Implantación de soluciones de Alta Disponibilidad

Seguridad y Alta Disponibilidad

Autor: Miguel Ángel García Felipe

I.E.S GREGORIO PRIETO

UD 6: “Implantación de soluciones de Alta Disponibilidad”

ÍNDICE:

• 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 «clusters».
  - SAN, NAS, FiberChannel.
  - Balanceadores de carga.

- Instalación y configuración de soluciones de alta disponibilidad.

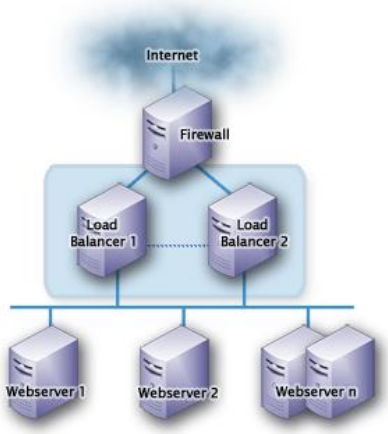
- Virtualización de sistemas:
  - Posibilidades de la virtualización de sistemas.
  - Herramientas para la virtualización.
  - Configuración y utilización de maquinas virtuales.

- Alta disponibilidad:

Concepto.

"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.

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.



Funcionamiento ininterrumpido.

Se refiere al término o las prácticas que permiten que un sistema no deje de estar operativo o en funcionamiento en ningún momento, esto supone, que en todo momento debe estar el sistema con disponibilidad absoluta.

Algunas de las técnicas de funcionamiento ininterrumpido son:

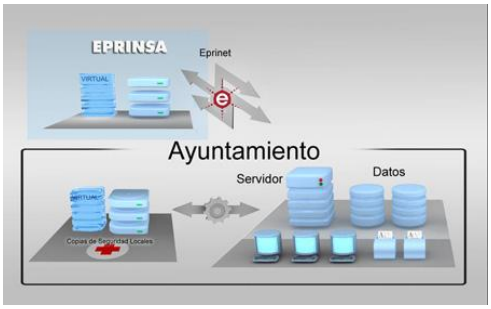
Centros de Respaldo.

Un centro de respaldo es un centro de procesamiento de datos (CPD) específicamente diseñado para tomar el control de otro CPD principal en caso de contingencia.

Grandes organizaciones, tales como bancos o Administraciones Públicas, no pueden permitirse la pérdida de información ni el cese de operaciones ante un desastre en su centro de proceso de datos. Terremotos, incendios o atentados en estas instalaciones

son infrecuentes, pero no improbables. Por este motivo, se suele habilitar un centro de respaldo para absorber las operaciones del CPD principal en caso de emergencia.

Un centro de respaldo se diseña bajo los mismos principios que cualquier CPD, pero bajo algunas consideraciones más. En primer lugar, debe elegirse una localización totalmente distinta a la del CPD principal con el objeto de que no se vean ambos afectados simultáneamente por la misma contingencia. Es habitual situarlos entre 20 y 40 kilómetros del CPD principal. La distancia está limitada por las necesidades de telecomunicaciones entre ambos centros.



En segundo lugar, el equipamiento electrónico e informático del centro de respaldo debe ser absolutamente compatible con el existente en el CPD principal. Esto no implica que el equipamiento deba ser exactamente igual. Normalmente, no todos los procesos del CPD principal son críticos. Por este motivo no es necesario duplicar todo el equipamiento. Por otra parte, tampoco se requiere el mismo nivel de servicio en caso de emergencia. En consecuencia, es posible utilizar hardware menos potente. La pecera de un centro de respaldo recibe estas denominaciones en función de su equipamiento:

- *Sala blanca*: cuando el equipamiento es *exactamente* igual al existente en el CPD principal.
- *Sala de back-up:* cuando el equipamiento es similar pero no exactamente igual.

En tercer lugar, el equipamiento software debe ser idéntico al existente en el CPD principal. Esto implica exactamente las mismas versiones y parches del software de base y de las aplicaciones corporativas que estén en explotación en el CPD principal. De otra manera, no se podría garantizar totalmente la continuidad de operación. Por último, pero no menos importante, es necesario contar con una réplica de los mismos datos con los que se trabaja en el CPD original. Este es el problema principal de los centros de respaldo. Existen dos políticas o aproximaciones a este problema:

- *Copia síncrona de datos*: Se asegura que todo dato escrito en el CPD principal también se escribe en el centro de respaldo antes de continuar con cualquier otra operación.
- *Copia asíncrona de datos:* No se asegura que todos los datos escritos en el CPD principal se escriban inmediatamente en el centro de respaldo, por lo que puede existir un desfase temporal entre unos y otros.

La copia asíncrona puede tener lugar fuera de línea. En este caso, el centro de respaldo utiliza la última copia de seguridad existente del CPD principal. Esto lleva a la pérdida de los datos de operaciones de varias horas (como mínimo) hasta días (lo habitual).

Esta opción es viable para negocios no demasiado críticos, donde es más importante la continuidad del negocio que la pérdida de datos. Por ejemplo, en cadenas de supermercados o pequeños negocios. No obstante, es inviable en negocios como la banca, donde es impensable la pérdida de una sola transacción económica.

En los demás casos, la política de copia suele descansar sobre la infraestructura de almacenamiento corporativo. Generalmente, se trata de redes SAN y cabinas de discos con suficiente inteligencia como para implementar dichas políticas. Tanto para la copia síncrona como asíncrona, es necesaria una extensión de la red de almacenamiento entre ambos centros. Es decir, un enlace de telecomunicaciones entre el CPD y el centro de respaldo. En caso de copia asíncrona es imprescindible que dicho enlace goce de baja latencia. Motivo por el que se suele emplear un enlace de fibra óptica, que limita la distancia máxima a decenas de kilómetros. Existen dos tecnologías factibles para la copia de datos en centros de respaldo:

- iSCSI.
- Fibre Channel.

Un centro de respaldo por sí sólo no basta para hacer frente a una contingencia grave. Es necesario disponer de un Plan de Contingencias corporativo. Este plan contiene tres subplanes que indican las medidas técnicas, humanas y organizativas necesarias en tres momentos clave:

- **Plan de respaldo:** Contempla las actuaciones necesarias *antes* de que se produzca un incidente. Esencialmente, mantenimiento y prueba de las medidas preventivas.
- **Plan de emergencia:** Contempla las actuaciones necesarias *durante* un incidente.
- **Plan de recuperación:** Contempla las actuaciones necesarias *después* de un incidente. Básicamente, indica cómo volver a la operación normal.

Sistemas de alimentación ininterrumpida

Un **sistema de alimentación ininterrumpida**, **SAI** (en inglés *Uninterruptible Power Supply*, ***UPS***), 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.
Los UPS dan energía eléctrica a equipos llamados cargas críticas, como pueden ser aparatos médicos, industriales o informáticos, incluso se utilizan en servidores y ordenadores de casi cualquier oficina o empresa, que requieren tener siempre

alimentación y que ésta sea de calidad, debido a la necesidad de estar en todo momento operativos y sin fallos (picos o caídas de tensión).

Tipos de sai.

Podemos distinguir tres tipos de SAI según su tipo de alimentación:

- **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.

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.

Tiempo de recuperación

Tiempo de recuperación esta cercanamente relacionado con la disponibilidad, que es el tiempo total requerido para un apagón planificado o el tiempo requerido para la recuperación completa de un apagón no planificado. Tiempo de recuperación puede ser infinito con ciertos diseños y fallos del sistema, recuperación total es imposible. Uno de tales ejemplos es un incendio o inundación que destruye un centro de datos y sus sistemas cuando no hay un centro de datos secundario para recuperación frente a desastres.

Disponibilidad de Datos

Es el grado para el cual las bases de datos y otros sistemas de almacenamiento de la información que registran y reportan fielmente transacciones del sistema. Especialistas de gestión de la información frecuentemente enfocan separadamente la disponibilidad de datos para determinar perdida de datos aceptable o actual con varios eventos de fracasos. Algunos usuarios pueden tolerar interrupciones en el servicio de aplicación pero no perdida de datos.

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.

Diseño de un sistema de alta disponibilidad

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 físico multipropósito** simple **de alta calidad con redundancia interna** comprensible **ejecutando todas las funciones** interdependientes 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.

- Soluciones de alta disponibilidad:

Servidores redundantes. RAID.

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. Dependiendo de su configuración (a la que suele llamarse «nivel»), los beneficios de un RAID respecto a un único disco son uno o varios de los siguientes: mayor integridad, mayor tolerancia a fallos, mayor rendimiento y mayor capacidad. En sus implementaciones originales, su ventaja clave era la habilidad de combinar varios dispositivos de bajo coste y tecnología más antigua en un conjunto que ofrecía mayor capacidad, fiabilidad, velocidad o una combinación de éstas que un solo dispositivo de última generación y coste más alto.

En el nivel más simple, un RAID combina varios discos duros en una sola unidad lógica. Así, en lugar de ver varios discos duros diferentes, el sistema operativo ve uno solo. Los RAID suelen usarse en servidores y normalmente (aunque no es necesario) se implementan con unidades de disco de la misma capacidad.

Diferentes tipos de RAID:

RAID 0

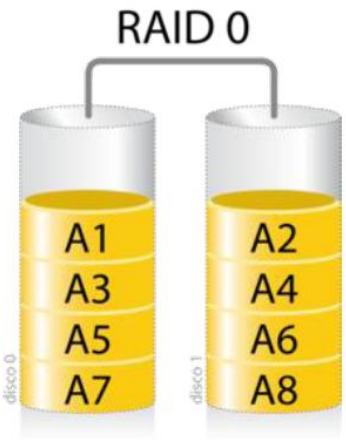


Diagrama de una configuración RAID 0.

Un **RAID 0** (también llamado **conjunto dividido** o **volumen dividido**) No tiene control de paridad ni es tolerante a fallos, lo que no lo hace utilizable como sistema de copia de seguridad. Este sistema multiplica la capacidad del menor de los discos por el número de discos instalados (aunque con algunas controladoras de gama alta se consigue que la capacidad total sea igual a la suma de la capacidad de los discos), creando una capacidad de almacenamiento equivalente al resultado de esta operación, utilizable como una sola unidad. A la hora de usar estos discos, divide los datos en bloques y escribe un bloque en cada disco, lo que agiliza bastante el trabajo de escritura/lectura de los discos, dándose el mayor incremento de ganancia en velocidad cuando está instalado con varias controladoras RAID y un solo disco por controladora.

RAID 1

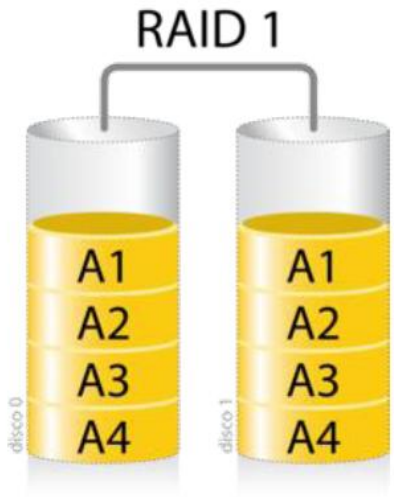


Diagrama de una configuración RAID 1.

El Raid 1 crea una copia exacta (espejo) de los datos en dos o más discos (array). Este sistema se suele utilizar cuando el rendimiento en la lectura resulta más importante que la capacidad de escritura. Si nos referimos a la seguridad, un Raid 0, como hemos comentado antes **no es tolerante al fallo de uno de sus discos**, sin embargo en un Raid 1 sí, ya que existe la misma información en cada uno de los discos.

Un Raid 1 clásico consiste en dos discos en espejo, lo que incrementa exponencialmente la fiabilidad respecto a un solo disco.

Al escribir, los datos deben de ser escritos en todos los discos del Raid 1, por lo que su rendimiento no mejora. El Raid 1 es un sistema muy utilizado cuando la disponibilidad es crítica 24 horas del día**.**

RAID 2

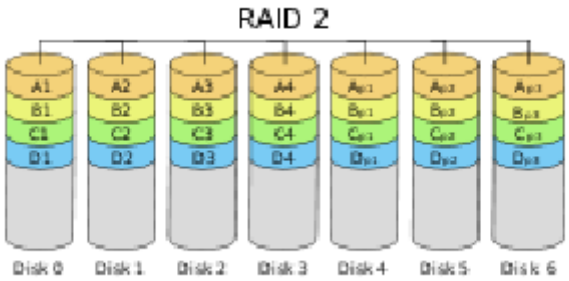


Diagrama de configuración RAID 2

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

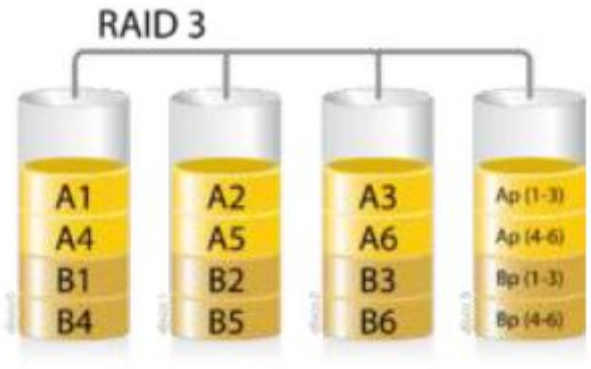


Diagrama de una configuración RAID 3.

Un **RAID 3** usa división a nivel de bytes con un disco de paridad dedicado. 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. Así, cualquier operación de lectura o escritura exige activar todos los discos del conjunto, suele ser un poco lento porque se producen cuellos de botella. Son discos paralelos pero no son independientes (no se puede leer y escribir al mismo tiempo).
En el ejemplo del gráfico, una petición del bloque «A» formado por los bytes A1 a A6 requeriría que los tres discos de datos buscaran el comienzo (A1) y devolvieran su contenido. Una petición simultánea del bloque «B» tendría que esperar a que la anterior concluyese.

RAID 4

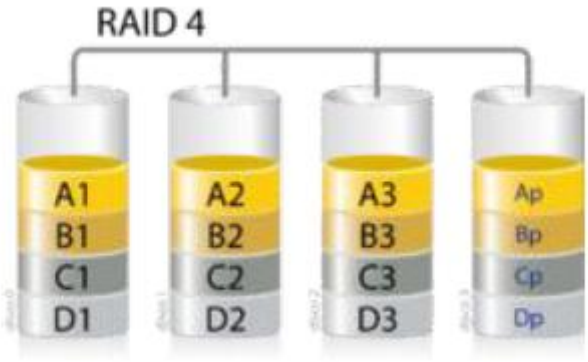


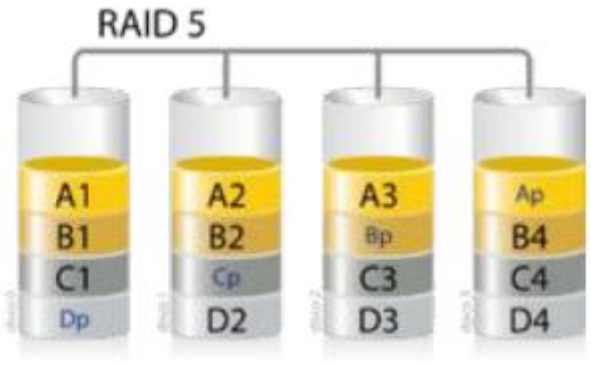
Diagrama de una configuración RAID 4.

Un **RAID 4**, también conocido como IDA (acceso independiente con discos dedicados a la paridad) usa división a nivel de bloques con un disco de paridad dedicado. Necesita un mínimo de 3 discos físicos. El RAID 4 es parecido al RAID 3 excepto porque divide a

nivel de bloques en lugar de a nivel de bytes. Esto permite que cada miembro del conjunto funcione independientemente cuando se solicita un único bloque. Si la controladora de disco lo permite, un conjunto RAID 4 puede servir varias peticiones de lectura simultáneamente. En principio también sería posible servir varias peticiones de escritura simultáneamente, pero al estar toda la información de paridad en un solo disco, éste se convertiría en el cuello de botella del conjunto.

En el gráfico de ejemplo anterior, una petición del bloque «A1» sería servida por el disco 0. Una petición simultánea del bloque «B1» tendría que esperar, pero una petición de «B2» podría atenderse concurrentemente.

RAID 5



Un **RAID 5** 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. RAID 5 necesitará un minimo de 3 discos para ser implementado.

Cada vez que un bloque de datos se escribe en un RAID 5, se genera un bloque de paridad dentro de la misma división (stripe). Un bloque se compone a menudo de muchos sectores consecutivos de disco. Una serie de bloques (un bloque de cada uno de los discos del conjunto) recibe el nombre colectivo de división (stripe). Si otro bloque, o alguna porción de un bloque son escritos en esa misma división, el bloque de paridad (o una parte del mismo) es recalculada y vuelta a escribir. El disco utilizado por el bloque de paridad está escalonado de una división a la siguiente, de ahí el término «bloques de paridad distribuidos». Las escrituras en un RAID 5 son costosas en términos de operaciones de disco y tráfico entre los discos y la controladora.

El RAID 5 requiere al menos tres unidades de disco para ser implementado. El fallo de un segundo disco provoca la pérdida completa de los datos.El número máximo de discos en un grupo de redundancia RAID 5 es teóricamente ilimitado, pero en la práctica es común limitar el número de unidades. Los inconvenientes de usar grupos

de redundancia mayores son una mayor probabilidad de fallo simultáneo de dos discos, un mayor tiempo de reconstrucción y una mayor probabilidad de hallar un sector irrecuperable durante una reconstrucción.

Las implementaciones RAID 5 presentan un rendimiento malo cuando se someten a cargas de trabajo que incluyen muchas escrituras más pequeñas que el tamaño de una división (stripe). En el caso de un fallo del sistema cuando hay escrituras activas, la paridad de una división (stripe) puede quedar en un estado inconsistente con los datos. Si esto no se detecta y repara antes de que un disco o bloque falle, pueden perderse datos debido a que se usará una paridad incorrecta para reconstruir el bloque perdido en dicha división. Esta potencial vulnerabilidad se conoce a veces como «agujero de escritura». Son comunes el uso de caché no volátiles y otras técnicas para reducir la probabilidad de ocurrencia de esta vulnerabilidad.

RAID 6

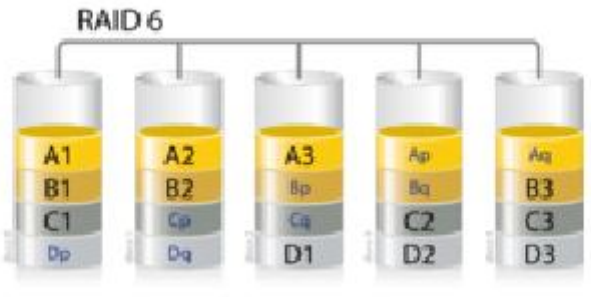


Diagrama de una configuración RAID 6.

Un **RAID 6** amplía el nivel RAID 5 añadiendo otro bloque de paridad, por lo que divide los datos a nivel de bloques y distribuye los dos bloques de paridad entre todos los miembros del conjunto. Al igual que en el RAID 5, en el RAID 6 la paridad se distribuye en divisiones (stripes), con los bloques de paridad en un lugar diferente en cada división.

El RAID 6 es ineficiente cuando se usa un pequeño número de discos pero a medida que el conjunto crece y se dispone de más discos la pérdida en capacidad de almacenamiento se hace menos importante, creciendo al mismo tiempo la probabilidad de que dos discos fallen simultáneamente. El RAID 6 proporciona protección contra fallos dobles de discos y contra fallos cuando se está reconstruyendo un disco. En caso de que sólo tengamos un conjunto puede ser más adecuado que usar un RAID 5 con un disco de reserva (hot spare).
La capacidad de datos de un conjunto RAID 6 es n-2, siendo n el número total de discos del conjunto.

Un RAID 6 no penaliza el rendimiento de las operaciones de lectura, pero sí el de las de escritura debido al proceso que exigen los cálculos adicionales de paridad. Esta

penalización puede minimizarse agrupando las escrituras en el menor número posible de divisiones (stripes), lo que puede lograrse mediante el uso de un sistema de archivos WAFL.

Sistemas de «clusters».

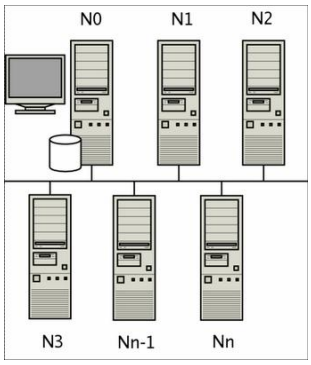
El término **cluster** (a veces españolizado como **clúster**) se aplica a los conjuntos o conglomerados de computadoras construidos mediante la utilización de hardwares comunes y que se comportan como si fuesen una única computadora.

Hoy en día desempeñan un papel importante en la solución de problemas de las ciencias, las ingenierías y del comercio moderno.

La tecnología de clústeres ha evolucionado en apoyo de actividades que van desde aplicaciones de supercómputo y software de misiones críticas, servidores web y comercio electrónico, hasta bases de datos de alto rendimiento, entre otros usos.

El cómputo con clústeres surge como resultado de la convergencia de varias tendencias actuales que incluyen la disponibilidad de microprocesadores económicos de alto rendimiento y redes de alta velocidad, el desarrollo de herramientas de software para cómputo distribuido de alto rendimiento, así como la creciente necesidad de potencia computacional para aplicaciones que la requieran.

Simplemente, un clúster es un grupo de múltiples ordenadores unidos mediante una red de alta velocidad, de tal forma que el conjunto es visto como un único ordenador, más potente que los comunes de escritorio.



Los clústeres son usualmente empleados para mejorar el rendimiento y/o la disponibilidad por encima de la que es provista por un solo computador típicamente siendo más económico que computadores individuales de rapidez y disponibilidad comparables.

De un clúster se espera que presente combinaciones de los siguientes servicios:

1. Alto rendimiento

2. Alta disponibilidad
3. Balanceo de carga
4. Escalabilidad

La construcción de los ordenadores del clúster es más fácil y económica debido a su flexibilidad: pueden tener todos la misma configuración de hardware y sistema operativo (clúster homogéneo), diferente rendimiento pero con arquitecturas y sistemas operativos similares (clúster semihomogéneo), o tener diferente hardware y sistema operativo (clúster heterogéneo), lo que hace más fácil y económica su construcción.

Para que un clúster funcione como tal, no basta solo con conectar entre sí los ordenadores, sino que es necesario proveer un sistema de manejo del clúster, el cual se encargue de interactuar con el usuario y los procesos que corren en él para optimizar el funcionamiento.

SAN, NAS, FiberChannel.

SAN:

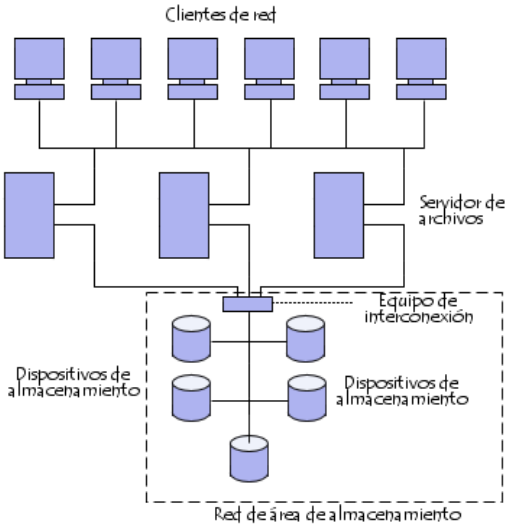
Una red de área de almacenamiento, en inglés SAN (storage area network), es una red concebida para conectar servidores, matrices (arrays) de discos y librerías de soporte. Principalmente, está basada en tecnología fibre channel y más recientemente en iSCSI. Su función es la de conectar de manera rápida,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

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:

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, 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, 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.

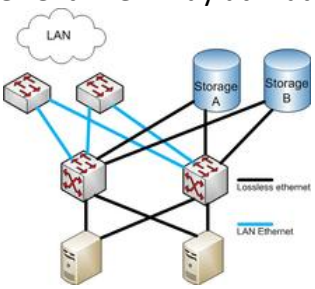
NAS es muy útil para proporcionar el almacenamiento centralizado a ordenadores clientes en entornos con grandes cantidades de datos. NAS puede habilitar sistemas fácilmente y con bajo costo con balance de carga, tolerancia a fallos y servidor web

para proveer servicios de almacenamiento. El crecimiento del mercado potencial para NAS es el mercado de consumo donde existen grandes cantidades de datos multimedia.

FiberChannel

Fiber Channel (FC), una tecnología de red Gigabit utilizada principalmente para redes de almacenamiento SAN y para la conexión de Cabinas de Discos DAS, capaz de funcionar sobre cables de fibra óptica (fiber-optic cables) y sobre cables de cobre (twisted pair copper wire), aunque en la práctica suele ser cableado de **fibra óptica (multimodo o monomodo)**. Cometaremos la posibles **topologías Fiber Channel** (punto a punto ó FC-P2P, bucle arbitrado o FC-AL, y red conmutado ó FC-SW) y las capas de Fiber Channel.

Fiber Channel Protocol (FCP) es un protocolo de transporte para la **transmisión de comandos SCSI sobre redes Fiber Channel**. Muy utilizado y extendido.

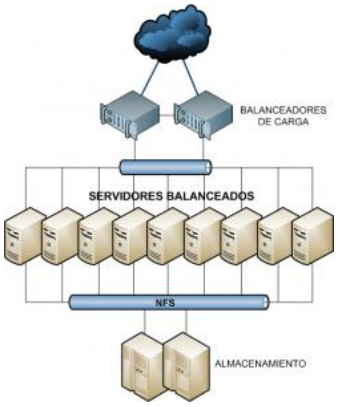


Balanceadores de carga.

Cuando un servidor de Internet se vuelve lento debido a la congestión de información, la solución más obvia es ampliar la memoria, ampliar el disco duro o actualizar el procesador. Pero el tráfico de Internet está en constante crecimiento y lo anteriormente expuesto es sólo una solución temporal. La opción más razonable es, a largo plazo, configurar más servidores y repartir las peticiones de los clientes entre ellos. Esto incrementa la velocidad de acceso del usuario al servidor, mejora la

fiabilidad del sistema y la tolerancia a fallos, permitiendo reparar o mantener cualquier servidor en línea sin que afecte al resto del servicio.

Así es como muchos de los sitios web más conocidos pueden abarcar toda la demanda que reciben, gracias al uso de un número de servidores "espejo" (mirrors) llamados granjas de servidores. Sin embargo, una vez utilizados varios servidores para responder todas las peticiones que van a una dirección, ¿Cómo las dividimos entre los distintos servidores? ¿Cómo podemos saber qué rendimiento ofrecemos y qué tiempo de CPU está generando cada petición? Simplemente el conectar más servidores a una red, no asegura la mejora del servicio.



PERO ¿QUÉ ES REALMENTE?

De forma sencilla, el balanceo de carga es la manera en que las peticiones de Internet son distribuídas 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.

MÉTODO ROUND ROBIN

El método más simple de todos, es la solución Round Robin. Las peticiones clientes son distribuídas equitativamente entre todos los servidores existentes. Este metodo ciclico no tiene en cuenta las condiciones y carga de cada servidor. Esto puede llevarnos a tener servidores que reciben peticiones de carga mucho mayor, mientras tenemos servidores que apenas se encuentran utilizando recursos.

Otra limitación es que los problemas de los servidores no son recogidos

inmediatamente. Esto puede llevarnos a estar enviando peticiones a un servidor que se encuentra fuera de servicio o que responde lentamente. Finalmente, el método Round Robin no aprovecha las diferentes prestaciones de los servidores (un PC Pentium normal puede estar obteniendo tantas peticiones como un multiprocesador Sun situado junto a él).

PRIMERA GENERACION DE BALANCEO DE CARGA

Las soluciones "reales" de balanceo de carga necesitan descubrir el rendimiento del servidor. La primera generación puede detectar el rendimiento del servidor via "passive polling", lo que significa que el balanceador de carga mide el tiempo de respuesta de los servidores y por ello tiene una idea de cómo están funcionando. De nuevo, tampoco se tiene en cuenta la variedad de servidores empleados. Además, sólo descubre que los servidores tienen un problema después de que se producen retrasos o, en el peor de los casos, cuando los servidores están completamente caídos.

SEGUNDA GENERACION DE BALANCEO

El balanceo de carga más seguro sólo se puede conseguir considerando el uso real de los servidores, permitiendo que los recursos existentes se empleen al máximo, al conocer cómo están siendo utilizados estos recursos incluso antes de que las peticiones de los clientes lleguen a ellos. El tráfico se enruta proactivamente, cambiando el antiguo concepto existente de balanceo de carga, hacia una solución de optimización del servidor, consiguiendo el mejor resultado posible con la tecnología disponible.

Para lograrlo, el balanceador de carga continuamente realiza peticiones de datos de cada servidor en la granja de servidores para monitorizar sus condiciones y direccionar las peticiones de los clientes hacia el servidor que se encuentre más disponible y en mejor estado para responder a dichas peticiones. Los parámetros solicitados, dependen del producto utilizado. Normalmente se emplea la utilización de la CPU del servidor, el uso de memoria y el número de conexiones abiertas.

La segunda generación de balanceadores posee funciones de mensajería, informando si los servidores están fuera de servicio, y si es así, cuándo serán devueltos a producción. La mayoría de los servidores "revividos" pasan un período de prueba durante el cual no se llenan completamente de peticiones.

Se puede incluso desconectar los servidores para repararse o para realizar el mantenimiento, a través del método de "apagado progresivo". El servidor, a partir de ese momento, no acepta nuevas peticiones pero permanece activo hasta que las transacciones de comercio electrónico y las descargas que se estén produciendo finalicen.

La segunda (algunas veces considerada la primera) regla más importante de una solución de balanceo de carga, es incrementar la fiabilidad del sitio web y del contenido y los servicios que está ofreciendo. Normalmente la segunda generación de balanceadores de carga hardware se vende en parejas, es decir, dos equipos iguales. Uno de ellos es la unidad activa y el segundo la unidad de repuesto o de back up. Una unidad de back up en modo stand by (en espera) con una misma dirección IP y MAC significa que incluso cuando el balanceador se ve afectado por un incidente como puede ser un fallo de cableado, fuego o error humano, hay una unidad de repuesto pre-configurada que pasa a ser operacional de forma inmediata.

- Virtualización de sistemas:

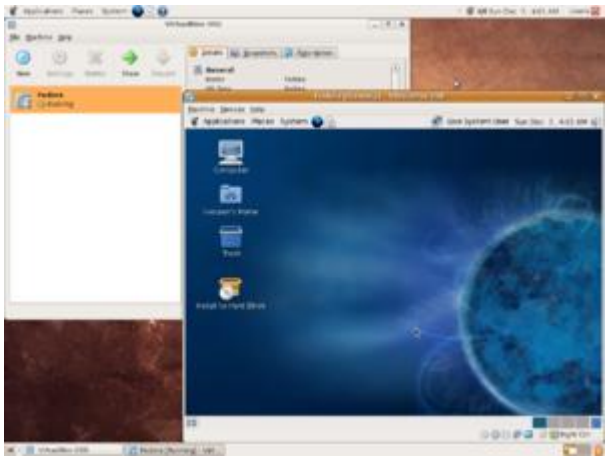
En Informática, **virtualización** es la creación -a través de software- de una versión virtual de algún recurso tecnológico, como puede ser una plataforma de hardware, un sistema operativo, un dispositivo de almacenamiento u otros recursos de red.

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.

Posibilidades de la virtualización de sistemas.

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).



VirtualBox

Existen diferentes formas de virtualización: es posible virtualizar el hardware de servidor, el software de servidor, virtualizar sesiones de usuario, virtualizar aplicaciones y también se pueden crear máquinas virtuales en una computadora de escritorio.

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

Herramientas para la 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 por (Hardware)

Virtualización asistida por Hardware son extensiones introducidas en la arquitectura de procesador x86 para facilitar las tareas de virtualización al software ejecutándose sobre el sistema. Si cuatro son los niveles de privilegio o "anillos" de ejecución en esta arquitectura, desde el cero o de mayor privilegio, que se destina a las operaciones del kernel de SO, al tres, con privilegios menores que es el utilizado por los procesos de usuario, en esta nueva arquitectura se introduce un anillo interior o ring -1 que será el que un hypervisor o Virtual Machine Monitor usará para aislar todas las capas superiores de software de las operaciones de virtualización.

La virtualización de almacenamiento

Se refiere al proceso de abstraer el almacenamiento lógico del almacenamiento físico, y es comúnmente usado en SANs ("Storage Area Network" Red de área de almacenamiento). Los recursos de almacenamiento físicos son agregados al "storage pool" (almacén de almacenamiento), del cual es creado el almacenamiento lógico.

Particionamiento

Es la división de un solo recurso (casi siempre grande), como en espacio de disco o ancho de banda de la red, en un número más pequeño y con recursos del mismo tipo que son más fáciles de utilizar. Esto es muchas veces llamado “zoning”, especialmente en almacenamiento de red.

Máquina virtual

La entenderemos básicamente como un sistema de virtualización, denominado "virtualización de servidores", que dependiendo de la función que esta deba de desempeñar en la organización, todas ellas dependen del hardware y dispositivos físicos, pero casi siempre trabajan como modelos totalmente independientes de este. Cada una de ellas con sus propias CPUs virtuales, tarjetas de red, discos etc. Lo cual podría especificarse como una compartición de recursos locales físicos entre varios dispositivos virtuales.

Hypervisor de almacenamiento

Es un 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.

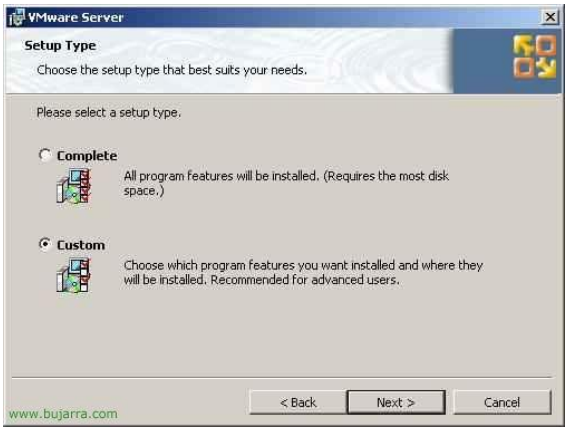
Su completo conjunto de funciones de control y monitorización del almacenamiento, operan como una capa virtual trasparente entre los pools de disco consolidados para mejorar su disponibilidad, velocidad y utilización.

Configuración y utilización de maquinas virtuales.

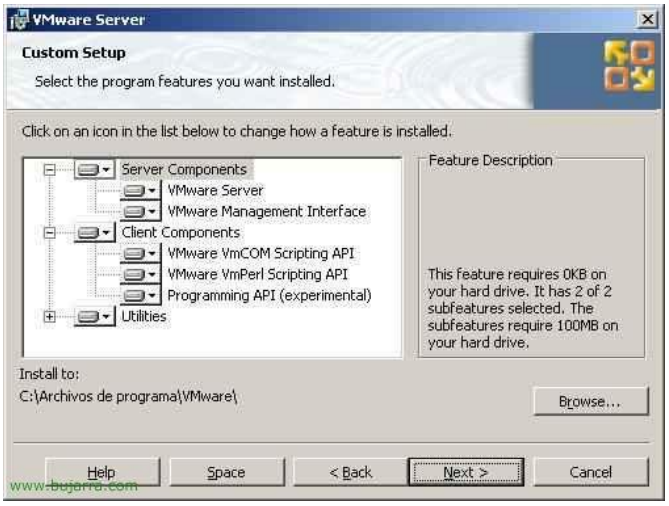
Instalación de VMware Server,

Lo primero de todo, necesitamos bajarnos el instalador desde la web de **www.vmware.com**. Y comenzamos a instalarlo, nos salta un asistente, "Siguiente",

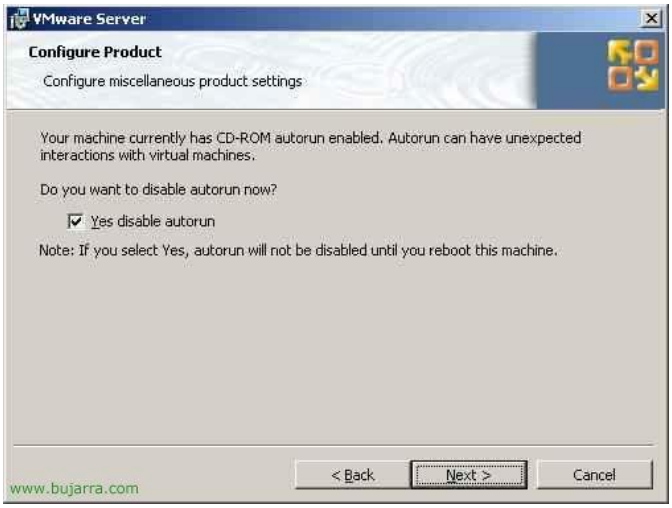
Aceptamos el acuerdo de licencia, "I accept the terms in the license agreement" & "Next",



Podemos realizar una instalación completa, yo sólo selecciono la personalizada para que veamos que componentes tenemos,



Podemos instalar sólo lo que es la parte servidora, que sería para alojar las MV (Server Components) o sólo la consola que sería para administrar local o remotamente el VMware Server (Client Components). Marcamos todo y "Next",



De acuerdo, marcamos el check para deshabilitar el autorun del CD por si acaso, "Next"

Y todo listo para comenzar la instalación, "Install",

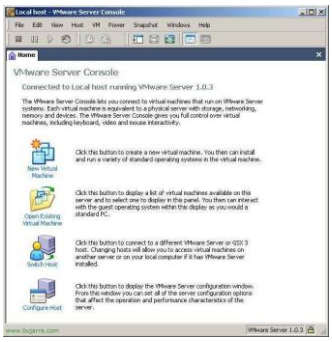
... esperamos unos minutos...

Y ya por fín pulsando en "Finish" finalizamos con la instalación, ya podemos jugar con las MV!

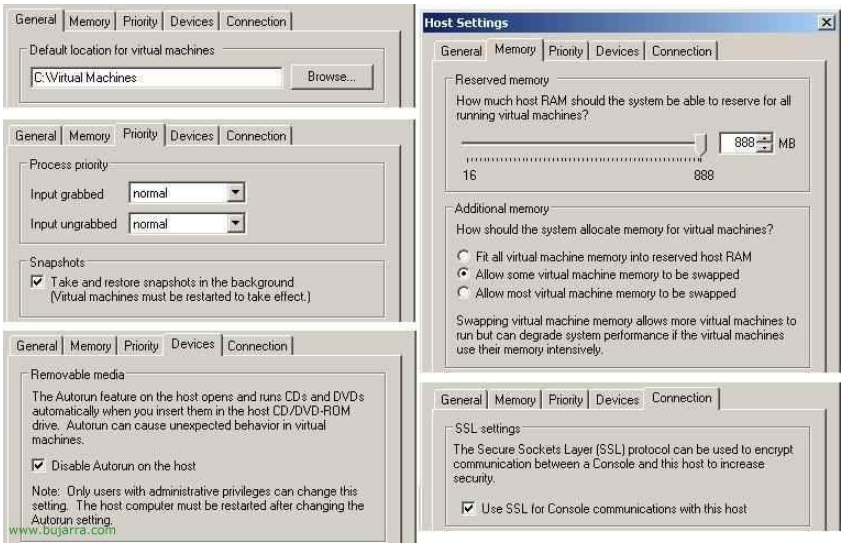
Configuración de VMware Server,

Para abrir la consola de VMware y poder administrarlo, se hace desde el icono del escritorio "VMware Server Console"

Cómo lo tenemos instalado en local, seleccionamos "Local host" y damos "OK",



Está sería la pantalla principal del VMware Server, desde aquí podemos crear máquinas virtuales ("New Virtual Machine"), abrir alguna existente ("Open Existing Virtual Machine"), cambiarnos de servidor a administrar por otro remoto ("Switch Host"), o configurar en el que estemos logeados ("Configure Host").

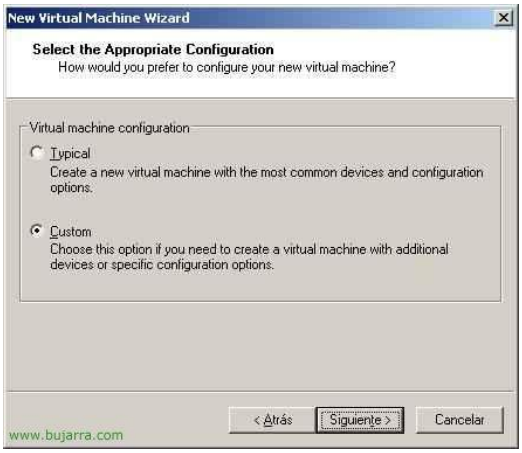


Si miramos las opciones que podemos configurar en el VMware Server, nos sale en la pestaña "General" donde guardaremos por defecto las MV. En la pestaña "Memory" es

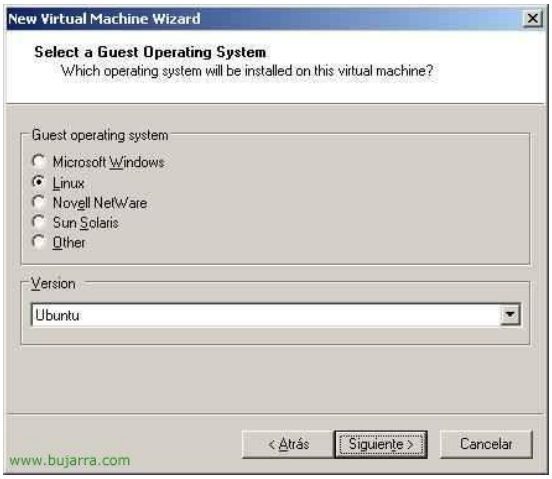
para gestionar la memoria RAM virtual de las maquinas, cuanta queremos dar a las MV y cuanta queremos a la máquina fisica o cuanta queremos pagine. En la pestaña "Priority" podemos darle más prioridad o no las MV, lo interesante son los "Snapshots" o imagenes, si queremos que nos genere imagenes de las MV o no. En la pestaña "Devices" tenemos lo comentado anteriormente, si queremos deshabilitar o habilitar el autorun de nuestos CDs en local. Y en la pestaña "Connection" es para que el tráfico entre la consola y la MV vata encriptado usando SSL, para ello marcaríamos "Use SSL for Console communications with this host".

Crear una máquina virtual en VMware Server,

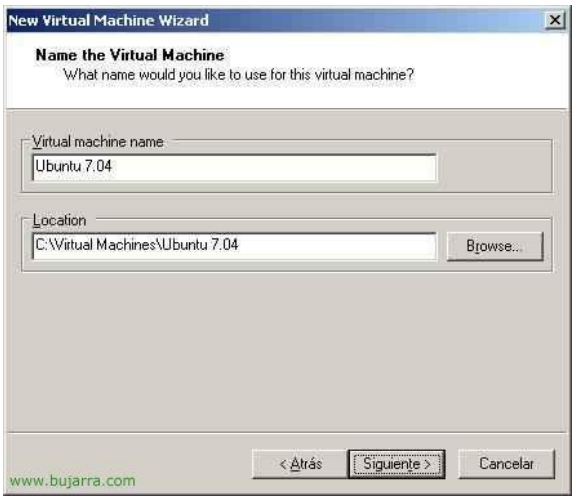
Para crear una máquina virtual, primero necesitamos tener por ahí un CD/DVD o una ISO con el S.O. que querramos instalar, lo metemos en la unidad del servidor. Para crear una MV, pinchamos en la consola en "File" > "New" > "Virtual Machine...", nos saldrá un asistente para personalizar la MV. "Siguiente",



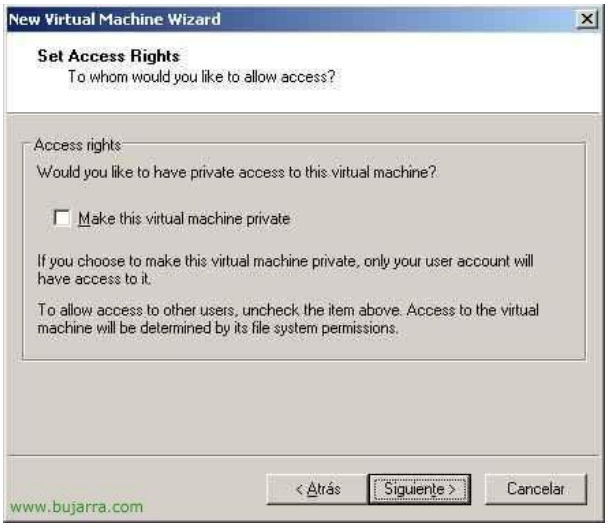
Seleccionamos "Custom" & "Siguiente"



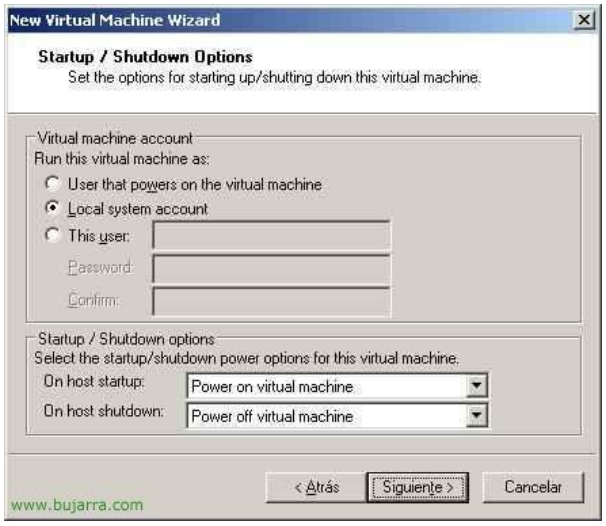
Seleccionamos el sistema operativo que le meteremos, si no está en el listado no pasa nada, "Siguiente",



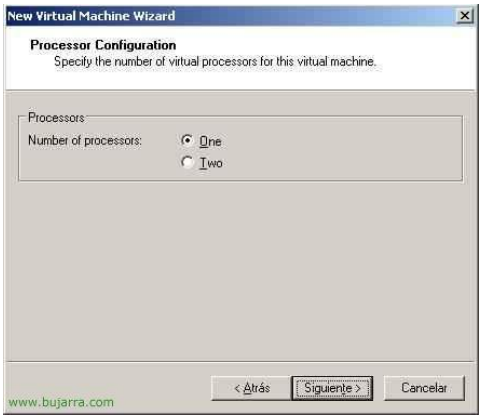
Le indicamos un nombre a la MV y una ruta donde almacenaremos toda su información (debe de tener tanto sitio como para almacenar un S.O entero!) y si está en otra partición que no en la de Sistema, mejor, "Siguiente"



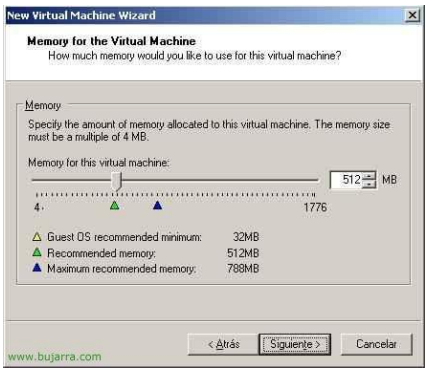
Podemos marcar el check de "Make this virtual machine private" para que sólo se pueda acceder con mi usuario a ella, "Siguiente",



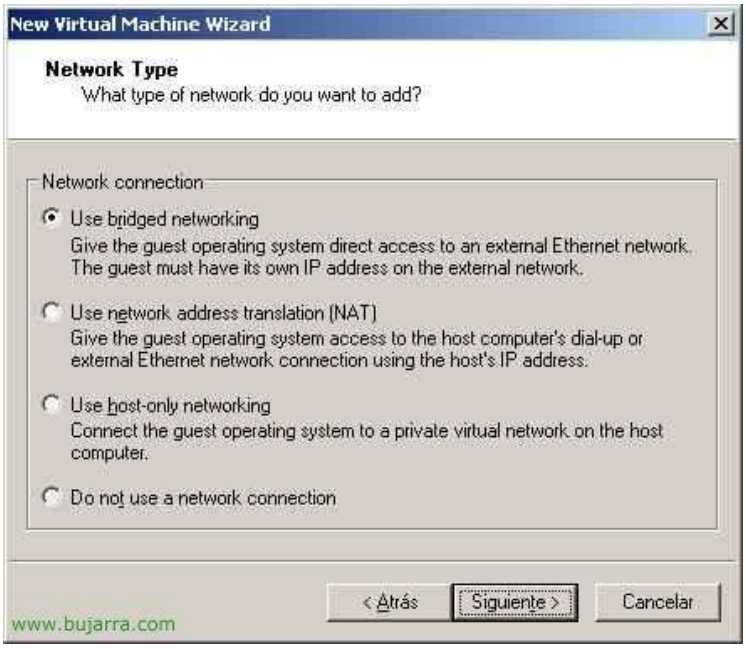
Tenemos varias opciones para el encendido y el apagado. Ya que se supone que donde instalemos VMware Server será un servidor dedicado a las MV, y si este servidor fisico lo apagamos, debe apagar las MV que tiene en su interior, o cuando el servidor físico se encienda deben de arrancar automáticamente también las MV, aquí es donde lo configuraremos: "On host startup: Power on virtual machine" y "On host shutdown: Power off virtual machine". "Siguiente",



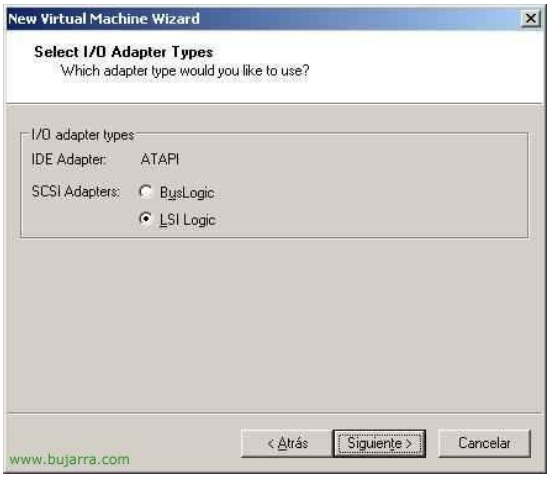
El número de procesadores que le querramos asignar...



Y esta sería la memoria RAM que le queremos asignar a la MV, dependiendo del S.O y sus funciones será más o menos, en un futuro le podremos asignar más si nos interesa (teniendo la MV apagada). "Siguiente",



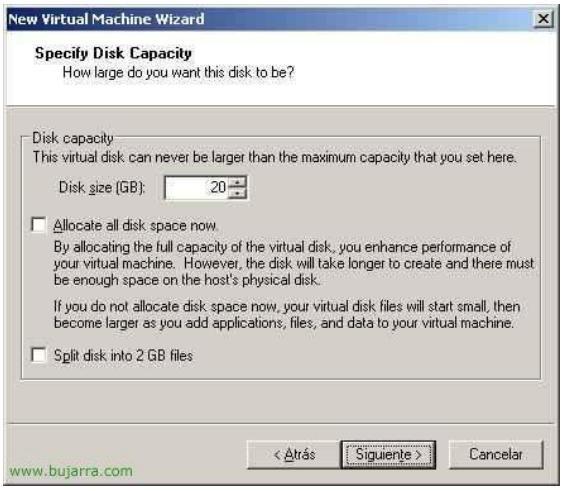
Es el tipo de conexion de red que tendrá, leemos las opciones y marcamos la que más nos interese, la normal suele ser la primera opción "Use bridget networking"& "Siguiente",



Dependiendo del S.O, marcaremos una u otra. Por ejemplo: "BusLogic" es para 2000 o NT y "LSI Logic" para XP o 2003, normalmente si es un S.O. modernito será esta última.

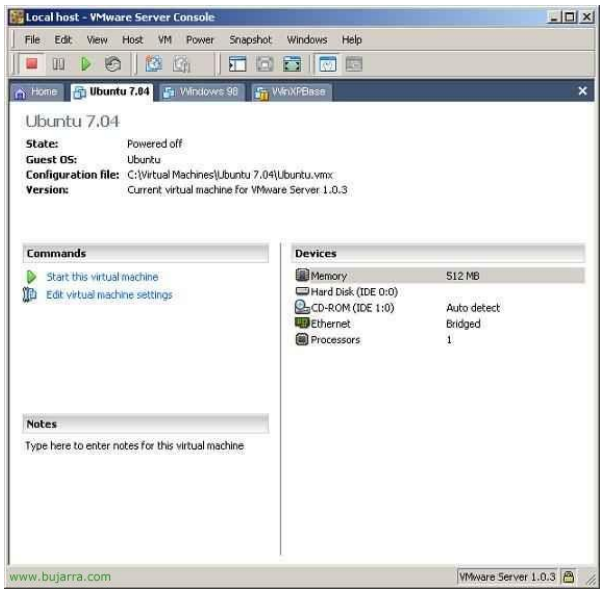
Creamos un nuevo disco (virtual), será un archivo y en nuestro PC virtual podremos formatear o toquetear particiones, y no se verá afectado para nada nuestro PC real, ya que se hace todo sobre el disco virtual que es un simple fichero. O podríamos usar el disco físico local, nada recomendado!!

Seleccionamos el tipo de disco que nos interese...

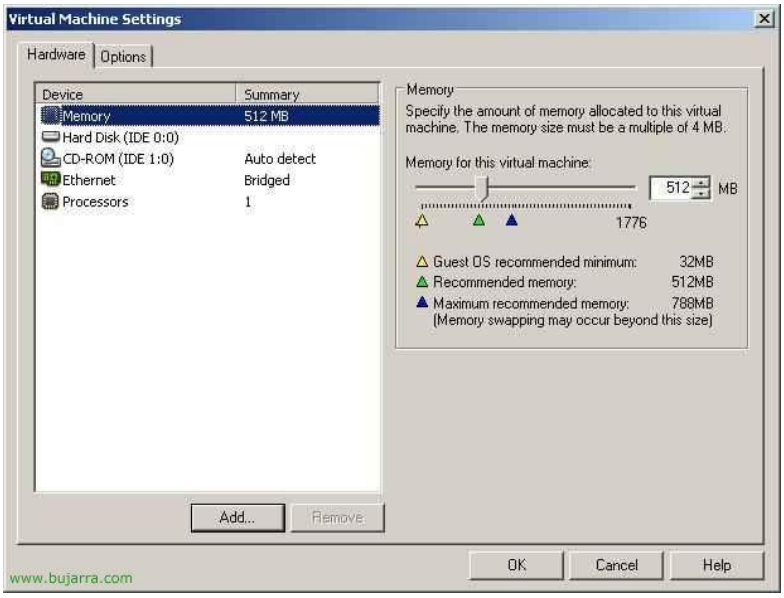


Le indicamos los Gb que queremos que tenga nuestro disco virtual, ojo! como nos quedemos cortos luego no se puede ampliar! es mejor ponerle de sobra, esto no nos lo ocupará al momento de nuestro disco fisico real a menos que marquemos "Allocate all disk space now", si no lo que se vaya usando irá ocupando.

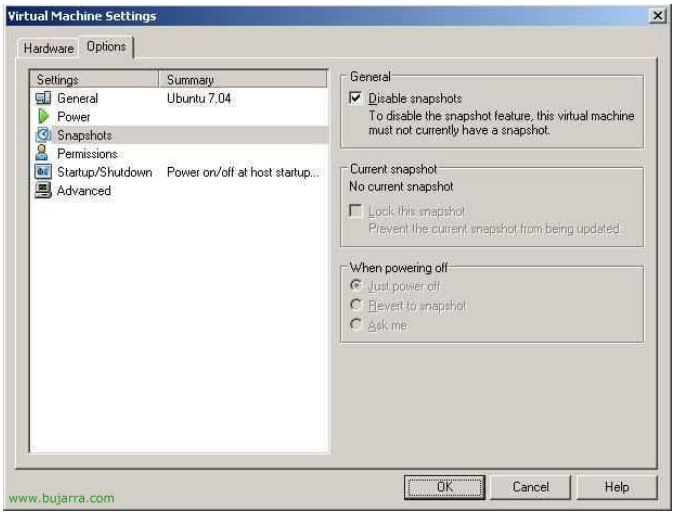
Indicamos el nombre del disco virtual, es un fichero VMDK, pulsamos en "Finalizar" para generar está MV.



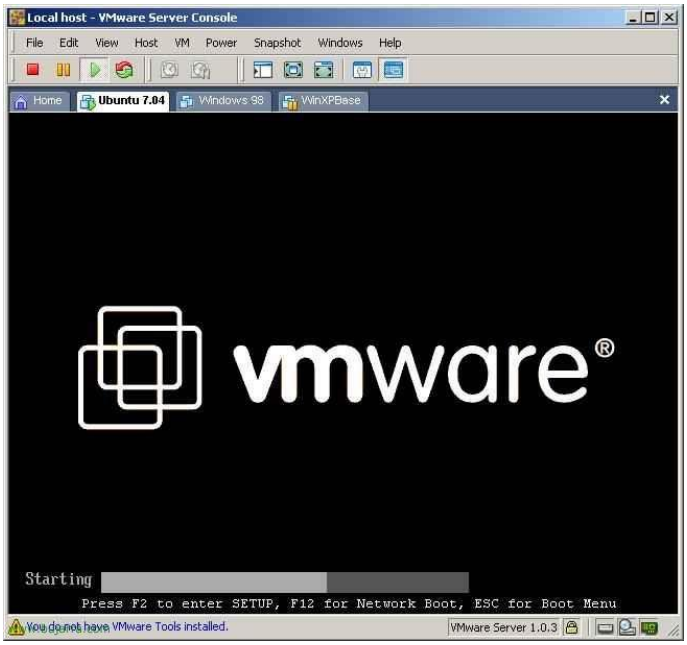
Esta sería la pantalla principal de nuestra MV apagada, vemos su hardware virtual, si pinchamos en "Edit virtual machine settings" tendremos más opciones.



En esta pestaña de "Hardware" podemos agregar más dispositivos desde "Add..." como disqueteras, más discos, más tarjetas de red... o quitar alguno que no nos interese que tenga.



En la pestaña de "Options" tenemos más opciones de configuración, si no nos interesa que nuestro disco se nos sature con imagenes automatizadas de la MV deberemos deshabilitar los snapshots...

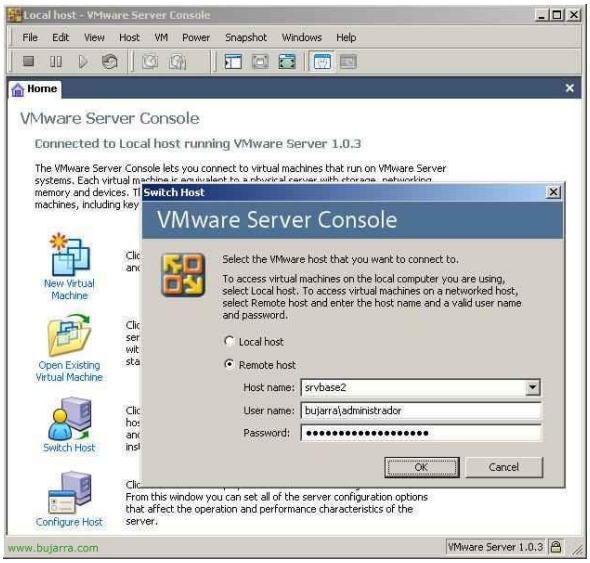


Y ya dandole al PLAY arrancaría la MV, podemos entrar en su BIOS virtual pulsando F2. Y comenzaría la instalación del S.O. con nuestro CD/DVD o imagen ISO, o si ya tenemos un S.O. instalado pues comienza el arranque normal.

Instalar herramientas de VMware, dispositivos USB, administración remota,

Es interesante tener las herramientas de VMware instaladas en las MV, para poder ejecutar scripts por ejemplo, para instalarlas, pulsamos en "VM" > "Install VMware Tools..."

Para conectar dispositivos USB que están conectados fisicamente en el servidor a las MV, debemos ponernos en la MV que nos interese, y en "VM" > "Removable Devices" > "USB Devices" > NOMBRE_DEL_DISPOSITIVO.



Y si queremos administrar un VMware Server de forma remota, abriendo la consola de VMware Server Console, nos pedirá a que host conectarse, simplemente marcamos "Remote host" y decimos cual, metemos los credenciales de un usuario con permisos de admin en la máquina y adelante.

Este sería el aspecto del VMware Server corriendo, sea local o remoto, veríamos que MV tenemos iniciadas o detenidas.