

TEMA 6

**IMPLANTACIÓN
DE
SOLUCIONES
DE
ALTA
DISPONIBILIDAD**

MARÍA ÁNGELES PEÑASCO SÁNCHEZ – TEMA 6 – SAD

Análisis de configuraciones de alta disponibilidad:

Alta disponibilidad

Concepto.

Funcionamiento ininterrumpido.

Integridad de datos y recuperación de servicio.

Soluciones de alta disponibilidad

Servidores redundantes. RAID.

Sistemas de «clúster».

SAN, NAS, Fiber Channel.

Balanceadores de carga.

Instalación y configuración de soluciones de alta disponibilidad

Virtualización de sistemas

Posibilidades de la virtualización de sistemas.

Herramientas para la virtualización.

Configuración y utilización de máquinas virtuales.

Alta disponibilidad Concepto.

Alta disponibilidad es un protocolo de diseño del sistema y su implementación asociada que asegura un cierto grado absoluto de continuidad operacional durante un período de medición dado. Disponibilidad se refiere a la habilidad de la comunidad de usuarios para acceder al sistema, someter nuevos trabajos, actualizar o alterar trabajos existentes o recoger los resultados de trabajos previos. Si un usuario no puede acceder al sistema se dice que está no disponible. El término tiempo de inactividad (downtime) es usado para definir cuándo el sistema no está disponible.

Funcionamiento ininterrumpido.

Para el funcionamiento ininterrumpido, es necesario un SAI por si tenemos un problema con algún servicio o cosa, los SAI soluciona eso dándole corriente eléctrica para que este no deje de funcionar.

Un sistema de alimentación ininterrumpida, SAI, es un dispositivo que gracias a sus baterías, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados. Otra de las funciones de los UPS es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna.

Clasificación de los SAI:

Off-line: la alimentación viene de la red eléctrica y en caso de fallo de suministro el dispositivo empieza a generar su propia alimentación. Debido a que no son activos, hay un pequeño tiempo en el que no hay suministro eléctrico. Típicamente generan una forma de onda que no es sinusoidal, por lo que no son adecuados para proteger dispositivos delicados o sensibles a la forma de onda de su alimentación. Su uso más común es en la protección de dispositivos domésticos como ordenadores, monitores, televisores, etc.



In-line: también conocido como de "línea interactiva". Es similar al off-line, pero dispone de filtros activos que estabilizan la tensión de entrada. Sólo en caso de fallo de tensión o anomalía grave empiezan a generar su propia alimentación. Al igual que los SAI de tipo off-line tienen un pequeño tiempo de conmutación en el que no hay suministro eléctrico. Típicamente generan una forma de onda pseudo-sinusoidal o sinusoidal de mayor calidad que los SAI off-line. Su uso más común es en la protección de dispositivos en pequeños comercios o empresas, tales como ordenadores, monitores, servidores, cámaras de seguridad y videograbadores, etc.



On-line: el más sofisticado de todos. El dispositivo genera una alimentación limpia con una onda sinusoidal perfecta en todo momento a partir de sus baterías. Para evitar que se descarguen las carga al mismo tiempo que genera la alimentación. Por tanto, en caso de fallo o anomalía en el suministro los dispositivos protegidos no se ven afectados en ningún momento porque no hay un tiempo de conmutación. Su principal inconveniente es que las baterías están constantemente trabajando, por lo que deben sustituirse con más frecuencia. Su uso más común es en la protección de dispositivos delicados o de mucho valor en empresas, tales como servidores, electrónica de red, ordenadores de monitorización, videograbadores y cámaras de seguridad, etc.



Integridad de datos y recuperación de servicio.

Integridad de datos se refiere a la corrección y completitud de los datos en una base de datos. Cuando los contenidos se modifican con sentencias INSERT, DELETE o UPDATE, la integridad de los datos almacenados puede perderse de muchas maneras diferentes. Pueden añadirse datos no válidos a la base de datos, tales como un pedido que especifica un producto no existente.

Pueden modificarse datos existentes tomando un valor incorrecto, como por ejemplo si se reasigna un vendedor a una oficina no existente. Los cambios en la base de datos pueden perderse debido a un error del sistema o a un fallo en el suministro de energía. Los cambios pueden ser aplicados parcialmente, como por ejemplo si se añade un pedido de un producto sin ajustar la cantidad disponible para vender.

Una de las funciones importantes de un DBMS relacional es preservar la integridad de sus datos almacenados en la mayor medida posible.

Soluciones de alta disponibilidad Servidores redundantes. RAID.

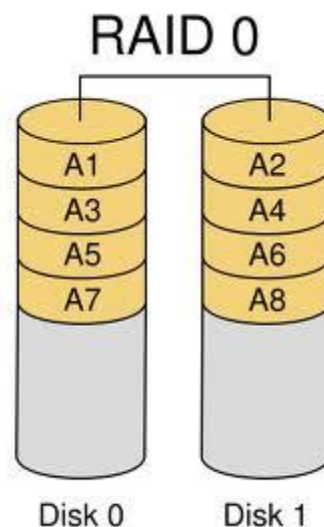
Los niveles RAID más comúnmente usados son:

RAID 0: Almacenamiento dividido. Mínimo 2 discos.

Este sistema RAID distribuye los datos equitativamente entre dos o más discos sin información de paridad que proporcione redundancia.

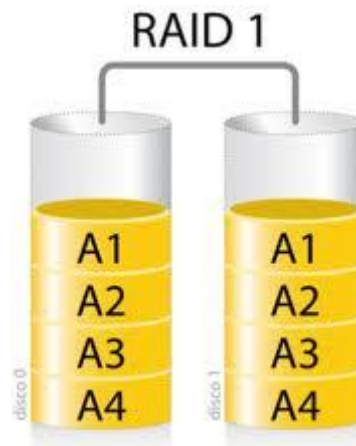
Ventajas: Mayor velocidad, rendimiento.

Inconvenientes: La información se divide 50%-50% si se rompe alguno pierdes todo.



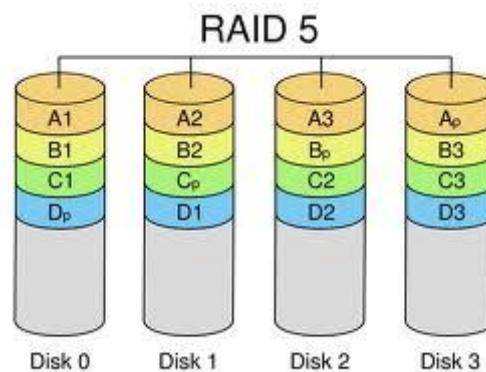
RAID 1: Almacenamiento en espejo. Mínimo 2 discos.

Este sistema RAID crea una copia exacta de un conjunto de datos en dos o más discos. Esto resulta útil cuando el rendimiento en lectura es más importante que la capacidad. Un conjunto RAID 1 sólo puede ser tan grande como el más pequeño de sus discos.



RAID 5: Almacenamiento dividido con paridad distribuida. Mínimo 3 discos.

Este sistema RAID usa división de datos a nivel de bloques distribuyendo la información de paridad entre todos los discos miembros del conjunto. El RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia. Generalmente, el RAID 5 se implementa con soporte hardware para el cálculo de la paridad.



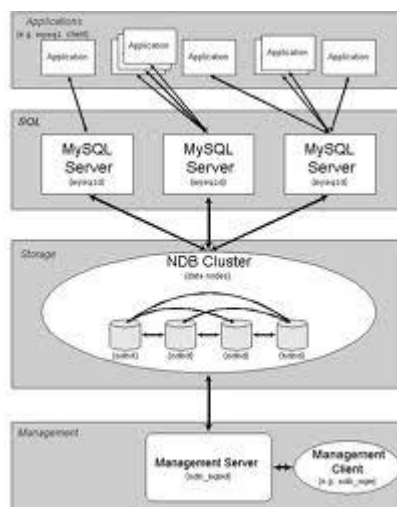
Sistemas de «clústers»

Un clúster de alta disponibilidad es un conjunto de dos o más máquinas que se caracterizan por mantener una serie de servicios compartidos y por estar constantemente monitorizándose entre sí. Podemos dividirlo en dos clases:

Alta disponibilidad de infraestructura: Si se produce un fallo de hardware en alguna de las máquinas del clúster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios en cualquiera de las otras máquinas del clúster (Failover). Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original (failback). Esta capacidad de recuperación automática de servicios nos garantiza la alta disponibilidad de los servicios ofrecidos por el clúster, minimizando así la percepción del fallo por parte de los usuarios.

Alta disponibilidad de aplicación: Si se produce un fallo del hardware o de las aplicaciones de alguna de las máquinas del clúster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios que han fallado en cualquiera de las otras máquinas del clúster. Y cuando la máquina que ha fallado se recupera, los servicios son nuevamente migrados a la máquina original. Esta capacidad de recuperación automática de servicios nos garantiza la integridad de la información, ya que no hay pérdida de datos, y además evita molestias a los usuarios, que no tienen por qué notar que se ha producido un problema.

No hay que confundir un clúster de alta disponibilidad con un clúster de alto rendimiento. El segundo es una configuración de equipos diseñado para proporcionar capacidades de cálculo mucho mayores que la que proporcionan los equipos individuales (véanse por ejemplo los sistemas de tipo Clúster Beowulf), mientras que el primer tipo de clúster está diseñado para garantizar el funcionamiento ininterrumpido de ciertas aplicaciones.



Cálculo de la Disponibilidad

En un sistema real, si falla uno de los componentes, es reparado o sustituido por un nuevo componente. Si este nuevo componente falla, es sustituido por otro, y así sucesivamente. El componente fijo se considera en el mismo estado que un nuevo componente. Durante su vida útil, uno de los componentes pueden ser considerado en uno de estos estados: Funcionando o en Reparación. El estado funcionando indica que el componente está operacional y el en reparación significa que ha fallado y todavía no ha sido sustituido por un nuevo componente.

En caso de defectos, el sistema va de funcionando en modo reparación, y cuando se hace la sustitución volverá al estado funcionando. Por lo tanto, podemos decir que el sistema tiene durante su vida, una media de tiempo para presentar fallas (MTTF) y un tiempo medio de reparación (MTTR). Su tiempo de la vida es una sucesión de MTTFs y MTTRs, a medida que este va fallando y siendo reparado. El tiempo de vida útil del sistema es la suma de MTTFs en ciclos $MTTF + MTTR$ ya vividos.

En forma simplificada, se dice que la disponibilidad de un sistema es la relación entre la duración de la vida útil de este sistema y de su tiempo total de vida. Esto puede ser representado por la fórmula de abajo:

$$\text{Disponibilidad} = \text{MTTF} / (\text{MTTF} + \text{MTTR})$$

En la evaluación de una solución de Alta Disponibilidad, es importante tener en cuenta si en la medición de MTTF son vistos como fallas las posibles paradas planificadas.

SAN, NAS, FiberChannel.

SAN: Una red SAN se distingue de otros modos de almacenamiento en red por el modo de acceso a bajo nivel. El tipo de tráfico en una SAN es muy similar al de los discos duros como ATA, SATA y SCSI. En otros métodos de almacenamiento, (como SMB o NFS), el servidor solicita un determinado fichero, p.ej. "/Home/usuario/wikipedia". En una SAN el servidor solicita "el bloque 6000 del disco 4". La mayoría de las SAN actuales usa el protocolo SCSI para acceder a los datos de la SAN, aunque no usen interfaces físicas SCSI. Este tipo de redes de datos se han utilizado y se utilizan tradicionalmente en grandes main frames como en IBM, SUN o HP. Aunque recientemente con la incorporación de Microsoft se ha empezado a utilizar en máquinas con sistemas operativos Microsoft.

Una SAN es una red de almacenamiento dedicada que proporciona acceso de nivel de bloque a LUNs. Un LUN, o número de unidad lógica, es un disco virtual proporcionado por la SAN. El administrador del sistema tiene el mismo acceso y los derechos a la LUN como si fuera un disco directamente conectado a la misma. El administrador puede particionar y formatear el disco en cualquier medio que él elija.

Dos protocolos de red utilizados en una SAN son Fibre Channel e iSCSI. Una red de canal de fibra es muy rápida y no está agobiada por el tráfico de la red LAN de la empresa. Sin embargo, es muy cara. Las tarjetas de canal de fibra óptica cuestan alrededor de \$ 1000.00 USD cada una. También requieren conmutadores especiales de canal de fibra. SCSI es una nueva tecnología que envía comandos SCSI sobre una red TCP / IP. Este método no es tan rápido como una red Fibre Channel, pero ahorra costes, ya que utiliza un hardware de red menos costoso.

A partir de desastres como lo fue el "martes negro" en el año 2001 la gente de TI, han tomado acciones al respecto, con servicios de cómo recuperarse ante un desastre, cómo recuperar miles de datos y lograr la continuidad del negocio, una de las opciones es contar con la Red de área de almacenamiento, sin embargo las compañías se pueden enfrentar a cientos de ataques, por lo que es necesario contar con un plan en caso de contingencia; es de vital importancia que el sitio dónde se encuentre la Red de almacenamiento, se encuentre en un área geográfica distinta a dónde se ubican los servidores que contienen la información crítica; además se trata de un modelo centralizado fácil de administrar, puede tener un bajo costo de expansión y administración, lo que la hace una red fácilmente escalable; fiabilidad, debido a que se hace más sencillo aplicar ciertas políticas para proteger a la red.



NAS: es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un Servidor con ordenadores personales o servidores clientes a través de una red (normalmente TCP/IP), haciendo uso de un Sistema Operativo optimizado para dar acceso con los protocolos CIFS, NFS, FTP o TFTP.

Generalmente, los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red (normalmente TCP/IP). También se podría considerar un sistema NAS a un servidor (Linux, Windows,...) que comparte sus unidades por red, pero la definición suele aplicarse a sistemas específicos.

Los protocolos de comunicaciones NAS están basados en ficheros por lo que el cliente solicita el fichero completo al servidor y lo maneja localmente, están por ello orientados a información almacenada en ficheros de pequeño tamaño y gran cantidad. Los protocolos usados son protocolos de compartición de ficheros como NFS o Microsoft Common Internet File System (CIFS).

Muchos sistemas NAS cuentan con uno o más dispositivos de almacenamiento para incrementar su capacidad total. Frecuentemente, estos dispositivos están dispuestos en RAID (Redundant Arrays of Independent Disks) o contenedores de almacenamiento redundante.

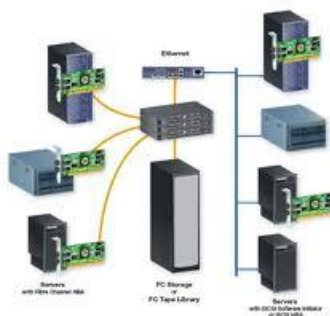


FIBER CHANNEL: El canal de fibra (del inglés fibre channel) es una tecnología de red utilizada principalmente para redes de almacenamiento, disponible primero a la velocidad de 1 Gbps y posteriormente a 2, 4 y 8 Gbps.

El canal de fibra está estandarizado por el Comité Técnico T11 del INITS (Comité Internacional para Estándares de Tecnologías de la Información), acreditado por el ANSI (Instituto Nacional de Estándares Estadounidenses).

Nació para ser utilizado principalmente en el campo de la supercomputación, pero se ha convertido en el tipo de conexión estándar para redes de almacenamiento en el ámbito empresarial. A pesar de su nombre, la señalización del canal de fibra puede funcionar tanto sobre pares de cobre, como sobre cables de fibra óptica.

El FCP (protocolo del canal de fibra) es el protocolo de interfaz de SCSI sobre fibre channel.



Balancedores de carga.

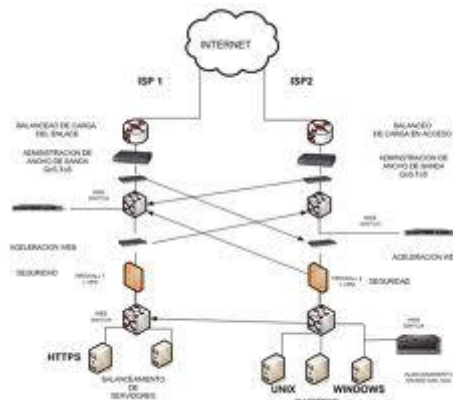
El balance o balanceo de carga es un concepto usado en informática que se refiere a la técnica usada para compartir el trabajo a realizar entre varios procesos, ordenadores, discos u otros recursos. Está íntimamente ligado a los sistemas de multiprocesamiento, o que hacen uso de más de una unidad de procesamiento para realizar labores útiles.



El balance de carga se mantiene gracias a un algoritmo que divide de la manera más equitativa posible el trabajo, para evitar los así denominados cuellos de botella.

De forma sencilla, el balanceo de carga es la manera en que las peticiones de Internet son distribuidas sobre una fila de servidores. Existen varios métodos para realizar el balanceo de carga. Desde el simple "Round Robin" (repartiendo todas las peticiones que llegan de Internet entre el número de servidores disponibles para dicho servicio) hasta los equipos que reciben las peticiones, recogen información, en tiempo real, de la capacidad operativa de los equipos y la utilizan para enrutar dichas peticiones individualmente al servidor que se encuentre en mejor disposición de prestar el servicio adecuado.

Los balanceadores de carga pueden ser soluciones hardware, tales como routers y switches que incluyen software de balanceo de carga preparado para ello, y soluciones software que se instalan en el back end de los servidores.



Instalación y configuración de soluciones de alta disponibilidad

Evaluación de riesgos

En efecto, la falla de un sistema informático puede producir pérdidas en la productividad y de dinero, y en algunos casos críticos, hasta pérdidas materiales y humanas. Por esta razón es necesario evaluar los riesgos ligados al funcionamiento incorrecto (falla) de uno de los componentes de un sistema informático y anticipar los medios y medidas para evitar incidentes o para restablecer el servicio en un tiempo aceptable. Como es sabido, un sistema informático de redes puede fallar de muchas formas.

Las causas de las fallas pueden clasificarse de la siguiente manera:

- Causas físicas (de origen natural o delictivo)
- Desastres naturales (inundaciones, terremotos, incendios)
- Ambiente (condiciones climáticas adversas, humedad, temperatura)
- Fallas materiales
- Fallas de la red
- Cortes de energía
- Causas humanas (intencionales o accidentales):
- Error de diseño (errores de software, aprovisionamiento de red insuficiente)
- Causas humanas (intencionales o accidentales):
- Error de diseño (errores de software, aprovisionamiento de red insuficiente)
- Causas operativas (vinculadas al estado del sistema en un momento dado):
- Errores de software
- Falla del software
- Todos estos riesgos pueden tener diferentes causas, entre las que se cuentan:
- Daños intencionales

Tolerancia a errores

Dado que las fallas no se pueden evitar por completo, existe una solución que consiste en configurar mecanismos de redundancia duplicando los recursos críticos. La capacidad de un sistema para funcionar a pesar de que alguno de sus componentes falle se conoce como tolerancia a errores. Cuando uno de los recursos falla, los otros recursos siguen funcionando mientras los administradores del sistema buscan una solución al problema. Esto se llama "Servicio de protección contra fallas" (FOS). Idealmente, si se produce una falla material, los elementos del material defectuoso deben ser intercambiables en caliente, es decir, capaces ser extraídos y reemplazados sin que se interrumpa el servicio.

Copia de seguridad

La configuración de una arquitectura redundante asegura la disponibilidad de los datos del sistema pero no los protege de los errores cometidos por los usuarios ni de desastres naturales, tales como incendios, inundaciones o incluso terremotos. Por lo tanto, es necesario prever mecanismos de copia de seguridad (lo ideal es que sean remotos) para garantizar la continuidad de los datos. Además, un mecanismo de copia de seguridad también se puede utilizar para almacenar archivos, es decir, para guardar datos en un estado que corresponda a una cierta fecha.

Virtualización de sistemas

Posibilidades de la virtualización de sistemas.

Virtualización es la creación -a través de software- de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.

Dicho de otra manera, se refiere a la abstracción de los recursos de una computadora, 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), dividiéndose el recurso en uno o más entornos de ejecución.

Esta capa de software (VMM) maneja, gestiona y arbitra los cuatro recursos principales de una computadora (CPU, Memoria, Almacenamiento y Conexiones de Red) y así podrá repartir dinámicamente dichos recursos entre todas las máquinas virtuales definidas en el computador central. Esto hace que se puedan tener varios ordenadores virtuales ejecutándose en el mismo ordenador físico.

La virtualización se encarga de crear una interfaz externa que encapsula una implementación subyacente mediante la combinación de recursos en localizaciones físicas diferentes, o por medio de la simplificación del sistema de control. Un avanzado desarrollo de nuevas plataformas y tecnologías de virtualización ha hecho que en los últimos años se haya vuelto a prestar atención a este concepto.

La máquina virtual en general simula una plataforma de hardware autónoma incluyendo un sistema operativo completo que se ejecuta como si estuviera instalado. Típicamente varias máquinas virtuales operan en un computador central. Para que el sistema operativo "guest" funcione, la simulación debe ser lo suficientemente grande (siempre dependiendo del tipo de virtualización).

Herramientas para la virtualización.

VirtualBox tiene un público fiel gracias a que es gratuito, con soporte multiplataforma, y un buen número de características que hacen de su funcionamiento en máquinas virtuales una verdadera joya.

Las descripciones de la máquina virtual y los parámetros se almacenan en su totalidad en archivos XML de texto sin formato para un fácil transporte y uso compartido de carpetas.

Su característica “Guest Additions”, disponible para Windows, Linux, o Solaris, hace que el usuario de VirtualBox se sienta en ambiente y unido a la comunidad, además de que permite instalar el software en una máquina virtual que otorga privilegios adicionales a la máquina para tareas como compartir archivos, unidades, periféricos, y mucho más.

VMware para usuarios de escritorio viene en dos principales formas: VMware Player y VMware Workstation.

VMware Player es una solución gratuita dirigida a los usuarios ocasionales que necesitan crear y ejecutar máquinas virtuales, pero no necesitan soluciones de avanzada a nivel de empresa.

VMware Workstation incluye todas las características de VMWare Player, la creación de máquinas virtuales fáciles, la optimización del hardware, y añade la capacidad de clonar máquinas, tomar varias instantáneas del sistema operativo invitado, y repetir los cambios realizados en la misma máquina virtual, muy útil para pruebas de software.

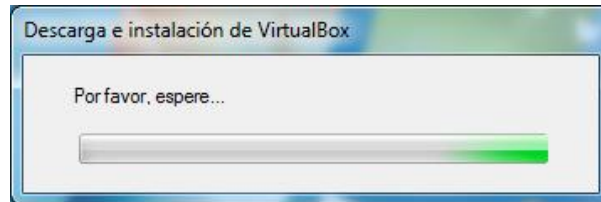
OTRAS HERRAMIENTAS

- VMware Server.
- Windows Server 2008 R2 Hyper-V.
- Microsoft Enterprise Desktop Virtualization (MED-V).
- VirtualBox.
- Parallels Desktop.
- Virtual Iron.
- Adeos.
- Mac-on-Linux.
- Win4BSD.
- Oracle VM.
- Microsoft Virtual PC.

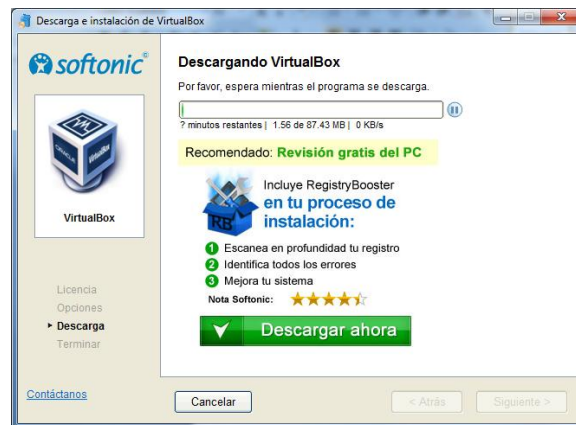
Configuración y utilización de maquinas virtuales.

Vamos a instalar una máquina virtual en Windows 7, hemos elegido VirtualBox, ya que con la que hemos realizado las prácticas VMWare Workstation, ya la teníamos instalada.

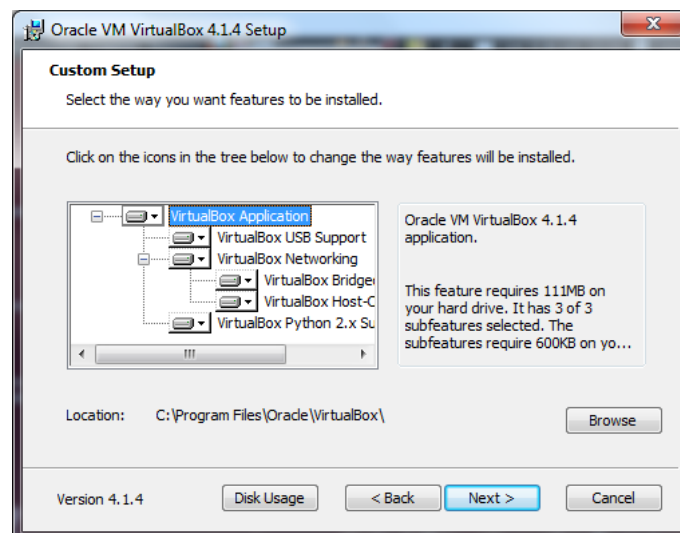
Empezamos con la instalación



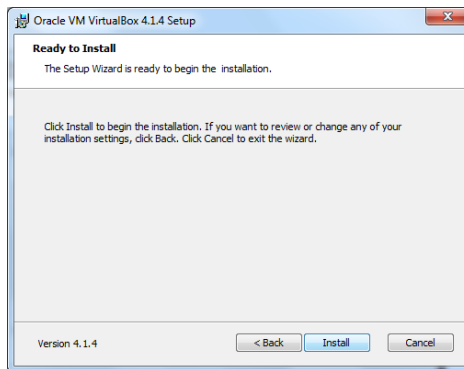
Los pasos a seguir son sencillos, aceptamos en la instalación



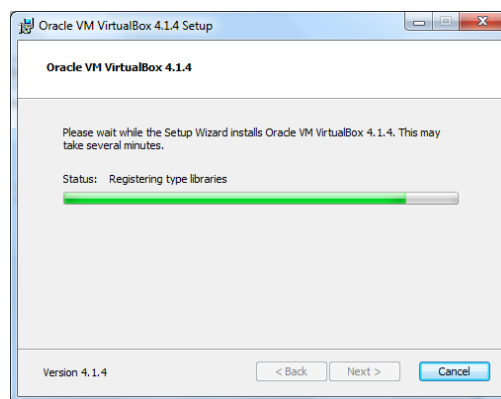
Seleccionamos la aplicación que te viene por defecto y le damos a siguiente



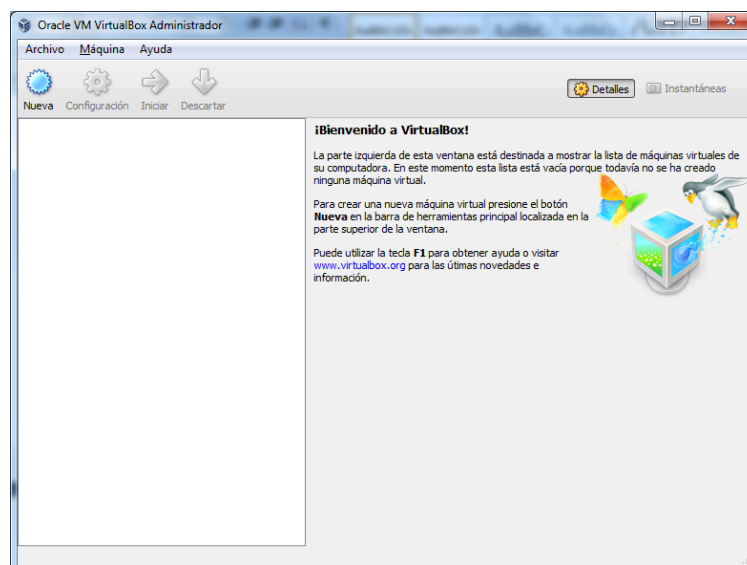
En la siguiente pantalla le damos a Instalar



Y en breves, se termina la instalación sin problema

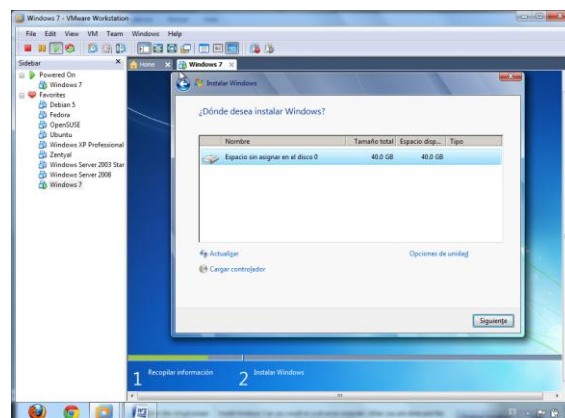
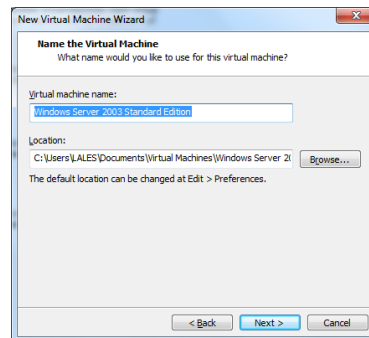


Abrimos VirtualBox y nos aparece esta pantalla de inicio, la aplicación es en español y es fácil de utilizar, al igual que VMWare Workstation.

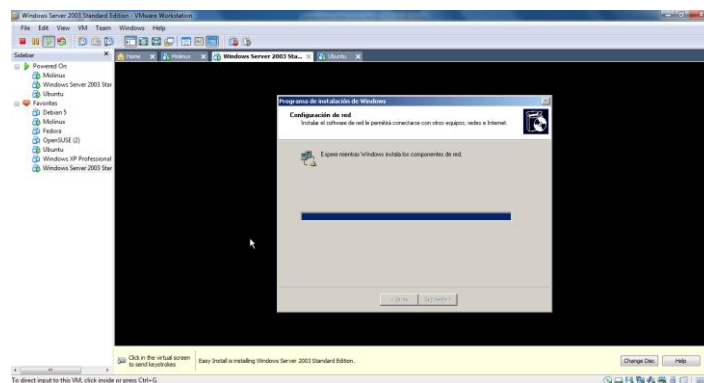


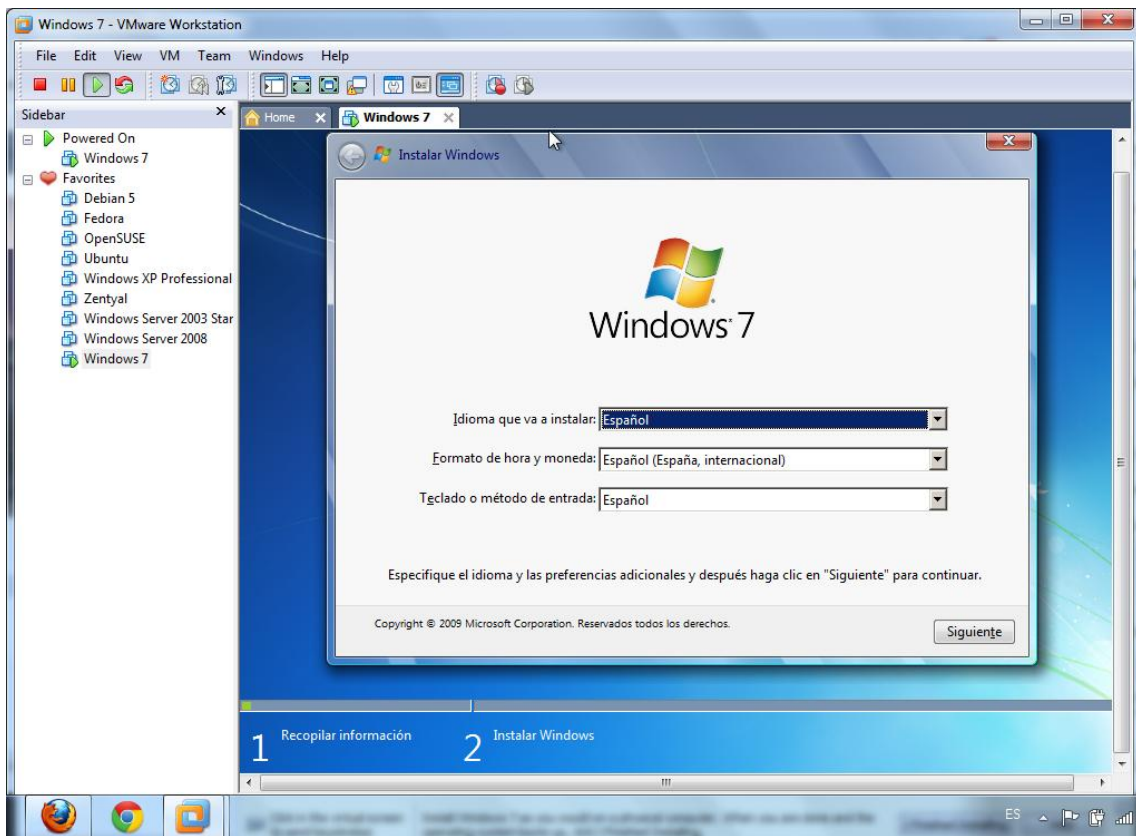
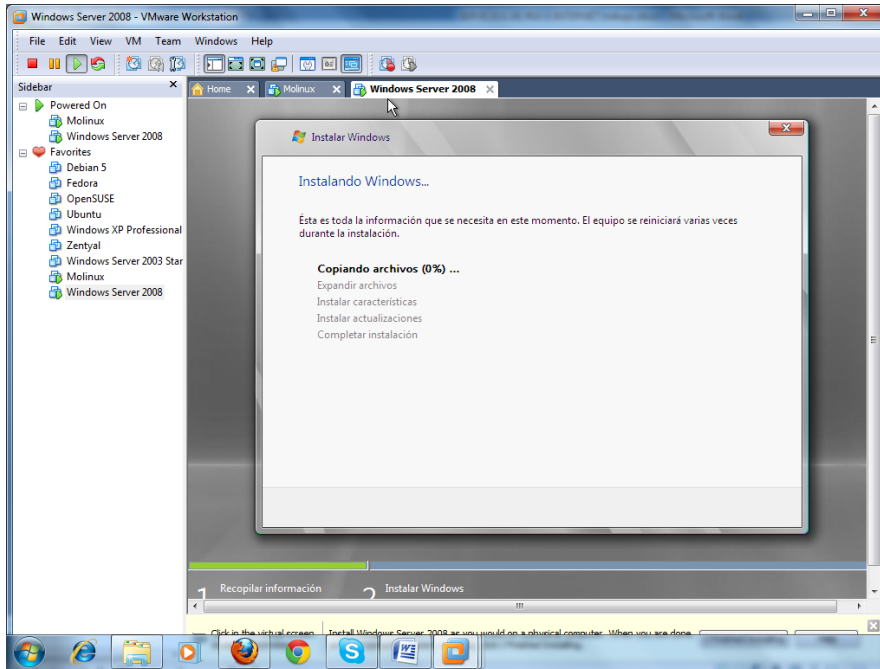
INSTALACIÓN DE DIFERENTES SISTEMAS OPERATIVOS WINDOWS EN UNA MÁQUINA VIRTUAL

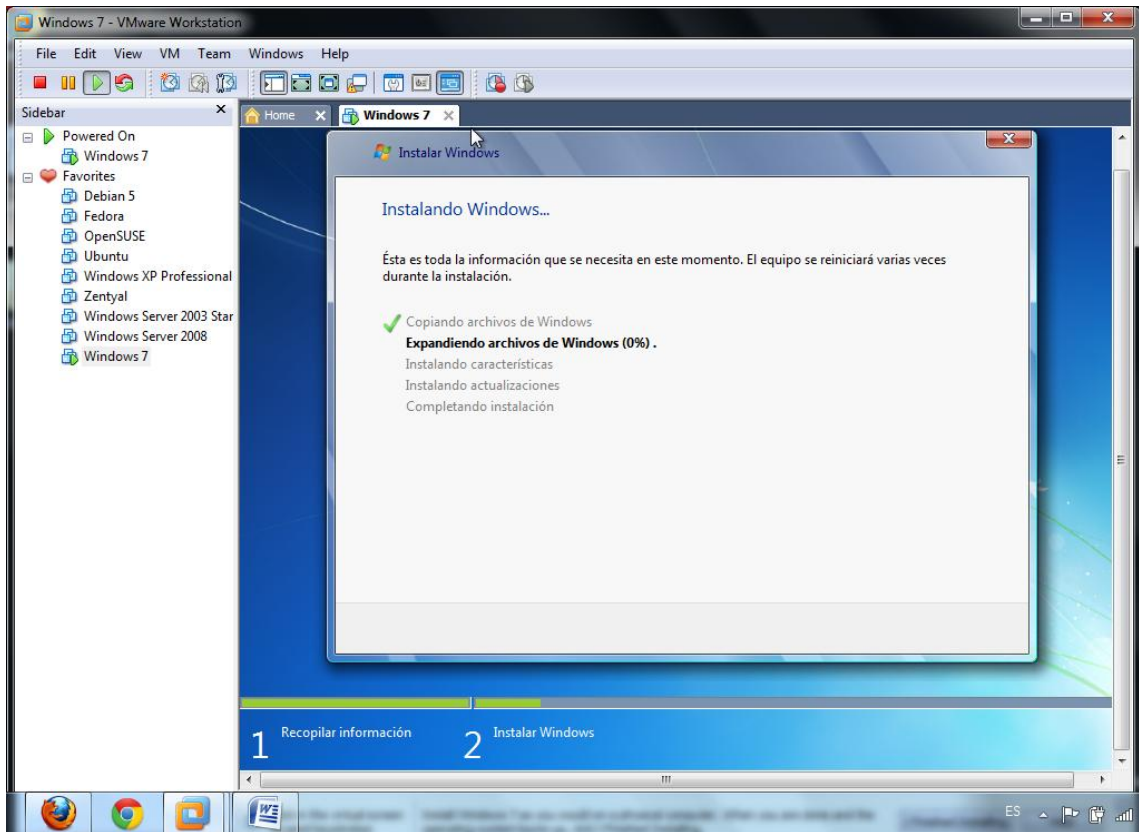
Vamos a instalar WS2003 y WS2008 y Windows 7, para los tres vamos a seguir los mismos pasos, para ello, buscamos en la máquina virtual la imagen del sistema operativo y seguimos los pasos igual que si estuviéramos instalando en un ordenador normal



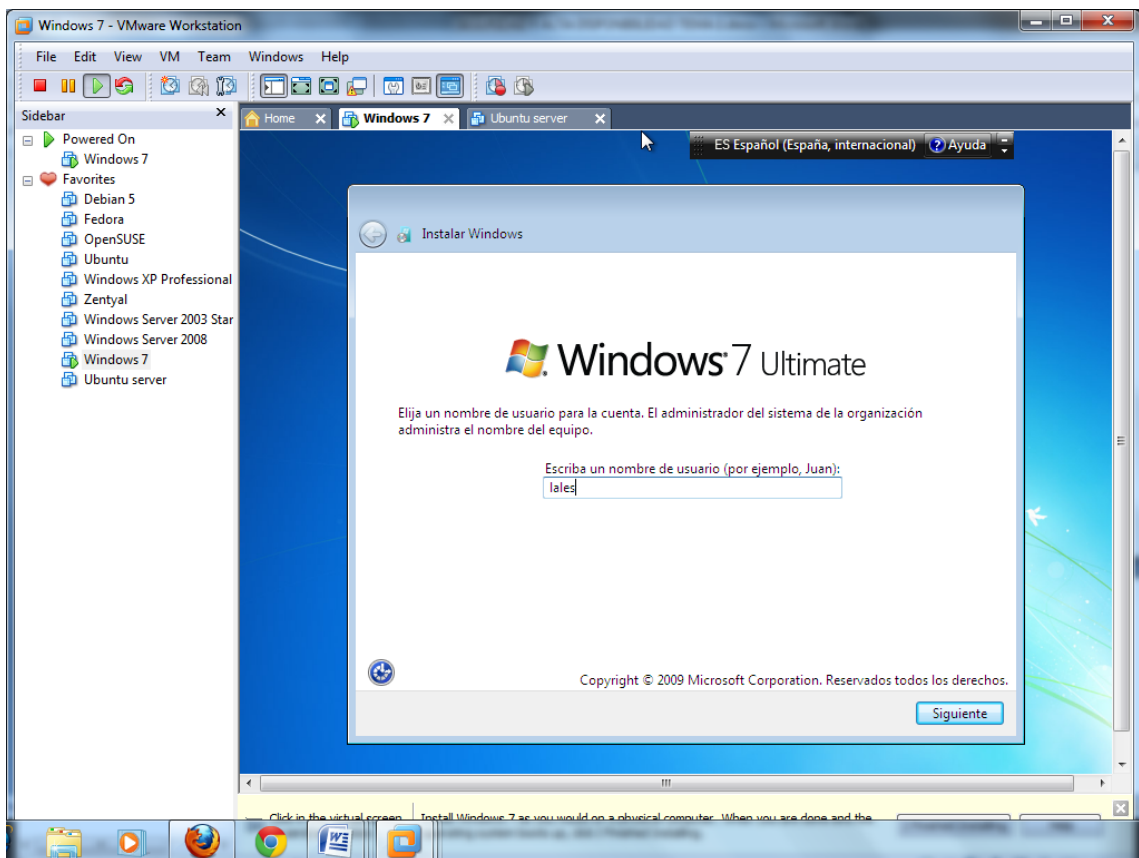
Seguimos los pasos que nos va indicando







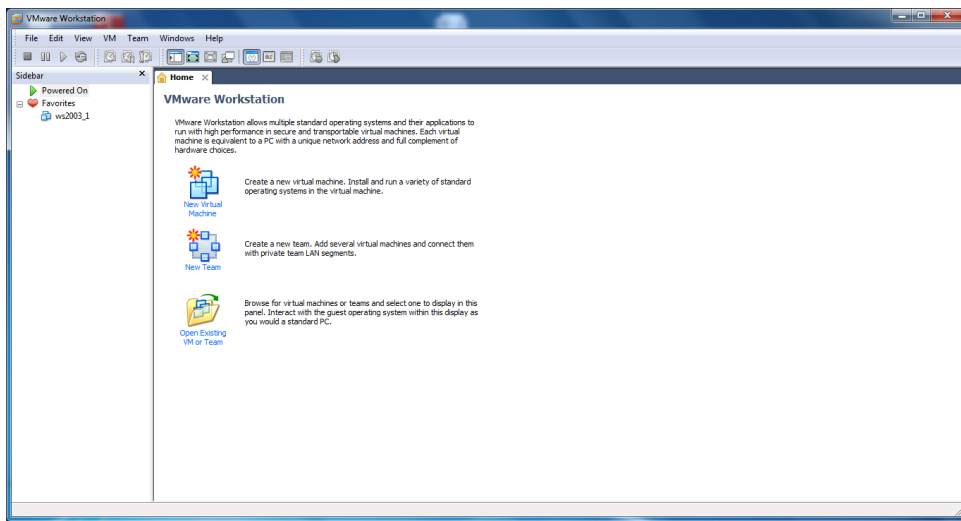
En todos los sistemas operativos nos va a pedir un nombre de usuario y contraseña



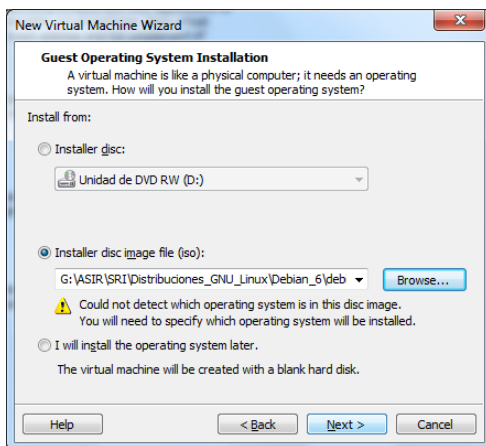
INSTALACIÓN DE DIFERENTES SISTEMAS OPERATIVOS LINUX EN UNA MÁQUINA VIRTUAL

Instalación de Debian en una máquina Virtual

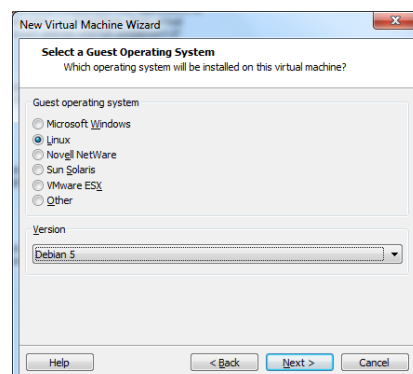
En primer lugar abrimos la máquina Virtual donde la instalaremos, esto va a ser igual en todos los Sistemas Operativos.

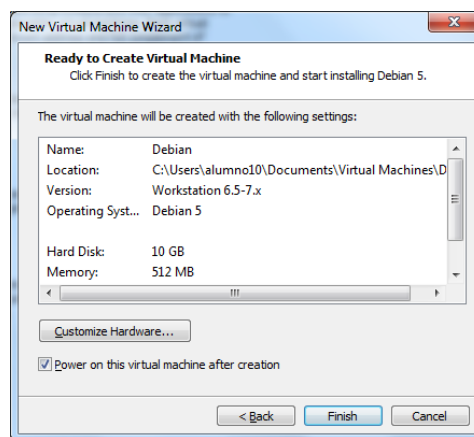
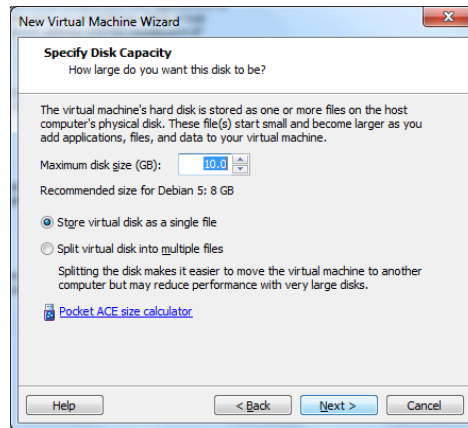
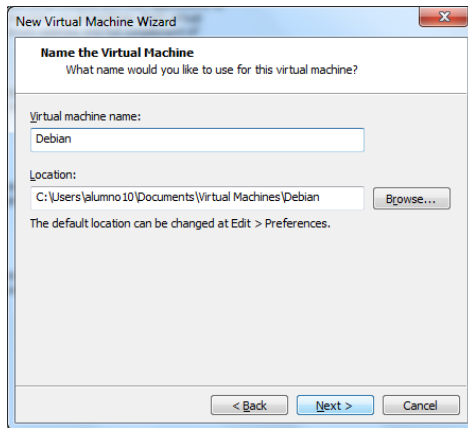


En la instalación elegimos la ubicación donde está la imagen, y aceptamos

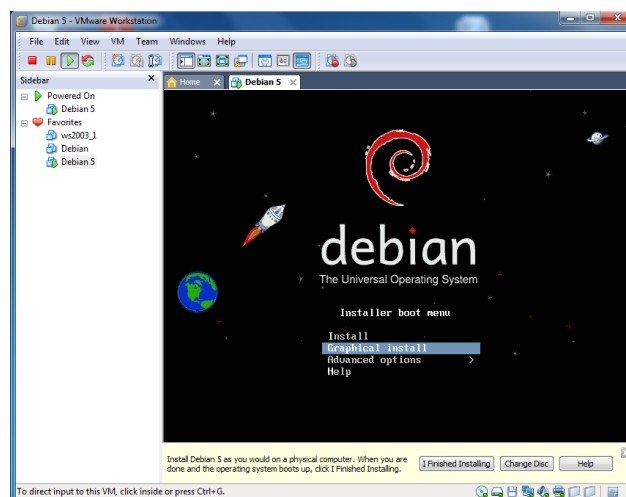


Elegimos el sistema y la versión

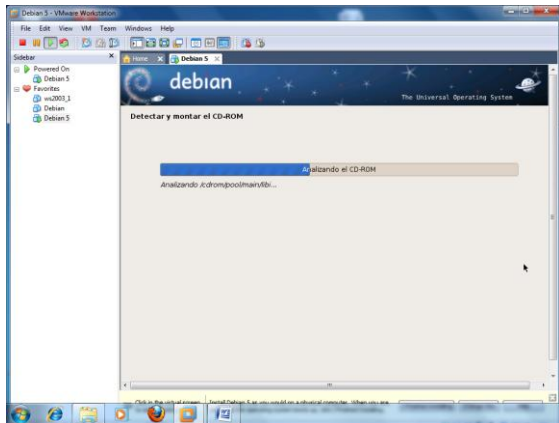
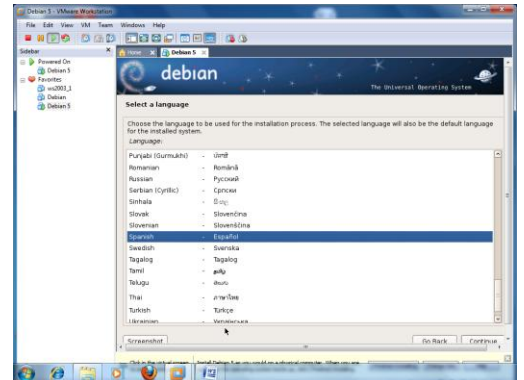




Hasta este proceso es todo igual en todos los Sistemas Operativos que vamos a instalar

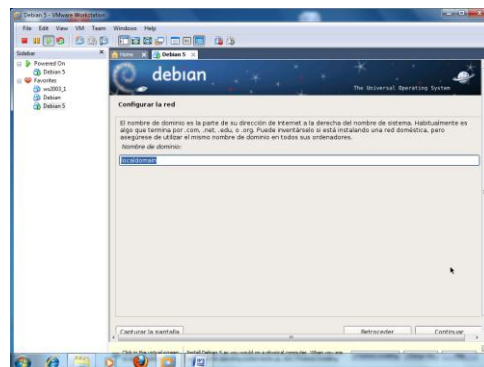
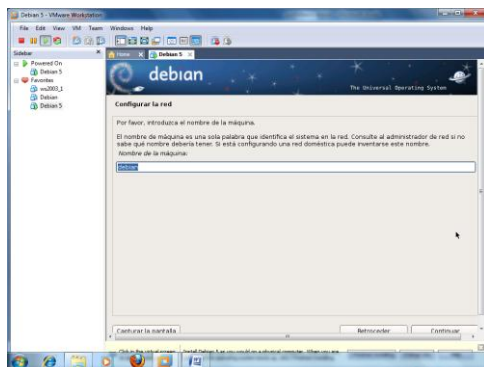


Elegimos el idioma que queremos en nuestro caso español

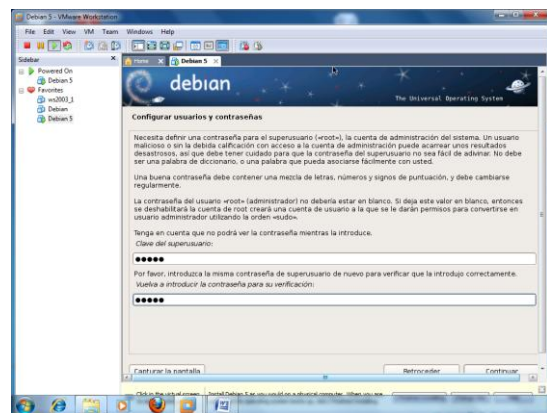
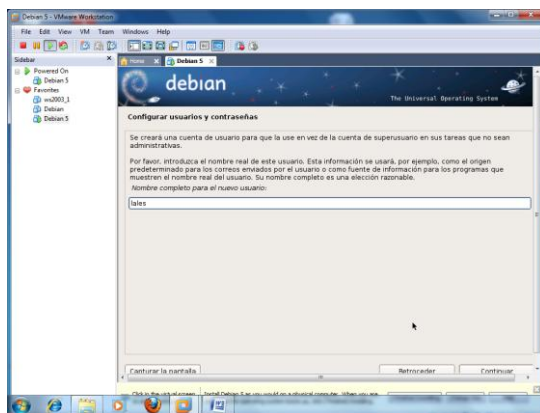


Y seguimos los pasos dándole a siguiente

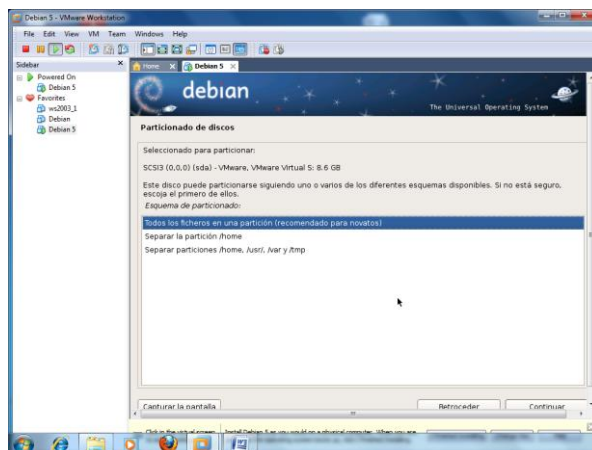
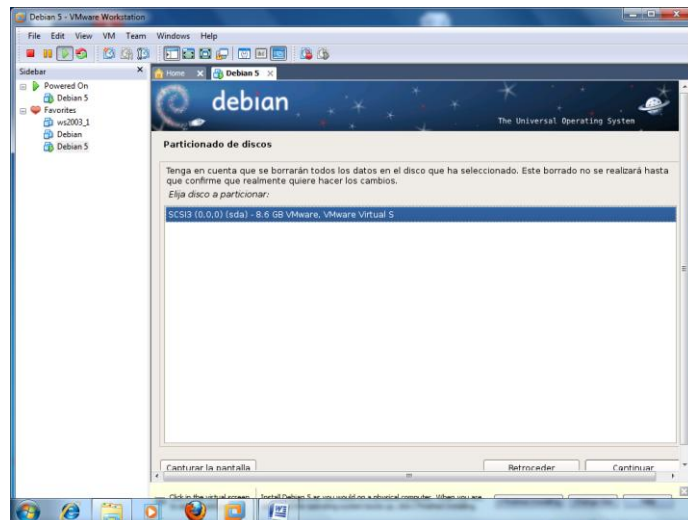
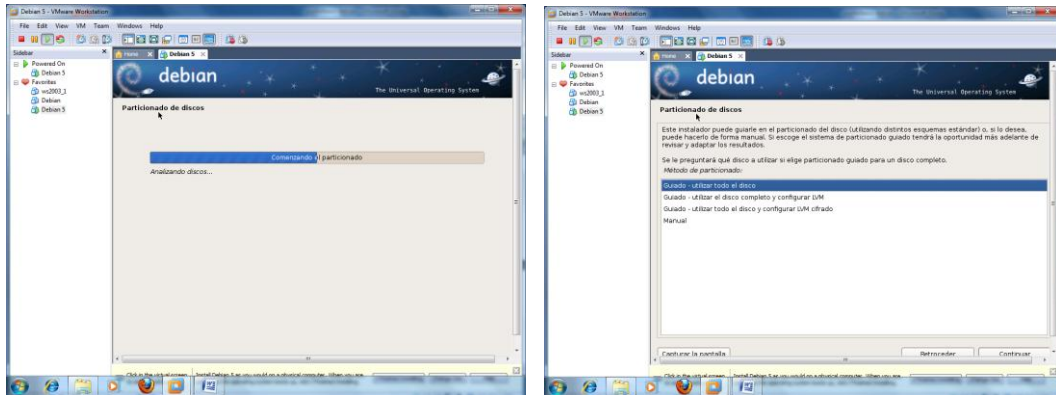
Elegimos el nombre de la red, que te viene Debian por defecto

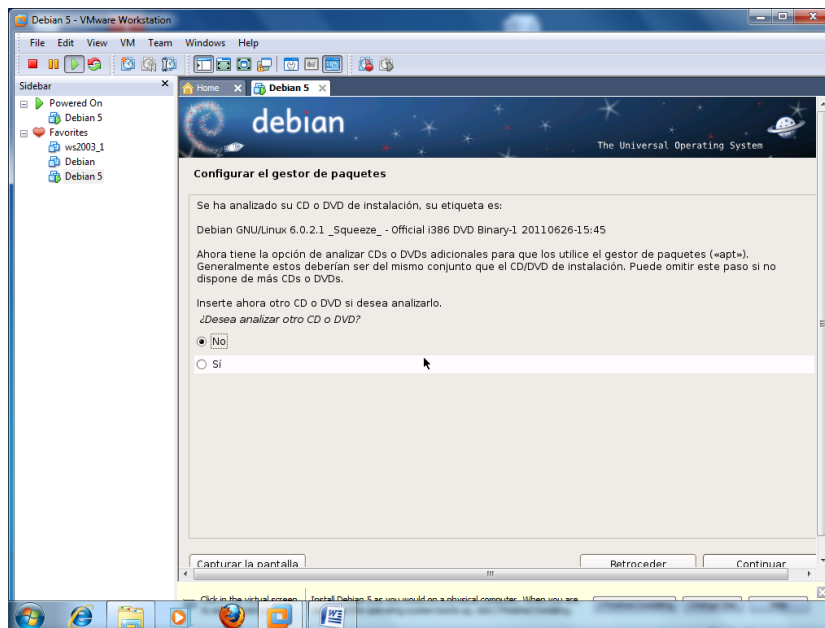
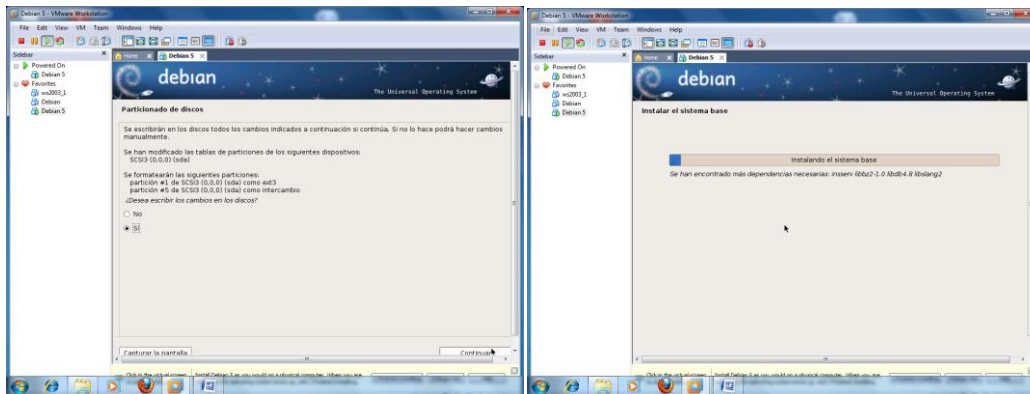
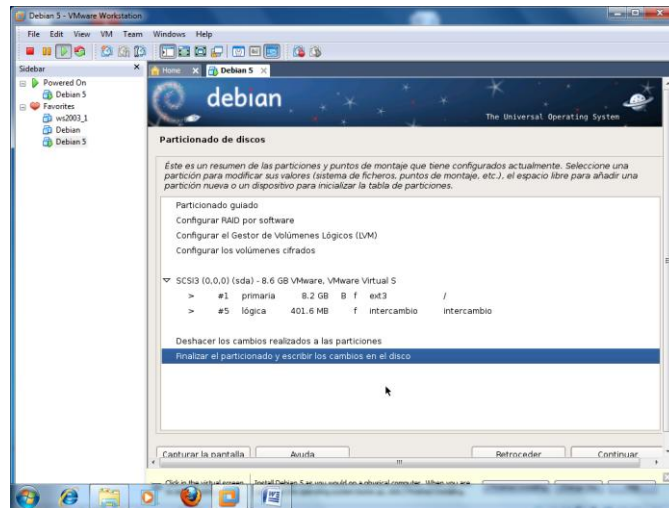


Y elegimos un nombre de usuario y contraseña

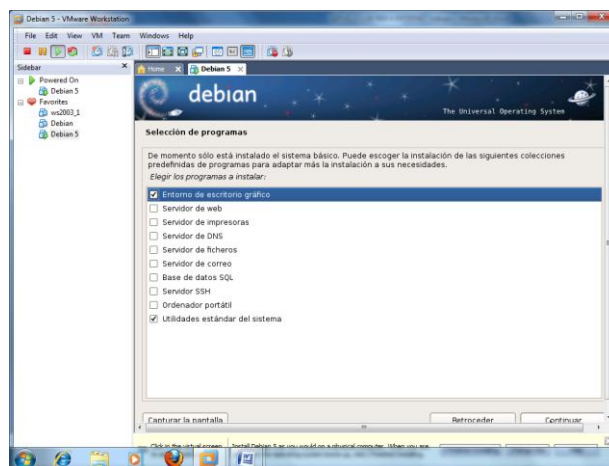
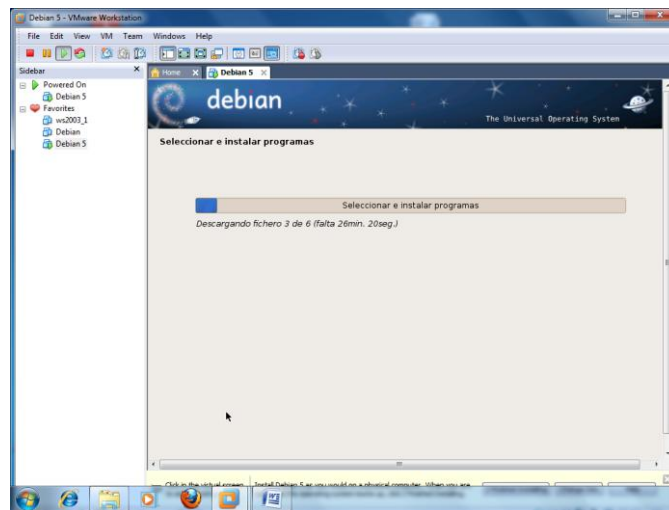


Elegimos donde se va a hacer la instalación, todo elegimos lo que nos da la máquina por defecto.





Después de varias pantallas aceptando la configuración que te da la máquina por defecto, empieza la instalación



Y este es el escritorio de Debian

