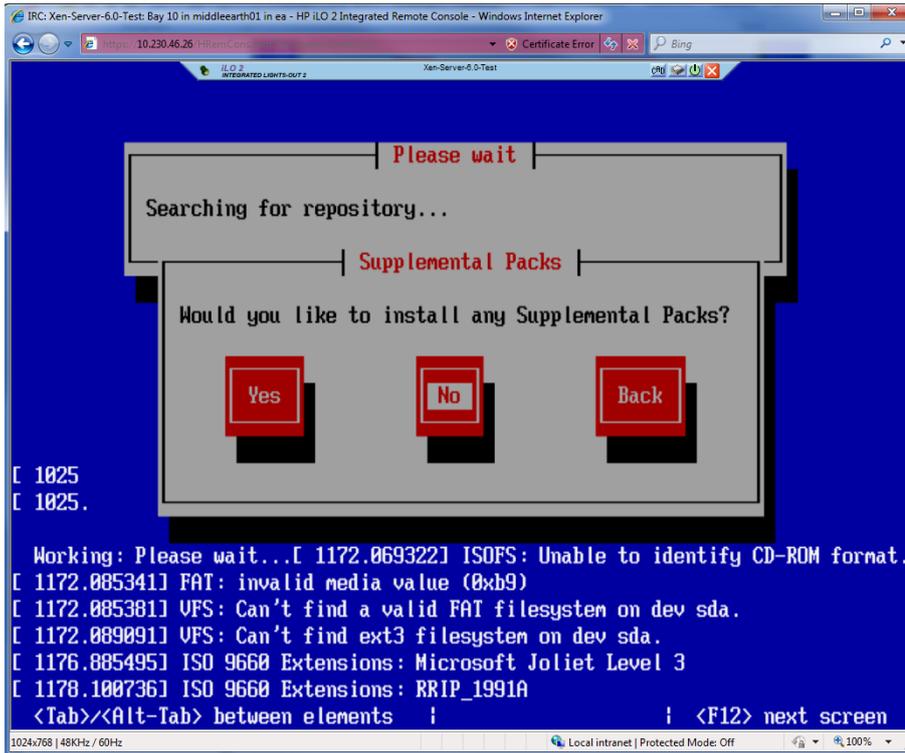
5) Elegimos el disco a donde va a ser instalado



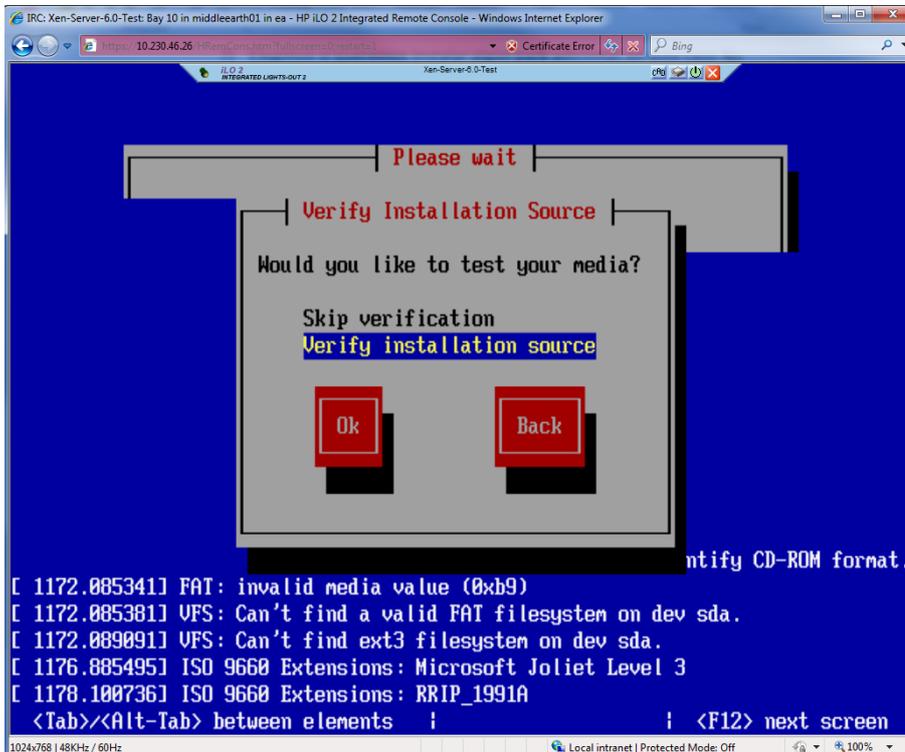
6) Elegimos la fuente de instalación, en este caso el medio local – CD



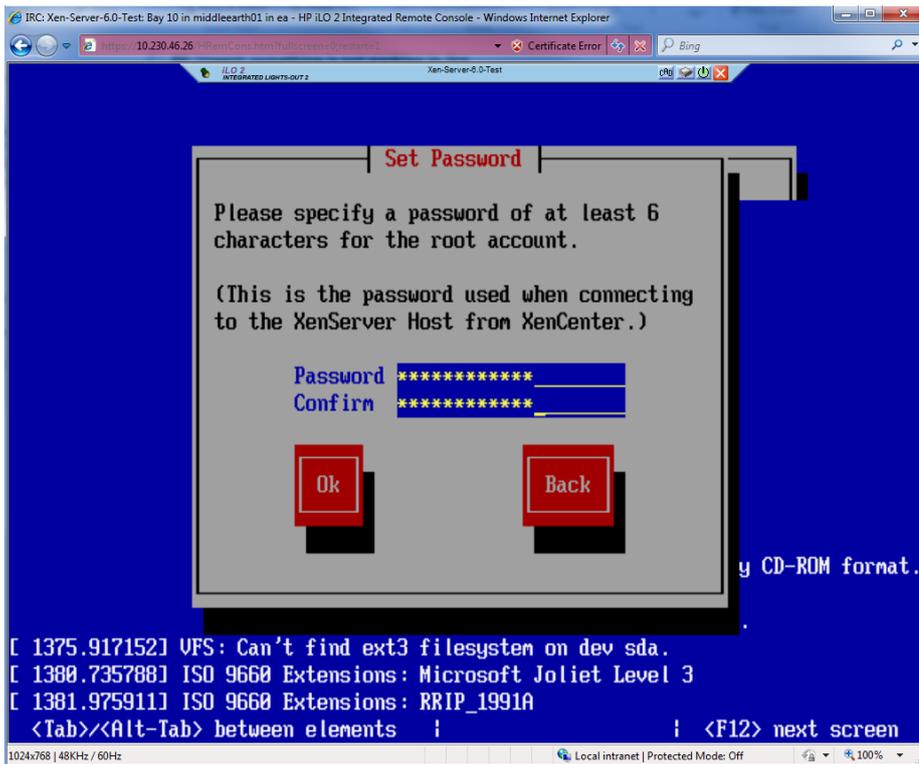
7) Elegimos si queremos instalar algún pack adicional, en este caso No



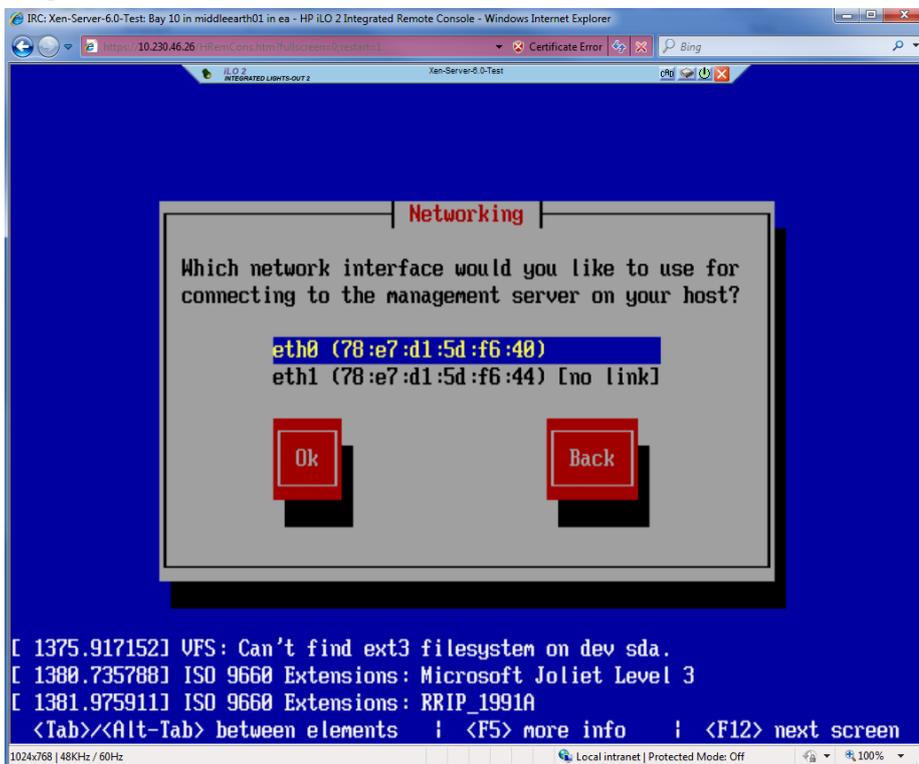
8) Verificamos la fuente de instalación



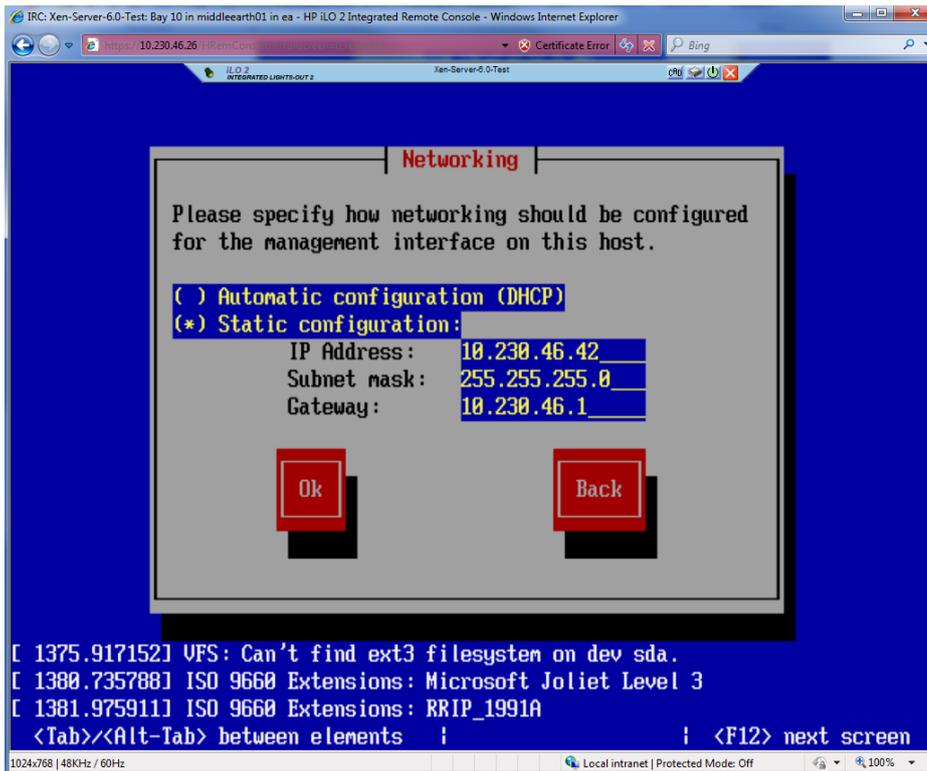
9) Ponemos el password de root



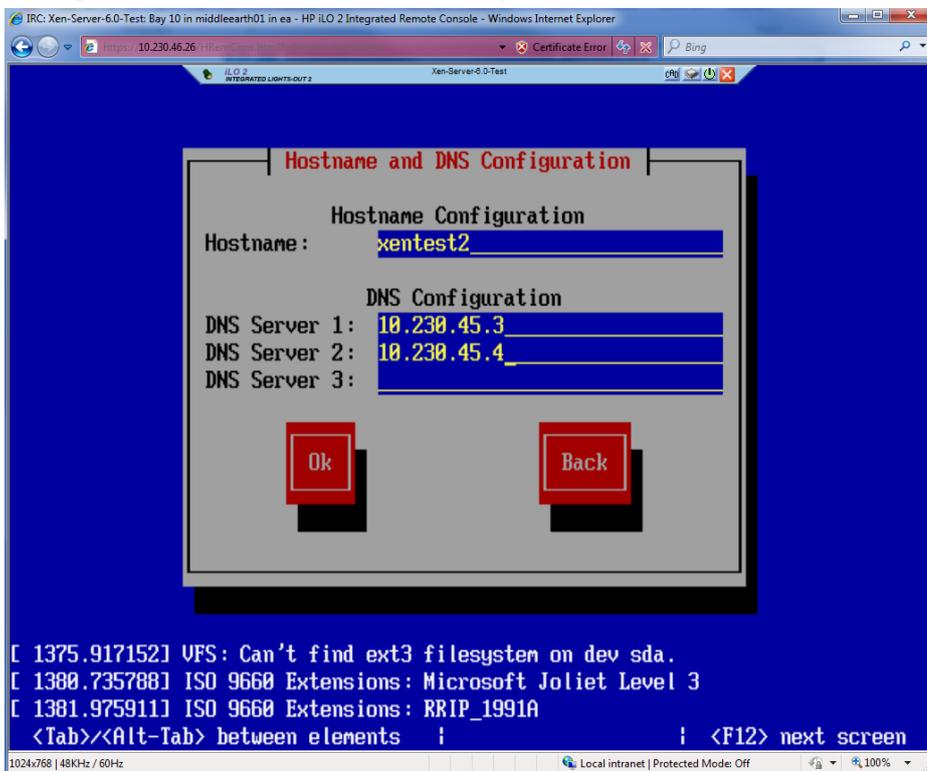
10) Elegimos la interfaz de red a utilizar



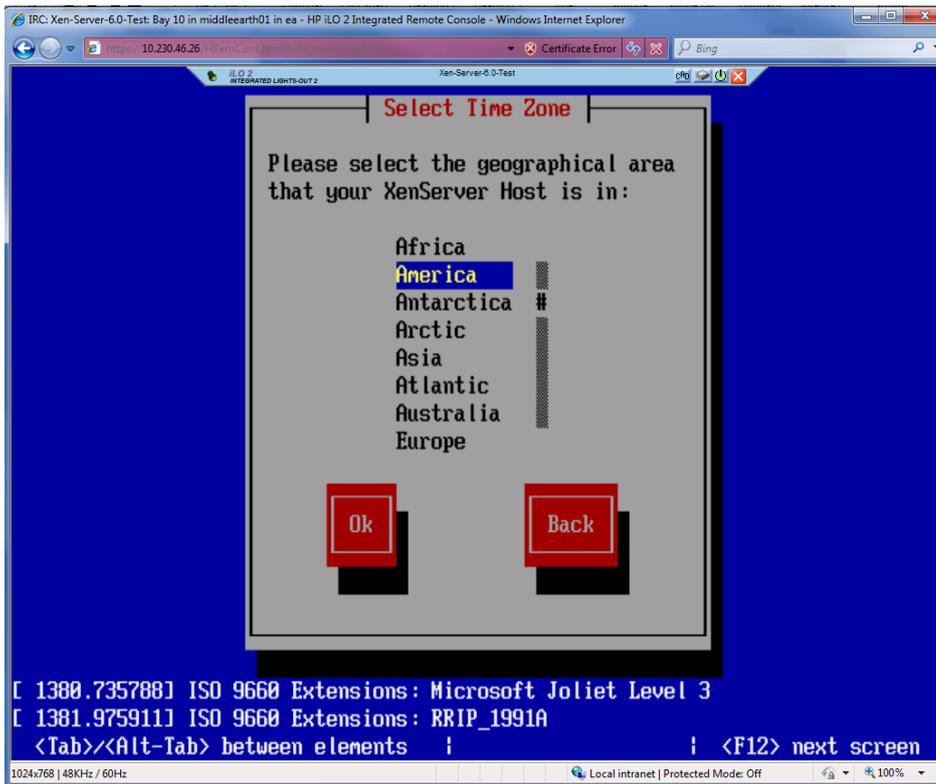
11) Configuramos la red, asignamos una IP estática, mascara de red y Gateway



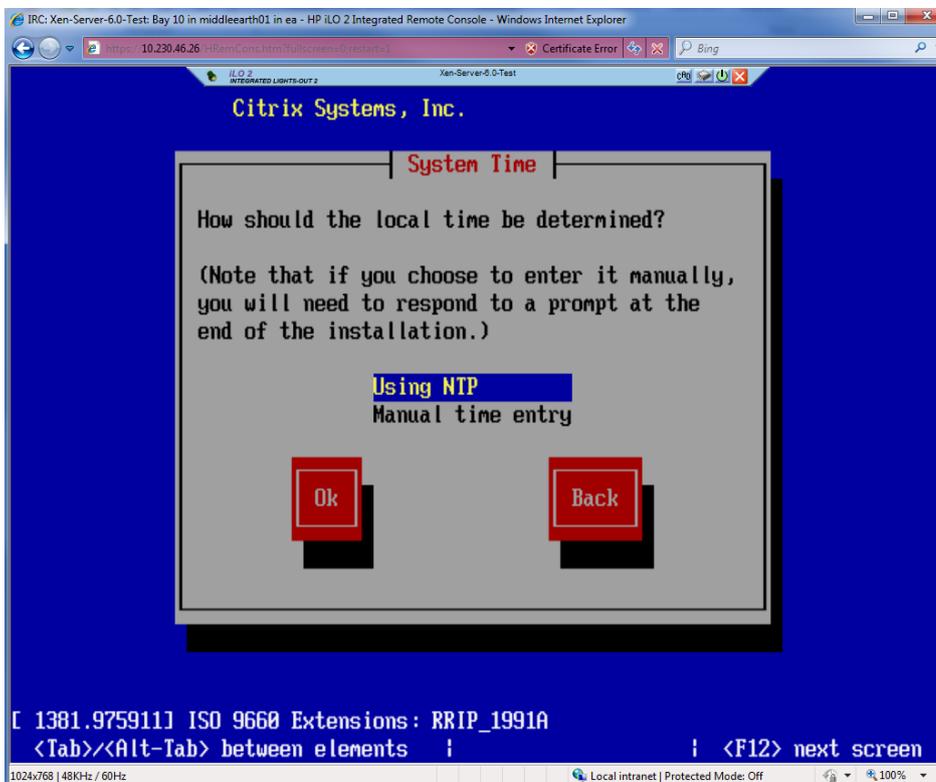
12) Configuramos el nombre del servidor y el servidor DNS



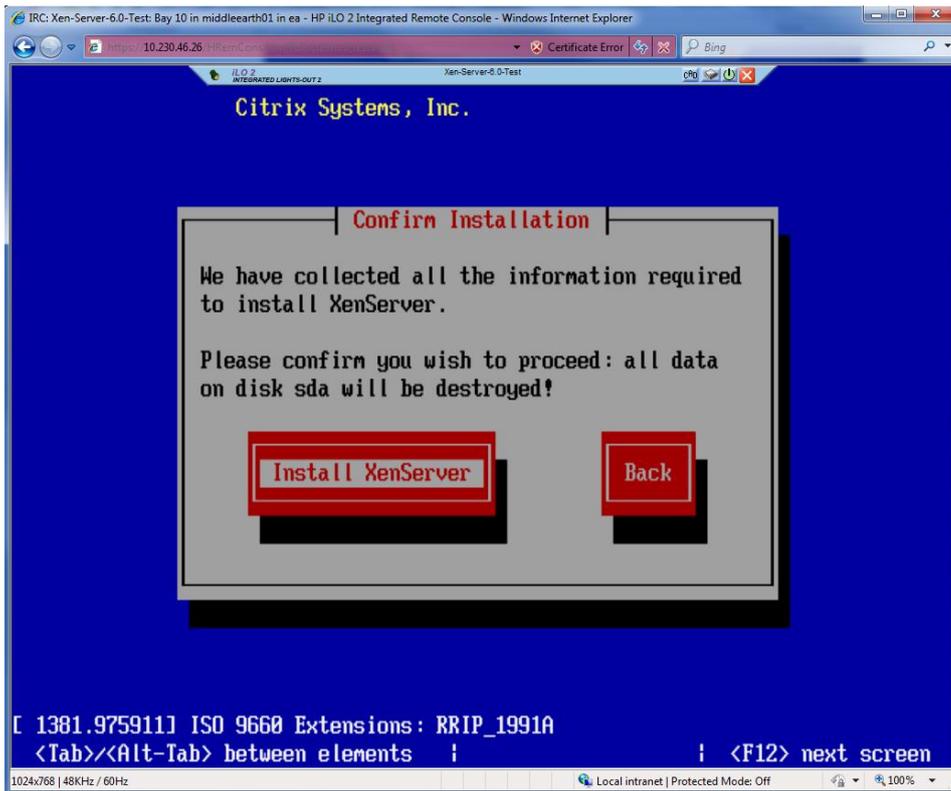
13) Elegimos la zona horaria



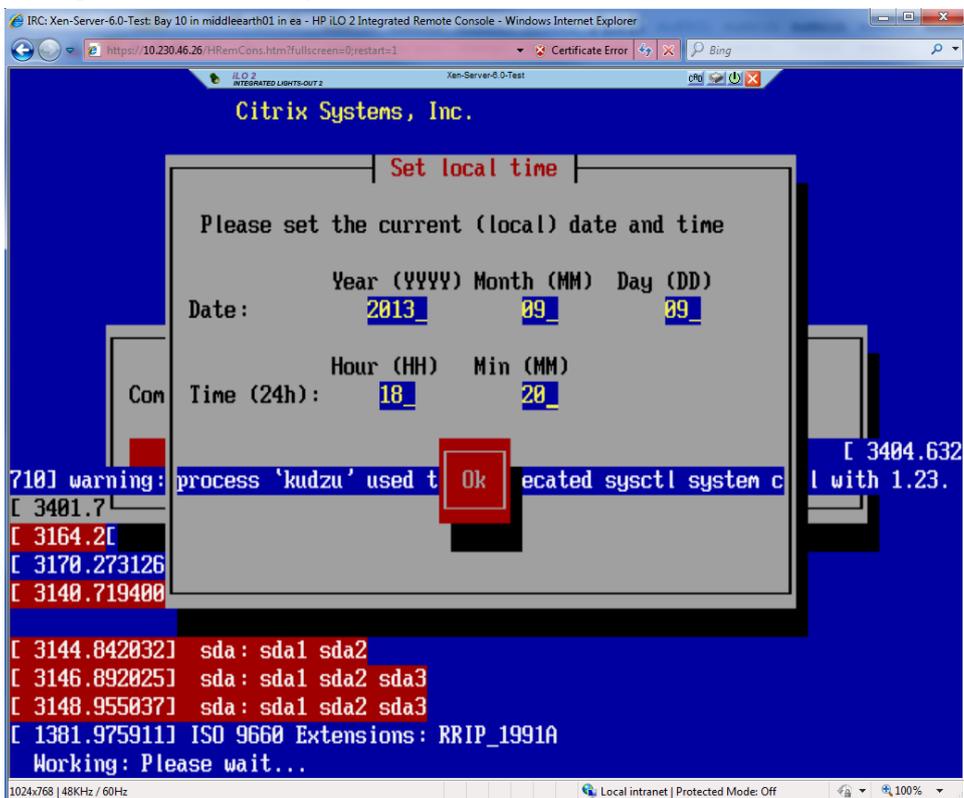
14) Elegimos si vamos a utilizar un servidor NTP o poner la hora manualmente, en este caso se pone la hora de forma manual



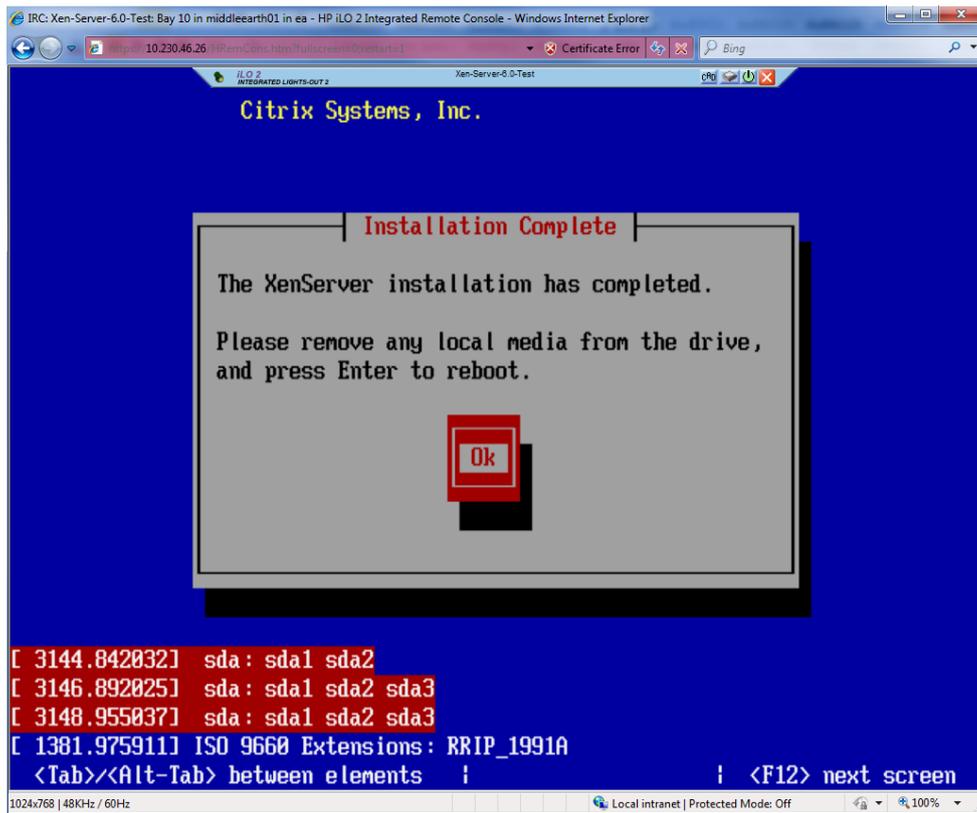
15) Largamos la instalación



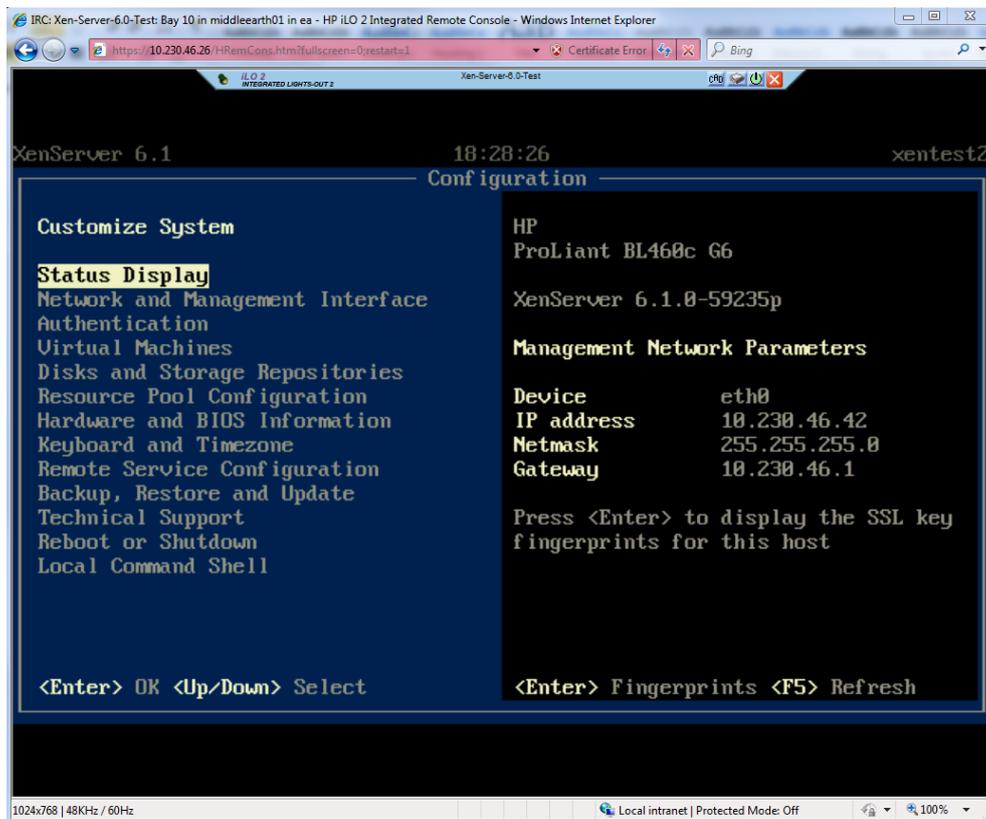
16) Configuramos la fecha y horario actual



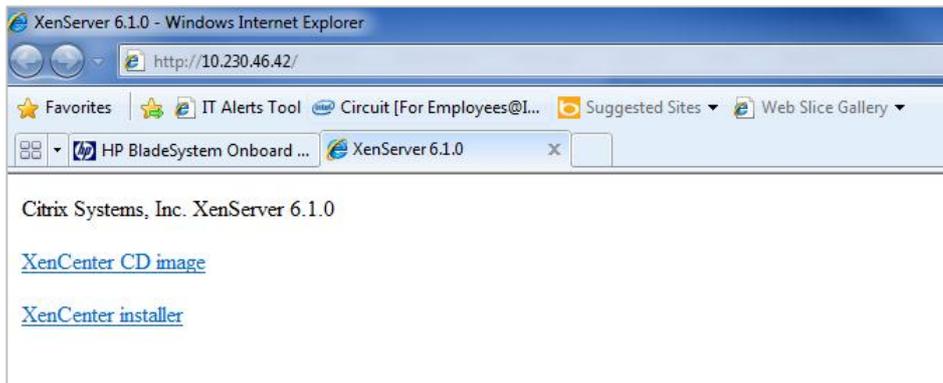
17) La instalación fue finalizada



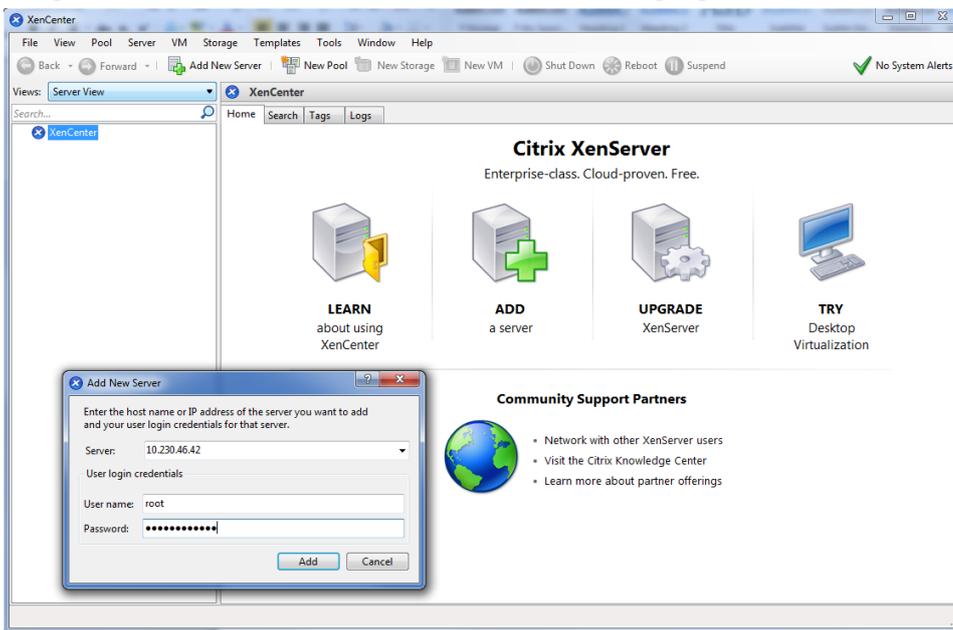
18) Ingresamos al servidor



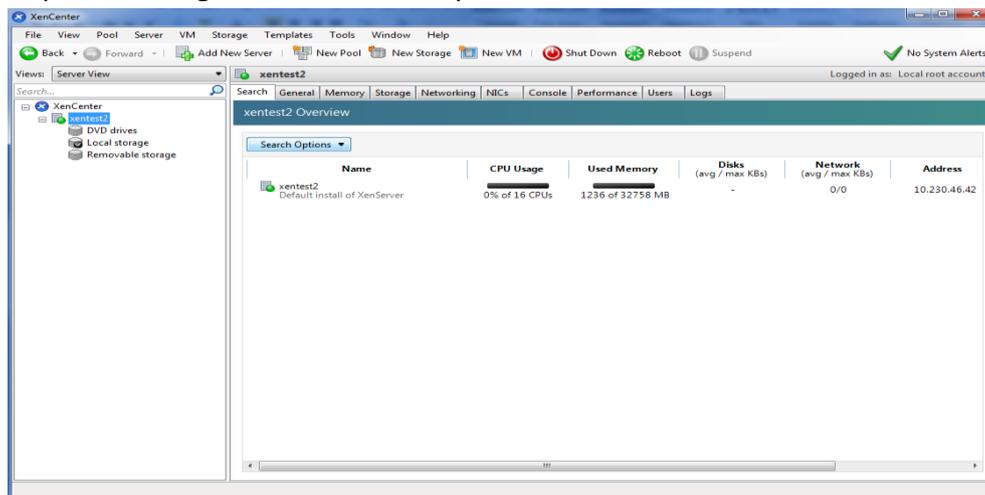
19) Luego ingresamos al Browser y ponemos la IP del servidor para descargar el XenCenter



20) Luego lo Administramos a través del XenCenter, agregando al servidor a la consola



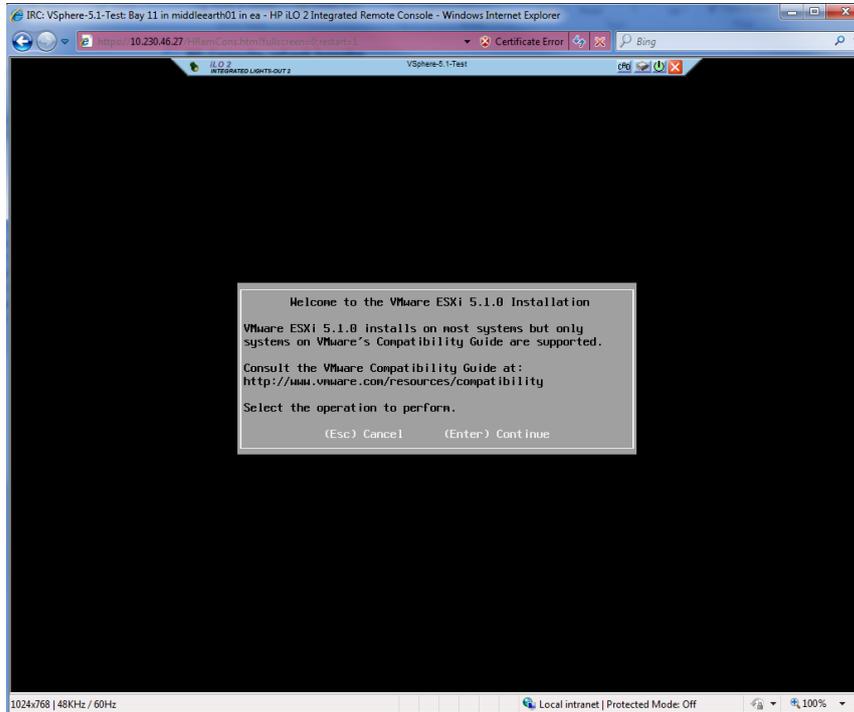
21) Ya podemos ingresar al XenServer por medio del XenCenter



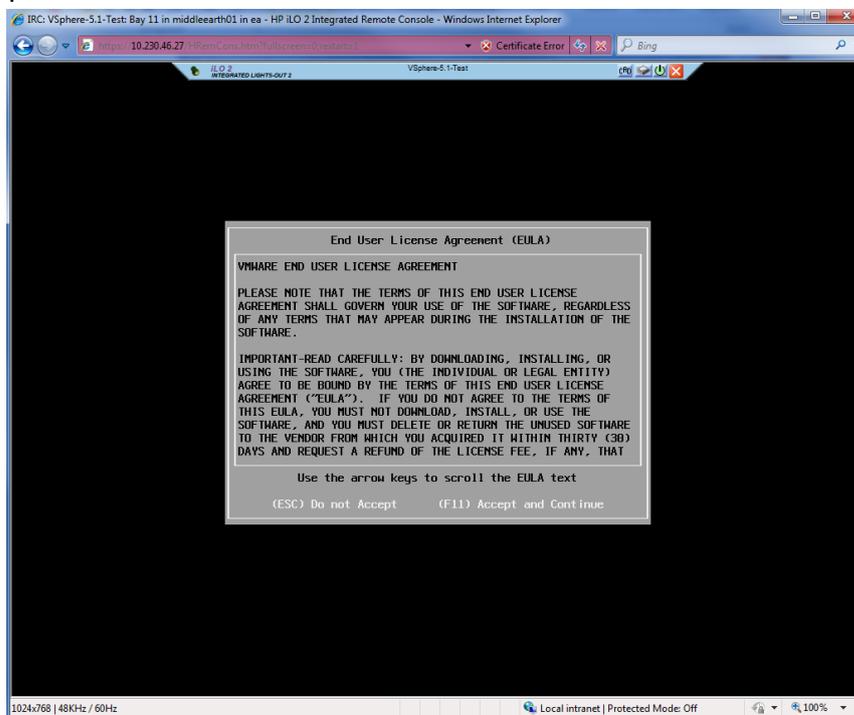
La instalación duro mucho tiempo (aproximadamente 45min) pero fue sencilla e intuitiva, el proceso de instalación te va guiando en su configuración.

4.4 Instalaciones y experiencia de usuario de ESXi 5.X

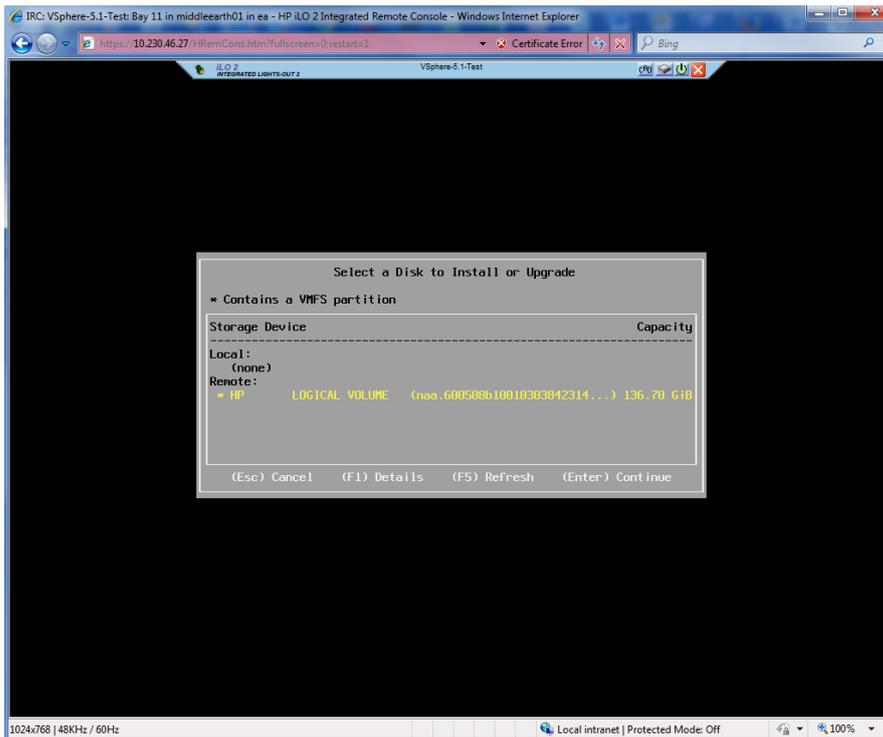
1) Ingresamos por el OnboardAdministrator e ingresamos por medio del CD a la instalación



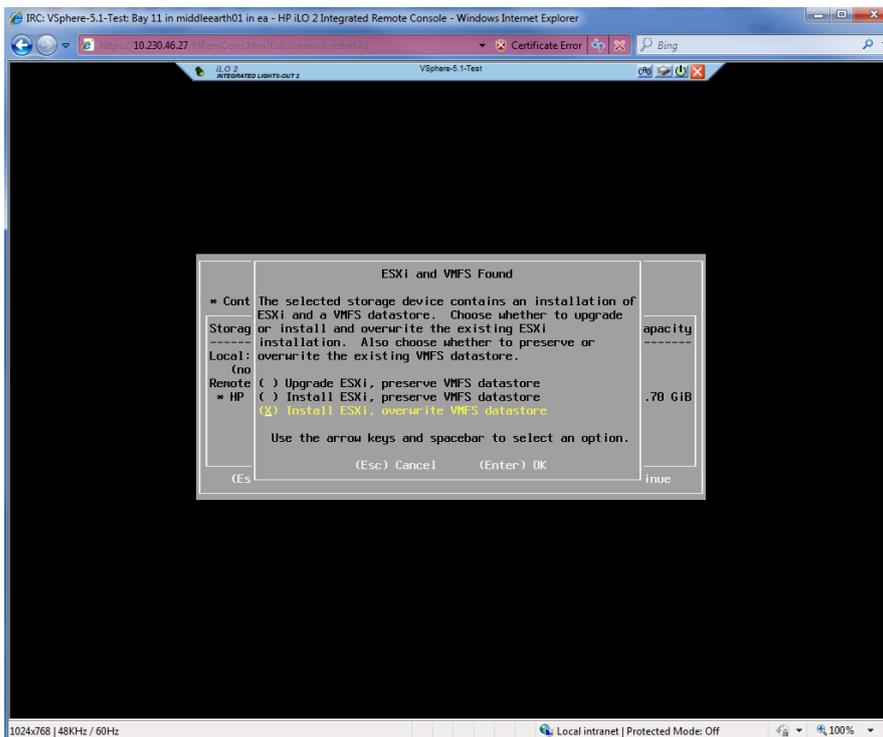
2) Aceptamos el acuerdo de licenciamiento



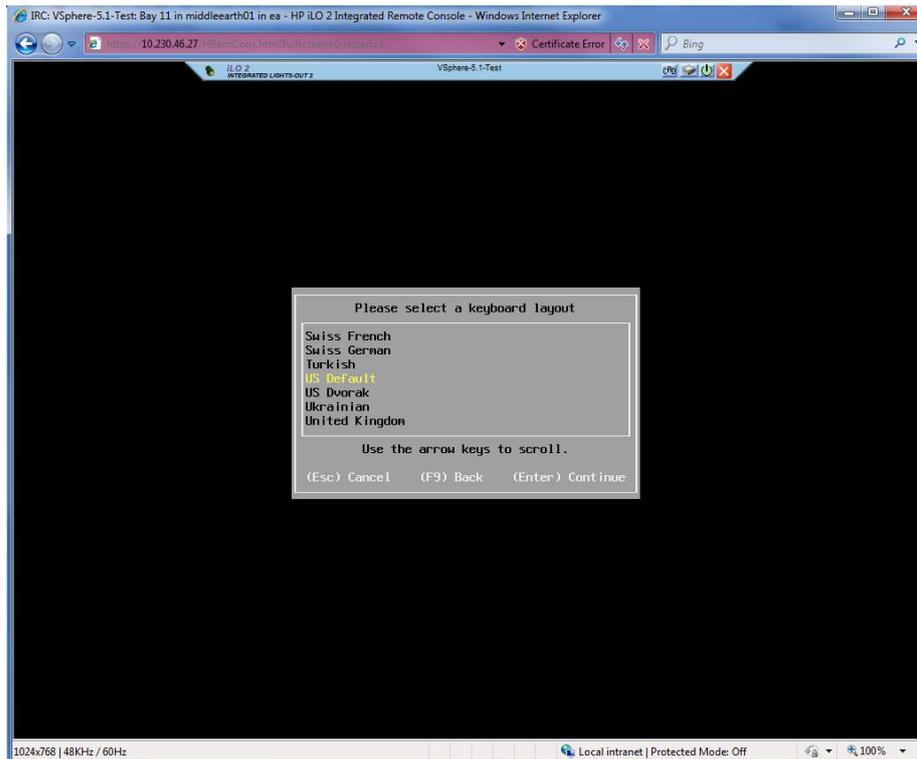
3) Elegimos el disco donde va a ser instalado



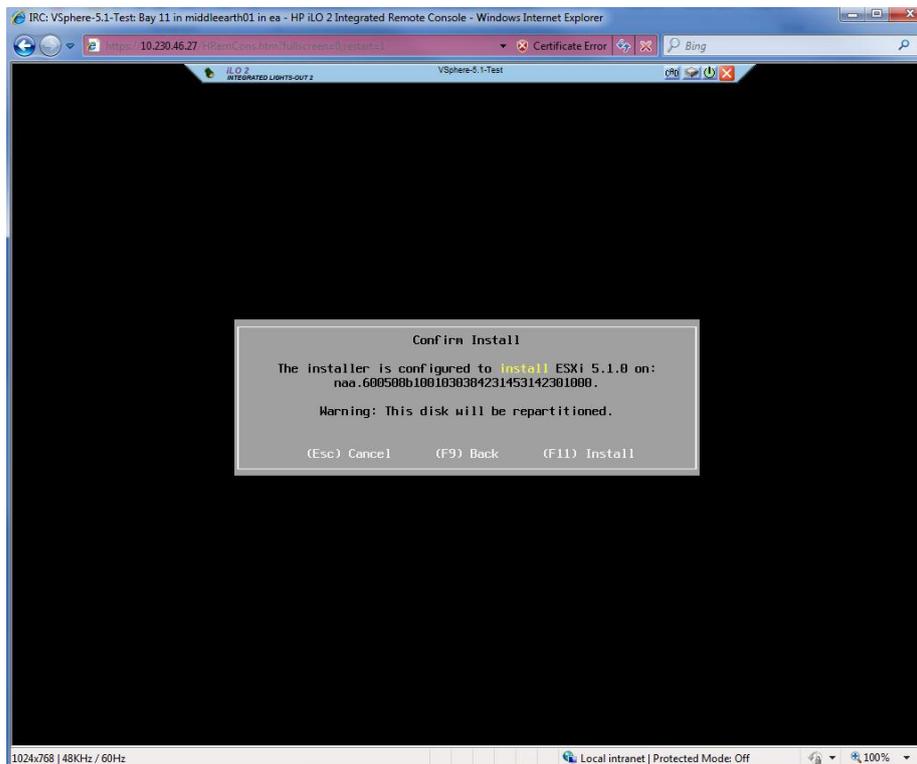
4) Elegimos Instalar y sobrescribir todo lo que tenga el disco



5) Elegimos el idioma del teclado



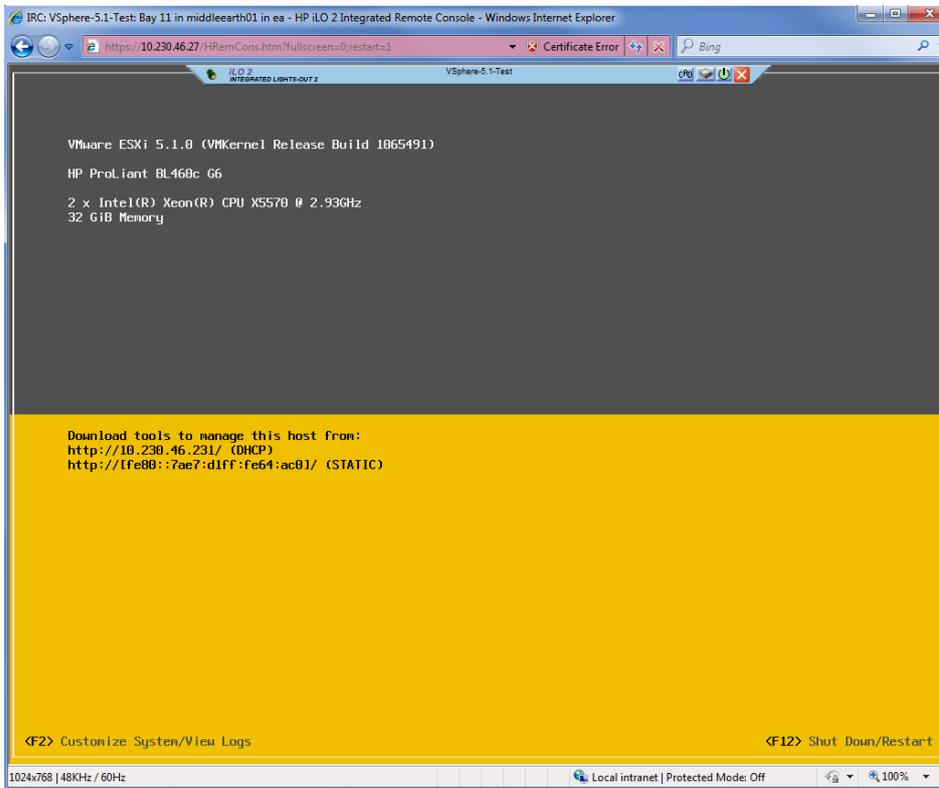
6) Confirmamos la instalación



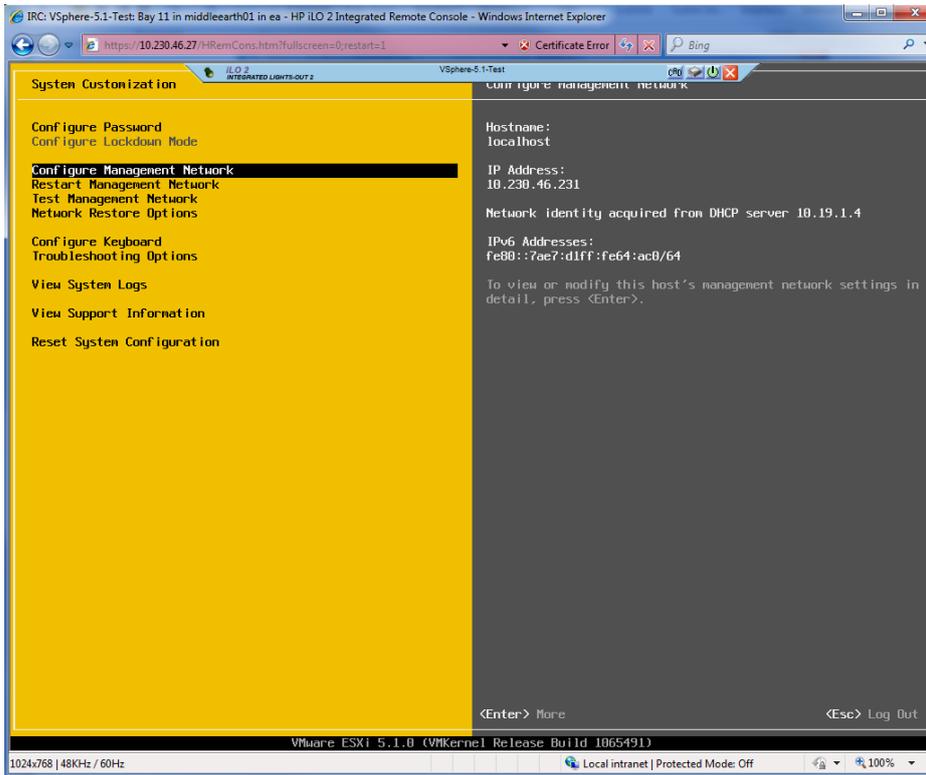
7) La instalación fue terminada, ahora rebooteamos



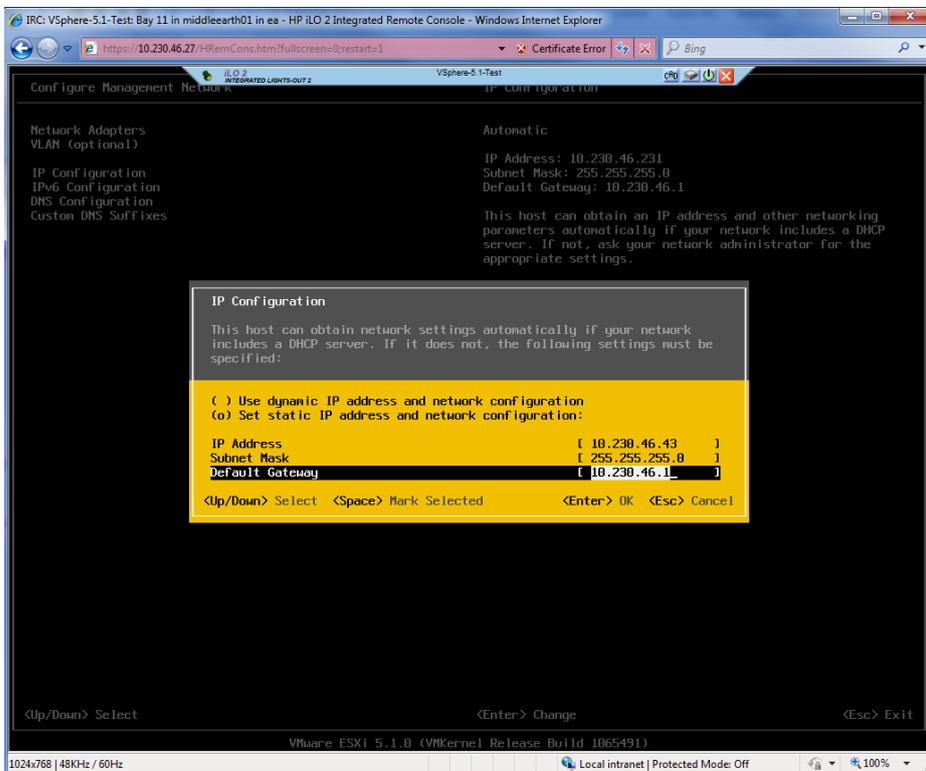
8) El servidor quedo listo para configurarlo



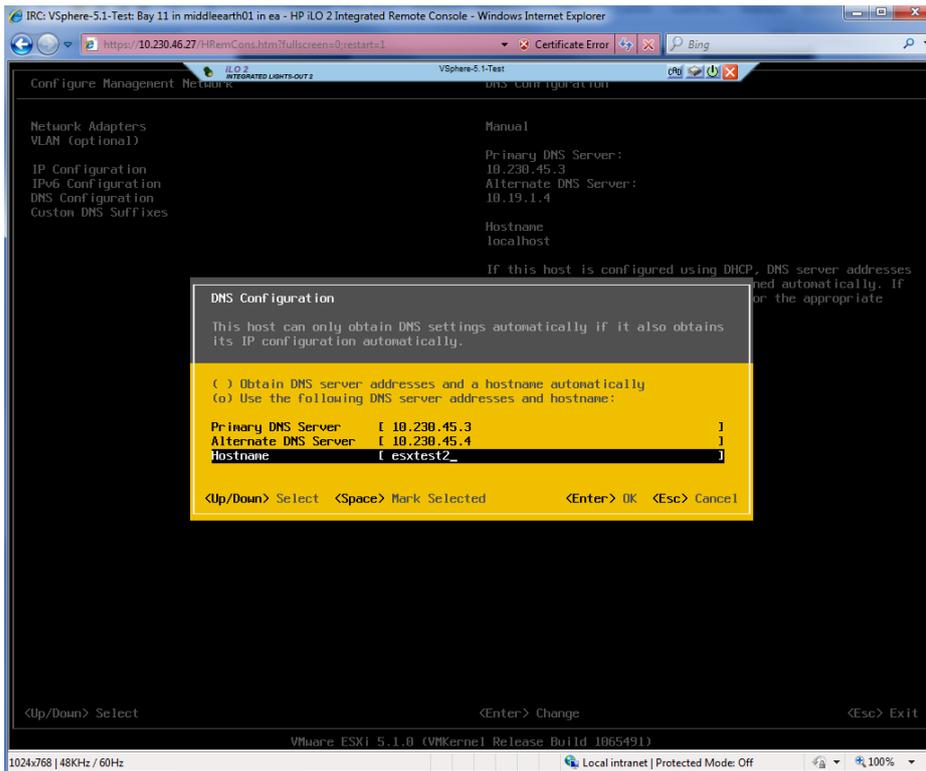
9) Configuramos las configuraciones de red



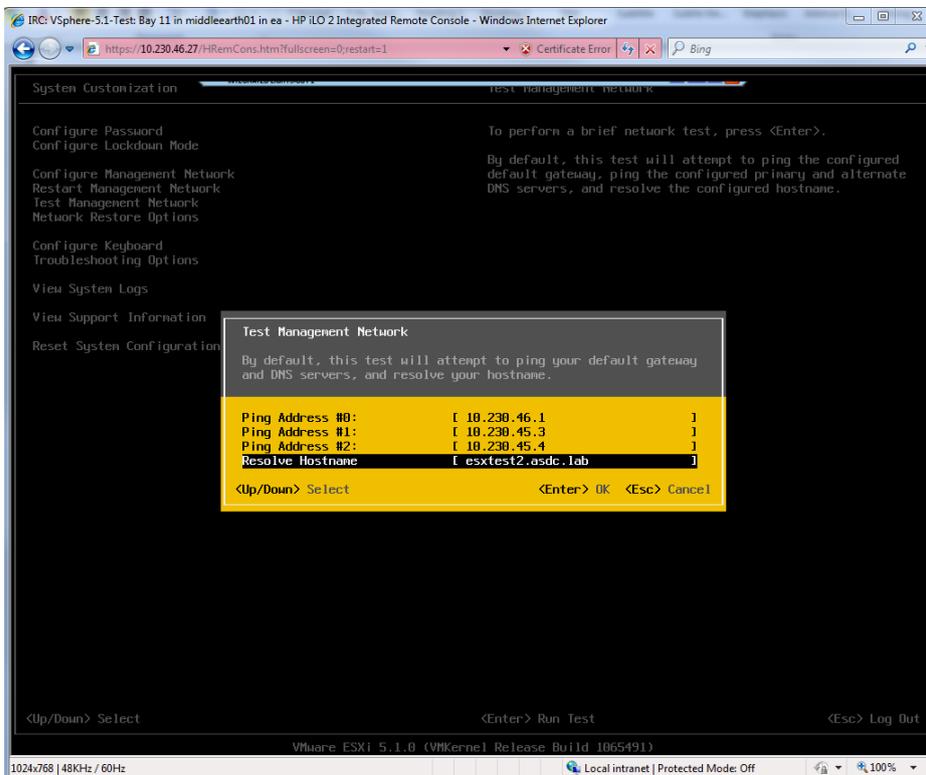
10) Configuramos el IP, mascara de subnet y Gateway



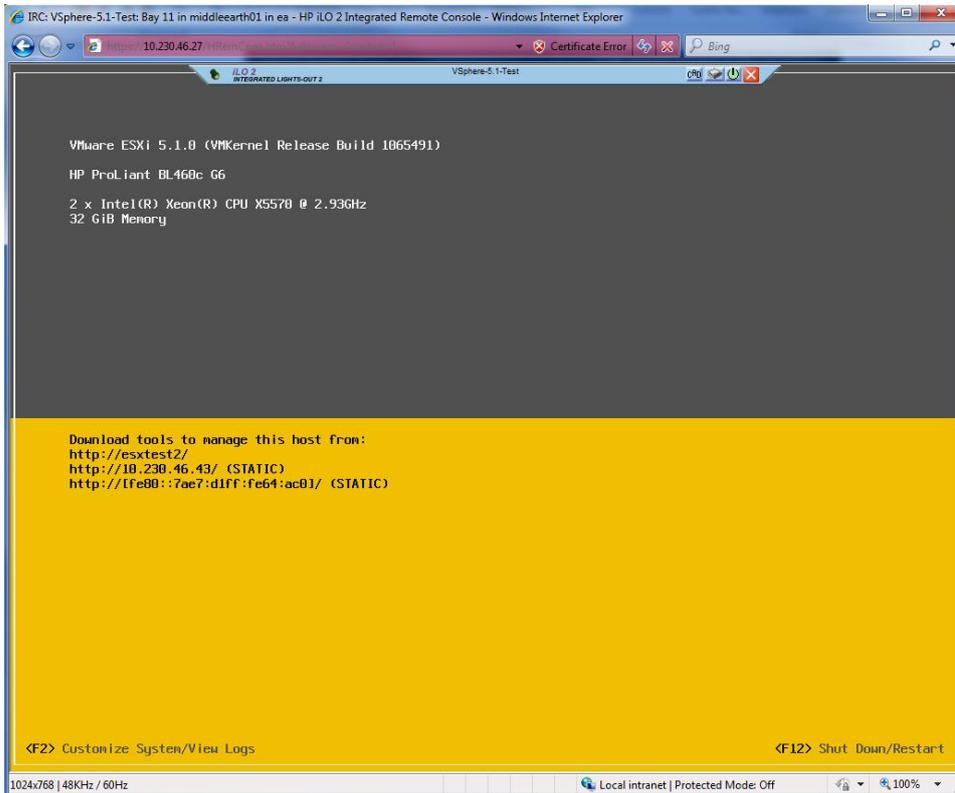
11) Luego configuramos los servidores DNS y el nombre del host



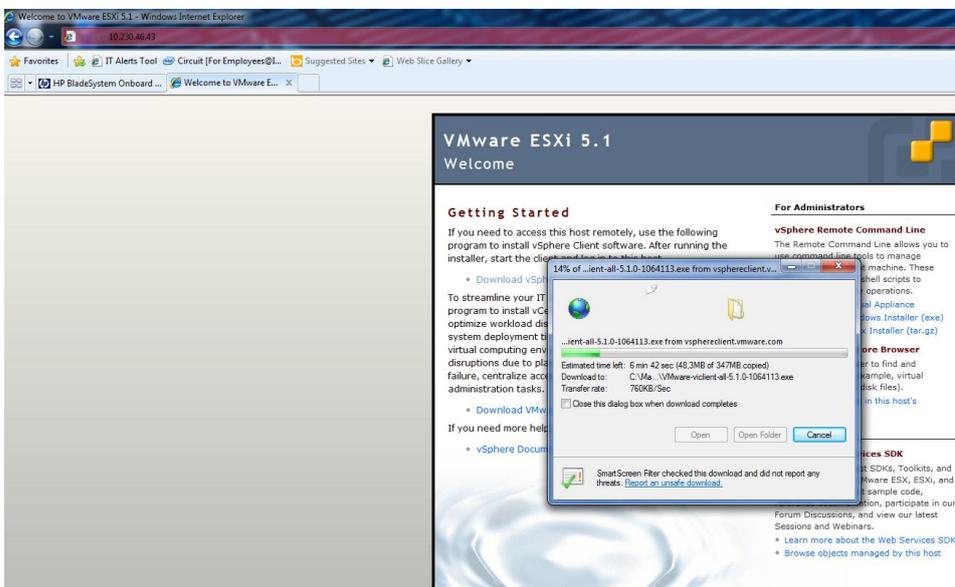
12) Luego hacemos una prueba de configuración



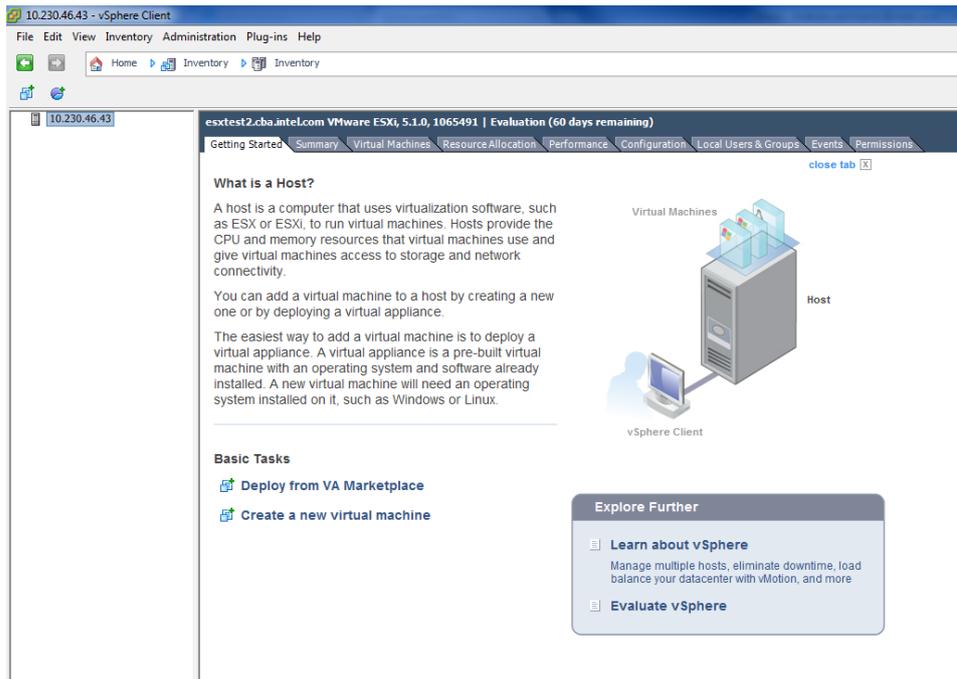
13) Queda listo para ser accedido por el cliente Vsphere



14) Ingresamos por medio del browser a la IP del host ESXi10.230.46.43 y descargamos el cliente Vsphere



15) Instalamos el Vsphere Client, e ingresamos al host



La instalación duro aproximadamente 30 min pero fue sencilla e intuitiva, el proceso de instalación te va guiando en su configuración, muy similar a la solución de Citrix

CAPITULO V - ESTUDIO COMPARATIVO DE HERRAMIENTAS

5.1 Estudio comparativo: Vsphere 5.x, Xen Server 6.X y Hyper v 2012 R2

5.1.1. Instalación del producto, Consola de administración y Experiencia de Usuario:

VmWare vSphere 5.x:

La instalación de VmWare vSphere es simple y Accesible para un Admin Jr con conocimientos básicos de Administración, lleva aproximadamente 20 minutos, la experiencia de usuario en la instalación es buena e intuitiva y posee muchas formas de montar la ISO o imagen.

La consola de Administración que utiliza es el Vsphere Client

Microsoft Hyper-V 2012R2

La instalación de Microsoft Hyper-V es simple y Accesible para un Admin Jr con conocimientos básicos de Administración siempre y cuando se realice dentro de un dominio sino su complejidad aumenta considerablemente, lleva aproximadamente 20 minutos, la experiencia de usuario en la instalación es buena e intuitiva y posee pocas maneras de montar la ISO o imagen.

La consola de Administración que utiliza es el Hyper-V Manager

Citrix XenServer 6.x:

La instalación de Citrix XenServer es simple y Accesible para un Admin Jr con conocimientos básicos de Administración, lleva aproximadamente 40 minutos su instalación, la experiencia de usuario en la instalación es buena e intuitiva y posee solo una manera de montar la ISO o imagen que es por medio de CIFS.

La consola de Administración que utiliza es el Xen Center

5.1.2. Posición en el Mercado:

VmWare vSphere 5.x:

VmWare actualmente es el número 1 del mercado debido a su temprano lanzamiento en el mercado y la madurez del producto entre otras cosas.

Entre sus fortalezas podemos encontrar: Estrategia de virtualización y roadmap que conducen a la Nube (privada e Híbrida), El liderazgo tecnológico y la innovación, Alta satisfacción del cliente y que Posee una gran base de clientes (especialmente entre las grandes empresas)

Entre sus debilidades podemos encontrar: Modelo de negocio que depende de los ingresos de vSphere para ampliar e invertir en otros mercados y que tarda en aplicar la tecnología de Nube

Microsoft Hyper-V 2012R2

Microsoft actualmente está en la cuadrilla de seguidores del número 1 (VmWare) y podemos decir que es el número 2 en lo que respecta posición del mercado.

Dentro de sus fortalezas podemos destacar: Entorno administrativo que es familiar para los administradores de Windows, Base instalada de Windows, especialmente para un gran número de empresas que utiliza Windows, Bajo precio, Empresa con fortaleza financiera.

Entre sus debilidades podemos encontrar: Dificultad para competir con el posicionamiento de VMware que ya posee una base adquirida, especialmente en las grandes empresas, Dificultad para competir con VMware con respecto a los canales de distribución y los proveedores de servicio, falta de una gestión centralizada y la creciente competencia con las soluciones basadas en código abierto, especialmente en el mercado de proveedores de servicios

Citrix XenServer 6.x:

Citrix XenServer podemos decir que está ubicado como número 3 en lo que respecta posición del mercado.

Dentro de sus fortalezas podemos destacar: XenServer ofrece un buen producto sin costo (excepto por costo de soporte), Al poseer el código abierto Xen, Citrix tiene una gran oportunidad de crecimiento en el mercado de proveedores de servicios de telecomunicaciones y en la nube y que Citrix tiene muy buenos canales de distribución.

Dentro de sus debilidades podemos comentar: Citrix posee competidores de software de código abierto como KVM y OpenStack, y no posee suficiente de apoyo de la comunidad ni de los proveedores asociados, Citrix redujo el enfoque y el conjunto de funcionalidades de XenServer en el área de la virtualización de servidores empresariales y XenServer no posee un modelo de negocio sólido para lograr cubrir las inversiones futuras.

5.1.3 Costos de Licencia y Soporte:

VmWare vSphere 5.x:

Actualmente vSphere 5.5 con Operation Manager se licencia por CPU física (socket, no core), sin restricciones en la cantidad de núcleos físicos o RAM virtual configurados. Asimismo, no hay restricciones de licencia sobre el número de máquinas virtuales que un host con licencia puede ejecutar.

Todos los vSphere con Operation Manager ediciones incluyen la edición de VMware vCenter Operations Management Suite Standard.

El soporte Básico o Producción: (Por ejemplo 1 año) - Producción (P): 24 Horas a los 365 días de año; Básico (B): 12 horas de lunes a viernes. Suscripción y soporte técnico es obligatorio.

Su costo es de 4245 dólares por socket + Soporte 1 año: \$891 dólares el Básico o \$1061 dólares el Producción.

Microsoft Hyper-V 2012R2

Actualmente Una sola licencia de Microsoft Hyper-V 2012 R2 Datacenter cubre 2 CPU físicas (en lugar de cubrir "por procesador" como era con Hyper-V Server 2008). El soporte de Hyper V es parte del soporte del sistema operativo (no está incluido en la licencia). Los precios no incluyen soporte. Su costo es de 3077 dólares por socket (6155 dólares hasta 2 sockets (más de 2 sockets aumento del 28%))

Soporte: Software Assurance (SA) durante 2 años (por 2 CPUs física) es de alrededor de 2.406 dólares por 2 años o 3.609 dólares por 3 años para la edición de DC de Windows Server 2012

Citrix XenServer 6.x:

El costo de Citrix es un costo de mantenimiento y su costo anual de 690 dólares x socket y Perpetua de 1250 dólares x socket.

Citrix también ofrece una opción comercial totalmente compatible de XenServer 6.5, que incluye actualizaciones envasados y mantenimiento, soporte 24x7 en todo el mundo y protecciones de licencia comercial. Ahora está disponible como edición única (evaluador de las anteriores ediciones Advanced, Enterprise y Platinum). Licencias ya no permiten características XenServer, sino que indican que una XenServer está bajo un contrato de soporte válido. XenServer 6.5 ya no requiere un servidor de licencias o archivo de licencia para habilitar las características, ya que todas las funciones están habilitadas de forma gratuita en el modo sin licencia. A nivel de características y funcionalidad, la única diferencia es que los usuarios de Citrix XenServer gratuitas no podrán utilizar XenCenter para la instalación automática de actualizaciones de seguridad, actualizaciones y mantenimiento. Citrix XenServer sí incluye XenCenter para la administración de servidores, pero no la gestión de parches.

5.1.4 Costos de Herramientas de Gestión y Gestión Centralizada:

VMware vSphere 5.x

La herramienta de gestión de VmWare vSphere 5.x es el **vCenter** y posee gestión centralizada.

La versión Standard (Hosts Ilimitados) su costo es de 4995 dólares (vCenter Standard) + \$1049 dólares de costo de Soporte Básico (12 x día de lunes a Viernes) o \$1249 dólares de Soporte Productivo (365 días del año 7x24).

La versión Foundation ((limitado a 3 hosts) + Soporte x 1 año) su costo es de 1495 dólares + \$545 dólares de costo de Soporte Básico (12 x día de lunes a Viernes) o \$645 dólares de Soporte Productivo (365 días del año 7x24).

El cliente vSphere para un solo servidor es gratis.

Microsoft Hyper-V 2012R2

La herramienta de gestión de Microsoft Hyper-V 2012R2 es el **System Center** y posee gestión centralizada.

La versión Datacenter (admite un número ilimitado de instancias del sistema operativo) su costo es de 3607 dólares (admite hasta 2 CPU)

La versión Standard (admite hasta 2 instancias de sistema operativo) su costo es de 1323 dólares (admite hasta 2 CPU)

Citrix XenServer 6.x:

La herramienta de gestión de Citrix XenServer 6.x es el **XenCenter** y posee gestión centralizada. XenCenter es gratis.

5.1.5 Gestión de Hosts Físicos:

VMware vSphere 5.x

La gestión de los host físicos de VMware vSphere podemos decir que es Limitada ya que solo abarca su despliegue y monitoreo.

Si bien no es el foco de vCenter la gestión de los hosts físicos, está comenzando a gestionar aspectos de la gestión física como: bare metal, host Deploy, vCenter Operations capabilities, vCenter Monitoring of physical hosts.

Microsoft Hyper-V 2012R2:

Básicamente todos los componentes de la suite de administración de System Center 2012 R2 proporcionan una gestión integral de los entornos físicos y virtuales desde la misma interfaz. Algunos de los muchos ejemplos son actualizaciones a través de Configuration Manager, así como la nueva capacidad de realizar 'Fabric Updates' y Storage Array Management a través de VMM (Virtual Machine Manager).

Citrix XenServer 6.x:

Citrix XenServer no posee administración de los host físicos.

5.1.6 Funcionalidad de Integración de RBAC (Role-based access control) con AD (Active Directory) Control de acceso basado en roles integrado con Active Directory

El control de acceso basado en roles (RBAC) es una función de seguridad para controlar el acceso de usuarios a tareas que normalmente están restringidas al supe usuario. Mediante la aplicación de atributos de seguridad a procesos y usuarios, RBAC puede dividir las capacidades de supe usuario entre varios administradores. La gestión de derechos de procesos se implementa a través de privilegios. La gestión de derechos de usuarios se implementa a través de RBAC.

VmWare vSphere 5.x

A pesar de que las operaciones diarias se realizan mediante vCenter Server, hay instancias para las que necesita trabajar con el anfitrión de vSphere en forma directa, como el respaldo de configuración y el acceso a archivos de registro. Para controlar el acceso al anfitrión, puede configurar los anfitriones de vSphere para que se unan a un dominio de Active Directory y, de este modo, los usuarios que intenten acceder al anfitrión se autenticarán automáticamente mediante el uso del directorio centralizado de usuarios. También puede definir y administrar los usuarios locales anfitrión por anfitrión y configurarlos mediante vSphere Client, vCLI o vSphere PowerCLI. Este segundo método se puede utilizar en lugar de la integración con Active Directory o bien, además de ella.

También puede crear roles locales, similares a los roles de vCenter, que definan qué cosas está autorizado a hacer el usuario en el anfitrión. Por ejemplo, se le puede conceder a un usuario acceso de solo lectura, el cual solo le permita ver información del anfitrión. O bien, se le puede conceder acceso como administrador, el cual le permita ver y modificar la configuración del anfitrión. Si el anfitrión está integrado con Active Directory, también se les pueden otorgar roles locales a los grupos y usuarios de Active Directory.

El único usuario definido de manera predeterminada en el sistema es el usuario raíz. La contraseña raíz inicial normalmente se determina de manera interactiva mediante la interfaz de usuario de la consola directa (DCUI, Direct Console User Interface) o como parte de una instalación automatizada. Puede cambiarse después usando vSphere Client, vCLI o vSphere PowerCLI.

A través de vSphere, se les pueden asignar privilegios administrativos a los usuarios para que reciban acceso total al shell automáticamente. Gracias al acceso total al shell, los usuarios administrativos con privilegios ya no necesitan "cambiar la ubicación del usuario" a "raíz" para ejecutar comandos privilegiados.

Con vSphere, toda la actividad del anfitrión, tanto del shell como de la interfaz de usuario de la consola directa (DCUI, Direct Console User Interface) se registra ahora en la cuenta del usuario que inició sesión. Esto garantiza la responsabilidad del usuario, lo que simplifica el monitoreo y la auditoría de las actividades en el anfitrión.

Microsoft Hyper-V 2012R2

Esto cubre la acción por lo que se puede asignar a alguien el derecho a recuperar los datos, pero a diferencia de RBAC en Exchange, por ejemplo, usted no puede entonces limitar aún más los orígenes de datos que puedan recuperar.

Existen siete roles proporcionadas: Usuario de sólo lectura, operador de Reporting, operador de recuperación, operador de cinta y administradores de cinta y completa Admin de DPM 2012. También hay dos roles de apoyo. Soporte de nivel 1 (help desk) sólo puede reanudar backups y tomar la acción automática recomendada para problemas. El soporte de nivel 2 (escalada) puede ejecutar copias de seguridad a petición y activar o desactivar a agentes.

Todos los roles son compatibles con la consola de Operations Manager y ámbito DPM 2012 consolas de Operations Manager se inician desde. Funciones no se aplican en la consola de DPM 2012 nativa en el servidor DPM 2012, como RBAC está construido sobre el sistema basado en papel de Operations Manager.

El nuevo modelo de seguridad de SCCM 2012 llamado RBAC (Role Based Access Control) es una nueva forma de implementar la seguridad en un entorno de SCCM basado en roles de seguridad y ámbitos de seguridad, dejando atrás el engorroso modelo de clases e instancias de versiones anteriores. La consola de SCCM 2012 tiene multitud de nodos y funciones y mediante la asignación de usuarios o grupos a los roles de seguridad y ámbitos podemos reducir los nodos que pueden ver y a los que pueden acceder haciendo que la administración de SCCM pueda estar muy compartimentada, por ejemplo podemos tener un administrador de aplicaciones, un administrador de Endpoint protección, un equipo de Helpdesk que solo pueda realizar ciertas tareas, etc....

Los tres elementos que intervienen en este modelo de seguridad son:

Rol de seguridad: Existen varios roles predefinidos, estos no se pueden eliminar pero podemos crear roles personalizados a partir de los predefinidos. Define las acciones que un usuario puede realizar en la consola.

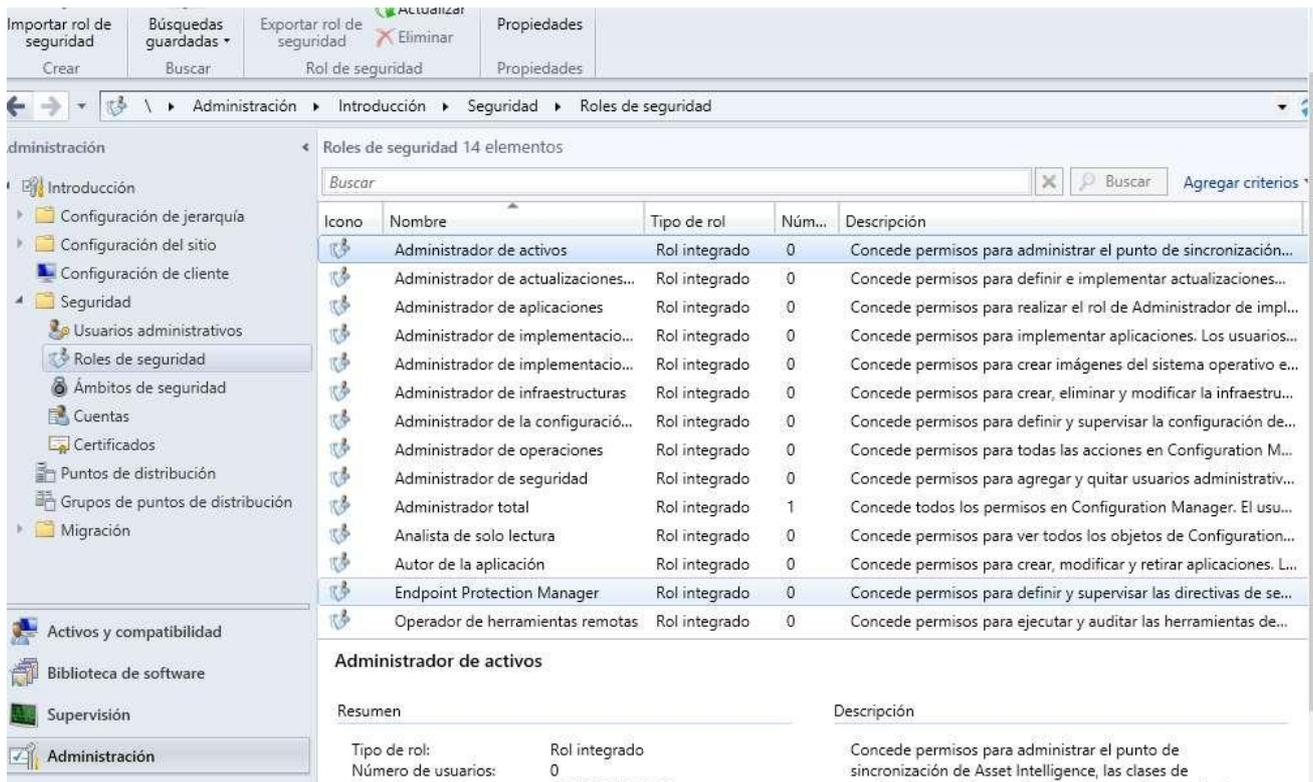


Figura 5.1: Roles de Seguridad

Ámbito: Los objetos de la consola pueden ser configurados para pertenecer a uno o más ámbitos.

Colecciones: desde el punto de vista de la seguridad podemos considerar las colecciones como límites de seguridad, es decir se definen roles y ámbitos a una o unas determinadas colecciones que son sobre las que se puede actuar.

Hay 6 roles predeterminados: Pool Admin, Pool Operator, VM Power Admin, VM Admin, VM Operator and Read Only

Citrix XenServer 6.x:

RBAC (Role Based Access Control) nos permite asignar usuarios, roles y permisos para el control de nuestro entorno XenServer. Esta funcionalidad no es nueva de 6.5.

RBAC depende de Directorio Activo para la autenticación de los usuarios. XenServer extrae la lista basada en el directorio de usuarios de AD, y Grupos a las cuales asignará los permisos necesarios. Por ello, es necesario que el pool sea integrado en el dominio.

El súper usuario root, seguirá estando activo, ya que se trata de un usuario local, con lo que en caso de problemas con nuestro AD, siempre podremos logar sobre la consola o mediante ssh con nuestra cuenta Root.

El principal argumento para poder conectar nuestro pool al dominio e incluir usuarios delegados es la auditoria de tareas que se realizan en nuestro Pool.

Una vez incluido en nuestro Directorio activo, los Administradores (que no tendrán acceso vía root) deberán utilizar su usuario de dominio para logar-se, al cual le dimos permisos específicos. Ello nos permitirá auditar y verificar en caso que sea necesario, todos los cambios realizados en nuestro pool con la información relativa al usuario que lo ejecuto.

5.1.7 Funcionalidad de Gestión multiplataforma de virtualización

Se analiza si las herramientas gestión de cada compañía pueden manejar además de su entorno de virtualización, diferentes entornos de diferentes proveedores.

VmWare vSphere 5.x

Por medio de vCenter Multi-Hypervisor Manager (componente gratuito del vCenter) puede gestionar hasta 50 hosts de Hyper v, el mismo no está disponible para el cliente vSphere web. Con la adición de vCloud Automation Center, VMware también puede gestionar herramientas de múltiples proveedores en la nube como por ejemplo Amazon Web Services entre otros.

Microsoft Hyper-V 2012R2

Por medio de System Center 2012 y SC Orchestrator dispone la posibilidad de gestionar Hosts de Citrix XenServer y VmWare vSphere (pero nunca con todas sus funcionalidades)

Citrix XenServer 6.x: Citrix Xen Server solo gestiona sus propios hosts

5.1.8 Funcionalidad de Gestión por navegador web (sin cliente e independiente)

Se analiza si las herramientas de virtualización de cada compañía pueden ser gestionadas de forma independiente por medio de una plataforma Web.

VmWare vSphere 5.x

Por medio de vSphere Web Client podremos encargarnos de la gestión de nuestros servidores virtuales por medio de la plataforma Web, la última versión incluye una notable mejora en la velocidad del cliente web y agrega capacidades para como por ejemplo los “quick filters” que nos permite crear filtros de manera muy rápida y sencilla en la búsqueda. Se agrega soporte para drag & drop de objetos a nivel del inventario, permitiéndonos así tener una navegación y uso del cliente mucho más amigable de lo que se tenía en versiones anteriores y oficialmente se agrega soporte para Mac OS con capacidades como la consola de HTML para visualizar e interactuar con las VMs, transferencia de OVF's y uso de ISOs locales.

Microsoft Hyper-V 2012R2

System Center está basado en el framework .NET, por lo cual no tiene plataforma de gestión Web. Sin embargo, hay componentes basados en web para algunos de los productos de SC y funciones como Service Manager Self Service Portal (SSP) u Operations Manager Web Console.

Citrix XenServer 6.x

Se retiró el Web Self Service con XenServer 6.2. Para gestión de grandes infraestructuras podemos utilizar Citrix Cloud Platform o se puede utilizar un producto gratuito de xvpsource.org XVP

5.1.9 Funcionalidad de Gestión avanzada de operaciones

Esta funcionalidad se refiere a la gestión de aspectos generales y físicos tales como la gestión del rendimiento, la gestión de la capacidad, alertas y comportamiento de los entornos virtuales.

El rol de la administración de operaciones es garantizar y restaurar los niveles de servicio mientras se optimizan continuamente las operaciones para mejorar la eficiencia y disminuir los costos.

VmWare vSphere 5.x

Posee gestión avanzada de operaciones por medio de vCenter Operations Management Suite Standard.

vCenter Operations Management Suite ofrece un nuevo enfoque basado en tres características que garantizan el éxito:

- **Automatización.** Las técnicas de análisis predictivas de autoaprendizaje facilitan un grado de automatización mucho mayor que las herramientas de administración tradicionales, por lo que la productividad de TI mejora en un 70 %, se reduce el uso de recursos en un 30 %, entre otras ventajas para el negocio, según lo analiza Forrester.
- **Integración.** La serie de productos proporciona un enfoque integrado hacia la administración del rendimiento, la capacidad y la configuración. Unifica disciplinas de administración y a une a los distintos equipos de infraestructura y operaciones.
- **Inclusión.** VCenter Operations Management Suite está desarrollada sobre una plataforma de operaciones abierta y extensible diseñada para entornos dinámicos de nubes híbridas. Ofrece un conjunto completo de capacidades de administración, entre ellas, de rendimiento, capacidad, cambio, configuración y cumplimiento normativo, descubrimiento y monitoreo de aplicaciones. Con vCenter Operations Management Suite, los equipos que trabajan en la infraestructura y en las operaciones obtienen automatización basada en políticas y administración unificada que aseguran la calidad del servicio de la manera más eficiente posible.

Microsoft Hyper-V 2012R2

Posee gestión avanzada de operaciones por medio de System Center Operations Manager.

System Center Operations Manager (SCOM) es un sistema de administración del centro de datos inter plataforma, para sistemas operativos e hipervisores. Utiliza una interfaz simple que muestra información del estado, la salud y el rendimiento del sistema. También proporciona alertas generadas de acuerdo a la identificación de situaciones de disponibilidad, seguridad, configuración o rendimiento. Funciona con Microsoft Windows Server y servidores basados en Unix.

La idea básica es colocar una pieza de software (agente) en el equipo que va a ser monitorizado. El agente vigila varios recursos en un equipo, incluyendo el Registro de Eventos de Windows, para mensajes específicos o “alertas” generadas por las aplicaciones que se ejecutan en el equipo monitorizado. Después de detectar una alerta, el agente la envía al servidor central de SCOM. Esta aplicación mantiene una base de datos que incluye un historial de alertas. El servidor aplica reglas de filtrado a las mismas a medida que llegan; una regla puede ser notificar a un humano, a través de un email o mensaje, generar un ticket de soporte de red, o desencadenar otro flujo de trabajo destinado a corregir la causa de la alerta de la forma apropiada.

SCOM utiliza el término “Management Pack” (Módulo de Gestión) para referir a un conjunto específico de reglas de filtrado para alguna aplicación monitorizada. Mientras que Microsoft y otros proveedores de software ponen a disposición general módulos de administración para sus productos, SCOM también proporciona herramientas para crear paquetes de administración personalizados. Si bien se necesita un rol de administrador para instalar agentes, configurar equipos monitorizados y crear módulos de administración, los permisos para simplemente ver la lista de alertas recientes pueden ser otorgados a cualquier cuenta de usuario válida.

Varios servidores SCOM pueden ser agrupados para monitorizar múltiples redes a la vez, abarcando el dominio lógico de Windows y los límites de la red física. En versiones previas de Operations Manager, se utilizaba un servicio web para conectar varios grupos administrados de forma separada, con una ubicación central. Desde Operations Managers 2007, el servicio web no se utiliza más. Se emplea una conexión directa TCP, utilizando el puerto 5723 para estas comunicaciones.

Citrix XenServer 6.x:

No posee gestión avanzada de operaciones.

5.1.10 Funcionalidad de Actualizaciones del Hypervisor

VmWare vSphere 5.x

VmWare posee actualizaciones del Hypervisor por medio del Update Manager, VSphere Update Manager automatiza la administración de parches y elimina las tareas manuales de seguimiento y aplicación de parches en anfitriones y máquinas virtuales de vSphere. Compara el estado de los anfitriones de vSphere con puntos de referencia y luego lleva a cabo la actualización y aplicación de parches para garantizar el cumplimiento normativo.

Con Update Manager se puede adquirir la visibilidad del estado general de los parches en toda la infraestructura virtual por medio de un tablero de cumplimiento normativo de parches y a la vez se puede implementar paquetes de parches sin conexión que se descarguen directamente de los sitios web de los proveedores.

VSphere 5 introdujo la posibilidad de tener actualizaciones simultáneas en varios hosts y también facilita la actualización de ESX a ESXi.

Microsoft Hyper-V 2012R2

Posee actualizaciones del Hypervisor por medio del Virtual Machine Manager (VMM). Virtual Machine Manager es una solución de administración para el centro de datos virtualizado, que permite configurar y administrar los hosts de virtualización, las redes y los recursos de almacenamiento, a fin de crear e implementar máquinas virtuales y servicios para nubes privadas que haya creado.

Citrix XenServer 6.x:

La consola de administración XenCenter nos permite ver, a través de la opción de menú Tools → Check for Updates, si existen actualizaciones pendientes de aplicar y sobre qué servidores.

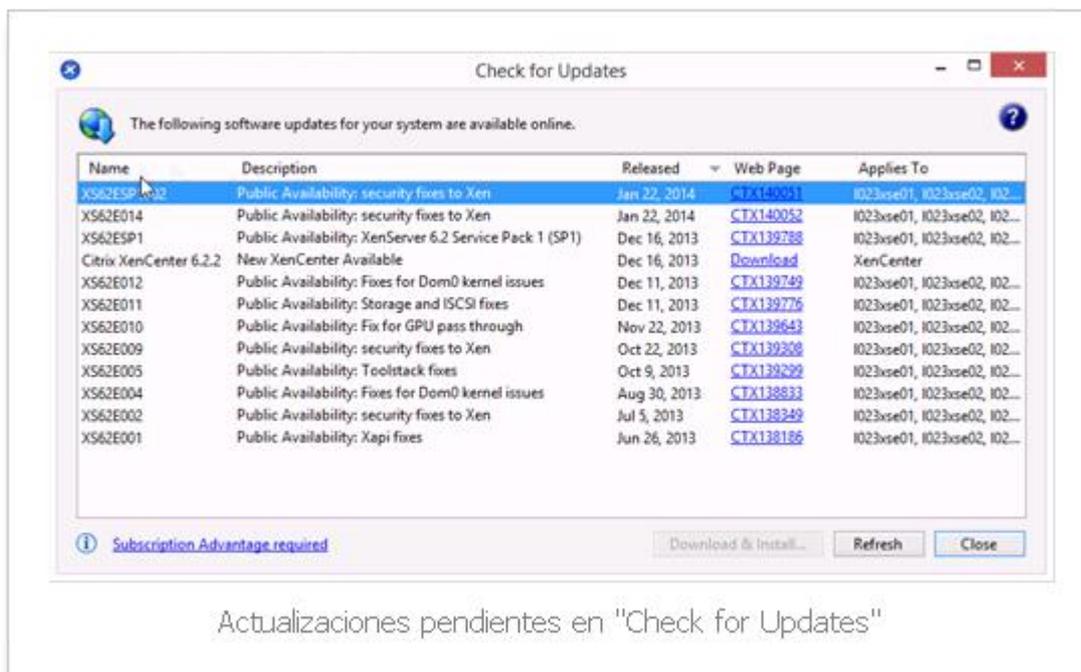


Figura 5.2: Chequeo de Actualizaciones Pendientes

A través de los enlaces disponibles en cada una de las actualizaciones listadas en “Check for Updates” se accede a la página web de Citrix en la que se debe informa de los problemas que resuelve o las características que mejora cada actualización, el enlace de descarga, los requisitos para poder aplicarla, acciones a realizar antes y después de aplicar la actualización, etc.

5.1.11 Funcionalidad de Actualizaciones de Máquinas virtuales

VmWare vSphere 5.x

Por medio del Update Manager podemos actualizar las máquinas virtuales en lo que respecta a Vmware tools, hardware virtual y a nivel aplicativo, dejando fuera la instalación de parches de algunos sistemas operativos

Microsoft Hyper-V 2012R2

Por medio del Virtual Machine Servicing Tool 2012 (VMST) es posible la actualización de máquinas virtuales.

Virtual machine servicing tool trabaja con System Center 2012, Virtual Machine Manager System Center 2012, Configuration Manager y Windows Server Update Services 3.0. Por lo cual se encarga de gestionar todos los parches de la VM en todos los ámbitos, desde Sistema operativo con el WSUS hasta su hardware virtual con el System Center.

Citrix XenServer 6.x:

Citrix XenServer 6.X no cubre la actualización de las máquinas virtuales dentro de sus funcionalidades

5.1.12 Funcionalidad de Snapshot en Vivo

Es la capacidad de poder sacar snapshot (instantáneas) con la máquina virtual prendida y el Sistema Operativo en funcionamiento.

VmWare vSphere 5.x

VmWare vSphere 5.x posee snapshot en vivo, incluyendo el snapshot de la memoria de la máquina virtual en el momento de ejecución.

Microsoft Hyper-V 2012R2

Hyper-V 2012 R2 posee Checkpoints (snapshot) en vivo, la cual incluye la vRAM de la máquina virtual en el momento de la ejecución.

Citrix XenServer 6.x:

XenServer posee snapshot en vivo

5.1.13 Funcionalidad de Backups Integrado

VmWare vSphere 5.x

Posee backup integrado por medio de vSphere Data Protection.

VSphere Data Protection es una solución de respaldo y recuperación diseñada para los entornos de vSphere. Con tecnología EMC Avamar, proporciona respaldos a nivel de imágenes y sin agentes de las máquinas virtuales en los discos. También brinda protección que reconoce aplicaciones para las aplicaciones de Microsoft fundamentales para el negocio (Exchange, SQL Server, SharePoint) y replicación de datos con capacidad de cifrado y uso eficiente de la red de área extendida (WAN, Wide Área Network). VSphere Data Protection se encuentra totalmente integrado con vCenter Server y vSphere Web Client.

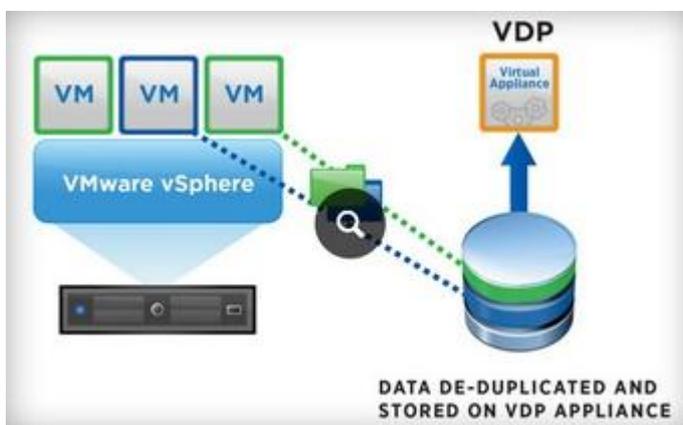


Figura 5.3: Funcionamiento de Vsphere Data Protection

VSphere Data Protection puede implementarse a datastores de Virtual SAN, sistemas de archivos de red (NFS, Network File System) y sistemas de almacenamiento de archivo de las máquinas virtuales (VMFS, Virtual Machine File System). La administración de vSphere Data Protection se realiza mediante vSphere Web Client. VSphere Data Protection se implementa como un virtual appliance con cuatro procesadores de CPU virtuales (vCPU, Virtual CPU) y, al menos, 4 GB de memoria, según la capacidad de datos de respaldo del dispositivo. Hay varias configuraciones de capacidad de datos de respaldo disponibles, desde 0,5 TB hasta 8 TB, por cada dispositivo de vSphere Data Protection. Los requisitos de capacidad dependen de la cantidad de máquinas virtuales protegidas, las cantidades de datos, los períodos de retención de datos de respaldo y los índices de modificación de datos, los cuales pueden variar considerablemente.

Respaldo a nivel de imagen

VSphere Data Protection (VDP) crea respaldos a nivel de imagen (de toda la máquina virtual). El dispositivo de VDP se comunica con la instancia de vCenter Server para tomar una snapshot de los archivos .vmdk de una máquina virtual. La deduplicación se produce dentro del dispositivo de VDP. Cada dispositivo de VDP puede respaldar, simultáneamente, hasta 8 máquinas virtuales si se utiliza el proxy interno, o hasta 24 máquinas virtuales si se implementan proxies externos.

Para crear y editar las tareas de respaldo, se utiliza la pestaña Backup de la interfaz de vSphere Data Protection de vSphere Web Client. Se pueden seleccionar máquinas virtuales y contenedores individuales, como centros de datos, clústeres y depósitos de recursos, para respaldar. En el caso de los contenedores, se realiza un respaldo de todas las máquinas virtuales que se encuentran dentro en el momento en que se ejecutan las tareas de respaldo. Las máquinas virtuales que se agreguen al contenedor después se incluirán en la siguiente ejecución de las tareas de respaldo. Asimismo, las que se quiten del contenedor ya no se incluyen en las tareas de respaldo. Las tareas de respaldo se pueden programar para que se ejecuten por día, semana o mes. También es posible ejecutar manualmente una tarea de respaldo.

Restauración del seguimiento de bloques cambiados (CBT, Changed Block Tracking)

VSphere Data Protection utiliza la CBT en los respaldos a nivel de imagen. El seguimiento de bloques cambiados también se utiliza, en algunos casos, con las restauraciones a nivel de imágenes para mejorar la velocidad y la eficacia. VSphere Data Protection evalúa automáticamente la carga de trabajo entre ambos métodos de restauración (restauración de todos los bloques, o cálculo y restauración de los bloques modificados únicamente) y utiliza el método más eficiente.

Como parte del proceso de restauración, las máquinas virtuales se pueden restaurar y poner en una ubicación diferente, o se las puede renombrar. (Se debe tener en cuenta que el seguimiento de bloques cambiados no se utiliza cuando se restaura una máquina virtual a una ubicación alternativa).

Respaldo y restauración a nivel del invitado que reconocen aplicaciones

VSphere Data Protection es compatible con respaldos a nivel de invitado que reconocen aplicaciones para Microsoft SQL Server, Exchange y SharePoint. Se instalan agentes que permiten los respaldos y las restauraciones de las bases de datos de las aplicaciones. En el caso de Microsoft Exchange, también se pueden restaurar buzones de correo individuales.

Replicación de datos de respaldo

La replicación de datos de respaldo proporciona un nivel adicional de protección contra la pérdida de datos y permite la recuperación ante desastres si se pierde el dispositivo de origen de VDP. Las tareas de replicación determinan qué respaldos se replican, y cuándo y dónde se replican estos respaldos. Los respaldos que se crean con un dispositivo de vSphere Data Protection pueden replicarse a otro dispositivo de vSphere Data Protection y a EMC Avamar. También se admite la replicación de los datos de respaldo almacenados en el sistema Data Domain. Solo se replican los

segmentos de datos de respaldo únicos para reducir la utilización del ancho de banda de la red, y el flujo de replicación se cifra por razones de seguridad.

Integración con sistemas Data Domain

vSphere Data Protection puede configurarse para usar sistemas Data Domain como objetivo de respaldo. Esto resulta útil porque los sistemas Data Domain pueden proporcionar escalabilidad adicional, deduplicación global y mayor eficacia de respaldo a través de Data Domain Boost (vSphere Data Protection incluye bibliotecas de Data Domain Boost). La replicación de datos de respaldo puede configurarse entre dos dispositivos de vSphere Data Protection con diferentes objetivos de Data Domain. La replicación se configura y los metadatos de respaldo se mantienen en el dispositivo de vSphere Data Protection, mientras que la replicación de los datos de respaldo se produce directamente entre los dispositivos de Data Domain. Solo se replican los segmentos de datos únicos, lo cual reduce la utilización de la red.

Microsoft Hyper-V 2012R2

Hyper-V posee varias herramientas de backup integradas.

La opción gratuita: Windows Server Backup

Copias de seguridad de Windows Server es una característica que proporciona un conjunto de asistentes y otras herramientas para poder realizar tareas básicas de copia de seguridad y recuperación en el servidor donde esté instalada. La misma incluye Copia de seguridad y restauración de máquinas virtuales individuales desde un servidor host de Hyper-V.

Data Protection Manager (DPM) como parte de System Center 2012 SP1

System Center 2012 –Data Protection Manager (DPM) permite la protección y recuperación de datos basadas en disco y basadas en cinta para servidores tales como SQL Server, Exchange Server, SharePoint, servidores virtuales, servidores de archivos, además de ofrecer compatibilidad con equipos portátiles y de escritorio con Windows. DPM también puede administrar el estado del sistema y la reconstrucción completa (BMR) de manera centralizada.

SCDPM se basa en un software centralizado instalado en un servidor, el cual se comunica a través de agentes (los agentes de SCDPM) para ejecutar las tareas de resguardo y recuperación. System Center Data Protection Manager utiliza el motor de base de datos SQL Server para alojar información de contexto y configuración. Permite resguardar datos de equipos que están en el mismo entorno de Active Directory Domain Services u otros bosques, siempre y cuando existan relaciones de confianza entre ellos que permitan la interacción de datos.

Durante la primera ejecución de backup, SCDPM transfiere el 100% de los datos hacia el servidor de resguardo. Para las próximas ejecuciones de una tarea de backup el software realiza un proceso de sincronización a través del cual analiza los cambios en contraste con el último backup y transfiere sólo de los cambios realizados en los equipos protegidos, incluyéndolos en el backup que se está generando a un nivel de byte con la posibilidad de mantener un histórico configurado en cada grupo de protección y tenerlo disponible para eventuales restauraciones y consultas. La sincronización de DPM es asíncrona, por lo cual no produce el bloqueo de operaciones de entrada y salida de disco (disk I/O) en los objetos protegidos.

System Center Data Protection Manager (SCDPM) utiliza la tecnología VSS de Windows Server (Volume Shadow Copy Service). Antes de VSS, no había una manera estándar para producir instantáneas de volúmenes que no contengan archivos corruptos dado que las escrituras en los archivos en uso estaban incompletas.

Windows Azure Backup Service

La Copia de seguridad de Azure es un servicio de Azure varios inquilinos que le permite realizar la copia de seguridad de los datos locales en Azure. Reemplaza su solución de copia de seguridad local o remota existente por una oferta confiable, segura y rentable basada en la nube. La Copia de seguridad de Azure se basa en una infraestructura de clase mundial escalable, duradera y de alta disponibilidad. Con esta solución, puede hacer una copia de seguridad de datos y aplicaciones desde sus servidores de System Center Data Protection Manager (SCDPM), los servidores de Windows o las máquinas cliente de Windows. La Copia de seguridad de Azure y SCDPM son las tecnologías fundamentales que constituyen la solución de copia de seguridad integrada en la nube de Microsoft.

Citrix XenServer 6.x

No posee backup integrado. Citrix retiró la protección de máquinas virtuales y Recuperación (VMPR) en XenServer 6.2. VMPR fue el método de copia de seguridad de instantáneas como dispositivos virtuales.

5.1.14 Funcionalidad de Pool de recursos

Nuestra infraestructura virtualizada se basa en hosts que tienen una capacidad determinada que podemos clasificar en CPU y RAM. Cada host dispone de una cantidad de recursos de este tipo limitados. El pool de recursos nos permite particionar y priorizar los recursos físicos de los hosts, como por ejemplo memoria RAM o CPU

VmWare vSphere 5.x

VmWare vSphere 5.x maneja los pool de recursos como formas de abstraer los recursos físicos disponibles en un clúster mediante las cuales podemos administrar:

- Límites de recursos para las máquinas virtuales pertenecientes a este resource pool.
- Reservas de recursos para las máquinas virtuales pertenecientes a este resource pool.
- Prioridades en la asignación de recursos a las máquinas virtuales en situaciones de contención de memoria o CPU.

Todo clúster dispone del denominado root resource pool, que contiene la totalidad de recursos que ese clúster puede aportar. A partir de este root resource pool, podemos crear otros niveles de resource pools, denominados child resource pools. Los resource pools que están al mismo nivel se denominan sibling resource pools.

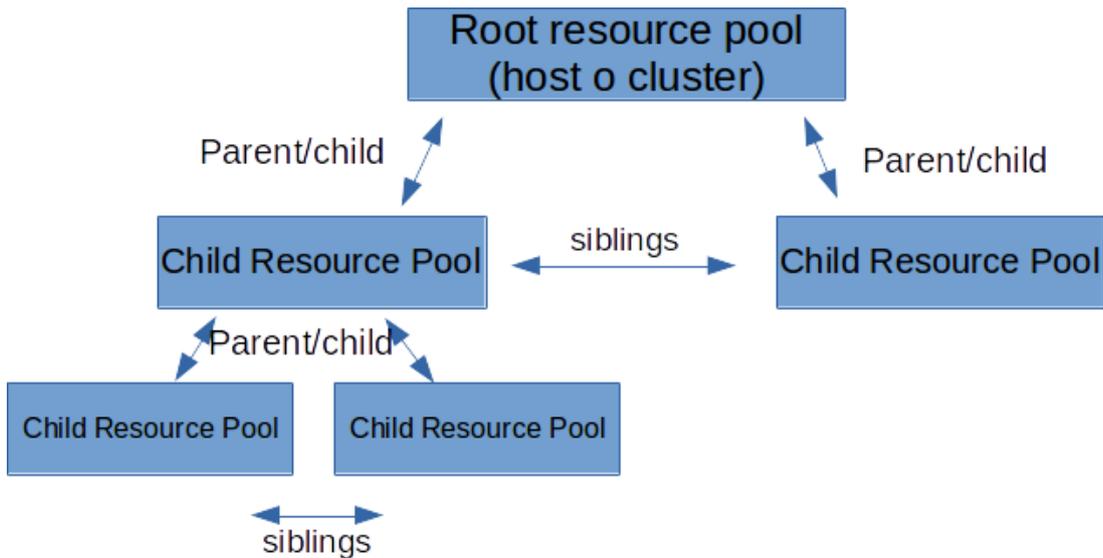


Figura 5.4: Manejo y Herencia del pool de recursos

Microsoft Hyper-V 2012R2

Hyper-V Server 2012 R2 nos aparece una nueva característica con vista a la agrupación de recursos para asignarlos y medirlos más fácilmente, los Grupos de recursos llamado Host Groups. El host Group agrupa determinados recursos físicos, en algo que denominaremos “Pool”, para ponerlos a disposición de las máquinas virtuales (VM), que serán nuestros clientes. Los tipos de recursos que ponemos a disposición en un Pool son los siguientes:

- Memoria.
- Procesador
- Ethernet
- VHD
- ISOs
- Virtual Floppy Disks (VFD).
- Fibre Channel Ports
- Fibre Channel connections

Esta opción no está disponible en el Administrador de Hyper-V, se deben de crear por PowerShell.

Citrix XenServer 6.x

XenServer no maneja pool de recursos

5.1.15 Funcionalidades de Seguridad

VmWare vSphere 5.x

VmWare vSphere utiliza la virtualización de nivel básico de hardware para que el hipervisor interactúe directamente con el hardware del host o equipamiento físico (servidor) sin la necesidad de un sistema operativo anfitrión. Este enfoque protege vSphere de las vulnerabilidades relacionadas con el sistema operativo, lo que disminuye notablemente las deficiencias de seguridad.

Las funcionalidades más notables con respecto a seguridad son:

- **Hypervisor de superficie reducida:** simplifica la implementación, el mantenimiento y la aplicación de parches, y reduce la vulnerabilidad ya que presenta una superficie de ataque mucho más pequeña.
- **Niveles de aceptación de software:** previenen la instalación de software no autorizado.
- **API robustas:** permiten el monitoreo sin agentes y, así, eliminan la necesidad de instalar software de terceros.
- **Firewall anfitrión (Host firewall):** protege la interfaz de administración del anfitrión de vSphere con un firewall sin estado que se puede configurar.
- **Registro y auditoría:** registran todas las actividades del anfitrión en la cuenta del usuario registrado, lo que simplifica el monitoreo y la auditoría de actividades en el anfitrión.
- **Sistema de registro seguro (Secure syslog):** mensajes de registro en servidores de registros locales o remotos, con registro remoto por conexiones SSL o TCP.
- **Integración con Active Directory:** configure el anfitrión de vSphere para que se una a un dominio de Active Directory. Las personas que solicitan acceso al anfitrión se autentican automáticamente mediante el uso del directorio centralizado de usuarios.

Otras Funciones de Seguridad.

VShield Endpoint

VMware vShield Endpoint mejora la protección de terminales por orden de magnitud descargando el procesamiento de agentes anti amenazas dentro de las máquinas virtuales invitadas a un virtual appliance dedicado y seguro suministrado por socios de VMware. VShield Endpoint mejora los índices de consolidación y el rendimiento, optimiza la implementación y monitoreo de antivirus, y garantiza el cumplimiento normativo mediante el registro de las actividades de las aplicaciones antivirus y antimalware.

También permite administrar las políticas de antivirus y antimalware para entornos virtualizados con las mismas interfaces de administración que utiliza para proteger su infraestructura física. VShield Endpoint refuerza la seguridad de la virtualización con una protección mejorada de los terminales mediante la descarga de los procesos de AV a un virtual appliance seguro suministrado por los socios de VMware. vShield Endpoint:

- Mejora los índices de consolidación y el rendimiento mediante la eliminación de sobrecargas de actividad del antivirus.
- Automatiza la implementación, y el monitoreo del antivirus y el antimalware.
- Satisface los requisitos de cumplimiento normativo y de auditoría con registros de la actividad del antivirus y el antimalware.

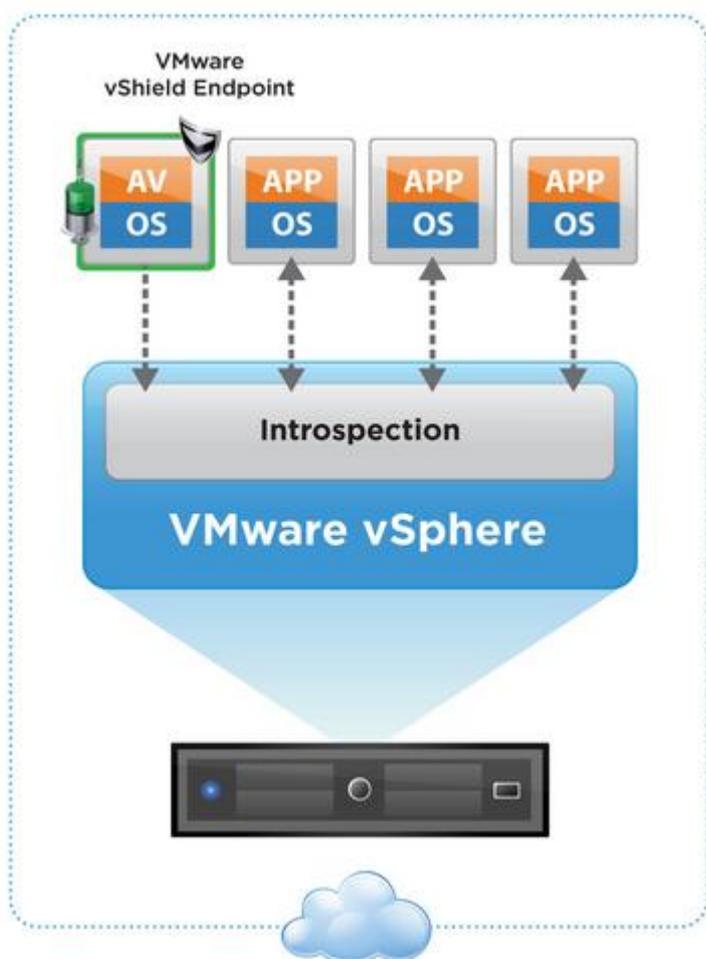


Figura 5.5: Funcionamiento de VMware vShield Point

Microsoft Hyper-V 2012R2

Windows Hyper-V hereda y adiciona varias funcionalidades de Windows con respecto a seguridad. Las más destacadas son:

Control de acceso: El control de acceso ayuda a proteger archivos, aplicaciones y otros recursos contra el uso no autorizado.

AppLocker: Windows AppLocker ofrece administración de control de acceso basada en directivas para las aplicaciones.

BitLocker: El cifrado de unidad BitLocker permite cifrar todos los datos almacenados en el volumen del sistema operativo y los volúmenes de datos configurados para equipos que ejecutan versiones compatibles de Windows. Mediante el uso de un Módulo de plataforma segura (TPM), también puede ayudar a asegurar la integridad de los componentes de inicio temprano.

Caja de seguridad de credenciales: La Caja de seguridad de credenciales se administra mediante el Panel de control del Administrador de credenciales

Unidad de disco duro cifrada: La característica de unidad de disco duro cifrada de BitLocker se proporciona para mejorar la administración y la seguridad de los datos.

Cuentas de servicio administradas de grupo: La cuenta de servicio administrada por grupo ofrece la misma funcionalidad que la cuenta de servicio administrada independiente dentro del dominio, pero también amplía esa funcionalidad por medio de varios servidores.

Kerberos: Kerberos es un mecanismo de autenticación que comprueba la identidad de un usuario o host.

NTLM: Los protocolos de autenticación NTLM autentican a usuarios y equipos en función de un mecanismo de desafío y respuesta que le demuestra a un servidor o a un controlador de dominio que un usuario conoce la contraseña asociada con una cuenta.

Contraseñas: El método más común para autenticar la identidad del usuario es usar una contraseña o frase de contraseña secreta, como parte del proceso de inicio de sesión.

Auditoría de seguridad: La auditoría de seguridad es una de las herramientas más potentes para mantener la seguridad del sistema. La auditoría de seguridad identifica ataques, hayan tenido éxito o no, que supongan una amenaza a su red, o ataques contra recursos que se han determinado como de valor en su evaluación de riesgos.

Asistente para configuración de seguridad: El Asistente para configuración de seguridad es una herramienta de reducción de superficie expuesta a ataques que guía a los administradores en la creación de directivas de seguridad basadas en la funcionalidad mínima requerida por los roles de un servidor.

Configuración de la directiva de seguridad: La configuración de directiva de seguridad consta de reglas configurables que sigue el sistema operativo cuando determina los permisos que ha de conceder en respuesta a una solicitud de acceso a los recursos.

Tarjetas inteligentes: Las tarjetas inteligentes ofrecen una solución de seguridad portátil y difícil de manipular para tareas. Como la autenticación de clientes, el inicio de sesión en dominios, la firma de código y el correo electrónico seguro.

Directivas de restricción de software: Las directivas de restricción de software (SRP) son una característica basada en directivas de grupo que identifica los programas de software que se ejecutan en los equipos de un dominio y controla la capacidad de ejecución de dichos programas.

TLS/SSL (Schannel SSP): Schannel es un proveedor de compatibilidad para seguridad (SSP) que implementa los protocolos de autenticación estándar de Internet de la Capa de sockets seguros (SSL) y la Seguridad de la capa de transporte (TLS).

Módulo de plataforma segura (TPM): La tecnología del Módulo de plataforma segura (TPM) está diseñado para ofrecer funciones relacionadas con la seguridad y el hardware.

Control de cuentas de usuario (UAC): UAC ayuda a atenuar los efectos de un programa malintencionado.

Inicio de sesión y autenticación de Windows: Esta colección incluye: Marco biométrico de Windows, Autenticación Kerberos, NTLM, Contraseñas y TLS/SSL (Schannel SSP)

Marco biométrico de Windows: El Marco biométrico de Windows (WBF) es un conjunto de servicios e interfaces que permiten un desarrollo y una administración uniformes de dispositivos biométricos, como lectores de huellas digitales. El WBF mejora la confiabilidad y la compatibilidad con servicios y controladores biométricos.

Con respecto a la protección de las máquinas virtuales que se ejecutan en el servidor de virtualización no se requieren componentes especiales ni diferentes para proteger la máquina virtual. Por ejemplo, si sus directivas y procedimientos requieren un software antivirus, ejecute un software antivirus en la máquina virtual. Si posee algún requisito de directiva para segmentar el servidor físico en una red en particular, siga la misma directiva para la máquina virtual.

Citrix XenServer 6.x:

Xen Server utiliza netfilter e iptables como firewall por lo cual no hay marcos específicos o APIs para antivirus integración con el firewall.

Un buen complemento de seguridad para Citrix XenServer es el Netscaler que puede ser utilizado como firewall, balanceador de carga y acelerador de aplicaciones entre otras cosas.

Entre sus funcionalidades más destacadas se encuentran el Netscaler Gateway que se encarga de asegurar el acceso de datos y los aplicativos de Citrix XenApp y XenDesktop y NetScaler App Firewall que asegura las aplicaciones Web, previene la divulgación de la información confidencial y ayuda en el cumplimiento de las regulaciones de seguridad de la información, tales como PCI-DSS. Cabe destacar que el complemento Netscaler es pago y adicional al Citrix XenServer.

5.1.16 Funcionalidades de Alta disponibilidad

VmWare vSphere 5.x:

VMware HA permite que múltiples hosts ESXi puedan ser configurados como un cluster para proveer de alta disponibilidad y una rápida recuperación ante fallos, para todas las máquinas virtuales en dichos hosts.

HA protege la disponibilidad de las siguientes formas:

- Protege contra fallas de servidores, reiniciando las máquinas virtuales en otros hosts dentro del clúster.
- Protege contra fallas de aplicaciones monitoreando continuamente una máquina virtual, y reseteándola en caso de detectar una falla.

HA provee de alta disponibilidad a las máquinas virtuales formando clusters donde residen los hosts y dichas MV. Los hosts en un clúster son monitoreados, y ante la falla de un host, las MV que residen en dicho host son reiniciadas en otros hosts que se encuentren disponibles en el clúster.

En vSphere 5, cuando se crea un clúster HA, uno de los hosts es designado como "Master host" o host maestro, para comunicarse con vCenter Server y monitorear el estado de los otros hosts y sus MV. Este host maestro debe ser capaz de detectar y tratar apropiadamente con los diferentes tipos de fallas que pueden afectar a un host. Se debe distinguir, por ejemplo, entre un host con fallas, de uno que ha llegado a estar aislado en la red.

El tamaño máximo de nodos que admiten los clúster en VmWare es de 32 nodos con un máximo de 4000 máquinas virtuales por clúster. Posee la funcionalidad de monitoreo y reseteo automático de máquina virtual

Microsoft Hyper-V 2012R2:

Hyper-V provee la Alta disponibilidad a través de las siguientes Herramientas:

Replicación: Aporta redundancia de máquinas virtuales, la misma se logra activando la replicación entre dos hosts Hyper-v y activando la replicación en las máquinas virtuales. Cada host posee entonces una copia de la máquina virtual; por lo cual si uno de los dos host se detuviera, el otro se haría cargo arrancando la máquina virtual.

Clúster de conmutación por error (host clustering): Es cuando ocurre un error en el host y la máquina virtual la cual estaba en el host se arranca automáticamente en un segundo host del clúster y las aplicaciones y servicios siguen estando, así disponibles para los usuarios.

Migración de las máquinas virtuales: Puede ser manual o automático durante la pérdida del host en ejecución. La migración consiste en desplazar la ejecución de una máquina virtual de un host a un host b. Existen 2 tipos de migración, la migración rápida y la migración en caliente.

Protocolo del bloque de mensajes del servidor (SMB): El protocolo del Bloque de mensajes del servidor (SMB) es un protocolo de uso compartido de archivos de red que permite que las aplicaciones de un equipo puedan leer y escribir archivos y solicitar servicios desde los programas de un servidor en una red de equipos. El protocolo SMB puede usarse sobre el protocolo TCP/IP u otros protocolos de red. Con el uso de un protocolo SMB, una aplicación (o el usuario de una aplicación) puede acceder a los archivos u otros recursos de un servidor remoto. Esto permite que las aplicaciones puedan leer, crear y actualizar archivos en un servidor remoto. También puede comunicarse con cualquier programa del servidor que esté configurado para recibir la solicitud de un cliente SMB. Windows Server 2012 presenta la nueva versión 3.0 del protocolo SMB.

En Windows Server 2012, podemos utilizar archivos compartidos SMB 3.0 como almacenamiento compartido para Hyper-V. Con esta nueva capacidad, Hyper-V puede almacenar archivos de máquinas virtuales, lo que incluye los archivos de configuración de disco duro virtual (VHD) e instantáneas, en archivos compartidos SMB.

El tamaño máximo de nodos que admiten los clúster en Hyper-V es de 64 nodos con un máximo de 8000 máquinas virtuales por clúster. Posee la funcionalidad de monitoreo y reseteo automático de máquina virtual

Citrix XenServer 6.x:

La función de High Availability (Alta disponibilidad) en XenServer es asegurar que las máquinas virtuales más importantes de un resource pool estén siempre disponibles. Por lo cual el resource pool debe proveer los suficientes recursos hardware.

High Availability (HA) puede reiniciar las máquinas virtuales de un host caído o que ha perdido la conectividad en otro host miembro del pool protegido, si existen recursos suficientes para mantener un nivel óptimo de rendimiento de todas las máquinas virtuales y si la configuración de High Availability (HA) lo permite. Además, HA previene que una máquina pueda estar en ejecución en dos hosts distintos, lo que podría provocar una corrupción de los discos virtuales VDI asociados a ella. Por ello, si lo que ocurre es un corte en la red del host que ejecuta las máquinas virtuales,

este mismo realizará un reinicio para apagar las que puedan estar en ejecución. Posteriormente, XenServer iniciará dichas máquinas en otro host del pool.

Otro punto muy importante es que HA promueve automáticamente a master del resource pool a otro host si el master original cae. De esta manera se asegura una conexión administrativa con el resource pool y la continuidad en su funcionamiento.

Citrix recomienda el uso de High Availability junto con almacenamiento en multipath (no tratado en esta versión del manual) y bonds de los interfaces de red.

El tamaño máximo de nodos que admiten los clúster en Citrix es de 16 hosts con un máximo de 4096 máquinas virtuales por pool de recursos. No posee la funcionalidad de monitoreo y reseteo automático de máquina virtual

5.1.17 Funcionalidades de Migración de máquinas virtuales en vivo:

VmWare vSphere 5.x:

Vmotion es la funcionalidad que tiene Vmware para la migración de máquinas virtuales en caliente, sin que pierda disponibilidad la misma. vMotion soporta 4 vMotion concurrentes sobre redes 1Gbit (esto significa 4 migraciones al mismo tiempo siempre teniendo en cuenta la capacidad de la red). A partir de vSphere 5.1 se permitió a los usuarios combinar vMotion y Storage vMotion en una sola operación. En entornos más pequeños, la capacidad de migrar al mismo tiempo tanto la memoria y el almacenamiento permite migrar a las máquinas virtuales que no han compartido el almacenamiento (storage). En entornos más grandes, esta capacidad permite migrar las máquinas virtuales entre clusters que no cuentan con un conjunto común de almacenes de datos.

Con la llegada de vSphere 5.1 también se mejoró el rendimiento de vMotion a través de la capacidad de equilibrar la carga VMotion sobre varios adaptadores. vSphere 5 también introduce una nueva característica llamada metro vMotion que ofrece un mejor rendimiento a través de redes de latencia largos y también aumenta el límite de latencia de ida y vuelta para las redes vMotion de 5 milisegundos a 10 milisegundos, permitiendo hasta 8 vMotion concurrentes.

Microsoft Hyper-V 2012R2

Microsoft Hyper V también realiza las migraciones de máquinas virtuales en caliente y por medio de esta funcionalidad también nos permite migrar de storage.

Microsoft Hyper V 2012R2 hizo las siguientes mejoras para migraciones de máquinas virtuales en vivo:

La primera fue Mejora del rendimiento (además de la opción TCP / IP) por medio de:

- Compresión: Esta es ahora la configuración predeterminada en Server 2012 R2 (el contenido de la máquina virtual que se está migrando es comprimido y luego copia en el servidor de destino a través de TCP / IP)

- La migración en vivo a través de SMB 3.0 (el contenido de la memoria de la máquina virtual se copia en el servidor de destino a través de una conexión SMB 3.0): SMB directo se utiliza cuando los adaptadores de red en los servidores de origen y de destino tienen acceso directo a memoria (RDMA); SMB Multicanal detecta automáticamente y utiliza varias conexiones cuando se identifica una configuración SMB multicanal adecuada.

La segunda mejora fue migraciones entre distintas versiones

La Tercera mejora fue migraciones concurrentes: migraciones simultáneas ilimitadas utilizando el ancho de banda de hasta 10 Gb. (Las que se pasan del límite se ponen en cola).

Hyper-V También permite la migración de storage en caliente pudiendo migrar la máquina virtual de un storage a otro sin perder disponibilidad.

Citrix XenServer 6.x:

Citrix por medio de XenMotion permite la migración en vivo de máquinas virtuales en hosts XenServer y sin tiempo de inactividad percibido. XenServer sólo admite una migración a la vez (es decir, la ejecución secuencial si se inician de forma múltiple)

También posee la funcionalidad de Storage Xen Motion de poder migrar máquinas virtuales de distintos storage en caliente.

5.1.18 Funcionalidades de Migración automática de máquinas virtuales y gestión de energía

VmWare vSphere 5.x:

Cuando hablamos de Vmotion y Storage Vmotion comentamos que era una forma manual de realizar balanceo de máquinas virtuales entre los hosts ESXi. Distributed Resource Schedule (DRS) fue creado sobre la idea de realizar el balanceo de carga de forma automática.

DRS funciona sobre clústeres de recursos previamente creados y tiene las siguientes 2 características principales:

- 1) Decidir en cual nodo del clúster va a correr la máquina virtual cuando esta prendida (colocación inteligente)
- 2) Evaluar la carga del clúster en tiempo real y dar de recomendaciones para que host migrarlo o migrarlo automáticamente con vMotion

Por defecto DRS chequea cada 5 minutos la carga del clúster para revisar si esta balanceada; también es accionada cuando se saca algún host del clúster o se realizan cambios de los recursos de alguna máquina virtual.

DRS habilita el uso del pool de recursos en clusters de host ESXi, si los host son parte de un clúster que tienen habilitado la alta disponibilidad (HA), también tienen que tener DRS habilitado para permitir crear el pool de recursos.

DRS permite configurar la agresividad del balanceo de carga con el cual VmWare va a mover sus máquinas virtuales.

Distribute Power Management (DPM) permite al clúster DRS reducir el consumo eléctrico permitiendo apagar y prender host dependiendo del consumo de los recursos del clúster. vSphere DPM supervisa la demanda acumulada de todas las máquinas virtuales en el clúster (memoria y CPU) y compara esta información con la capacidad total de los recursos disponibles de todos los hosts del clúster. Si suficientes hosts se encuentra el exceso de capacidad, DPM coloca uno o más hosts en modo de espera y luego los apaga migrando sus máquinas virtuales a otros hosts. A la inversa, cuando se considera la capacidad insuficiente, DRS trae anfitriones de modo de espera (los enciende) y utiliza vMotion para migrar máquinas virtuales a estos hosts

Microsoft Hyper-V 2012R2:

Virtual Machine Manager (VMM) puede realizar el balanceo de carga dentro de los clústeres del host que admitan la migración en vivo. La Optimización dinámica (Dynamic Optimization) migra máquinas virtuales dentro de un clúster según la configuración que se especifica. También puede ayudar a ahorrar energía en un entorno virtualizado desactivando hosts cuando no se necesitan y volviéndolos a activar cuando se necesitan, a esto lo llamamos Optimización de Energía (Power Optimization).

Para la Optimización dinámica, Virtual Machine Manager (VMM) migra máquinas virtuales dentro del clúster del host para mejorar el balanceo de carga entre hosts y para corregir cualquier infracción de la restricción de selección de ubicación para máquinas virtuales.

La Optimización dinámica puede configurarse en un grupo host, para migrar máquinas virtuales dentro de los clústeres de hosts con una frecuencia y una agresividad especificadas. La agresividad determina la cantidad de desequilibrio de carga que se requiere para iniciar una migración durante la Optimización dinámica. De forma predeterminada, las máquinas virtuales se migran cada 10 minutos con agresividad media. Cuando se configure la frecuencia y la agresividad para la Optimización dinámica, un administrador debe tener en cuenta el coste de recursos para migraciones adicionales en comparación con las ventajas de equilibrar la carga de hosts en un clúster de hosts. De forma predeterminada, un grupo host hereda la configuración de Optimización dinámica para su grupo host primario.

La Optimización dinámica puede configurarse para clústeres con dos o más nodos. Si un grupo host contiene hosts independientes o clústeres de hosts que no admiten la migración en vivo, no se realiza la Optimización dinámica de esos hosts. Todos los hosts que están en modo de mantenimiento también se excluyen de la Optimización dinámica. Adicionalmente Virtual Machine Manager (VMM) solo migra máquinas virtuales de alta disponibilidad que usan almacenamiento compartido. Si un clúster de hosts contiene máquinas virtuales que no son de alta disponibilidad, esas máquinas virtuales no se migran durante la Optimización dinámica.

La Optimización dinámica bajo demanda también está disponible para clústeres de hosts individuales mediante el uso de la acción Optimizar hosts en el área de trabajo VM y servicios. La Optimización dinámica bajo demanda puede realizarse sin configurar la Optimización dinámica en grupos host. Tras solicitar la Optimización dinámica para un clúster de hosts, VMM enumera las máquinas virtuales que se migrarán para la aprobación por parte del administrador.

Para la Optimización de energía, los equipos deben tener un controlador de administración de placa base (BMC) que permita la administración fuera de banda.

La Optimización de energía es una característica opcional de la Optimización dinámica y solo está disponible cuando se configura un grupo host para migrar máquinas virtuales mediante la Optimización dinámica. Mediante la Optimización dinámica, Virtual Machine Manager ayuda a ahorrar energía desactivando los hosts que no son necesarios para satisfacer los requisitos de recursos de un clúster de hosts y activándolos de nuevo cuando se vuelven a necesitar.

De forma predeterminada, Virtual Machine Manager realiza la optimización de energía todo momento cuando la característica está activada. Así también, puede programar las horas y los días durante la semana cuando se realiza la optimización de energía. Por ejemplo, puede programar inicialmente la optimización de energía solo los fines de semana, cuando prevé el uso de pocos recursos en los hosts. Después de observar los efectos de la optimización de energía en su entorno, puede aumentar las horas.

La optimización de energía se asegura de que el clúster mantiene un quórum si se produce un error en un nodo activo. Antes de desactivar un host para la Optimización de energía, VMM migra todas las máquinas virtuales a otros hosts del clúster de hosts. Cuando se vuelva a necesitar un

host, VMM activará el host y realizará la Optimización dinámica para migrar máquinas virtuales y equilibrar la carga con el clúster de hosts. Cuando la Optimización de energía se deshabilita en un grupo host o cuando finaliza un período programada de Optimización de energía, se produce el mismo proceso con todos los hosts que se desactivaron mediante la Optimización de energía.

Citrix XenServer 6.x:

Workload Balancing (WLB) es un poderoso componente de XenServer que incluye muchas funcionalidades diseñadas para optimizar el balanceo de carga de los entornos, tal como la gestión de recursos y energía entre otras. Adicionalmente podemos configurar el criterio que utiliza WLB para realizarnos recomendaciones de optimización. Sus dos principales tareas son: Determinar el mejor host en cual correr la máquina virtual y aceptar las recomendaciones del optimizador de carga.

Workload Balancing (WLB) consta en 4 capas (Recolección (COLLECTION), Análisis (ANALYSIS), Alertas (ALERTS) y balanceo de carga (WORKLOAD BALANCING)).

La primera capa, una de las más importantes, recopila y archiva las métricas de XenServer. Su sistema de alertas está basado en los parámetros que recopila. El sistema de monitorización XenCenter utiliza RRDs, que pierde precisión con el paso del tiempo, pero la tecnología de Balanceo de Carga permite mantener las métricas controladas con gran precisión. La segunda capa se encarga de analizar las tendencias de las métricas teniendo en cuenta el historial del sistema, generar informes y asignar costes. Permite a los administradores TI programar alertas y los informes que proporciona permiten mejorar considerablemente la planificación.

La tercera capa tiene la función de crear alertas y sugerir el posicionamiento de las máquinas virtuales. Analiza las entradas y el historial de datos para avisar a los usuarios sobre posibles problemas y, además, realiza recomendaciones a los administradores sobre posibles migraciones de máquinas virtuales.

La cuarta capa automatiza el balanceo de cargas de trabajo basándose en las recomendaciones realizadas por la tercera capa. Los administradores pueden configurar un despliegue para responder a las recomendaciones de manera automática y tomar así las medidas adecuadas para mejorar el rendimiento en un despliegue.

Workload Balancing (WLB) también posee gestión de energía pudiendo solamente enviar una recomendación o convertir esa recomendación en automática y haciéndose cargo y apagando el host.

5.1.19 Capacidades de Configuración de Nodos / Hosts Físicos.

VmWare vSphere 5.x:

Los hosts en VMWare permiten un máximo de 512 máquinas virtuales por nodo y un máximo de 4096 CPU virtuales por host

Un máximo de 320 CPUs lógicas (threads) y un máximo de 6TB de memoria por host

Microsoft Hyper-V 2012R2:

Los hosts en Hyper-V permiten un máximo de 1024 máquinas virtuales por nodo y un máximo de 2048 CPU virtuales por host

Un máximo de 320 CPUs lógicas (threads) y un máximo de 4TB de memoria por host

Citrix XenServer 6.x:

Los hosts en Citrix permiten un máximo de 500 máquinas virtuales por nodo y un máximo de 4000 CPU virtuales por host

Un máximo de 160 CPUs lógicas (threads) y un máximo de 1TB de memoria por host

5.1.20 Pruebas de Performance

Como punto de partida se realizaron las pruebas en el laboratorio armado, como las pruebas dieron igualadas con respecto a la performance general y dejamos de poseer acceso al laboratorio armado, decidimos buscar más información en documentos de investigación.

Luego del análisis en el cual se describe una prueba de cada solución en el mismo hardware, con la misma topología de red y corriendo las mismas pruebas en las mismas máquinas virtuales, los resultados generales fueron similares a las realizadas en el laboratorio con una pequeña diferencia cuando se realizaron pruebas de stress personalizadas.

Los resultados mostraron que las 3 soluciones combinan muy buen rendimiento hypervisor con muy buenas herramientas de gestión.

Las pruebas se realizaron sobre servidores Blade debido a la facilidad de instalación y configuración que consolida el poder, la red y la gestión remota en una sola unidad.

El plan de prueba consistía en revisar el rendimiento del servidor Windows y Linux en el hardware físico, en un hypervisor en modo de reposo, así como otra prueba en un hypervisor bajo aumento de los niveles de carga. Las métricas incluyen CPU, RAM, red y almacenamiento de rendimiento I / O, el tiempo y la interrupción durante migraciones de máquinas virtuales, la velocidad y la agilidad en la creación de plantillas de VM y el despliegue y manejo general de una serie de escenarios de desastres, tales como la pérdida brusca de un anfitrión y de conmutación por error a un sitio alternativo.

Las pruebas de Linux fueron extraídas de una suite estándar de pruebas y se basan en herramientas y escenarios comunes, y son medidos por el tiempo transcurrido para completar.

Estos incluyen la conversión de un archivo WAV a MP3 150 MB utilizando el codificador LAME en Linux, así como el uso de bzip2 y gzip para comprimir y descomprimir archivos de gran tamaño.

Estas son pruebas de un único subproceso que se ejecutan en la serie, pero con el aumento de la concurrencia, lo que permite un rendimiento que se medirá con dos, cuatro, seis, ocho y doce prueba concurrente pasa corriendo. Mediante la ejecución de estas pruebas en una máquina virtual con cuatro CPU virtuales (CPU virtual), hemos sido capaces de medir qué tan bien el hypervisor aumenta la carga de trabajo en la máquina virtual en términos de CPU, RAM y rendimiento I / O, ya que todos los archivos se leyeron desde el almacenamiento compartido.

Las pruebas llevadas a cabo en Windows elegimos centrarnos en unos pocos puntos de referencia específicos, basados principalmente en la CPU y el rendimiento de la memoria RAM, pero también incluyendo la criptografía AES, que desempeña un papel importante en muchas cargas de trabajo de producción.

Una vez más, se llevaron a cabo todas las pruebas en el mismo hardware físico, con la misma matriz EqualLogic PS6010XV iSCSI para el almacenamiento, y en máquinas virtuales idénticas construidas bajo cada solución. Todas las pruebas de Windows se ejecutan en Windows Server 2008 R2, y todas las pruebas de Linux se ejecutan en Red Hat Enterprise Linux 6 - con la excepción

de Microsoft Hyper-V. Debido a Hyper-V no soporta Red Hat Enterprise Linux 6, se utilizó RHEL 5.5, que puede haber tenido un impacto menor en los resultados de pruebas de Hyper-V de Linux. **Los resultados de las pruebas de rendimiento muestran las tres herramientas muy igualadas, sin grandes ganadores o perdedores. Las principales diferencias surgieron en las pruebas de hypervisor cargados, donde el rendimiento de Windows de XenServer y el rendimiento de Hyper-V Linux no fue el óptimo.** En general, **VmWare vSphere y Microsoft Hyper-V convirtieron en los mejores resultados de Windows**, mientras que en Linux las pruebas estuvieron muy igualadas. **En las pruebas de ancho de banda de cifrado, XenServer y vSphere resultaron tres veces más rápidas que la tecnología Hyper-V**, mostraron las ventajas de apoyar instrucciones AES-NI de Intel Westmere la CPU. Se muestran a continuación Gráficas de algunos de estos resultados de la prueba.

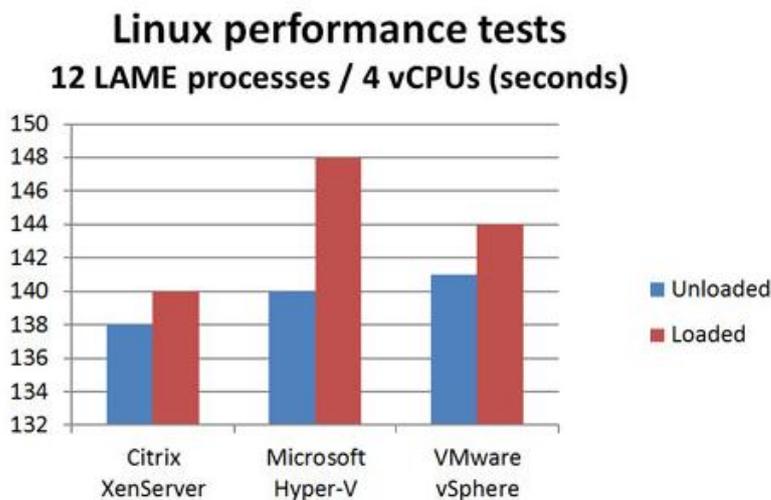


Figura 5.6: Comparativo de pruebas de performance en Linux

Microsoft Hyper-V se destacó cuando se ejecuta un Linux VM de forma aislada, pero no fue tan consistente como los demás a mantener el rendimiento de Linux cuando está cargado con varias máquinas virtuales activas.

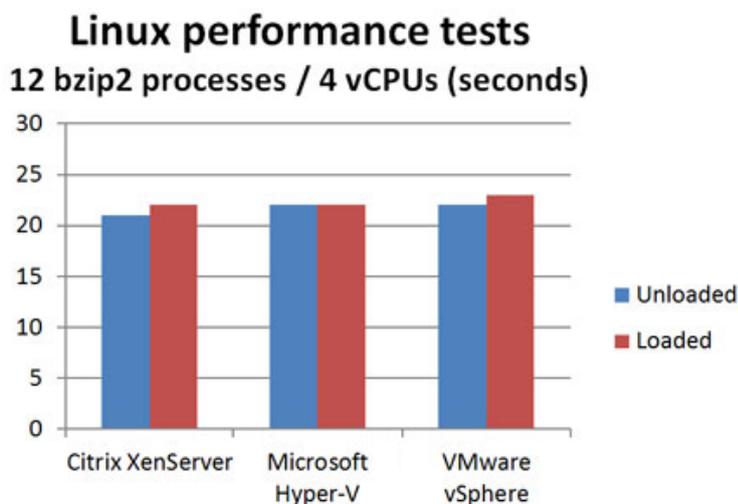


Figura 5.7: Comparativo de pruebas de performance en Linux

Citrix XenServer resultó ser el mejor rendimiento bruto de Windows, pero no siempre se mantienen bajo una gran carga.

Windows performance tests Inter-core bandwidth (GB/s)

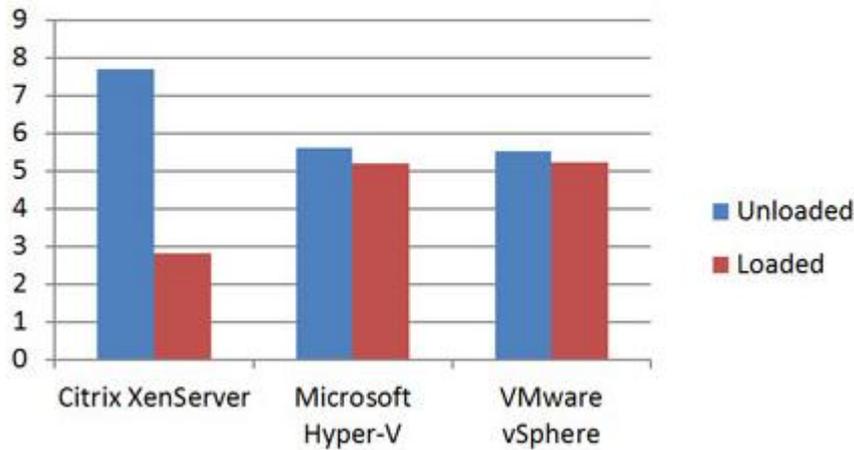


Figura 5.8: Comparativo de pruebas de performance en Windows

Microsoft Hyper-V y VMware vSphere son las herramientas más consistentes cuando se ejecuta Windows máquinas virtuales.

Windows performance tests Crypto bandwidth (GB/s)

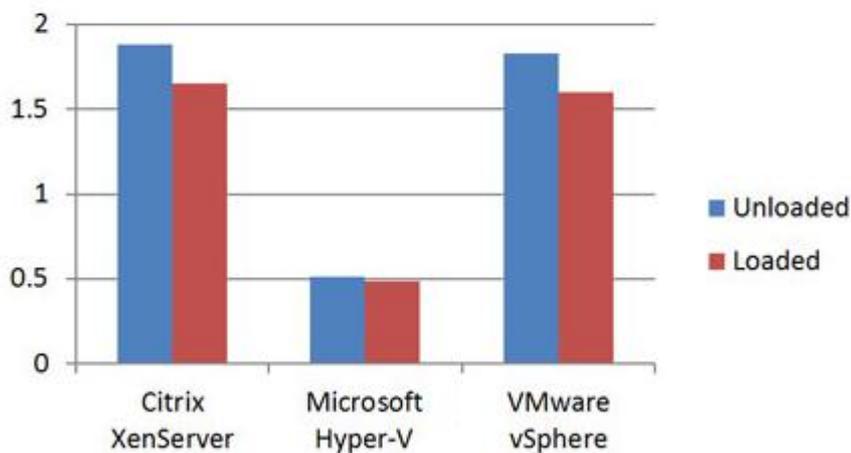


Figura 5.8: Comparativo de pruebas de performance en Windows

Citrix XenServer y VMware vSphere apoyan instrucciones AES-NI de Intel Westmere la CPU, y Microsoft Hyper-V no. Con esto se hace una gran diferencia.

CAPITULO VI – RESULTADOS y CONCLUSION

6.1. Resultados Obtenidos

Empresa/Producto	VmWare vSphere 5.5	Microsoft HyperV 2012R2	Citrix XenServer 6.5
Edición	Enterprise Plus	DataCenter	Commercial Edition
Instalación	Accesible para un Admin Jr	Accesible para un Admin Jr, siempre y cuando este en dominio	Accesible para un Admin Jr
Tiempo de instalación	20 minutos	20 minutos	40 minutos
Consola de administración	Vsphere Client	Hyper-V Manager	Xen-Center
Experiencia de usuario	Rápida consola	Rápida consola	Rápida consola
Manejo de ISOs-Cd room	Simple-varias maneras	Simple-pocas maneras	Compleja-necesidad de CIFS
Posición en el Mercado	Primero	Segundo	Tercero
Licencia y soporte	\$4245 x socket + Soporte 1 año: \$891 (B) o \$1061 (Prod)	\$3077 x socket (\$ 6155 hasta 2 sockets (mas de 2 sockets aumento del 28%))	Annual: \$690 x socket, Perpetua: \$ 1250 x socket
Herramienta de Gestión	\$4995(vCenter Standard) + \$1049 (Soporte Básico) o \$1249 (Soporte Productivo) \$1495(vCenter Foundation) + \$545(Soporte Básico) o \$645(Soporte Productivo)	\$3607 System Center 2012 R2 Datacenter (hasta 2 CPU) \$1323 System Center 2012 R2 Standard (hasta 2 CPU)	XenCenter es gratis
Licencias incluidas en el Sistema operativo virtualizado	No (pero posee proporciones con Sistema Operativo Linux Suse SLES)	Si (Sistemas operativos Windows Ilimitados)	No
Gestión Centralizada	Si (a través de vCenter)	Si (a través de System Center 2012R2)	Si (a través del XenCenter)
Gestión de hosts Físicos	Limitada (deploy y monitoreo)	Si (Actualizaciones y gestión de storage)	No
Control de acceso basado en roles integrado con Active Directory	Si (vCenter y Hosts ESXi) mejorado con SSO	Si (por medio de System Center 2012)	Si (XenCenter y Hosts)
Gestión multi plataforma de virtualización	Limitado (Hyper - V y Amazon Web Services)	Si (Citrix XenServer y VmWare vSphere)	No
Gestión por navegador web (sin cliente e independiente)	Si	Limitado (Algunas funcionalidades)	Limitado (aplicaciones de 3eros)
Gestión avanzada de operaciones	Si (vCenter Operations Management Suite Standard)	Si (SC Operations Manager)	No
Actualizaciones del Hypervisor	Si (por medio de Update manager)	Si (por medio de VMM 2012)	Si (por medio de Xen Center)
Actualizaciones de maquinas virtuales	Limitado (Update Manager)	Si (por medio de VMSTque integra VMM 2012 y WSUS)	No
Snapshot en Vivo	Si	Si	Si
Backup integrado	Si (vSphere Data Protection)	Si (WSB & DPM & Azure Backup)	No
Seguridad	Alto Nivel	Alto Nivel	Medio Nivel
Pool de Recursos	Si (Resource pool)	Si (host Groups)	No
Alta disponibilidad	Si (32h,4000vm),Monitoreo y VmReset	Si (64 h,8000vm),Monitoreo y VmReset	Si (16h,4000vm)
Migración en Vivo de Maquinas virtuales	Si (vMotion, de 4 a 8 concurrentes y Storage vMotion)	Si (Ilimitadas concurrentes, nuevo método de compresión y opciones SMB3 y migración de storage)	Si (XenMotion - 1 concurrente y StorageXenMotion)
Migración automática de máquinas virtuales y gestión de energía	Si (DRS) y (DPM)	Si (DO y PO)	Si (WLB)
Nodos/Hosts	512vm,4095vCPU,6TB memoria	1024vm,2048vCPU,4TB memoria	500vm,4000vCPU,1TB memoria
Performance General	Muy buena	Muy buena	Muy buena
Recomendación	Grandes Empresas con diferente variedad de Sistemas Operativos	Medianas Empresas o Grandes empresas con mayoría de maquinas virtuales Windows	Pequeñas empresas con entornos pequeños y que insuman un costo bajo

6.2 Conclusiones

En relación al objetivo específico “Investigar las tecnologías VmWare: Vsphere 5.x, Citrix: Xen Server 6.x y Microsoft: Hyper-V 2012”, se hizo un análisis y estudio detallado de cada una de las tecnologías mencionadas que me permitió tener una visión completa de cada una de ellas pudiendo identificar sus fortalezas y debilidades.

En relación al objetivo específico “Realizar análisis de viabilidad técnica de la implementación de las herramientas sobre el hardware disponible”, se pudo realizar en análisis de viabilidad técnica pudiendo instalar y probar las 3 herramientas en el hardware disponible.

En relación al objetivo específico “Realizar un estudio comparativo de las mismas sobre un mismo requerimiento de hardware en este caso: un hardware HP enclosure y Blades Gx de última generación”, se pudo llegar a la conclusión que las herramientas de **VmWare y Microsoft** sacan una **gran diferencia** a nivel de **funcionalidades** que su competidor Citrix, al igual que la herramienta de **Citrix** posee un **costo muy bajo** en comparación con las herramientas de Microsoft y VMware. Con respecto a **fiabilidad y performance** las **3 herramientas se encuentran igualadas** y hoy en día, las 3 poseen las funcionalidades principales y más utilizadas, no obstante podemos concluir que **cada herramienta tiene sus fortalezas y debilidades** y que pueden ser aprovechadas por las diferentes empresas dependiendo su tamaño, presupuesto y complejidad en sus entornos.

En relación al objetivo específico “Crear un documento para la toma de decisión”, se creó un documento (página 102) en la cual muestra las principales características y beneficios de cada herramienta pudiendo ser de gran utilidad para la toma de decisión de las empresas sin invertir su tiempo en el análisis.

En relación al objetivo general y como conclusión final podemos decir que pudimos elaborar un documento comparativo que permita a las empresas tanto medianas como grandes, poder tomar una decisión con cierto grado de eficacia a la hora de tener que elegir por algún método de virtualización.

Por lo cual si sos una **empresa pequeña** y con poco presupuesto para el área de IT o estas comenzando en el mundo de la virtualización y tenes **entornos pequeños** que virtualizar podría ser una buena opción utilizar la herramienta de **Citrix**. Si posees una **mediana empresa** o una empresa grande con **entornos no tan complejos** y con **máquinas virtuales** en su mayoría **Windows** sería una buena opción utilizar **Hyper-V** por su balance entre costo y funcionalidades que aporta. Ahora si sos una **gran empresa** con presupuesto, **entornos complejos** y no te gusta correr ni el mínimo riesgo podrías descansar en la fiabilidad y la trayectoria de VMware que sigue siendo la empresa número uno en virtualización.

Bibliografía

- **Introducción a Virtualización:**
<http://www.muypymes.com/2010/04/21/como-funciona-la-virtualizacion-y-para-que-sirve>
- **Introducción a productos de VmWare:**
<http://www.vmware.com/>
- **Características de Microsoft Hyper-V:**
<http://www.microsoft.com/en-us/server-cloud/hyper-v-server/default.aspx>
- **Características de Citrix XenServer:**
<http://www.citrix.com/products/xenserver/overview.html>
<http://miniacademia.wordpress.com/2013/10/16/introduccion-a-citrix-xenserver/>
- **Características de VmWare Vsphere 5.1**
<http://www.vmware.com/files/pdf/products/vsphere/vmware-what-is-new-vsphere51.pdf>
- **Virtualización y Virtualización por Sistema Operativo:**
Link: <http://es.wikipedia.org/wiki/Virtualizaci%C3%B3n>
- **Libro Descubre y domina Vsphere 5**
Autor: José María González
- **Libro Windows Server 2012 Hyper-V Cookbook**
Autor: Leandro Carvalho
- **Libro VmWare Vsphere 5 en el ceno del data center.**
Autor: Eric Maille, Rene-Francois Mennecier
- **Tutoriales de XenServer:**
<http://www.josemariagonzalez.es/video-tutoriales/videos-formacion-xenserver>
- **Citrix XenServer:**
<http://miniacademia.wordpress.com/2013/10/16/introduccion-a-citrix-xenserver/>
- **Hyper V**
<http://technet.microsoft.com/es-es/library/hh831531.aspx>
- **Vsphere**
<http://www.vmware.com/files/es/pdf/products/vsphere/>

Herramientas Comparativas

- **Posición en el Mercado**

<http://www.gartner.com/technology/reprints.do?id=1-1WR7CAC&ct=140703&st=sb>

- **Licencia y soporte**

http://www.vmware.com/files/pdf/vsphere_pricing.pdf

<http://www.vmware.com/products/vsphere/pricing>

<https://www.microsoft.com/en-us/server-cloud/products/windows-server-2012-r2/default.aspx#fbid=Kw7ERJ8yXRk>

<http://store.citrix.com/store?SiteID=citrix&Action=DisplayProductDetailsPage&productID=315979800>

- **Herramienta de Gestión**

http://www.vmware.com/files/pdf/vsphere_pricing.pdf

<https://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/Purchasing.aspx>

- **Licencias incluidas en el Sistema operativo virtualizado**

http://www.vmware.com/files/pdf/vsphere_pricing.pdf

<https://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/Purchasing.aspx>

- **Control de acceso basado en roles integrado con Active Directory**

<https://www.vmware.com/ar/products/esxi-and-esx/management#sthash.b7N3wYSc.dpuf>

<http://sccm.es/mis-articulos-y-practicas/147-9-serie-articulos-configuraciones-rbac-control-de-acceso-basado-en-roles.html>

<http://blogs.itpro.es/cristiansan/2015/02/20/xenserver-role-based-access-control-y-audit/>

- **Gestión multi plataforma de virtualización**

<https://www.vmware.com/support/mhm/doc/vcenter-multi-hypervisor-manager-11-release-notes.html>

<https://technet.microsoft.com/en-us/library/hh420338.aspx>;

<http://channel9.msdn.com/posts/System-Center-2012-Multi-Hypervisor-Management-for-VMware--Citrix>

- **Gestión por navegador web (sin cliente e independiente)**

<http://hispavirt.com/tag/vsphere-5-5/>

<http://www.xvpsource.org/>

<http://1staff.com/Blog/post/2012/12/03/How-To-Install-the-Operations-Manager-Web-Console.aspx>

- **Gestión avanzada de operaciones**

<http://www.vmware.com/files/pdf/vcenter/VMware-vCenter-Operations-DS-EN1.pdf>

<https://www.microsoft.com/en-us/server-cloud/products/system-center-2012-r2/>

- **Actualizaciones del Hypervisor**

<https://www.vmware.com/ar/products/vsphere/features/update-manager>

<https://technet.microsoft.com/es-es/library/gg610610.aspx>

<http://www.miniacademia.es/xenserver-instalacion-de-actualizaciones-en-hosts-xenserver-individuales/>

- **Actualizaciones de máquinas virtuales**

<http://www.bujarra.com/uso-de-vmware-update-manager/>

<https://technet.microsoft.com/en-us/library/jj149757.aspx>

- **Backup integrado**
<https://www.vmware.com/ar/products/vsphere/features/data-protection>
<https://technet.microsoft.com/es-es/library/jj614621.aspx>
<https://azure.microsoft.com/es-es/documentation/articles/backup-introduction-to-azure-backup/>
<https://technet.microsoft.com/es-es/library/hh758104.aspx>
- **Seguridad**
<https://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-security-guide.pdf>
<https://technet.microsoft.com/library/hh831778.aspx>
<http://www.vmware.com/ar/products/vsphere/features/endpoint.html>
<http://blogs.technet.com/b/davidcervigon/archive/2009/04/06/gu-a-de-seguridad-para-hyper-v.aspx>
- **Pool de Recursos**
<https://virt.es/curso-de-vmware-5-5-resource-pools/>
<https://technet.microsoft.com/en-us/library/gg610645.aspx>
- **Alta disponibilidad**
<http://www.vmware.com/files/pdf/VMware-High-Availability-DS-EN.pdf>
<https://support.citrix.com/servlet/KbServlet/download/21018-102-664364/High%20Availability%20for%20Citrix%20XenServer.pdf>
- **Migración en Vivo de Máquinas virtuales**
<http://www.vmware.com/files/pdf/VMware-VMotion-DS-EN.pdf>
<http://www.miniacademia.es/xenserver-xenmotion/>
- **Migración automática de máquinas virtuales y gestión de energía**
<https://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-resource-management-guide.pdf>
<https://technet.microsoft.com/es-es/library/gg675109.aspx>
<https://www.citrix.com/blogs/2015/01/22/citrix-xenserver-workload-balancing-wlb-why-xendesktop-and-xenapp-customers-really-should-take-note/#comments>
http://docs.citrix.com/content/dam/docs/en-us/xenserver/xenserver-65/XenServer-6.5.0_WLB_Administrators_Guide.pdf
- **Performance**
<http://www.infoworld.com/article/2623813/virtualization/virtualization-shoot-out--citrix--microsoft--red-hat--and-vmware.html?page=3>

Glosario

IUA: Instituto Universitario Aeronáutico

SR: Storage repository

SR: Shared storage

VMM (Virtual Machine Monitor)

HA: High Availability

Datos Personales del Alumno

Apellido y Nombres: Sarmiento Matías Oscar

Dirección: San Jerónimo 3619

Teléfonos: (0351) 155060557

e-mail: sarmientomatias@hotmail.com

Datos Personales del Asesor

Apellido y Nombres: Casanovas, Eduardo

Título: Ingeniero

Dirección:

Teléfono: (0351)4435000

e-mail: ecasanovas@iua.edu.ar

Firma del alumno

Firma del asesor