Seguridad y Alta Disponibilidad

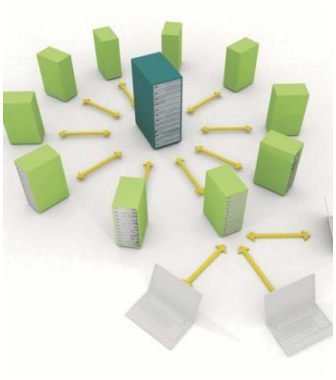
ÍNDICE

IMPLANTACIÓN DE SOLUCIONES DE ALTA DISPONIBILIDAD

1. Análisis de configuraciones de alta disponibilidad:

1.1. Alta disponibilidad:

a) Concepto



Alta disponibilidad (High availability) 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.

La alta disponibilidad consiste en una serie de medidas tendientes a garantizar la disponibilidad del servicio, es decir, asegurar que el servicio funcione durante las veinticuatro horas.

El término "disponibilidad" hace referencia a la probabilidad de que un servicio funcione adecuadamente en cualquier momento.

El término "fiabilidad", que se utiliza en algunos casos, se refiere a la probabilidad de que un sistema funcione normalmente durante un período de tiempo dado. Esto se denomina "continuidad del servicio".

b) Funcionamiento ininterrumpido.

TIEMPO DE INACTIVIDAD.

Típicamente tiempo de inactividad planificado es un resultado del mantenimiento que es perjudicial para la operación del sistema y usualmente no puede ser evitado con la configuración del sistema actualmente instalada. Eventos que generan tiempos de inactividad planificados quizás incluyen parches al software del sistema que requieran un rearranque o cambios en la configuración del sistema que toman efecto después de un rearranque. En general el tiempo de inactividad planificado es usualmente el resultado de un evento lógico o de gestión iniciado.

Tiempos de inactividad no planificado surgen de algún evento físico tales como fallos en elhardware o anomalías ambientales. Ejemplos de eventos con tiempos de inactividad no planificados incluyen fallos de potencia, fallos en los componentes de CPU o RAM, una caída por recalentamiento, una ruptura lógica o física en las conexiones de red, rupturas de seguridad catastróficas o fallos en el sistema operativo, aplicaciones y middleware.

Muchos puestos computacionales excluyen tiempo de inactividad planificado de los cálculos de disponibilidad, asumiendo, correcta o incorrectamente, que el tiempo de actividad no planificado tiene poco o ningún impacto sobre la comunidad de usuarios computacionales. Excluyendo tiempo de inactividad planificado, muchos sistemas pueden reclamar tener alta disponibilidad fenomenal, la cual da la ilusión de disponibilidad continua. Sistemas que exhiben verdadera disponibilidad continua son comparativamente raros y caros, y ellos tienen diseños cuidadosamente implementados que eliminan cualquier punto de fallo y permiten que el hardware, la red, el sistema operativo, middleware y actualización de aplicaciones, parches y reemplazos se hagan en línea.

CÁLCULOS PORCENTUALES.

Disponibilidad es usualmente expresada como un porcentaje del tiempo de funcionamiento en un año dado. En un año dado, el número de minutos de tiempo de inactividad no planeado es registrado para un sistema, el tiempo de inactividad no planificado agregado es dividido por el número total de minutos en un año (aproximadamente 525.600) produciendo un porcentaje de tiempo de inactividad; el complemento es el porcentaje de tiempo de funcionamiento el cual es lo que denominamos como disponibilidad del sistema. Valores comunes de disponibilidad, típicamente enunciado como número de "nueves" para sistemas altamente disponibles son:

- 99,9% = 43.8 minutos/mes u 8,76 horas/año ("tres nueves")
- 99,99% = 4.38 minutos/mes o 52.6 minutos/año ("cuatro nueves")
- 99,999% = 0.44 minutos/mes o 5.26 minutos/año ("cinco nueves")

Es de hacer notar que tiempo de funcionamiento y disponibilidad no son sinónimos. Un sistema puede estar en funcionamiento y no disponible como en el caso de un fallo de red. Se puede apreciar que estos valores de disponibilidad son visibles mayormente en documentos de ventas o marketing, en lugar de ser una especificación técnica completamente medible y cuantificable.

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 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

c) Integridad de datos y recuperación de servicio.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro.

Es preciso anotar, además, que la seguridad no es ningún hito, es más bien un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se ciñen sobre cualquier información, teniendo siempre en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener. Una vez conocidos todos estos puntos, y nunca antes, deberán tomarse las medidas de seguridad oportunas.

La integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) Grosso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información.

Integridad de datos en general: hace referencia a que todas las características de los datos (reglas, definiciones, fechas, etc.) deben ser correctos para que los datos estén completos.

Los mecanismos de autenticación hacen referencia a las funciones que permiten confirmar la identidad (integridad) de la entidad o entidades pares que se comunican. Sin embargo los mecanismos de integridad hacen referencia a las funciones que permiten confirmar la corrección de los datos intercambiados entre las entidades pares. Los mecanismos de integridad pueden estar basados o utilizar técnicas similares al control de errores.

La integridad de datos es un aspecto central en todos los protocolos de comunicaciones. Tanto en comunicaciones orientadas a conexión como no orientadas a conexión es común el uso de un código de redundancia para la protección de la cabecera o la unidad de datos del protocolo (PDU) completa intercambiada entre entidades pares. Además, en las comunicaciones orientadas a conexión se suelen usar números de secuencia para asegurar que las unidades de datos no sufren pérdidas, duplicaciones o desórdenes.

Estos mecanismos intrínsecos a los propios protocolos de comunicaciones pueden ser utilizados como mecanismos de integridad. Por ejemplo, si el código de redundancia de una unidad de datos del protocolo (UDP) es encriptada entonces un intruso podría modificar la UDP pero no podría modificar el código de redundancia para hacerlo conforme a los cambios. La entidad receptora podría detectar el error entre el código de redundancia recibido y el calculado y concluir que hubo una violación de la integridad de los datos. Igualmente, el uso de números de secuencia encriptados protege a las unidades de intercambiadas de las retransmisiones, borrado o desorden. Otras técnicas a considerar serían el uso de sellos de tiempo e identificadores de uso único.

El servicio de integridad asegura que datos son recibidos exactamente a como han sido enviados por una entidad autorizada, es decir sin duplicaciones, retransmisiones, modificaciones o inserciones.

Cuando se detecta una violación en la integridad de los datos el servicio de integridad puede o bien avisar de que se ha producido este hecho o utilizar mecanismos para la recuperación de la perdida de integridad de los datos. Así se han definido las siguientes modalidades del servicio.

1. Integridad orientada a conexión con mecanismos de recuperación: Proporciona la integridad de todos las unidades de datos de usuario de una comunicación orientada a conexión de nivel N y detecta cualquier modificación, inserción, borrado o retransmisión de cualquier unidad de datos dentro de una secuencia entera de unidad de datos del servicio (UDS) haciendo uso de mecanismos de recuperación de la integridad si fuera necesario. El uso de este servicio junto con el servicio de autenticación de entidad par proporciona un alto grado de protección frente a la mayoría de ataques activos.

2. Integridad orientada a conexión sin mecanismos de recuperación: Este servicio es semejante al anterior con la diferencia de que en este caso sólo se detecta las violaciones en la integridad de los datos pero no se articulan mecanismos de recuperación de la integridad.

3. Integridad orientada a conexión sobre campos selectivos: Este servicio asegura la integridad de campos específicos dentro de las unidades de datos de usuario de nivel N en una comunicación orientada a una conexión y toma una determinación de si los campos seleccionados han sido modificados, insertados, borrados o retransmitidos.

4. Integridad no orientada a conexión: Este servicio asegura la integridad de una sola unidad de datos del servicio (UDS) en comunicaciones no orientadas a conexión teniendo alguna forma de detección de la modificación de una UDS.

Adicionalmente también pueden existir algunos mecanismos que garanticen la detección de retransmisiones.

5. Integridad no orientada a conexión sobre campos selectivos: Este servicio asegura la integridad de campos específicos dentro de una sola unidad de datos del servicio (UDS) en comunicaciones no orientadas a conexión. Este servicio toma alguna determinación si los campos seleccionados han sido modificados.

2. Soluciones de alta disponibilidad:

2.1. Servidores redundantes. RAID.

Los sistemas redundantes, en ingeniería de computadores, son aquellos en los que se repiten aquellos datos o hardware de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir por su uso continuado.

Se presenta como una solución a los problemas de protección y confiabilidad. Este tipo de sistemas se encarga de realizar el mismo proceso en más de una estación, ya que si por algún motivo alguna dejara de funcionar o colapsara, inmediatamente otro tendría que ocupar su lugar y realizar las tareas del anterior.

Las técnicas de redundancia han sido usadas por la industria militar y aeroespacial por muchos años para alcanzar una alta confiabilidad. Una base de datos replicada es un ejemplo de sistema distribuido redundante.

En informática, el acrónimo RAID (del inglés Redundant Array of Independent Disks, conjunto redundante de discos independientes, hace referencia a un sistema de almacenamiento que usa múltiples discos duros o SSD entre los que distribuyen o replican los datos. Existen diferentes tipos de raid:

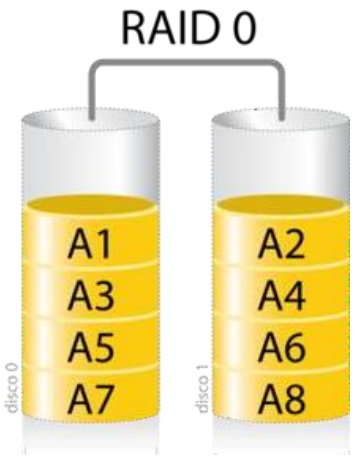
RAID 0

También llamado partición de los discos, los datos son distribuidos a través de discos paralelos. RAID 0 distribuye los datos rápidamente a los usuarios, pero no ofrece más protección a fallas de hardware que un simple disco.

El RAID 0 se usa normalmente para incrementar el rendimiento, aunque también puede utilizarse como forma de crear un pequeño número de grandes discos virtuales a partir de un gran número de pequeños discos físicos.

Una buena implementación de un RAID 0 dividirá las operaciones de lectura y escritura en bloques de igual tamaño, por lo que distribuirá la información equitativamente entre los dos discos.

Debido a su alta velocidad, pero hay que tener en cuenta de que, si un disco rompe, se pierde absolutamente TODA la información de TODOS los discos.



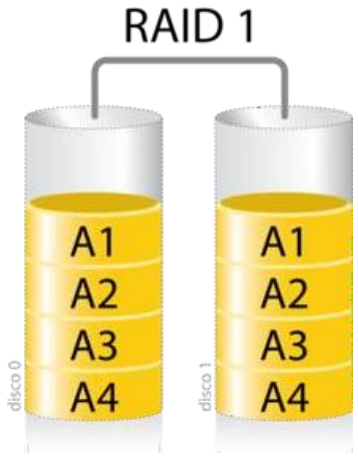
RAID 1

También llamado Disk espejo provee la más alta medida de protección de datos a través de una completa redundancia. Los datos son copiados a dos discos simultáneamente. La disponibilidad es alta pero el costo también dado que los usuarios deben comprar dos veces la capacidad de almacenamiento que requieren.

Esto resulta útil cuando el rendimiento en lectura es más importante que la capacidad.

Adicionalmente, dado que todos los datos están en dos o más discos, con hardwarehabitualmente independiente, el rendimiento de lectura se incrementa aproximadamente comomúltiplo lineal del número de las copias; es decir, un RAID 1 puede estar leyendo simultáneamente dos datos diferentes en dos discos diferentes, por lo que su rendimiento se duplica.

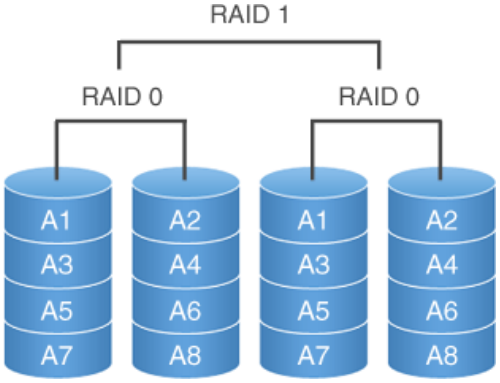
En caso de rotura de un disco, la información todavía está en el otro. Este el RAID que cualquier empresa por muy pequeña que sea debería de tener en su servidor de datos.



RAID 0+1

Combina Disk espejo y partición de datos. El resultado es gran disponibilidad al más alto desempeño de entrada y de salida para las aplicaciones de negocios más críticas. A este nivel como en el RAID 1 los discos son duplicados. Dado que son relativamente no costosos, RAID 0/1 es una alternativa para los negocios que necesitan solamente uno o dos discos para sus datos, sin embargo, el costo puede convertirse en un problema cuando se requieren más de dos discos.

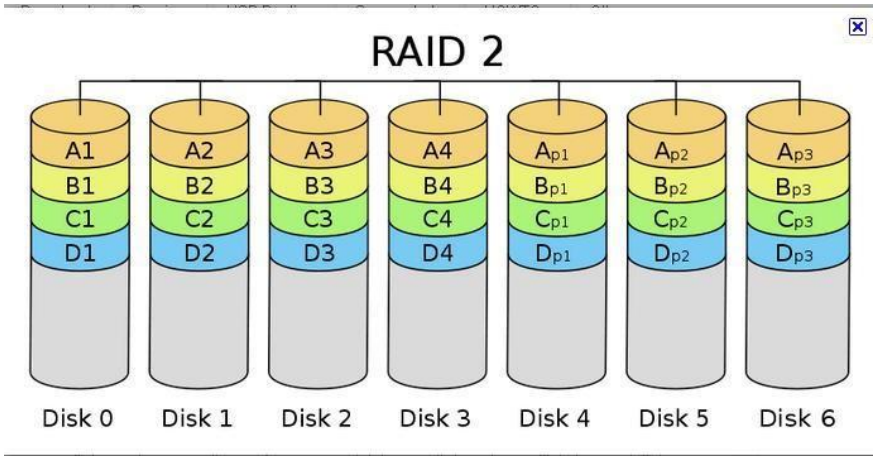
Combina el RAID 0 y el RAID 1. RAID (0+1) permite la perdida de múltiples discos debido a la redundancia de discos duros.



RAID 2

Un RAID 2 divide los datos a nivel de bits en lugar de a nivel de bloques y usa un código de Hamming para la corrección de errores. Los discos son sincronizados por la controladora para funcionar al unísono. Éste es el único nivel RAID original que actualmente no se usa. Permite tasas de trasferencias extremadamente altas.

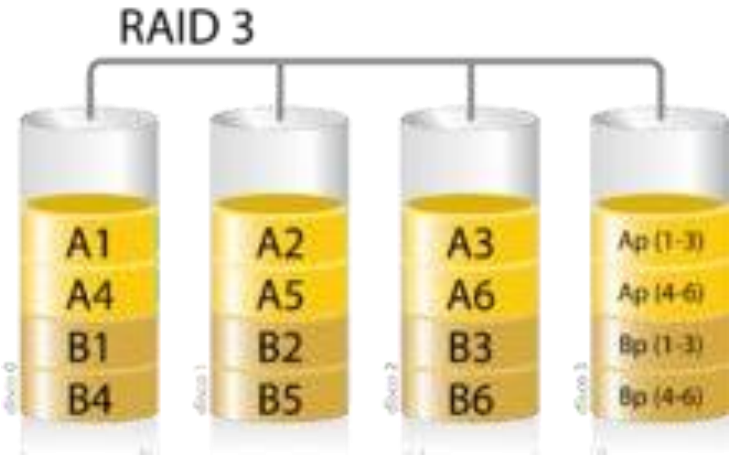
Teóricamente, un RAID 2 necesitaría 39 discos en un sistema informático moderno: 32 se usarían para almacenar los bits individuales que forman cada palabra y 7 se usarían para la corrección de errores.



RAID 3

Logra redundancia sin espejo completo. El flujo de los datos es particionado a través de todos los HD de datos en el arreglo. La información extra que provee la redundancia está escrita en un HD dedicado a la paridad. Si cualquier HD del arreglo falla, los datos perdidos pueden ser reconstruidos matemáticamente desde los miembros restantes del arreglo. RAID 3 es especialmente apropiado para procesamiento de imagen, colección de datos científicos, y otras aplicaciones en las cuales grandes bloques de datos guardados secuencialmente deben ser transferidos rápidamente.

El RAID 3 se usa rara vez en la práctica. Uno de sus efectos secundarios es que normalmente no puede atender varias peticiones simultáneas, debido a que por definición cualquier simple bloque de datos se dividirá por todos los miembros del conjunto, residiendo la misma dirección dentro de cada uno de ellos.

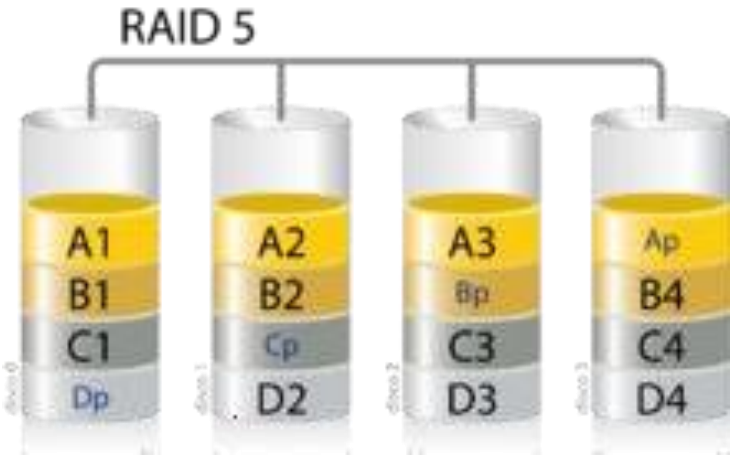


RAID 5

Todos los HD en el arreglo operan independientemente. Un registro entero de datos es almacenado en un solo disco, permitiendo al arreglo satisfacer múltiples requerimientos de entrada y salida al mismo tiempo. La información de paridad está distribuida en todos los discos, aliviando el cuello de botella de acceder un solo disco de paridad durante operaciones de entrada y salida

concurrentes. RAID 5 está bien recomendado para procesos de transacciones on-line, automatización de oficinas, y otras aplicaciones caracterizadas por gran número de requerimientos concurrentes de lectura. RAID 5 provee accesos rápidos a los datos y una gran medida de protección por un costo más bajo que el Disk espejo.

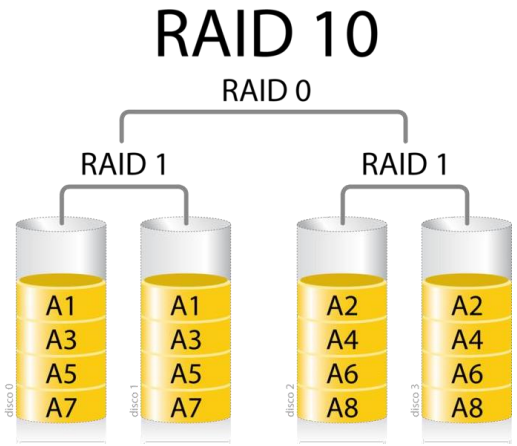
El RAID 5 ha logrado popularidad gracias a su bajo coste de redundancia. Generalmente, el RAID 5 se implementa con soporte hardware para el cálculo de la paridad. RAID 5 necesitará un mínimo de 3 discos para ser implementado.



RAID 10

La información se distribuye en bloques como en RAID-0 y adicionalmente, cada disco se duplica como RAID-1, creando un segundo nivel de arreglo. Se conoce como "striping de arreglos duplicados". Se requieren, dos canales, dos discos para cada canal y se utiliza el 50% de la capacidad para información de control. Este nivel ofrece un 100% de redundancia de la información y un soporte para grandes volúmenes de datos, donde el precio no es un factor importante. Ideal para sistemas de misión crítica donde se requiera mayor confiabilidad de la información, ya que pueden fallar dos discos inclusive (uno por cada canal) y los datos todavía se mantienen en línea. Es apropiado también en escrituras aleatorias pequeñas.

El RAID 10 es a menudo la mejor elección para bases de datos de altas prestaciones, debido a que la ausencia de cálculos de paridad proporciona mayor velocidad de escritura.



2.2. Sistemas de «clusters».

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 cluster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios en cualquiera de las otras máquinas del cluster (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 cluster, 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 cluster, el software de alta disponibilidad es capaz de arrancar automáticamente los servicios que han fallado en cualquiera de las otras máquinas del cluster. 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 cluster de alta disponibilidad con un cluster 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 Cluster Beowulf), mientras que el primer tipo de cluster 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 puede 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 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:

Disponibilidad = MTTF / (MTTF + 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.

2.3. SAN, NAS, FiberChannel.

a) SAN.

Una red de área de almacenamiento, en inglés SAN (storage area network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida, segura y fiable los distintos elementos que la conforman.

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. La mayoría de las SAN actuales usan 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 tradicionalmenteen 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.

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.

Las SAN se componen de tres capas:

- **Capa Host**. Esta capa consiste principalmente en Servidores, dispositivos ó componentes (HBA, GBIC, GLM) y software (sistemas operativos).

- **Capa Fibra**. Esta capa la conforman los cables (Fibra óptica) así como los SAN Hubs y los SAN switches como punto central de conexión para la SAN.

- **Capa Almacenamiento**. Esta capa la componen las formaciones de discos (Disk Arrays, Memoria Caché, RAIDs) y cintas empleados para almacenar datos.

La red de almacenamiento puede ser de dos tipos:

- **Red Fibre Channel**. La red Fibre Channel es la red física de dispositivos Fibre Channel que emplea Fibre Channel Switches y Directores y el protocolo Fibre Channel Protocol (FCP) para transporte (SCSI-3 serial sobre Fibre Channel).

- **Red IP**. Emplea la infraestructura del estándar LAN con hubs y/o switches Ethernet interconectados. Una SAN IP emplea iSCSI para transporte (SCSI-3 serial sobre IP)

b) NAS.

NAS (del inglés Network Attached Storage) es el nombre dado a una tecnología de almacenamiento dedicada a compartir la capacidad de almacenamiento de un ordenador (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, FTPo TFTP.

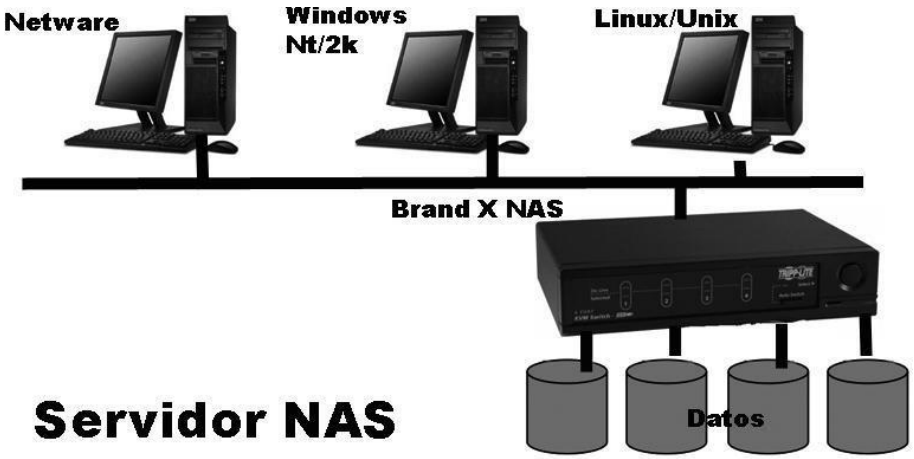
Generalmente, los sistemas NAS son dispositivos de almacenamiento específicos a los que se accede desde los equipos a través de protocolos de red (normalmente TCP/IP). También se podría considerar un sistema NAS a un servidor (Linux, Windows,...) que comparte sus unidades por red, pero la definición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

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

NAS es muy útil para proporcionar el almacenamiento centralizado a ordenadores clientes en entornos con grandes cantidades de datos. NAS puede habilitar sistemas fácilmente y con bajo costo con balance de carga, tolerancia a fallos y servidor web para proveer servicios de almacenamiento. El crecimiento del mercado potencial para NAS es el mercado de consumo donde existen grandes cantidades de datos multimedia.

El precio de las aplicaciones NAS ha bajado en los últimos años, ofreciendo redes de almacenamiento flexibles para el consumidor doméstico con costos menores de lo normal, con discos externos USB o FireWire.



c) FiberChannel.

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 pararedes 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

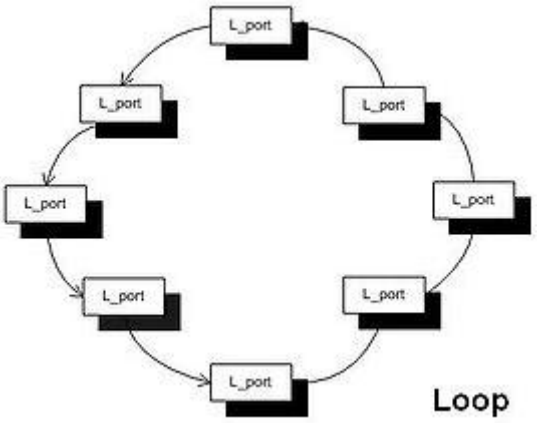
Un enlace en el canal de fibra consiste en dos fibras unidireccionales que transmiten en direcciones opuestas. Cada fibra está unida a un puerto transmisor (TX) y a un puerto receptor (RX). Dependiendo de las conexiones entre los diferentes elementos, podemos distinguir tres topologías principales de canal de fibra:

- **Punto a punto (FC-P2P).**

Dos dispositivos se conectan el uno al otro directamente. Es la topología más simple, con conectividad limitada a dos elementos.

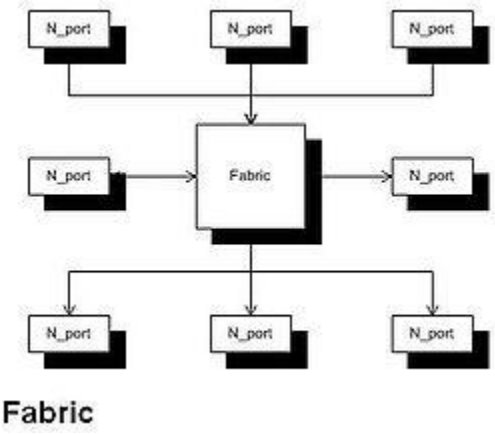
- **Anillo arbitrado (FC-AL).**

En este diseño, todos los dispositivos están en un bucle o anillo, similar a una red token ring. El añadir o quitar un elemento del anillo hace que se interrumpa la actividad en el mismo. El fallo de un dispositivo hace que se interrumpa el anillo. Existen concentradores de canal de fibra que conectan múltiples dispositivos entre sí y que pueden puentear los dispositivos que han fallado. Un anillo también se puede hacer conectando cada puerto al siguiente elemento formando el anillo. A menudo, un anillo arbitrado entre dos dispositivos negociará para funcionar como conexión P2P, pero ese comportamiento no es requerido por el standard.



- **Medio conmutado (FC-SW).**

Todos los dispositivos o bucles de dispositivos se conectan a conmutadores (switches) de canal de fibra, conceptualmente similares a las modernas implementaciones ethernet. Los conmutadores controlan el estado del medio físico, proporcionando interconexiones optimizadas



2.4. Balanceadores de carga.

Un balanceador de carga fundamentalmente es un dispositivo de hardware o software que se pone al frente de un conjunto de servidores que atienden una aplicación y, tal como su nombre lo indica, asigna o balancea las solicitudes que llegan de los clientes a los servidores usando algún algoritmo (desde un simple Round Robin hasta algoritmos más sofisticados).

Entre los fabricantes más populares de balanceadores por hardware se tiene a F5 y a Citrix.

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.

Balanceo de carga en servidores web.

Uno de los principales problemas de los mayores sitios web en Internet es cómo gestionar las solicitudes de un gran número de usuarios. Se trata de un problema de escalabilidad que surge con el continuo crecimiento del número de usuarios activos en el sistema.

Este servicio se puede brindar tanto con un enrutador como con una computadora con dos placas de red y software específico.

Hay balanceadores de carga tipo round-robin (uno a uno) y por pesos (que son capaces de saber cuál de los nodos está más libre y lanzarle la petición). El más conocido es LVS, sin embargo, hay otros, como el Red Hat Piranha.

Y en la plataforma para Windows Server se tiene al ISA Server (Microsoft Internet Security and Acceleration Server).

Existen softwares para el balance de carga, como "Wingate" en donde se pueden añadir dos redes y no es tan dificil de configurar.

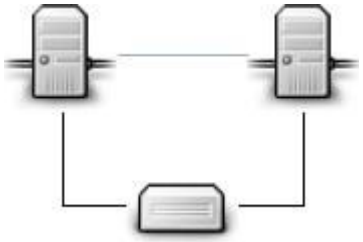
Clúster de balanceo de carga.

Un clúster de balanceo de carga o de cómputo adaptativo está compuesto por uno o más ordenadores (llamados nodos) que actúan como frontend del cluster, y que se ocupan de repartir las peticiones de servicio que reciba el cluster, a otros ordenadores del cluster que forman el back-end de éste. Un tipo concreto de cluster cuya función es repartir la carga de proceso entre los nodos en lugar de los servicios es el cluster openMosix.

Las características más destacadas de este tipo de cluster son:

- Se puede ampliar su capacidad fácilmente añadiendo más ordenadores al cluster.
- Robustez. Ante la caída de alguno de los ordenadores del cluster el servicio se puede ver mermado, pero mientras haya ordenadores en funcionamiento, éstos seguirán dando servicio.

3. Instalación y configuración de soluciones de alta disponibilidad.



En el mundo empresarial existen muchas aplicaciones que dada su naturaleza crítica deben proporcionar un servicio ininterrumpido de 24 horas al día, 7 días a la semana. Para conseguir estos niveles de disponibilidad se utiliza una configuración avanzada de hardware y software denominada en su conjunto Cluster De Alta Disponibilidad (HA, High Availability).

Esto implica que, en entornos de producción con cargas elevadas de trabajo, una parada del servicio tenga consecuencias mínimas para los usuarios, que podrán seguir trabajando de forma transparente, ya que este sistema tiene la capacidad de ofrecer el servicio asignado a las máquinas de forma continua, incluso en caso de fallo de una de ellas.

Paradójicamente, añadiendo más componentes al sistema total puede socavar esfuerzos para lograr alta disponibilidad. Esto es debido a que sistemas complejos tienen inherentemente más puntos de fallos potenciales y son más difíciles de implementar correctamente. La mayoría de los sistemas altamente disponibles extraen a un patrón de diseño simple: un sistema físicomultipropósito simple de alta calidad con redundancia interna comprensible ejecutando todas las funciones intedependientes emparejadas con un segundo sistema en una localización física separada.

Este clásico patrón de diseño es común entre instituciones financieras, por ejemplo. La industria de la informática y las comunicaciones ha establecido el Servicio Forum de la Disponibilidad acogerá la creación de productos de infraestructura de red, servicios y sistemas de alta disponibilidad. El mismo principio de diseño básico se aplica más allá de la informática en diversos campos como potencia nuclear, aeronáutica y cuidados médicos.

4. Virtualización de sistemas

En Informática, 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.1

Dicho de otra manera, se refiere a la abstracción de los recursos de un ordenador, llamado 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), 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 unsistema 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).

Existen diferentes formas de virtualización:

- Es posible virtualizar el hardware de servidor
- El software de servidor
- Virtualizar sesiones de usuario
- Virtualizar aplicaciones
- Crear máquinas virtuales en un equipo de escritorio.

4.1. Posibilidades de la virtualización de sistemas.

Los dos conceptos más importantes para entender qué es la virtualización son los de anfitrión e invitado. Ambos conceptos se refieren a nuestro sistema operativo, y por lo tanto deberíamos hablar de sistema operativo anfitrión y sistema invitado.

- El **anfitrión es el ordenador en el cual instalamos nuestro programa de virtualización** y que asignará o prestará determinados recursos de hardware a la máquina virtual que creemos.
- El **invitado es el ordenador virtual que hemos creado**, mediante nuestro programa de virtualización y al cual hemos asignado determinados recursos para funcionar.

Tipos de virtualización

La virtualización se puede hacer desde un sistema operativo Windows, ya sea XP, Vista u otra versión que sea compatible con el programa que utilicemos, en el que virtualizamos otro sistema operativo como Linux o viceversa, que tengamos instalado Linux y queramos virtualizar una versión de Windows.

Virtualización Hardware

La virtualización de hardware o plataforma de virtualización se refiere a la creación de unamáquina virtual que actúa como un verdadero ordenador con un sistema operativo. El Software ejecutado en estas máquinas virtuales se separa de los recursos de hardware subyacentes. Por ejemplo, un equipo que ejecuta Microsoft Windows puede alojar una máquina virtual que se parecea un ordenador con sistema operativo Ubuntu Linux, basada en Ubuntu, el software se puedeejecutar en la máquina virtual.

En la virtualización de hardware, la máquina host es la máquina real en la que la virtualización se lleva a cabo, y el equipo invitado es la máquina virtual. El anfitrión y el invitado las palabras se utilizan para distinguir el software que se ejecuta en la máquina real desde el software que se ejecuta en la máquina virtual. El software o firmware que crea una máquina virtual en el hardwaredel host que se llama hipervisor o monitor de máquina virtual.

Los diferentes tipos de virtualización de hardware incluyen:

Virtualización Completa: Virtualización en donde la máquina virtual simula un hardware suficiente para permitir un sistema operativo “huésped” sin modificar (uno diseñado para la misma CPU) para ejecutar de forma aislada.

Virtualización parcial: La máquina virtual simula múltiples instancias de gran parte (pero no de todo) del entorno subyacente del hardware, particularmente los espacios de direcciones. Tal entorno acepta compartir recursos y alojar procesos, pero no permite instancias separadas de sistemas operativos “huésped”.

Para virtualización Un entorno de hardware no es simulado, el software (los programas) clientes se ejecutan en sus propios equipos pero aislados, como si se estuvieran ejecutando en un sistema separado. Los programas de los huéspedes deben ser modificados específicamente para funcionar en este entorno.

Virtualización Escritorio

La virtualización de escritorio es el concepto de separar la virtualización en la máquina física anfitrión.Una forma de virtualización de escritorio, infraestructura de escritorio virtual (VDI), puede ser pensado como una forma más avanzada de virtualización de hardware: En lugar de interactuar directamente con un ordenador central a través de un teclado, ratón y monitor conectado a ella, el usuario interactúa con el ordenador anfitrión a través de una conexión de red (como una LAN inalámbrica a internet, wi-fi o incluso Internet) utilizando otro ordenador de sobremesa o un dispositivo móvil. Además, el equipo anfitrión en este escenario se convierte en un equipo servidor capaz de alojar múltiples máquinas virtuales al mismo tiempo para varios usuarios

Los clientes ligeros, que se ven en la virtualización de escritorio, son equipos simples y / o económicos que están diseñadas principalmente para conectarse a la red, sino que puede carecer de importante espacio de disco duro, memoria RAM o el poder, incluso el procesamiento.

Virtualización Memoria

Virtualización de la memoria, la agregación de los recursos de RAM de los sistemas en red en una sola agrupación de memoria.

La memoria virtual, es una técnica de administración de la memoria real que permite al sistema operativo brindarle al software de usuario y a sí mismo un espacio de direcciones mayor que la memoria real o física. Es decir permite asignar mayor memoria de trabajo, aislándola de la aplicación de la memoria física.

Virtualización Software

Virtualización a nivel de sistema operativo, el alojamiento de múltiples entornos virtualizados dentro de una única instancia de sistema operativo.

Virtualización de aplicaciones, el alojamiento de aplicaciones individuales en un entorno separado del sistema operativo subyacente.

Virtualización de servicios, emulando el comportamiento de los servicios que dependen de los componentes del sistema (por ejemplo, de terceros, en evolución, o no ejecutado) que son necesarios para el ejercicio de una aplicación bajo prueba (AUT) para fines de desarrollo o prueba. Enlugar de la virtualización de los componentes de todo, se virtualiza sólo partes específicas quedependen de forma fundamental para la ejecución de las tareas de desarrollo y pruebas.

Virtualización Almacenamiento

Proceso de abstraer el almacenamiento lógico del almacenamiento físico, y es comúnmente usado en SANs (Red de área de almacenamiento). Los recursos de almacenamiento físicos sonagregados al "storage pool" (almacén de almacenamiento), del cual es creado el almacenamiento lógico.

Sistema de archivos distribuido.

Almacenamiento hipervisors: En pack portátil de gestión centralizada, utilizado para mejorar el valor combinado de los sistemas de disco de almacenamiento múltiples, incluyendo los modelos diferentes e incompatibles, complementando sus capacidades individuales con el aprovisionamiento extendido, la réplica y la aceleración del rendimiento del servicio.

Virtualización Datos

La virtualización de datos, la presentación de datos como un nivel abstracto, independientemente de los sistemas de bases de datos subyacentes, las estructuras y de almacenamiento.

Virtualización de base de datos, el desacoplamiento de la capa de base de datos (lógica), que se encuentra entre el almacenamiento y las capas de aplicación dentro de la pila de aplicaciones.

Virtualización Red

Virtualización de la red, la creación de una red virtual espacio de direcciones dentro o a través de subredes de la red.

4.2. Herramientas para la virtualización.

Entre los principales proveedores de software que han desarrollado tecnologías de virtualización integrales (que abarcan todas las instancias: servidor, aplicaciones, escritorio) se encuentran, por ejemplo VMware y Microsoft. Estas compañías han diseñado soluciones específicas para virtualización, como VMware Server yWindows Server 2008 Hyper-V para la virtualización de servidores. Si bien la virtualización no es un invento reciente, con la consolidación del modelo de laComputación en la nube, la virtualización ha pasado a ser uno de los componentes fundamentales, especialmente en lo que se denomina infraestructura de nube privada.

Ejemplos

- VMware Workstation
- VMware Server
- Windows Server 2008 R2 Hyper-V
- Microsoft Enterprise Desktop Virtualization (MED-V)
- VirtualBox
- Parallels Desktop
- Virtual Iron
- Adeos
- Mac-on-Linux
- Win4BSD
- Win4Lin Pro
- y z/VM
- openvz
- Oracle VM
- XenServer
- Microsoft Virtual PC

VirtualBox . Entre los sistemas operativos soportados en VBox se encuentran la familia de Windows completa, entre los Linux soporta Debian, Fedora, Red Hat, Ubuntu, Gentoo, ArchLinux, Turbolinux, Mandriva, OpenSUSE, XandrOS, Oracle, entre otros; de la familia Sun a Solaris y Opensolaris; de los BSD a FreeBSD, OpenBSD y NetBSD; de OS/2 a Wrap e eComStation. VirtualBox soporta virtualización de hardwara tanto para Intel VT-x como para AMD-V. Los discos duros son emulados en una de estos tres formatos: VirtualBox Virtual Disk Image (VDI); VMware Virtual Machine Disk Format (VMDK); y Microsoft Virtual PC VHD. Esto significa que una máquina de VirtualBox puede usar discos que fueron creados en VMware o Microsoft Virtual PC, a parte de su propio formato nativo.

Xen es un hypervisor con soporte para las arquitecturas x86-64, Itanium, PowerPC 970, y IA-32. Puede ejecutar un buen número de sistemas operativos invitados en una sola máquina física de manera simultánea. Xen utiliza una forma de virtualización llamda paravirtualización, lo que significa que los invitados se ejecutan en un sistema operativo modificado usando una hiperllamada especial conocida como ABI en lugar de las características específicas de la arquitectura. Debido a esto Xen puede tener un gran performance incluso en hosts de arquitectura x86, la cual tiene inconvenientes conocidos con los procedimientos de virtualización tradicionales.

Basada en el kernel y el sistema operativo Linux, OpenVZ es una tecnología de virtualización a nivel de sistema operativo. Comparada con VirtualBox y Xen, es un poco más limitada porque requiere que tanto el anfitrión como los invitados sean Linux. OpenVZ cuenta con un servidor físico que ejecuta múltiples instancias de sistemas operativos aislados, conocidas como containers, son los Virtual Private Servers (VPSs), o Virtual Environments (VEs).
Cada container es una entidad aislada y funciona extensivamente como un servidor físico lo haría.

QEMU es un emulador de procesadores que depende de traducciones dinámicas para obtener velocidad mientras mantiene la probabilidad.Tiene soporte para emulación de varias arquitecturas, entre las que se encuentran IA-32 (x86) PCs, x86-64 PCs, MIPS R4000, Sun's SPARC sun4m, Sun's SPARC sun4u, ARM development boards, SH4 SHIX board, PowerPC, ETRAX CRIS y MicroBlaze. Conjuntamente con emulación de CPU, ofrece un conjunto de modelos de dispositivos, permitiendo ejecutar un amplio arreglo de sistemas invitados no modificados. QEMU además cuenta con un modo acelerado para soportar mixtas traducciones binarias del código del kernel y la ejecución nativa de código del usuario.

Bochs, propiedad de Mandriva, es un emulador portable de las arquitecturas x86 y x86-64 IBM PC, mayormente escrito en C++. Soporta emulación de procesador, memoria, discos, pantalla, red, Bios y otros periféricos comunes de las computadoras. Bochs es ampliamente usado por aficionados de los sistemas operativos, desarrollado desde que trae reporte de errores y archivos de volcado que otros no tienen.

Linux-VServer es un virtual private server mejorado con funcionalidades de virtualizacón de sistema operativo al kernel de Linux a través aislamiento a nivel del kernel mismo. Los Virtual private servers son típicamente usados en servicios de alojamiento web, donde son efectivos separando cuentas de clientes, puesta en común de recursos y encasillando cualquier posible brecha de seguridad. Linux-VServer es capaz de ejecutar múltiples máquinas virtuales a la vez, cada una aislada para grantizar la seguridad mientras se utilizan los recursos eficientemene.

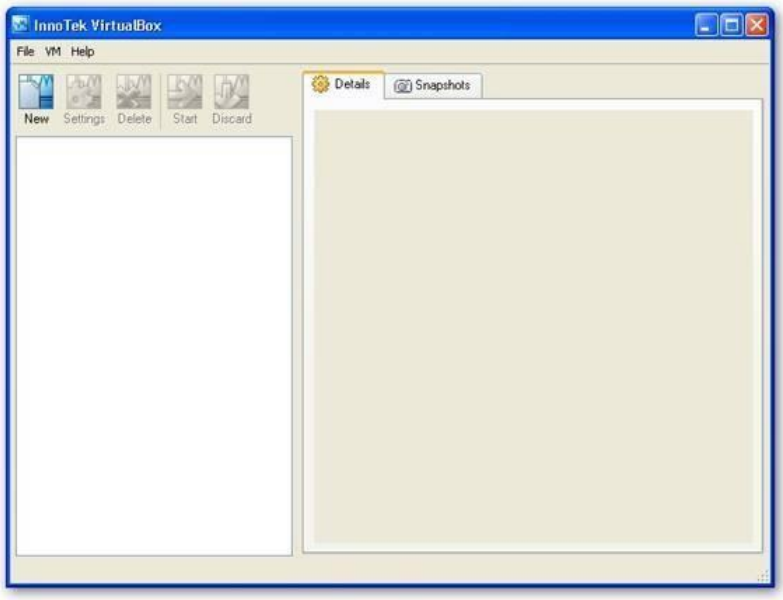
KVM es una infraestructura de virtualización del kernel Linux que posee virtualización nativa usando Intel VT-x o AMD-V. El soporte de paravirtualización está disponible para máquinas invitadas Linux y Windows usando el VirtIO framework, el cual incluye una tarjeta de red paravirtual, un controlador de disco, un balloon device para ajustar el uso de memoria, y gráficos VGA usando controladores VMware.

Cuando hablamos de virtualización no podemos dejar de incluir a VMware. VMware ofrece una serie de productos para virtualización como son VMware Workstation, VMware Server, VMware ESX, etc. Es una aplicación multiplataforma, pero también es empresarial, se ejecuta directamente en el servidor sin necesidad de periféricos adicionales.

4.3. Configuración y utilización de máquinas virtuales.

Crear una máquina virtual con VirtualBox

Una vez instalada la aplicación podemos comenzar a utilizarla. Al ejecutar VirtualBox se abre la ventana principal de la aplicación:

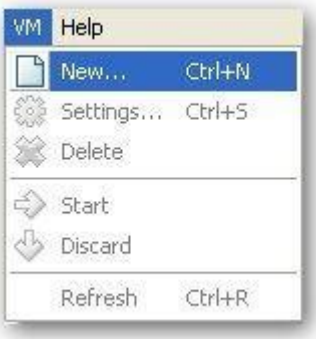


Ventana principal de VirtualBox

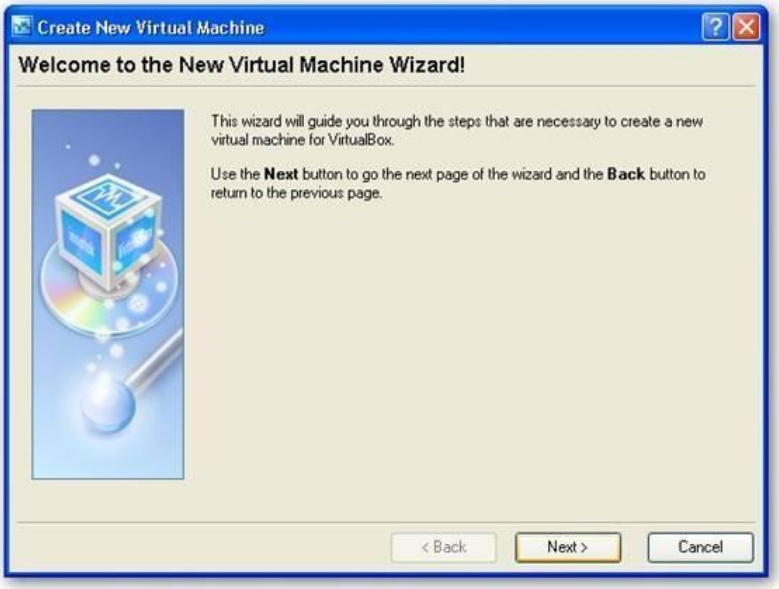
Lo primero que hay que hacer es crear la máquina virtual en la que instalaremos un sistema operativo, en este caso se tratará de una distribución de Linux, Ubuntu 6.10. Por cada sistema operativo que se desee emular con VirtualBox se debe crear una máquina virtual.

Para crear la máquina virtual se debe pulsar el botón *New* 

de la barra de herramientas o elegir esa misma opción en el menú *VM -> New*



Así aparecerá la ventana de bienvenida para la creación de una nueva máquina virtual.



Ventana de bienvenida a la creación de una nueva máquina virtual

Al pulsar en el botón *Next* aparece la ventana en la que se dará nombre a la máquina virtual que se va a crear y en la que se elige en la lista desplegable el tipo sistema operativo que se va a instalar.

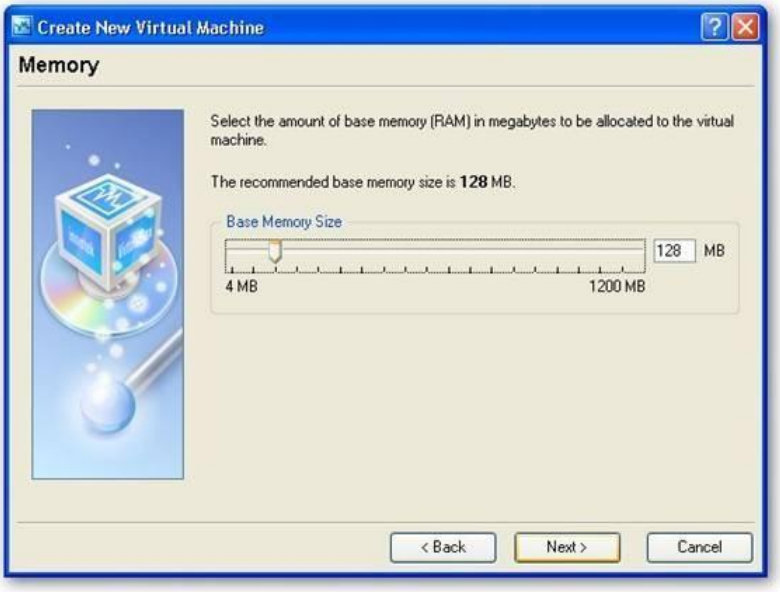
Lista de sistemas operativos que se pueden instalar en VirtualBox

El nombre de la máquina virtual puede ser cualquiera, en este caso la vamos a llamar *ubuntu* y en el tipo del sistema operativo, en este caso al tratarse de una distribución de Linux, se debe elegir la versión de kernel que tiene, para nuestro ejemplo *Linux 2.6*.

La elección del tipo de sistema operativo sirve para que VirtualBox nos muestre por defecto las opciones de memoria, espacio en disco duro, etc., que son mas adecuados para el S.O. a instalar. De todas formas estas opciones por defecto se pueden modificar en las siguientes ventanas de creación de la máquina virtual.

Ventana de definición del sistema operativo a instalar

En la siguiente ventana debemos elegir la memoria RAM necesaria, por defecto para el tipo de sistema operativo que vamos a instalar VirtualBox nos recomienda 128 MB. Hay que tener en cuenta que la memoria que se va a utilizar para la máquina virtual es parte de la memoria de la máquina real y si se elige demasiada el rendimiento tanto de la máquina real como la virtual se verán ralentizados.



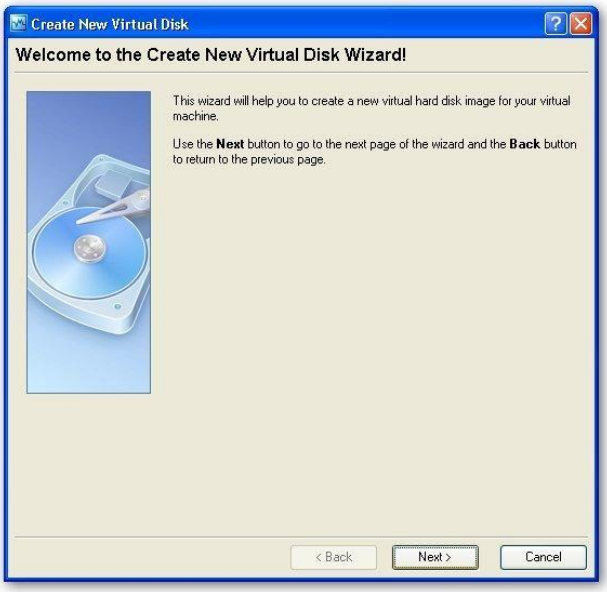
Ventana de elección de la memoria RAM de la máquina virtual

El siguiente paso es la elección del disco duro principal de la máquina virtual. Es importante destacar que los discos duros que utiliza la máquina virtual no son discos duros reales sino ficheros que VirtualBox gestiona. No debemos confundir las unidades de disco duro reales que tengamos enla máquina anfitriona con los discos duros usados por las máquinas virtuales.

En el proceso de elección del disco duro podemos elegir entre uno creado con anterioridad (botón *Existing*) o crear uno nuevo para la ocasión. Para facilitar la tarea al usuario, el proceso de creación de una máquina virtual dispone de un asistente para la elección del disco duro.

Ventana de elección del disco duro de la máquina virtual

A continuación procederemos a crear un disco duro desde cero. Para ello se debe pulsar el botón *New.* La primera ventana del asistente es la de bienvenida.



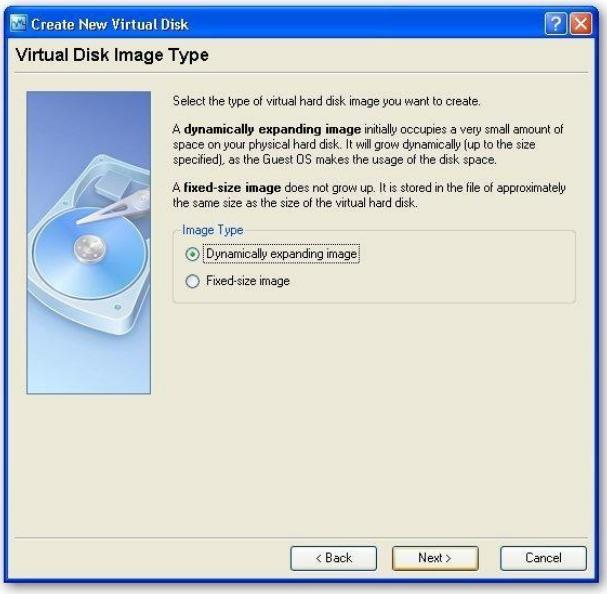
Asistente de creación de un disco duro para la máquina virtual

En la siguiente ventana se elegirá el tipo de disco duro. Podemos elegir entre dos opciones:

- **Tamaño dinámico:** el fichero real asociado al disco duro ocupará muy poco espacio, y se irá incrementando a medida que se ocupe el disco duro.
- **Tamaño fijo:** el fichero asociado ocupará todo el espacio del disco duro desde el principio.

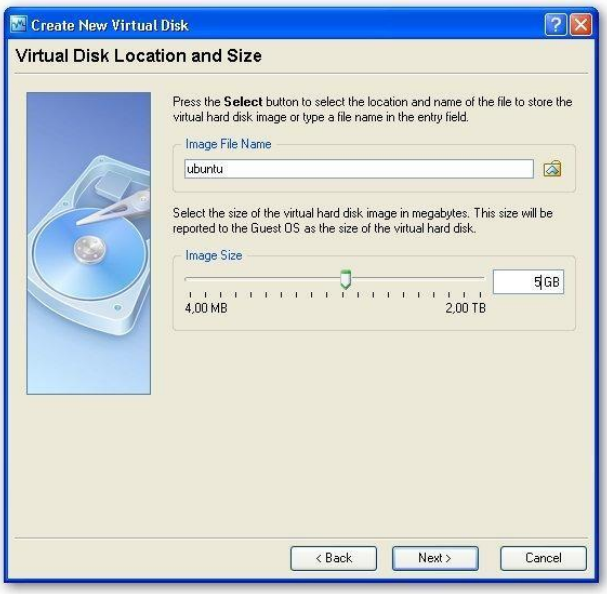
El tamaño dinámico permite usar menos espacio para la máquina virtual y no desperdiciar disco no utilizado. Sin embargo, es algo más lento puesto que VirtualBox debe gestionar el crecimiento del fichero.

Para nuestra máquina virtual vamos a elegir la opción por defecto de tamaño dinámico.



Ventana de elección del tipo de disco duro de la máquina virtual

En la última ventana del asistente para la creación del disco duro de la máquina virtual se elige el nombre del fichero donde se va a guardar y el tamaño del disco duro.

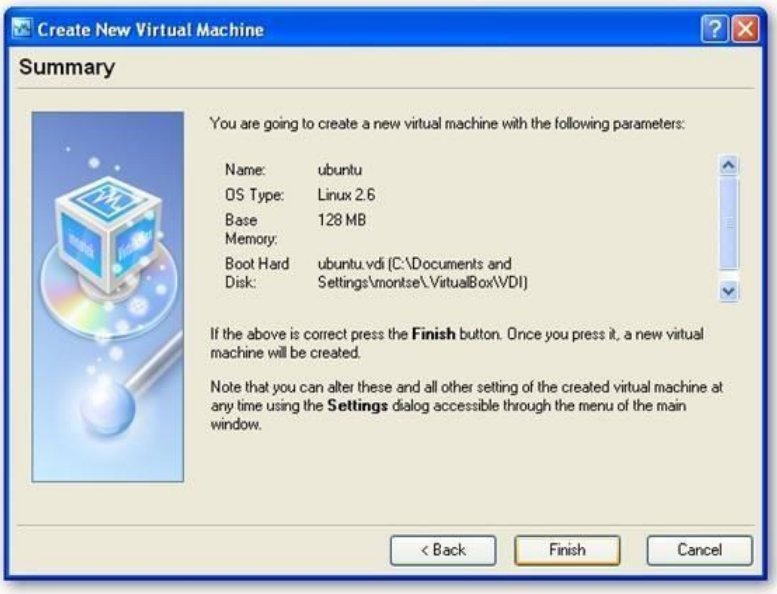


Ventana para elegir el tamaño y localización del disco duro de la máquina virtual

En la última ventana del asistente se nos muestra el resumen de características del disco duro virtual creado.

Ventana final del asistente para la creación de un disco duro para la máquina virtual

Al pulsar el botón *Finish* terminamos con la creación del disco duro virtual y aparece la ventana con el resumen de características de la máquina virtual creada.

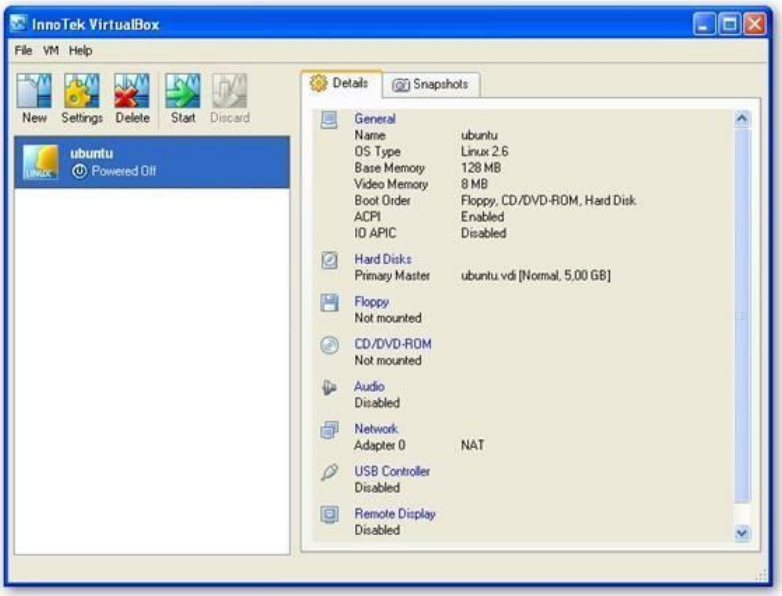


Ventana resumen de la máquina virtual creada

Así damos por finalizada la creación de la máquina virtual. Ahora en la ventana principal de VirtualBox aparece la nueva máquina virtual.

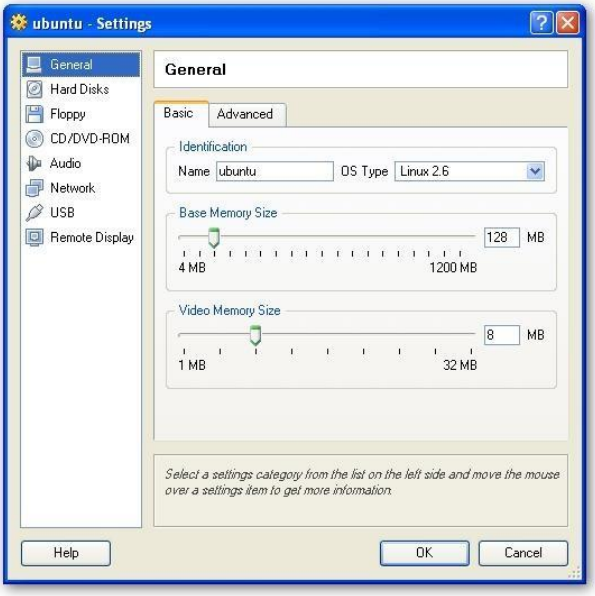
Modificando las características de la máquina virtual

Una vez creada la máquina virtual se pueden llevar a cabo, si se quiere, una serie de modificaciones en las opciones ya elegidas o en otras que VirtualBox elige por defecto.



Ventana de VirtualBox con la nueva máquina virtual creada

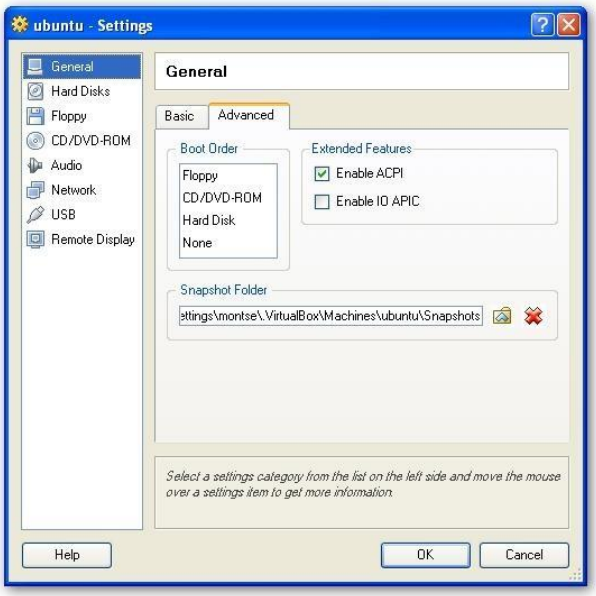
En la pestaña *Details* de la ventana principal de VirtualBox aparece todo lo relativo a la máquina virtual creada. Ya se ha visto que las principales características de la máquina (RAM, disco duro) se eligen en el proceso de su creación, pero hay otros detalles que se pueden cambiar después, por ejemplo, qué dispositivos físicos queremos que estén disponibles en la máquina virtual: audio, cdrom, usb, etc. Para ello se debe pulsar en cualquiera de los enlaces que aparecen en la parte derecha de la ventana (General, Hard Disks, Floppy,), de esta forma accedemos a la ventana de características de la máquina, ventana *Settings*.



Ventana de características de la máquina virtual: pestaña de parámetros básicos

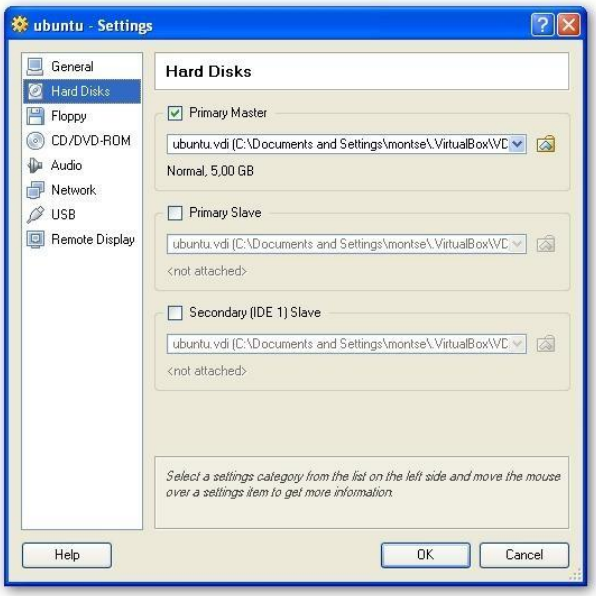
En la parte izquierda aparece el menú de la ventana y las distintas categorías que se pueden modificar. Comenzaremos con la ventana de parámetros generales.

La ventana de parámetros generales tiene dos pestañas: parámetros básicos y avanzados. En la pestaña de parámetros básicos se podrá revisar y modificar de nuevo el nombre y el sistema operativo de la máquina, la memoria RAM y se podrá asignar la memoria de video. Desde la pestaña de parámetros avanzados se podrá cambiar el orden de arranque de la máquina y activar características como la interfaz avanzada de configuración y energía (ACPI). Además se especificará eldirectorio en el que se guardarán las instantáneas de la máquina virtual, concepto este último que se explicará más adelante.



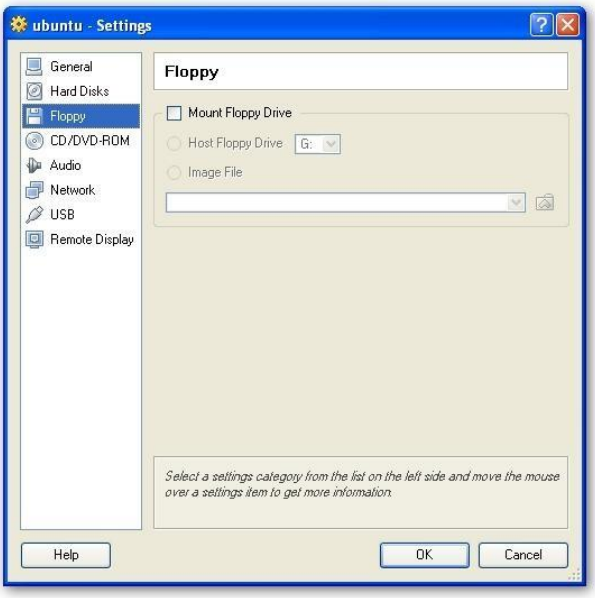
Ventana de características de la máquina virtual: pestaña de parámetros avanzados

La siguiente ventana será la configuración de discos duros. Como se puede observar, como disco duro principal aparece el que se configuró en el asistente. Desde aquí se podrán añadir dos más o cambiar los ya existentes.



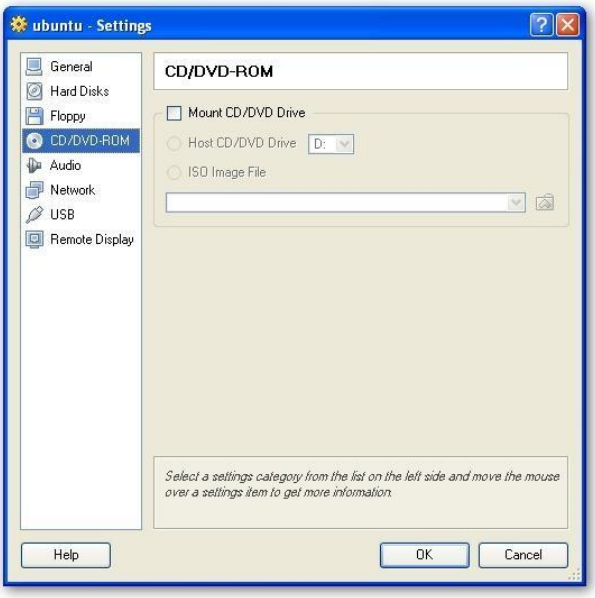
Ventana de características de la máquina virtual: configuración de discos duros

La siguiente característica a definir será el uso o no de floppy. Se puede elegir entre montar la unidad física o bien elegir una imagen de disco y montarla.



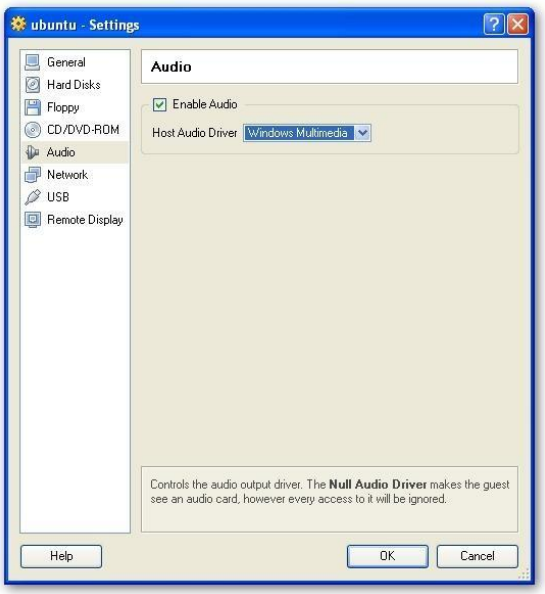
Ventana de características de la máquina virtual: configuración de floppy

La configuración del CD/DVD-ROM sigue el mismo esquema que la del floppy. Se puede elegir entre montar el dispositivo físico o montar una imagen. Este último caso es muy útil, puesto que muchas de las distribuciones de Linux se pueden encontrar en Internet en forma de imagen. Se podrían descargar, montar como CD-ROM e instalar sin necesidad de quemar un CD.



Ventana de características de la máquina virtual: configuración del CD/DVD-ROM

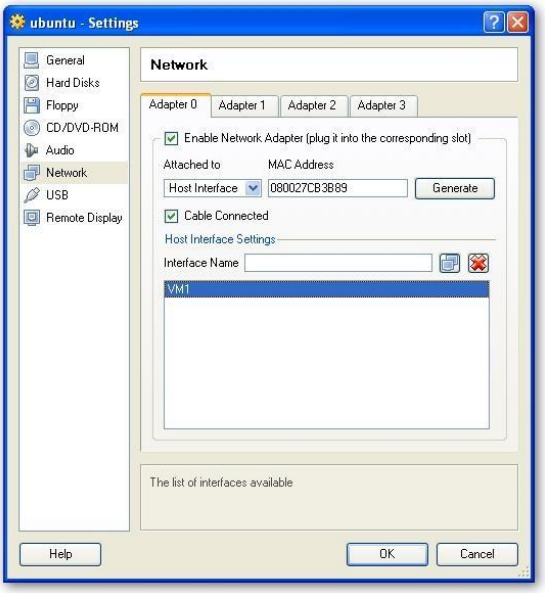
El siguiente parámetro a configurar será el sonido, que por defecto está deshabilitado. Si se quiere habilitar, se selecciona la casilla *Enable audio* y se elige el driver adecuado. Si el sistema operativo anfitrión es Windows, la elección del driver *Windows multimedia* suele dar un buen resultado.



Ventana de características de la máquina virtual: configuración del sonido

Pasemos al siguiente parámetro a configurar: la red. VirtualBox puede simular hasta cuatro tarjetas de red para cada máquina virtual instalada. Al usar el asistente, se habilita la primeramáquina virtual y se establece el protocolo NAT (Network Address Translation). De esta manera, la máquina virtual puede conectarse al mundo exterior usando la red del anfitrión, aunque el resto de las máquinas físicas conectadas a la red no serán capaces de verla a ella.

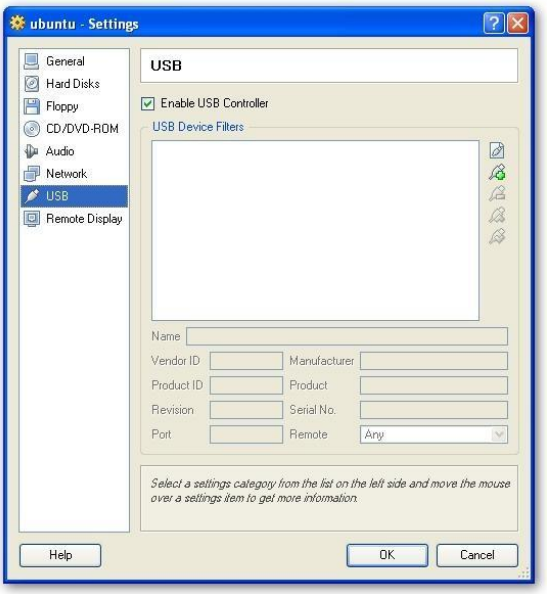
Otra forma de conectar la máquina virtual al mundo exterior es usar un interfaz de red en la máquina anfitriona que funcionará como una nueva tarjeta de red y que podrá usar la máquina virtual. Este nuevo interfaz de red se configura desde el anfitrión, y se usa desde la máquina virtual. Para crear un nuevo interfaz de red, se seleccionará *Host Interface* en el desplegable *Attached to*. Para crear un nuevo interfaz de red en el anfitrión, se le asigna un nombre en el cuadro de texto *Interface Name* y se pulsa el botón *Add new host interface*  Si todo va bien, se podrá comprobar cómo en las conexiones de red del anfitrión aparece una nueva.



Ventana de características de la máquina virtual: configuración de la red

Creación de un nuevo interfaz de red para la máquina virtual

La siguiente característica de interés es el soporte USB. Si se elige, se podrán utilizar los dispositivos USB de la máquina anfitriona. Se podrán decidir cuales usar y cuáles no, para no interferir en las máquinas, mediante el uso de filtros.



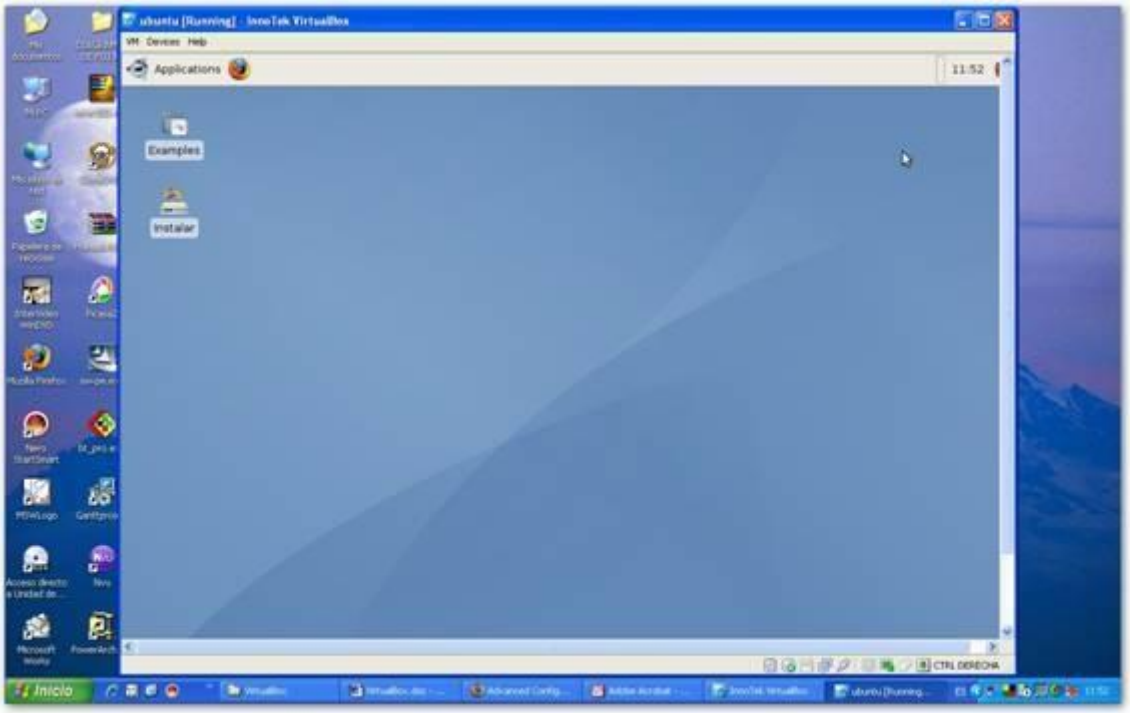
Ventana de características de la máquina virtual: configuración de los dispositivos USB

Una vez configurada la máquina virtual pulsamos el botón *OK* de la ventana de características y volvemos a la ventana principal de VirtualBox. Ahora ya se puede proceder a arrancarla pulsando el botón *Start* 

e instalar el nuevo sistema operativo, como si de una máquina real se tratara.

La máquina virtual en funcionamiento

Una vez creada la máquina virtual e instalado el sistema operativo, se puede trabajar con ella como si fuese un PC real.



Ventana de VirtualBox con una máquina virtual arrancada

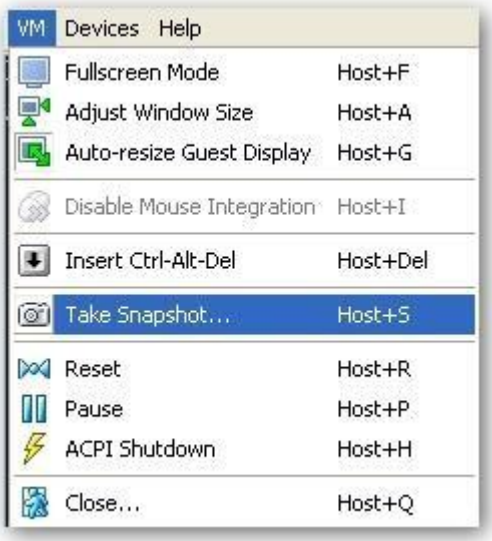
Cuando se pincha en la ventana de la máquina virtual, el ratón queda capturado por ella, es decir, el ratón se convierte en un dispositivo del PC virtual. Al arrancar la máquina virtual, aparece un cuadro de texto que nos lo advierte.

Ventana aviso sobre captura del ratón por parte de la máquina virtual

Para volver a liberar el ratón, se puede usar la llamada "host key", que por defecto es el botón ctrl. derecho del teclado. Al pulsarlo, se libera el ratón y vuelve a ser usado por el PC real.

Se puede controlar la máquina virtual desde los menús, pudiendo apagar la máquina, ejecutar un ctrl.+alt+sup, ejecutar un reset, o lo más importante, obtener una instantánea.

Una instantánea representa el estado de la máquina virtual en un momento determinado. Se puede obtener una instantánea de la máquina en cualquier momento, y de esta manera se puede volver a recuperar este mismo estado siempre que se quiera. Por ejemplo, una aplicación muy útil de las instantáneas es crear una justo antes de hacer alguna instalación con riesgo.



Menú VM de la máquina virtual arrancada

Para obtener una instantánea, se despliega el menú VM y se selecciona la entrada *Take snapshot* o bien se pulsa la tecla*host+S*.

A partir de este momento, sólo nos queda crear todas las máquinas virtuales que queramos y probar con ellas instalando programas, utilizando los dispositivos USB, navegando por la red, etc.

BIBLIOGRAFÍA

- http://es.wikipedia.org/wiki/Alta_disponibilidad
- http://es.kioskea.net/contents/surete-fonctionnement/haute-disponibilite.php3
- http://www.alegsa.com.ar/Dic/integridad%20de%20datos.php
- http://www.personal.fi.upm.es/~lmengual/ARQ_REDES/Arquitecturas_Seguridad.pdf
- http://es.wikipedia.org/wiki/Cl%C3%BAster_de_alta_disponibilidad
- http://es.wikipedia.org/wiki/Canal_de_fibra
- http://es.wikipedia.org/wiki/Balanceador_de_carga
- http://es.wikipedia.org/wiki/Balance_de_carga
- http://www.linalco.com/alta-disponibilidad-cluster-ha-linux.html
- http://es.wikipedia.org/wiki/Virtualizaci%C3%B3n
- http://www.genbeta.com/a-fondo/virtualizacion-introduccion-a-los-sistemas-virtualizados
- http://www.itnews.ec/marco/000039.aspx
- http://fraterneo.blogspot.com/2011/01/8-soluciones-para-virtualizacion-en.html
- http://recursostic.educacion.es/observatorio/web/es/component/content/articl