INSTALACIÓN, CONFIGURACIÓN Y ADMINISTRACIÓN

USERS

Argentina $ 22.- // México $ 49.-

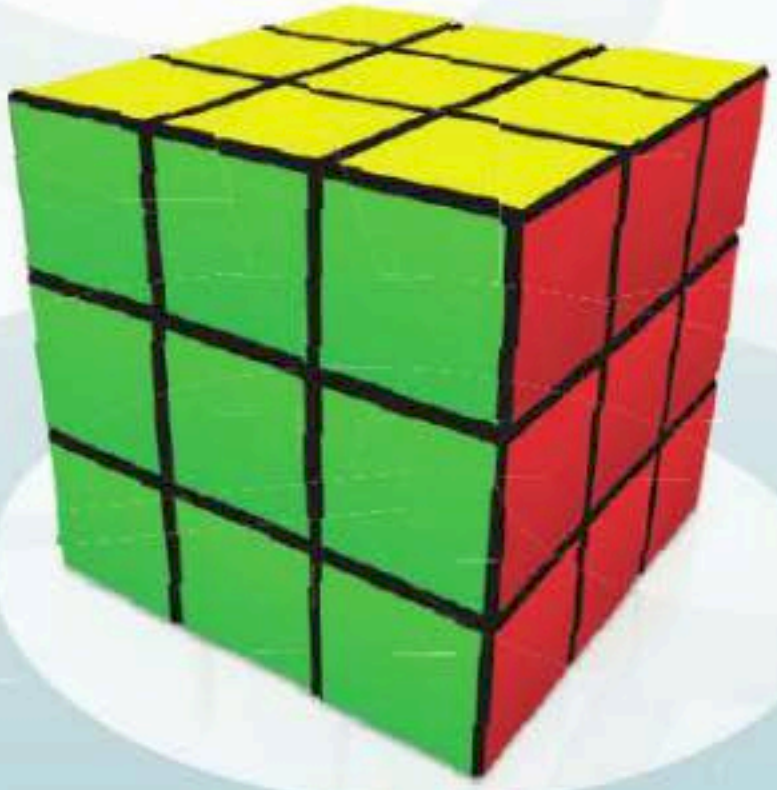
Técnico en REDES &SEGURIDAD

14

HARDWARE DE SERVIDORES

Conoceremos en detalle los componentes de un servidor de red, así como las consideraciones importantes para armarlo. También veremos qué son las matrices RAID y analizaremos su implementación.

- HARDWARE DE UN SERVIDOR
- TECNOLOGÍAS EFI Y UEFI
- SEGURIDAD EN SERVIDORES
- HARDWARE MANAGEMENT
- ADMINISTRACIÓN REMOTA



USERS

Técnico en REDES &SEGURIDAD

Coordinador editorial
Paula Budris

Asesores técnicos
Federico Pacheco
Javier Richarte

Nuestros expertos
Valentín Almirón
José Bustos
Gustavo Cardelle
Rodrigo Chávez
Alejandro Gómez
Javier Medina
Gustavo Martín Moglie
Pablo Pagani
Gerardo Pedraza
Ezequiel Sánchez

Impreso en Sevagraf S.A. Impreso en Argentina.

Técnico en redes y seguridad / coordinado por Paula Budris. - 1a ed. - Buenos Aires: Fox Andina, 2013
576 p. ; 28 x 20 cm. (Users; 22)

ISBN 978-987-1857-78-4

1. Informática. 2. Redes. I. Budris, Paula, coord.
CDD 004.68

En esta clase veremos...

Componentes de hardware que encontraremos en un servidor de red. Analizaremos las tecnologías asociadas y realizaremos procedimientos prácticos.

En la clase anterior vimos la forma adecuada de instalar, configurar y administrar impresoras de red. Primero conocimos los tipos de impresoras de red existentes y luego aprendimos a ponerlas en marcha. Revisamos la manera en que se debe administrar una impresora de red, y vimos los protocolos IPP y LPD. Dimos los detalles relacionados con la impresión en red para Linux y conocimos una práctica guía de comandos CUPS. Aprendimos a imprimir desde diversos dispositivos móviles y explicamos las ventajas de la tecnología conocida como Cloud Print.

En esta clase nos dedicaremos a repasar las características del hardware de un servidor de red. Conoceremos cada uno de los componentes de hardware que corresponden a un servidor y consideraremos sus particularidades.

Para continuar, veremos la tecnología RAID y presentaremos el procedimiento detallado para montar una matriz RAID.

Analizaremos el BIOS Setup de un servidor y las ventajas de la tecnología UEFI. Daremos diversos consejos de seguridad aplicada a los servidores de red, y describiremos los recursos y tecnologías del hardware management.

14

El hardware de un servidor

En estas páginas conoceremos las diferencias que se pueden apreciar entre el hardware usado en servidores de red y el que encontramos comúnmente en los equipos de escritorio.

En el ámbito de los **servidores** reinan los procesadores, las memorias y los discos duros, que seguramente en un futuro no muy lejano pasarán a formar parte de nuestros equipos de escritorio; al menos, en la mayoría de los casos esto viene sucediendo históricamente. En líneas generales, el hardware interno de los servidores de red no difiere tanto del hardware de un equipo de escritorio. Veremos aquí esas sutiles diferencias entre ambos mundos.

LAS FUENTES DE ENERGÍA MÁS UTILIZADAS EN SERVIDORES SON LAS REDUNDANTES.

Microprocesadores

En el caso de los servidores actuales, tanto Intel como AMD ofrecen procesadores de múltiples núcleos: de hasta ocho o diez. **Opteron** es la línea de procesadores para servidores de AMD, mientras que **Xeon** e **Itanium** pertenecen a Intel.

Motherboards

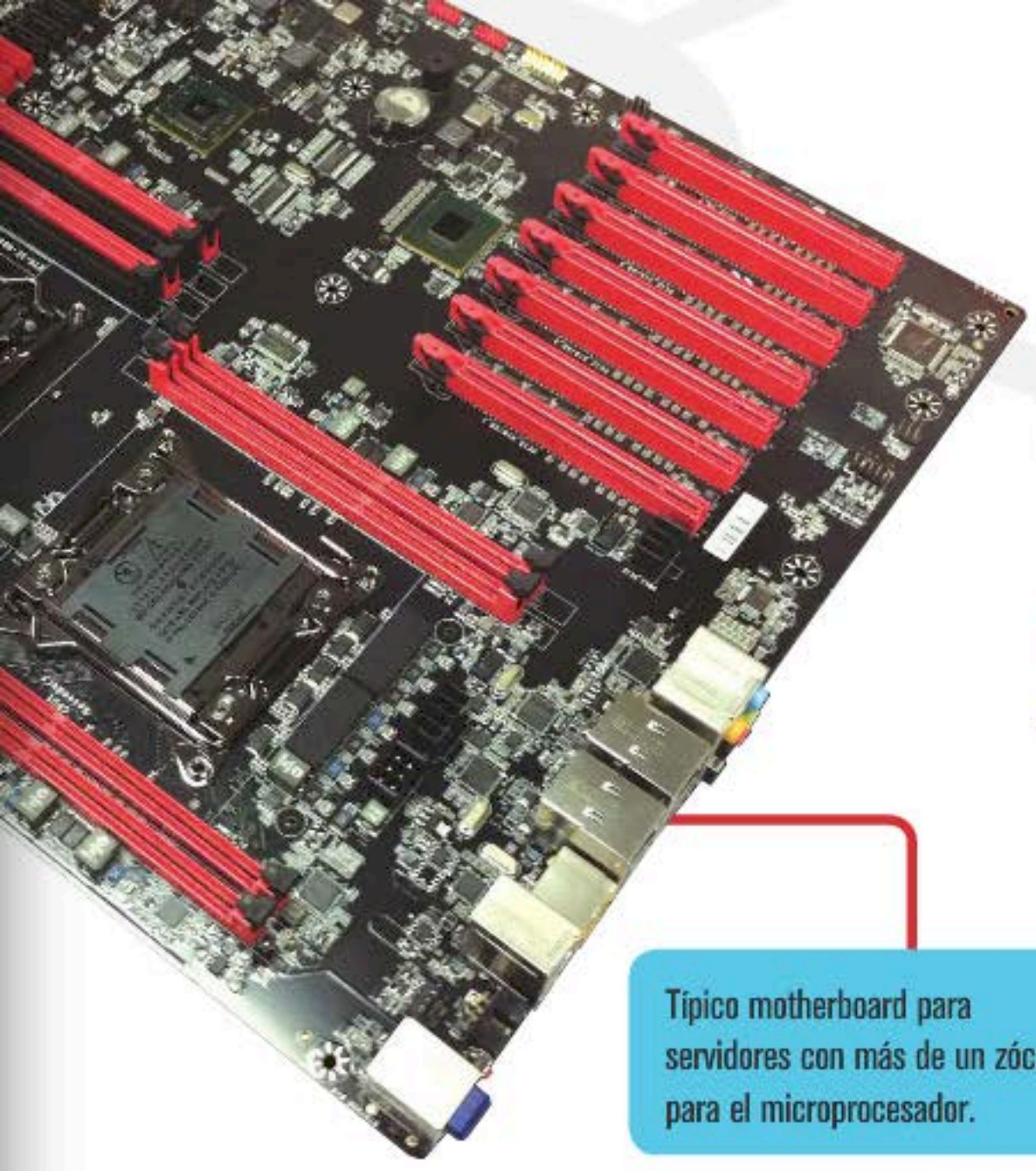
La mayoría de los **motherboards** permiten colocar dos, cuatro, ocho y más de estos procesadores en la misma placa, con lo cual el poder de cómputo se multiplica. También poseen varios zócalos para instalar memoria RAM del tipo *Fully Buffered*, generalmente, de cuatro hasta ocho módulos. En cuanto a la capacidad máxima soportada, varía entre 32 y 128 GB.
Debemos notar que estos motherboards no tienen interfaz de audio integrada, ya que no es necesaria. Suelen traer una placa de video incorporada, de prestaciones limitadas, porque tampoco este es el principal apartado al que apuntan los servidores. En muchos casos, también integran una interfaz de red Ethernet de 10/100/1000 Mbps.
Con respecto a los zócalos de expansión con los que cuenta un típico motherboard orientado a servidores, lo más común actualmente es el PCI Express 3.0 16x y el PCI-X, extensión del clásico bus PCI, pero que funciona a 64 bits, y 66 o 133 MHz.
Es prácticamente obligada la inclusión de una controladora de disco **Ultra SCSI 320**, con salida tanto interna como externa.

Almacenamiento

Los discos de interfaz **SCSI 320** y **SAS** son los más elegidos en este ámbito.
La velocidad de giro de estas unidades puede ser de 10.000 revoluciones por minuto, aunque también existen modelos de 15.000 y 20.000 rpm; recordemos que los discos de una computadora de escritorio giran a **7200 rpm**.
Con respecto a la capacidad de la o las unidades utilizadas, debemos saber que esta depende directamente de las tareas que han sido asignadas al server y también de la cantidad de usuarios que este debe servir, entre otros factores.
Lo más habitual es ver unidades dispuestas de tal modo que componen un array RAID, para aumentar ya sea la velocidad, la seguridad, o ambas.

Memorias Fully Buffered

Uno de los puntos fuertes de este tipo de memorias es su casi nulo margen de error: se estima un error de lectura en 1.142.000 años. Los módulos FB-DIMM utilizan pistas bidireccionales en serie, que pasan por cada módulo de memoria, en vez de tener canales individuales que envían información a los módulos, concepto bastante parecido al principio de funcionamiento de las placas PCI Express (también de tecnología serie).



Típico motherboard para servidores con más de un zócalo para el microprocesador.

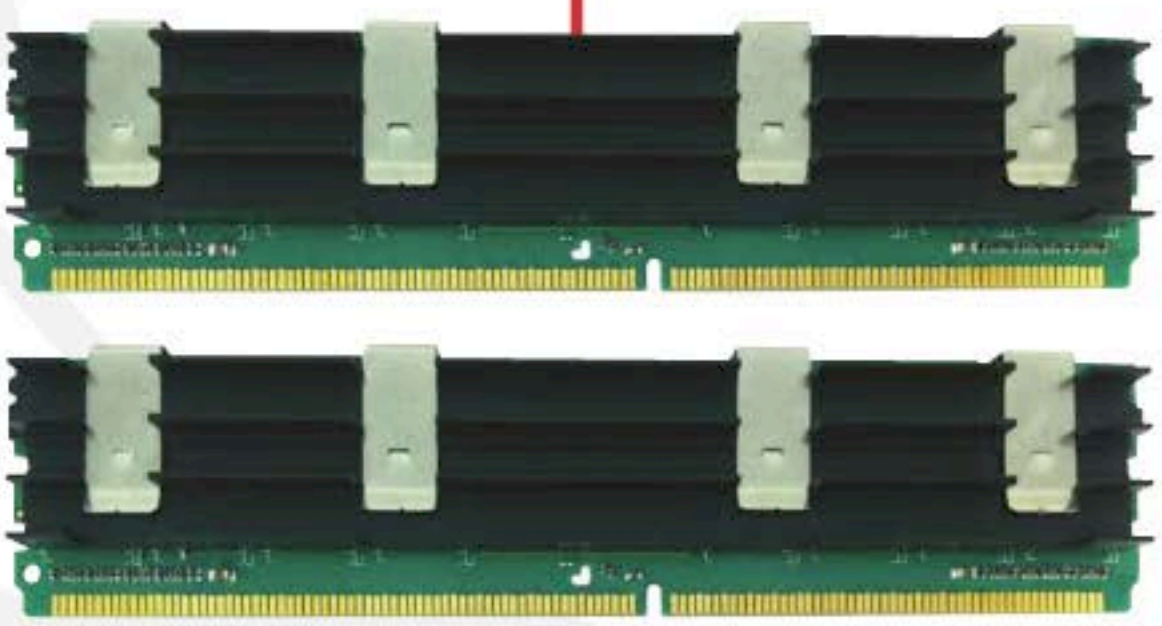
Aquí vemos un modelo de disco duro **Cheetah**, fabricado por Seagate.

Gabinete

Teniendo en cuenta a los grandes servidores, el mercado ofrece **gabinetes especiales**, que pueden ser de tres tipos: tower, rackeables o blade. Los tower son los usados comúnmente en equipos de escritorio, con la diferencia de que en los servidores son más amplios, y cuentan con una gran cantidad de bahías para alojar unidades de disco duro y espacio suficiente para ubicar motherboards de gran tamaño. En este caso, se tiene muy en cuenta la ventilación: podemos encontrar hasta cuatro y diez ventiladores incorporados.

Los **gabinetes rackeables** son módulos que se pueden agregar y atornillar a una caja o torre llamada rack (del inglés, "estante"). Por lo tanto, podemos decir que un rack no es más que un conjunto de equipos (servers, switches, routers, patcheras, etc.) que se van apilando en forma modular, como si se tratara de estantes.
Este método se usa, además, en otras áreas, como en los equipos de sonido, telefonía, comunicación y medicina, ya que el ancho del rack es estándar: 19 pulgadas. En cuanto a la altura, esta puede ser variable. La mínima unidad se conoce como 1U, y existen servidores de 2U, 4U y hasta 8U. El espacio de estos gabinetes es reducido en comparación con los de formato torre. La ventilación se torna prioritaria en este tipo de servidores, pero al ser modulares, las ventajas que ofrecen son amplias.
Por último, los cases de tipo **blade** son similares a los rackeables, con la diferencia de que los primeros se ubican en forma vertical en relación al rack y son capaces de alojar hasta diez a lo ancho del estante. De esta manera, se aprovecha mejor el espacio disponible en el rack. Por ejemplo, en un rack de 42U, normalmente podemos alojar 42 dispositivos de 1U de alto.

Los módulos de memoria **Fully Buffered** funcionan con 1,8 Volts.



Fuentes de energía

Las fuentes de energía más utilizadas, y recomendadas, en servidores son las llamadas **redundantes**, también conocidas como **fuentes duales**. Estos dispositivos permiten que, si en un servidor una de las fuentes sufre una falla, la otra tome el control, mientras la primera puede ser reemplazada, todo esto, sin apagar ni reiniciar el server. Obviamente, se requieren motherboards especiales para estos casos, y los costos son bastante elevados. Por eso, solo se justifica su uso en grandes servidores de archivos, de correo o web servers. ■

Componentes internos de un servidor

A continuación realizaremos un repaso de los principales componentes que se encargan de marcar la diferencia en un servidor, como el motherboard, el microprocesador, la memoria y el disco duro.

Cuando hablamos de los componentes de un servidor, nos referimos a los mismos componentes básicos que encontramos en un equipo de escritorio, pero especializados para brindar mayor poder de cómputo y, por sobre todo, mayor fiabilidad. La razón de ser de un servidor es, justamente, dar un servicio a los usuarios en forma continua y predecible. Lo normal es que los servidores den **servicio 24x7**, es decir, las 24 horas, los 7 días de la semana.

LOS DISCOS SAS HAN REEMPLAZADO A LOS TRADICIONALES DISCOS SCSI, Y SE CONVIRTIERON EN EL ESTÁNDAR PARA SERVIDORES DE GAMA MEDIA Y ALTA.

Esta característica **non-stop** es, sin dudas, uno de los principales requerimientos, sobre el que tienen que trabajar los ingenieros que diseñan servidores comerciales. En el mercado podemos encontrar servidores con distintos tipos de prestaciones, pero la **robustez** y la **confiabilidad** deben estar entre las principales.

El **Cisco Nexus 5000** provee de capacidad **Fiber Channel Over Ethernet** de 10 Gigabits.

Módulo TPM Infineon. Permite ejecutar una gran variedad de algoritmos, y asegura la información en descanso y en tránsito.

El espacio en los **data centers** suele ser costoso y, por lo tanto, escaso, motivo por el cual los servidores se diseñan para poder ahorrar lugar en los racks. Dependiendo de la función que cumpla el servidor, ocupará más o menos unidades (U) de un rack. El diseño de gabinete condiciona la disposición y el tamaño que deben tener los componentes internos.

Motherboard

El motherboard es el principal componente de un servidor, y su misión es dar soporte a los demás elementos. Puede contener más de un socket, para así poder conectar más de un procesador y varios módulos de memoria.

Microprocesador

Los procesadores para servidor se caracterizan por tener mayor capacidad y velocidad de cómputo, pero también, por la mayor cantidad de memoria caché. La capacidad de cómputo está dada

por la cantidad de procesadores que posee el system board y por la cantidad de cores que tiene cada procesador.
La **memoria caché**, que se encuentra dentro del procesador, permite realizar operaciones con más velocidad. La gran diferencia que tienen los procesadores para servidores es, justamente, la cantidad de memoria caché con que cuentan. Poseen, típicamente, tres niveles de memoria. La L1 se encuentra dentro del procesador y es la más veloz, la más cara y, en consecuencia, la de menor capacidad. Es del tipo SDRAM y se utiliza, principalmente, para almacenar las instrucciones; suele tener menos de 150 KB.
La L2 suele utilizarse para instrucciones y datos, y oscila entre 256 y 512 KB por core. Por último, la L3 está fuera del die y es compartida por todos los cores. Su capacidad varía considerablemente, y su beneficio se percibe en aplicaciones que utilizan ciertas instrucciones o datos en forma repetitiva.

Los procesadores que Intel comercializa para servidores son el Xeon y el Itanium (también conocido como IA64). Los **Xeon** son, típicamente, x86, pero también tienen soporte para direccionamiento de 64 bits; son utilizados en servidores que van desde la gama inicial hasta los de misión crítica. Presentan algunas características especiales, como la posibilidad de detectar errores y corregirlos. En cuanto a la seguridad, implementan un set de instrucciones AES-NI que permiten acelerar la encriptación de datos y reducir la cantidad de ciclos utilizados por el algoritmo.
Por su parte, los procesadores **Itanium** fueron desarrollados en conjunto entre HP e Intel, y se orientan a competir con los procesadores IBM Power y SPARC. Últimamente, se han visto envueltos en una gran controversia, luego de que Microsoft, Oracle y otras grandes empresas anunciaron sus intenciones de discontinuar el desarrollo y soporte de sus productos para esta plataforma. El sistema operativo que mejor ha recibido a esta familia de procesadores es HP-UX, así como otros sistemas Linux.
Por su parte, AMD produce la línea de procesadores **Opteron**, que ofrecen una excelente relación precio/prestaciones. Utilizan la arquitectura de instrucciones AMD64, pero ofrecen soporte nativo para 32 bits. La tecnología de Opteron conocida como **Hyper Transport** permite que un procesador acceda a la memoria principal de otro en el mismo motherboard, lo cual incrementa la velocidad de acceso. Existen numerosos sistemas operativos con soporte para estos procesadores, entre los que se destacan Windows, Solaris y Red Hat. Los **procesadores SPARC**, desarrollados por Sun Microsystems, son ampliamente conocidos en el mundo Solaris y BSD. Están basados en la arquitectura RISC, que es completamente abierta. En la actualidad, Oracle, que adquirió a Sun Microsystems, utiliza procesadores Intel para su sistema operativo Solaris, pero reserva el procesador SPARC para sus equipos de gama alta, como la línea M.
Otro procesador que no podemos dejar de nombrar es el **IBM Power**, también basado en la arquitectura RISC, y soportado por los sistemas operativos AIX, Linux y OS/400 (I Series).

Facebook Open Compute Server

Facebook ha desarrollado un estándar de servidor adaptado a sus necesidades, y en 2011 creó el proyecto Open Compute Server. La iniciativa tiene como objetivo contribuir a la madurez de la industria proveyendo los diseños de los componentes de servidores y otros elementos del data center. Es así que se diseñaron equipos de bajo costo y eficientes en términos energéticos. Cada componente ha sido revisado y adaptado. El motherboard fue simplificado al quitar los componentes innecesarios, como múltiples slots de expansión. El chasis no contiene partes plásticas, pintura o tornillos, lo que garantiza un menor costo de adquisición y mantenimiento.

Samsung Green Solution. Módulo RAM de 16 GB DDR3 y disco SSD de 512 GB con interfaz SATA de 6 Gbps.

Memoria

Al igual que en el mundo de los procesadores, la memoria RAM utilizada en servidores tiene características propias que la diferencian de las típicamente usadas en computadoras de escritorio. Los módulos de RAM **Fully Buffered** empleados por los procesadores Xeon y SPARC, entre otros, utilizan comunicación serie en vez de paralela con el controlador de la memoria, lo que incrementa el bus sin necesidad de aumentar la cantidad de pines. Por otra parte, debemos saber que la arquitectura utilizada en este tipo de memorias implementa un buffer que permite detectar y corregir errores (ECC), sin generar sobrecarga en el procesador ni en el controlador de la memoria.

LOM PERMITE ENCENDER Y APAGAR UN SERVIDOR EN FORMA REMOTA, AUN CUANDO EL SISTEMA OPERATIVO NO ESTÉ INSTALADO O NO RESPONDA.

Controlador de discos

El controlador de discos (HDC) está compuesto, esencialmente, por un chip y un circuito que es responsable de la administración de los discos. También puede controlar unidades ópticas (CD/DVD), unidades de cinta, etc.
La controladora es la que define qué tipo de disco puede usarse según la interfaz que soporte. Las interfaces típicas de servidores son IDE (prácticamente discontinuada), SATA (típicamente, para **servidores entry level**), Fiber Channel o SCSI, y sus derivados. El **controlador de discos** puede estar integrado al motherboard o puede consistir en una placa de expansión (PCI, PCI-X). Una placa madre puede contar con distintos tipos de controladores de disco conectados en simultáneo, ya sea onboard o mediante placas externas.

Intel Server Board S2400SC2. Soporta 2 procesadores Xeon E5, 8 módulos DDR3, 14 discos, 4 slots PCI Express y 1 slot PCI.

El de un servidor suele incluir la funcionalidad RAID mediante hardware. El controlador RAID permite realizar un arreglo de discos con la finalidad de brindar mayor fiabilidad y/o performance. La ventaja de que el arreglo de disco se realice mediante un controlador de hardware dedicado es que libera ciclos de procesamiento de la CPU. Existen distintos tipos de RAID, que van del 0 al 6, y permiten que el sistema operativo vea los discos dentro del arreglo como una sola unidad.
El RAID 0 brinda mayor performance, pero no otorga redundancia. EL RAID 1 se conoce comúnmente como espejado, porque mantiene dos discos con la misma información. En caso de que uno de ellos falle, el RAID puede seguir dando servicio con el disco espejado. El RAID 10 o 1+0 combina el RAID 0 con el 1, y otorga fiabilidad y performance. Los arreglos que van del 2 al 6 proveen distintos niveles de confiabilidad y rendimiento.

Discos duros

Los discos duros para servidores más utilizados hoy en día son SAS (Serial Attached SCSI), SATA (Serial ATA) y SSD (Solid State Drive). Los SAS se utilizan en un rango de servidores que va de gama media a alta o misión crítica. Poseen gran capacidad de almacenamiento: un solo disco puede almacenar entre 1 y 4 TB (4096 GB). La velocidad de rotación del disco puede llegar hasta 15.000 rpm, y la velocidad de transferencia se establece en 6 GB/seg. Los discos SATA se utilizan en servidores entry o de gama media, pero no en los de misión crítica, ya que su tasa de I/O es menor que la de los discos SAS. Su capacidad oscila entre 250 GB y 4 TB. Por último, los discos SSD tienen una capacidad limitada, cuyo tope oscila en los 400 GB, y un altísimo precio, por lo que su uso se restringe a propósitos específicos.
La caché de disco permite optimizar la velocidad de acceso a la información, y así evitar la necesidad de acceder al disco cuando los datos están en la memoria de la controladora.
El uso de este tipo de memoria caché es muy beneficioso para aplicaciones con manejo intensivo de disco, como las bases de datos. Al contar con este componente activo, cualquier base de datos funciona más eficientemente, tanto para leer como para escribir. El problema potencial de este tipo de memoria si se usa para escritura es que, frente a un apagado inesperado del sistema, puede haber información que se pierda, y esto genere posibles problemas de consistencia en la base de datos o en las aplicaciones ejecutadas.
Otra característica particular que presentan los discos para servidores es que son hot swap, es decir, pueden intercambiarse en caliente, sin necesidad de apagar el equipo.

Módulo TPM

Como comentamos anteriormente, los procesadores modernos incorporan instrucciones especializadas, las cuales les permiten gestionar con mayor eficiencia las tareas de encriptación. Pero también existe un módulo especializado, denominado **TPM** (*Trusted Platform Module*), que permite almacenar llaves de encriptación, generar números aleatorios (no pseudoaleatorios, como se puede realizar mediante software), calcular hashes, y realizar otras funciones relacionadas.

Los módulos TPM permiten tener un mayor nivel de seguridad y reducir la carga de trabajo de la CPU. Su arquitectura es abierta y está definida en el estándar ISO/IEC 11889. Actualmente, existen numerosos fabricantes que los comercializan, lo que implica que podemos encontrar estos módulos en casi todos los equipos modernos.

Aquí vemos el **Proliant DL360**; es posible apreciar los componentes dispuestos en bloques.

Fuente de poder

Otra de las características distintivas en los servidores es la fuente de alimentación eléctrica. En general, estos poseen fuentes redundantes, es decir que, ante la falla de una de ellas, la otra continúa brindando energía al motherboard y sus componentes. Además, las fuentes son **hot swap**, lo que permite retirar una defectuosa y colocar otra nueva sin necesidad de apagar el equipo o interrumpir el servicio. El hecho de contar con dos fuentes de poder distintas permite enchufarlas a distintos tomas o fases eléctricas. Las fuentes utilizadas en servidores entry level implementan una variante de ATX llamada **EPS** (*Entry-Level Power Supply Specification*).

El estándar EPS ofrece mayor estabilidad y poder eléctrico. La potencia que brinda va desde 550 W hasta 800 W, y tiene 8 voltajes de salida (3.3 V, 5 V, 12 V1, 12 V2, 12 V3, 12 V4, -12 V, y 5 VSB). Este estándar fue desarrollado en conjunto por Intel, Dell, Hewlett Packard, Silicon e IBM.

Tarjeta de red

Como muchos de los componentes presentes en un servidor, la placa de red posee características significativamente distintas de las de una terminal de usuario.

Existen dos tipos de placas: las que utilizan cables de cobre y las que usan fibra óptica. Los cables de cobre emplean un conector RJ-45, y el estándar usado es CAT5 o CAT6, según las velocidades deseadas; CAT6 permite velocidades de hasta 10 Gigabit. Los enlaces de fibra óptica se usan, principalmente, para conectarse con **SAN** (*Storage Area Network*) utilizando el estándar Fiber Channel (FCP), un protocolo de transporte comparable con TCP, que transporta comandos SCSI.

Existe una gran variedad de conectores para fibra óptica. Los más comunes son **LC** (*Lucent Connector*) y **SC** (*Subscriber Connector*).

Otra arquitectura de comunicaciones utilizada en servidores de altas prestaciones es InfiniBand, que provee de una gran capacidad de transporte, baja latencia y **QoS** (*Quality of Service*). Esta arquitectura establece una conexión entre el servidor y los nodos de alta performance, como un storage.

Tarjeta de video

A diferencia de lo que sucede en equipos de escritorio, la placa de video pasa casi inadvertida en un servidor, donde raramente es utilizada, ya que cuenta con mínimos requisitos gráficos. Estas placas suelen estar embebidas en el **system board** y representan uno de los componentes más baratos.

Administración remota

Dado que los servidores no suelen ser fácilmente accesibles para los administradores, cuentan con facilidades para administrarlos en forma remota. Para este fin existen las herramientas *Remote Management Support*.

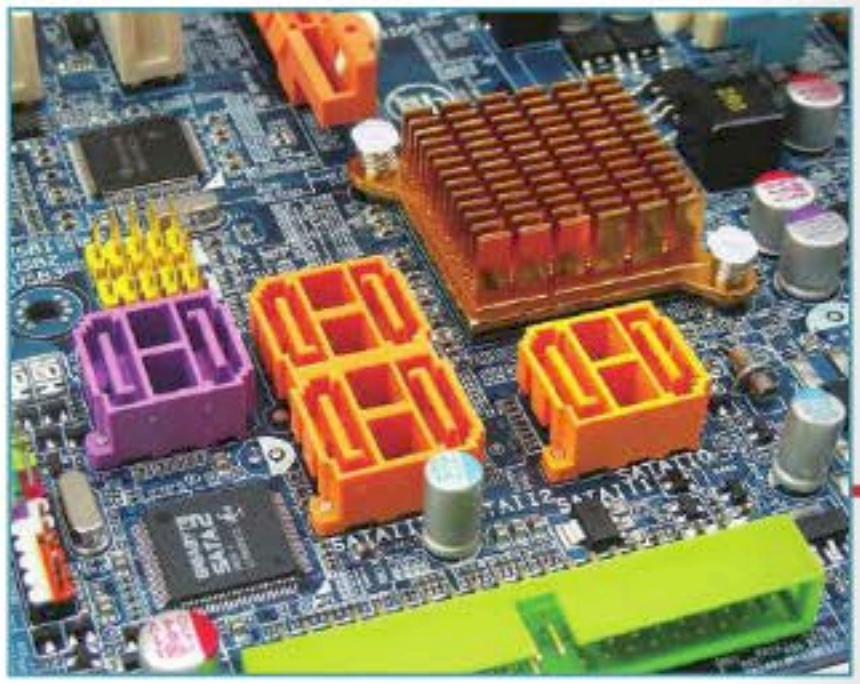
ILO (*Integrated Lights Out*) es una tecnología desarrollada por HP, y una de las más difundidas, que permite ver los eventos del servidor, como el reinicio del equipo, el cambio de partes, etc. También da la posibilidad de ver e interactuar con la pantalla como si estuviéramos delante del servidor. Es posible forzar el reinicio o apagado, de la misma manera que si lo hiciéramos oprimiendo los botones correspondientes. Esta funcionalidad puede usarse si el servidor tiene o no un sistema operativo instalado o si está apagado. Esta capacidad se llama *Out of Band Management* o *Lights-Out Management* (**LOM**). ■

Fuente de poder silenciosa, especial para usar en servidores.

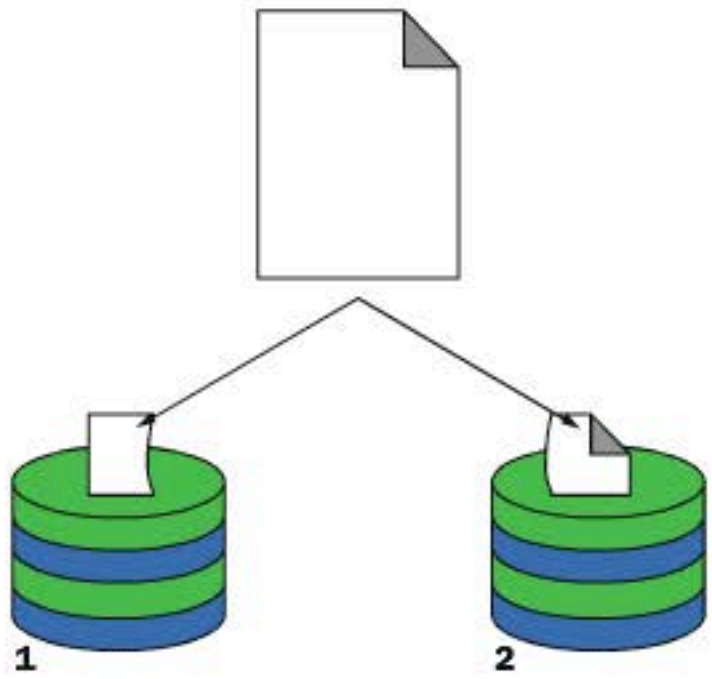
Tecnología RAID

En la actualidad, esta tecnología se encuentra presente en la gran mayoría de los motherboards, pero muy pocos usuarios sacan provecho de las numerosas ventajas que ofrece.

Un **sistema RAID** es un conjunto de dos o más discos cuya finalidad es obtener ciertos beneficios, como mayor velocidad y/o seguridad, dependiendo de la cantidad de componentes utilizados y su configuración. Esta tecnología se volvió más popular en los últimos años gracias a la inclusión de interfaces Serial ATA en las placas madre de línea baja, media y alta. Anteriormente, era preciso tener hardware especial para montar un conjunto RAID, como controladoras SCSI o Parallel-ATA compatibles.
Hoy en día, esas placas especiales no son necesarias, ya que prácticamente todo motherboard incorpora varios puertos Serial ATA con posibilidad de montar un set RAID. Sin embargo, la primera versión de RAID data del año 1987, cuando se lo implementó por primera vez en una universidad estadounidense con el único fin de que dos o más discos conformaran una unidad que sumara la capacidad de todos como un único volumen. En 1988, se definieron los niveles de RAID del 1 al 5. Pero la primera patente que trata sobre combinar discos duros para tener mayor tolerancia a fallos es del año 1978, y aunque el método era similar, no se llamaba RAID.



Tanto los motherboards de gama alta, como también los de gama media y baja incorporan puertos **Serial ATA** con soporte para montar matrices RAID.



En una matriz RAID 0, cada archivo es dividido en segmentos que se distribuyen en cada uno de los discos físicos que conforman el volumen.

Tipos de RAID

La elección de los diferentes niveles de RAID dependerá de las necesidades del usuario en lo que respecta a factores como seguridad, velocidad, capacidad, costos, etc. Cada nivel de RAID ofrece una combinación específica de tolerancia a fallos (redundancia), rendimiento y costos, desarrollados para brindar soluciones a los diferentes requisitos de almacenamiento.
La mayoría de los niveles RAID pueden satisfacer de manera efectiva solo uno o dos de estos criterios.
No hay un nivel de RAID mejor que otro, sino que cada uno es apropiado para determinadas aplicaciones y ámbitos. Resulta frecuente el uso de varios niveles de RAID para distintas aplicaciones del mismo servidor. Oficialmente, existen siete niveles (del 0 al 6), definidos y aprobados por el **RAID Advisory Board** (**RAB**). Luego, están las posibles combinaciones de estos niveles (1+0, 5+0, etc.). Los niveles RAID 0, 1, 0+1 y 5 son los más usados.

RAID 0

Se usa para obtener altas velocidades de transferencia, pero sin tolerancia a fallos. Es también conocido como **stripping**,

que significa "separación" o "fraccionamiento", porque los datos se dividen en pequeños segmentos que se distribuyen entre dos o más unidades físicas. Este nivel de array o matriz no ofrece tolerancia a fallos. Como no posee redundancia, RAID 0 no ofrece ninguna protección de los datos. Si uno de los discos físicos de la matriz tiene problemas, el resultado es la pérdida de los datos. Por lo tanto, RAID 0 no se ajusta realmente a la sigla RAID, ya que no hay redundancia. Simplemente, se trata de una serie de unidades de disco conectadas en paralelo que permiten una transferencia simultánea de datos a todos ellos, con lo cual se obtiene una gran velocidad en las operaciones de lectura y escritura. La velocidad de transferencia de datos aumenta en relación al número de discos que forman el conjunto.

Esto representa una gran ventaja en operaciones secuenciales con archivos de gran tamaño. Así, este método es aconsejable cuando se trabaja con aplicaciones de retoque fotográfico, audio, video o CAD; es decir, es una buena solución para cualquier aplicación que necesite un almacenamiento a gran velocidad pero que no requiera tolerancia a fallos. Para implementar una solución RAID 0 se precisa un mínimo de dos unidades de disco.

Un sistema RAID en stripping aumenta considerablemente la velocidad de transferencia, sobre todo, la lineal, no muy presente en la práctica, pero sí en la lectura aleatoria y la que insume buffer de disco. En general, el incremento en el rendimiento en este tipo de matriz RAID suele ser del 50%.

En todos los casos, y como un factor que juega en contra, se nota un leve aumento en el consumo de CPU, pero los valores no son alarmantes en absoluto. Otro factor en el que se aprecia una gran mejora en el rendimiento es en el tiempo de carga del sistema operativo, y lo mismo sucede al iniciar aplicaciones pesadas.

LA ELECCIÓN DE LOS NIVELES DE RAID DEPENDE DEL USUARIO EN LO QUE RESPECTA A SEGURIDAD, VELOCIDAD, CAPACIDAD, ETC.

JBOD

Si bien la concatenación de discos, también llamada **JBOD** (*Just a Bunch Of Drives*, solo un montón de discos) no es uno de los niveles RAID numerados, sí es un método popular de combinar múltiples discos duros físicos en un solo disco virtual. Como su nombre lo indica, los discos son meramente concatenados entre sí, de manera que se comportan como un único disco. De esta forma, la concatenación es como el proceso contrario al de particionar: mientras este toma un disco físico y crea dos o más unidades lógicas, JBOD usa dos o más discos físicos para crear una unidad lógica. Al tratarse de un conjunto de discos independientes sin redundancia, puede ser visto como un método similar al de RAID 0. JBOD es usado a veces para combinar varias unidades pequeñas (obsoletas) en una unidad mayor con un tamaño útil. Una ventaja de JBOD sobre RAID 0 es que, en caso de que un disco falle, en RAID 0 suele producirse la pérdida de todos los datos del conjunto, dado que la información está distribuida en "rodajas" por las unidades que componen la matriz, mientras que en JBOD solo se pierden los datos del disco afectado, pero se conservan los de los restantes. Sin embargo, JBOD no supone ninguna mejora de rendimiento.

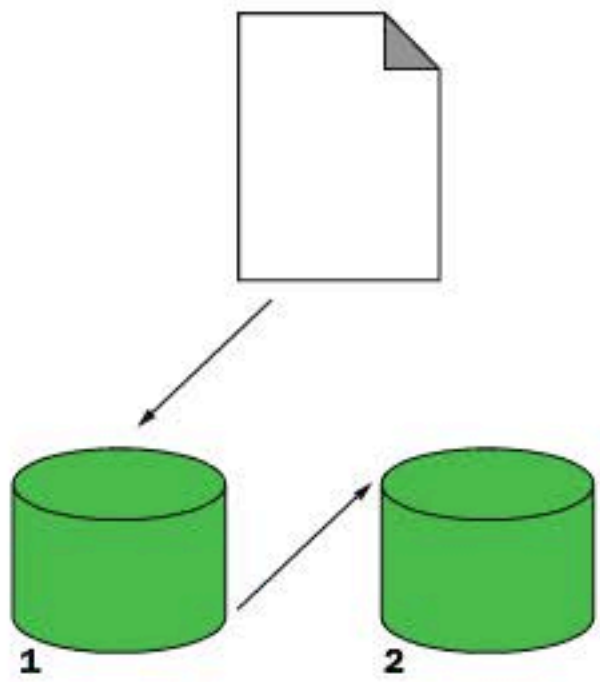
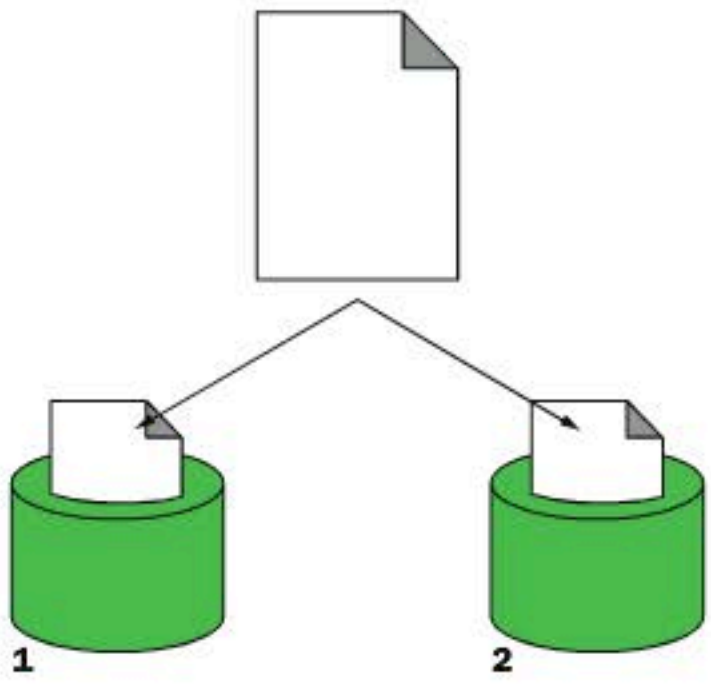


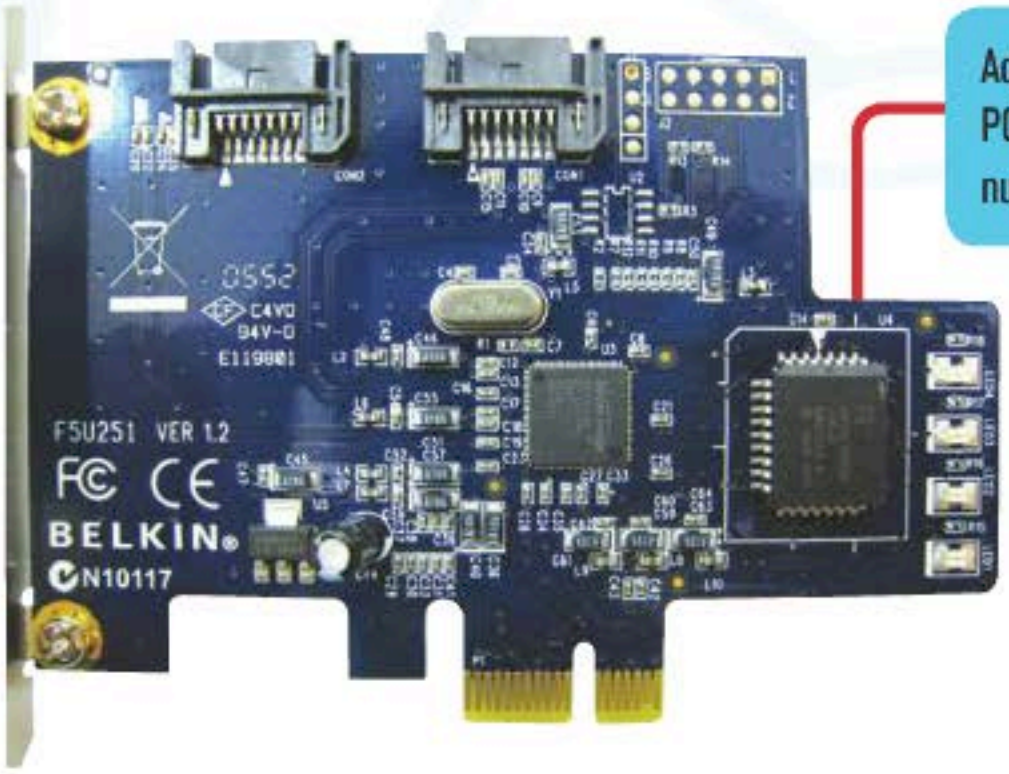
Diagrama de un array JBOD, donde dos unidades forman un solo volumen, una a continuación de la otra.

RAID 1

Este método también se denomina **mirroring**, que significa "espejado", porque cada disco que conforma el conjunto es un espejo del otro. Se basa en el uso de discos adicionales, sobre los que se realiza una copia en todo momento de los



Sistema RAID 1. Cada bit que se escribe en el disco se replica en el resto de las unidades; si uno falla, toda la información permanecerá intacta en otra unidad.



Aquí vemos una controladora **Serial ATA RAID** en formato PCI Express 1x, ideal si no tenemos una incorporada en nuestro motherboard o si esta se encuentra dañada.

datos que se están modificando. RAID 1 ofrece una excelente disponibilidad de los datos mediante la redundancia total de estos. Para lograrlo, se duplican todos los datos de una unidad o matriz en otra; así, se asegura la integridad de los datos y la tolerancia a fallos, ya que ante un problema, la controladora sigue trabajando con los discos no dañados sin detener el sistema. Los datos se pueden leer desde la unidad duplicada sin que se produzcan interrupciones.

RAID 1 es una alternativa costosa para los grandes sistemas, porque las unidades se deben añadir en pares con el fin de aumentar la capacidad de almacenamiento. Pero es una buena solución para las aplicaciones que requieren redundancia cuando hay solo dos unidades disponibles. Los servidores de archivos son un buen ejemplo. Al igual que en RAID 0, se necesita un mínimo de dos unidades para implementar una solución de este tipo.

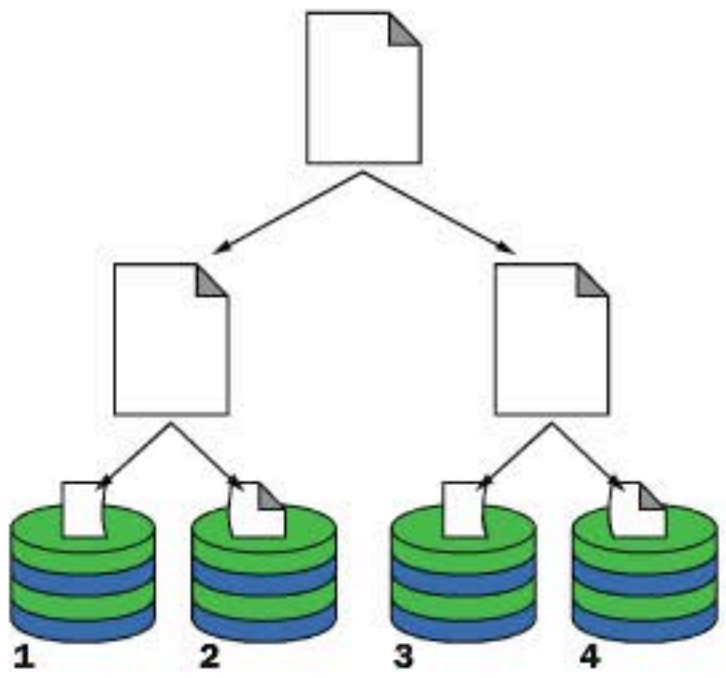


Diagrama de un RAID combinado (0+1), donde se gana en velocidad y en seguridad de los datos. La desventaja es el alto costo de su implementación.

RAID 0+1

También llamado RAID 0/1 o RAID 10, es una combinación de los arrays vistos anteriormente, que ofrece velocidad y tolerancia a fallos al mismo tiempo. El nivel de RAID 0+1 segmenta la información para mejorar el rendimiento y, además, utiliza un conjunto de discos espejados para lograr la redundancia de datos. Al ser una variedad RAID híbrida, unifica las ventajas de rendimiento que brinda RAID 0 con la redundancia que aporta RAID 1. Sin embargo, la principal desventaja es que se necesita un mínimo de cuatro unidades, y solo dos de ellas se utilizan para el almacenamiento efectivo de información. RAID 0+1 es la solución ideal para cualquier uso que requiera alto desempeño y tolerancia a fallos, pero no, una gran capacidad. Normalmente, se lo implementa en entornos como servidores de aplicaciones, que permiten a los usuarios acceder a una aplicación en el servidor y almacenar datos en sus discos duros locales, o como los servidores web, que permiten a los usuarios entrar en el sistema para localizar y consultar información. Este nivel de RAID es el más rápido y el más seguro, pero, como desventaja, el más costoso de implementar.

RAID 2

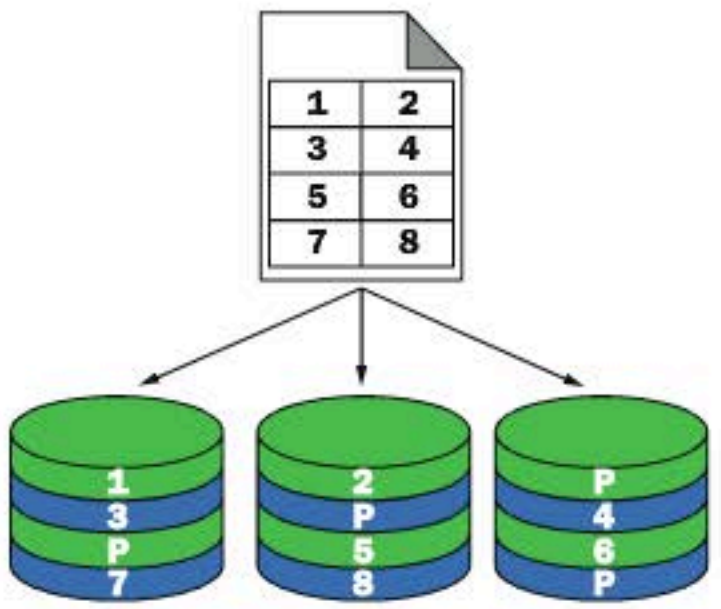
El nivel 2 de RAID adapta la técnica comúnmente empleada para detectar y corregir errores en memorias de estado sólido. El código **ECC** (*Error Correction Code*) se intercala a través de varios discos a nivel de bit. El sistema empleado se conoce como **hamming**, ya que se utiliza tanto para detección como para corrección de errores (*Error Detection and Correction*).

Si bien RAID 2 no hace uso completo de las amplias capacidades de detección de errores contenidas en los discos, las características del código hamming también restringen las configuraciones posibles de matrices para RAID 2, particularmente, el cálculo de paridad de los discos. Está orientado a aplicaciones que requieran una alta tasa de transferencia, y resulta menos conveniente para aquellas otras que tienen una alta tasa de demanda de accesos.

RAID 3

Destina un único disco del conjunto al almacenamiento de información de paridad. La información de **ECC** (*Error Checking and Correction*) se emplea para detectar errores. La recuperación de datos se consigue mediante cálculos, gracias a la información registrada en los otros discos.

Este método ofrece altas tasas de transferencia, alta fiabilidad y alta disponibilidad, a un costo ligeramente inferior a un RAID 1 (espejado). Sin embargo, su rendimiento de transacciones es deficiente porque todos los discos del conjunto operan



RAID 5: rápido, confiable y costoso. Se requieren al menos tres discos duros para montar un RAID 5.

al mismo tiempo. Para implementar una solución RAID 3, se necesita contar con un mínimo de tres discos duros.

RAID 4

La tolerancia a fallos se basa en el uso de un disco dedicado a almacenar la información de paridad calculada a partir de los datos que están en los otros discos. Ante una falla de cualquiera de los discos, la información se puede reconstruir en tiempo real mediante una operación manejada por la controladora. Debido a su organización interna, este RAID es especialmente indicado para el almacenamiento de archivos de gran tamaño, lo cual lo vuelve ideal para aplicaciones de video, sonido o gráficas donde se requiera, además, seguridad de los datos.
Se necesita un mínimo de tres unidades para implementar una solución RAID 4. La ventaja sobre RAID 3 radica en que se puede acceder a los discos de manera individual.

RAID 5

Ofrece tolerancia a fallos y optimiza la capacidad del sistema al permitir el uso de hasta el 80% de la capacidad total de los discos. Esto se logra mediante el cálculo de información de paridad y su almacenamiento alternativo por bloques distribuidos en todos los discos del conjunto. La información se graba a modo de bloques, alternativamente, en todos ellos. Así, si cualquiera de las unidades de disco falla, se puede recuperar la información sobre la marcha, sin que el servidor deje de funcionar.
El RAID 5 es el nivel de RAID más eficiente y el de uso obligado para las aplicaciones de servidor básicas en una empresa.
En comparación con otros niveles de RAID con tolerancia a fallos, RAID 5 ofrece la mejor relación costo-rendimiento en un entorno con varias unidades. Gracias a la combinación del fraccionamiento de datos y a la paridad como método para recuperar datos en caso de fallas, es una solución ideal para los entornos de servidores en los que gran parte del acceso a disco es aleatoria, la protección y disponibilidad de los datos es fundamental, y el costo es un factor importante. Este nivel de array es especialmente indicado para trabajar con sistemas operativos multiusuario, como Linux, UNIX o Windows Server. Se requiere un mínimo de tres unidades para implementar una solución de esta clase.

Consideraciones

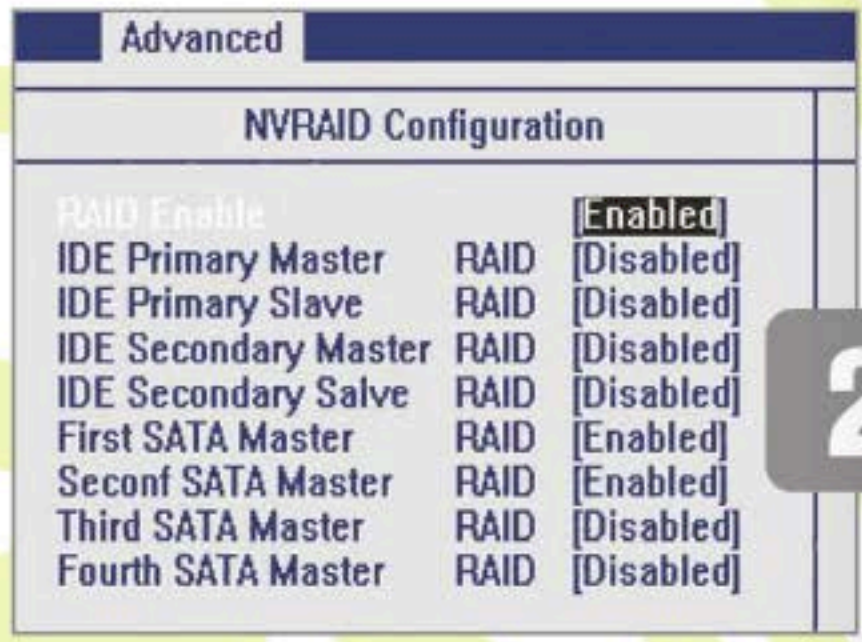
Existe un parámetro muy importante que se configura desde el propio BIOS Setup de la controladora RAID (no debemos confundirlo con el BIOS Setup del motherboard); se ingresa a él mediante alguna combinación de teclas indicada en pantalla, como `CTRL+I`. Allí se seleccionan los discos duros que formarán parte del array, qué método RAID usarán (`Stripe` o `Mirror`), el tamaño de cada bloque stripe y otros aspectos.
El tamaño del bloque de datos es un factor importante.
Por ejemplo, si elegimos un valor de 32 KB para cada bloque, un archivo de 320 KB que se aloje en el volumen será dividido en diez bloques, y se guardarán cinco en cada unidad física, suponiendo que el RAID esté conformado por dos discos. Así se repartirán el trabajo entre ambos y se ganará en performance.
Un valor ideal puede ser 64 KB, por ser un balance ideal entre velocidad y cantidad de accesos al disco. Por ejemplo, si elegimos un valor de 16 KB para los bloques de datos, cada archivo deberá dividirse en gran cantidad de bloques, y los accesos al disco aumentarán. Por consiguiente, la actividad de la controladora y de los discos será mayor. Si elegimos un valor muy grande para el bloque de datos, como 256 KB, muchos archivos pequeños se guardarán en un solo disco y no se obtendrá ganancia en velocidad. ■

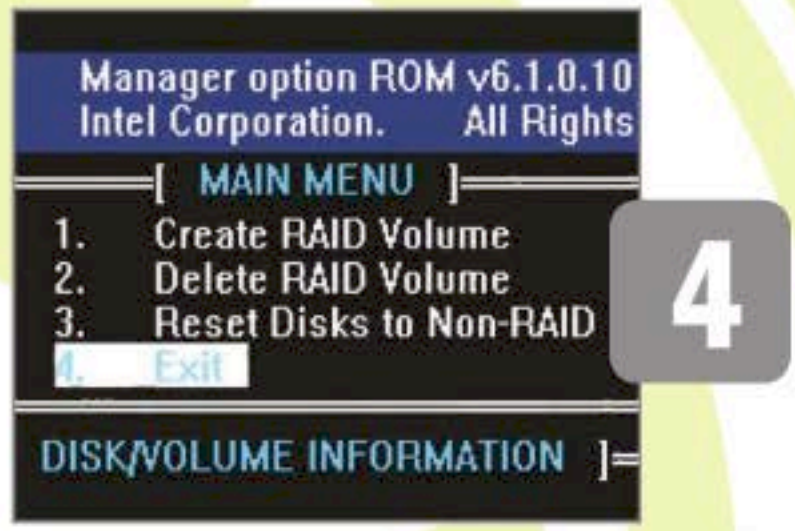
RAID en Windows Server 2003

No bien comienza la instalación de Windows Server 2003, en la parte inferior de la pantalla aparece un mensaje que nos advierte que, para instalar el sistema en unidades conectadas a controladoras SCSI o RAID, debemos pulsar la tecla F6. Al hacerlo, más adelante, se nos solicitará un disquete para cargar esos controladores y hacer que Windows reconozca el volumen donde instalarse. En Windows Server 2008 y 2012, estos drivers se pueden cargar vía pen drive o CD.

Cómo montar una matriz RAID 1

Los discos duros pueden tener distintas capacidades, marcas, modelos y normas de transferencia, pero lo ideal es adquirir dos discos idénticos.



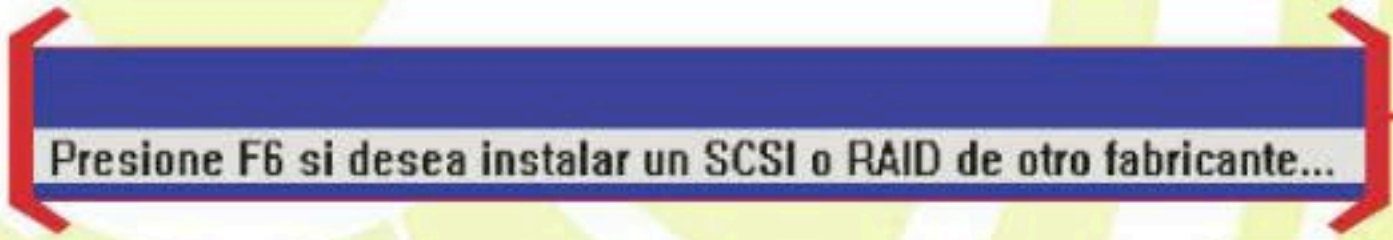


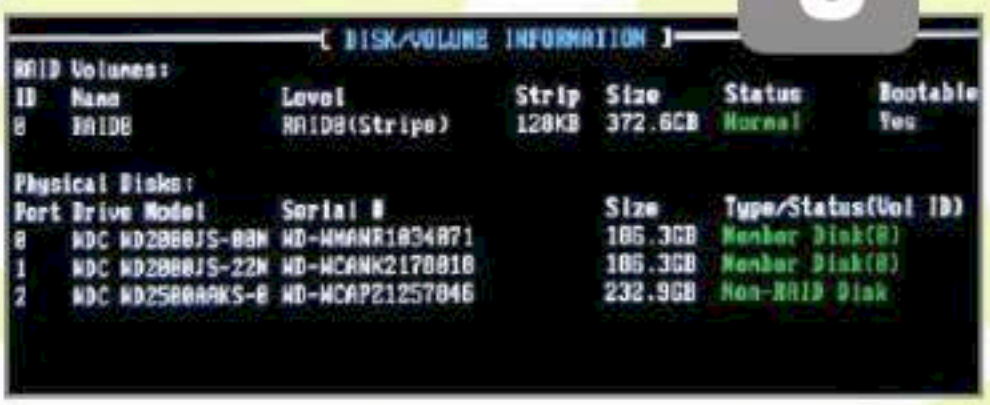
1 Los elementos para montar un RAID (tanto stripping como mirroring) son: al menos dos discos duros (pueden ser Serial ATA, IDE o SCSI) y un motherboard con una controladora RAID incorporada. En caso de que nuestra placa madre no tenga una, es posible adquirirla por separado y colocarla en un slot **PCI Express**.

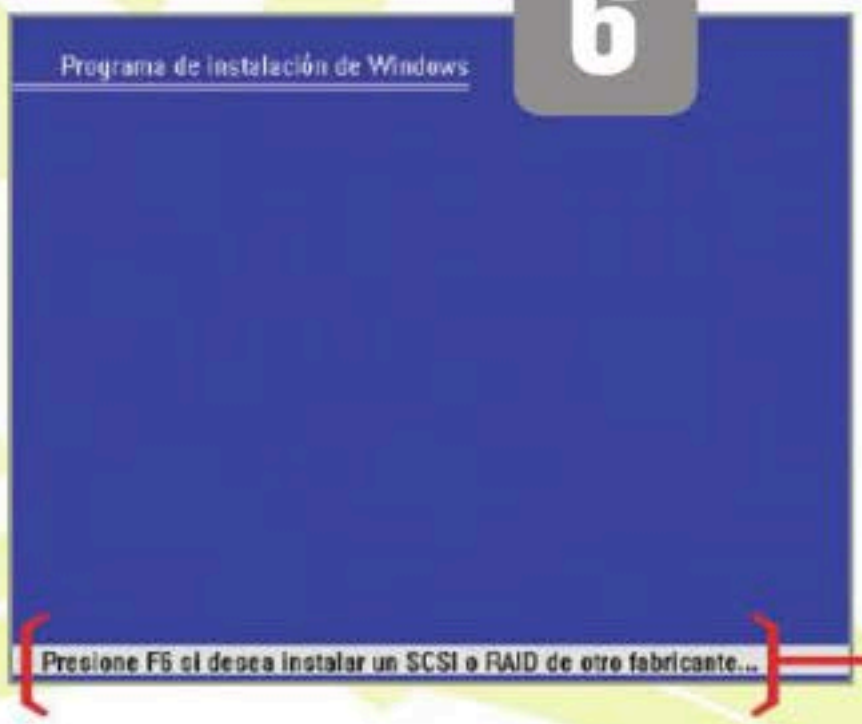
2 En el **Setup del BIOS** del motherboard debemos seleccionar el modo de trabajo de la controladora Serial ATA en **RAID**. En los modelos de motherboards que no tengan esta controladora nativa en el chipset, o si se trata de una controladora externa, debemos elegir la opción **SCSI** como primer ítem en la secuencia de booteo.

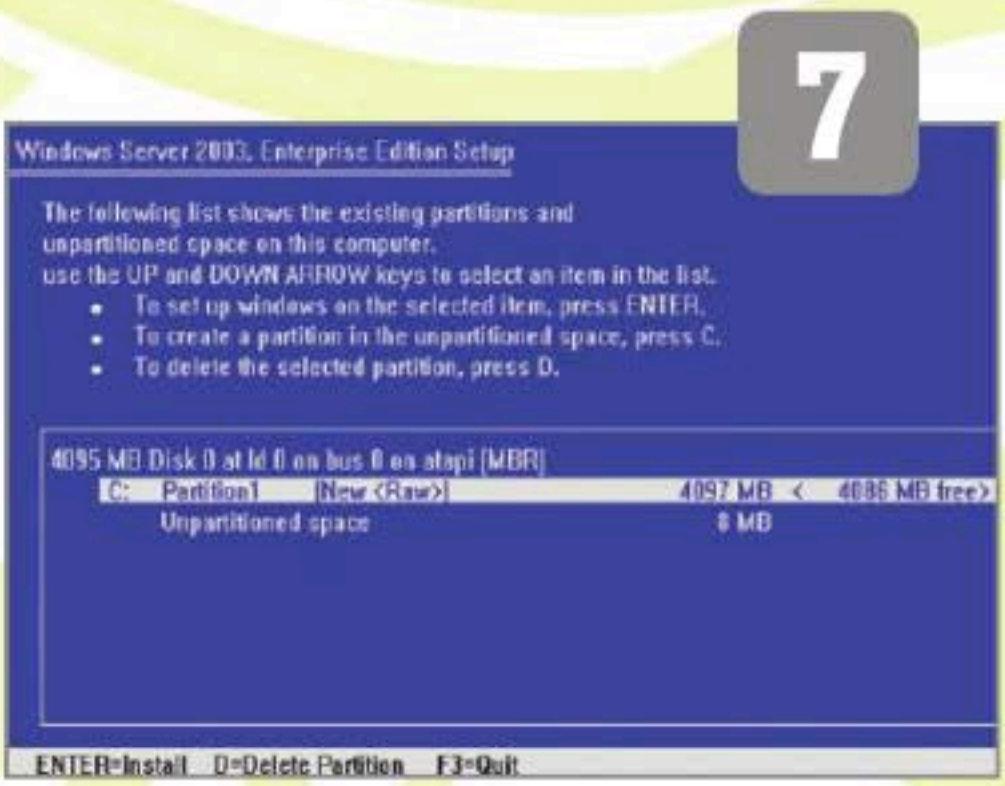
3 La siguiente pantalla que vemos corresponde a la controladora RAID. Allí se indica cómo ingresar al **Setup** de su BIOS; es con las teclas **CTRL+I** o **CTRL+A**. Desde aquí podremos crear y borrar sets RAID y, además, ver el estado SMART de los discos duros.

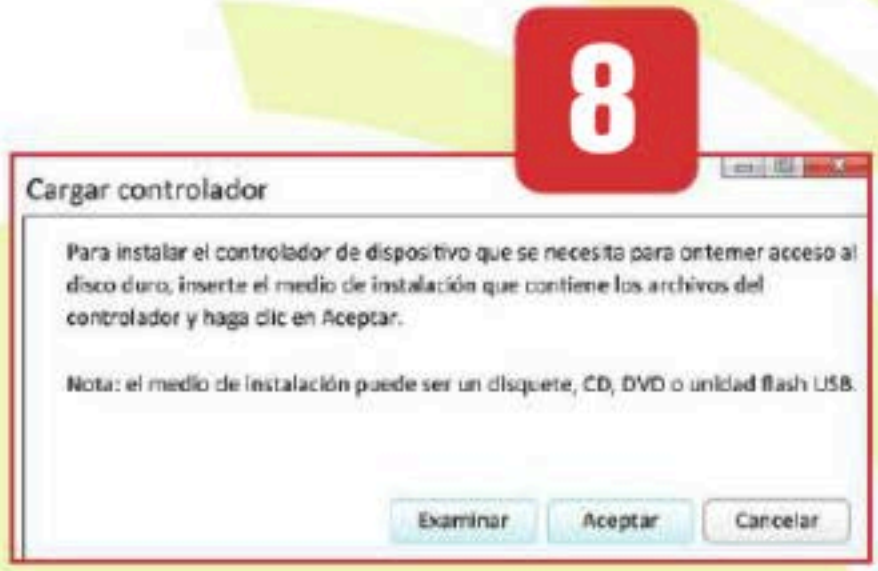
4 Una vez dentro del Setup de la controladora, podemos crear un array ingresando en la función **Create RAID Volume**. Allí elegimos qué discos formarán parte del set, en caso de que tengamos más de dos.











5 Debemos elegir uno de estos dos caminos: modo **Stripe** (RAID 0) o modo **Mirror** (RAID 1). En caso de preferir mayor velocidad, seleccionamos el primero. Entonces, deberemos establecer el valor para los bloques de datos; se recomienda 64 o 128 KB.

6 Al comienzo de la instalación de Windows Server 2003, en la parte inferior de la pantalla aparece un mensaje que nos advierte que, para instalar el sistema en unidades conectadas a controladoras SCSI o RAID, debemos pulsar la tecla **F6**. Más adelante se nos solicitará un disquete (provisto con el motherboard, o es posible crearlo desde un instalador ubicado en la carpeta **Drivers/RAID** del CD-ROM de la placa madre).

7 Una vez ingresados los controladores de la interfaz RAID, aparece un volumen que suma la capacidad de los discos (en caso del modo **Stripe**). Entonces, procedemos a seleccionarlo como volumen destinado a instalar Windows Server 2003.

8 En la instalación de Windows Server 2008 o 2012, un aire renovador mejoró el proceso de carga de drivers para controladoras RAID. Ahora, estos pueden ingresarse vía CD-ROM o pen drive USB, con lo cual este último paso del procedimiento se torna más cómodo y ☒exible para el usuario. El resto del procedimiento es idéntico al de la instalación de Server 2003.

El BIOS Setup de un servidor

Aquí analizaremos todos los detalles del BIOS Setup, encargado del arranque y la administración de dispositivos en un servidor.

El **BIOS** o *Basic Input/Output System* es el software encargado de inicializar la computadora y administrar los periféricos. Entre sus varias funciones, se encarga de testear los componentes principales del equipo e inicializar el sistema operativo.
El BIOS es el primer software que ejecuta el equipo al encenderlo. Construye una capa de software que independiza al hadrware del sistema operativo, lo que permite que este interactúe de una manera estandarizada con los distintos periféricos, sin importar su modelo o fabricante.
Los dispositivos se catalogan como de entrada o de salida. Entre los más comunes encontramos teclado y mouse, como dispositivos de entrada; y monitor, de salida.

La implementación del menú de configuración UEFI de ASUS permite tener una mejor visualización del estado del equipo.

Funcionamiento

Uno de los errores más comunes es confundir al utilitario o menú que se utiliza para configurar el BIOS con el BIOS en sí.

De hecho, los primeros equipos IBM que implementaron la funcionalidad BIOS no contaban con un menú de configuración, pero naturalmente sí tenían un BIOS para controlar los dispositivos e inicializar el equipo.
La primera acción que realiza el BIOS es chequear el correcto funcionamiento de los dispositivos y periféricos; esta acción se denomina Power-OnSelf-Test (POST). Algunos de los dispositivos que testea son la CPU, la memoria RAM, las interrupciones, el chipset y los periféricos básicos (video, teclado, disco duro y lector

Interfaz ACPI

Advanced Configuration and Power Interface es el estándar que permite que el sistema operativo pueda controlar el consumo eléctrico. Fue desarrollado por Intel y otras empresas, y da la posibilidad de administrar el consumo del equipo, el procesador y los dispositivos. Esto permite que el S.O. encienda, apague, suspenda o hiberne el equipo, y que controle la performance y, en consecuencia, el consumo eléctrico. Tanto Intel como AMD han desarrollado distintas tecnologías para reducir el consumo eléctrico del procesador cuando su uso es bajo. **SpeedStep** de Intel y **Cool'n'Quiet** de AMD son las implementaciones más conocidas.

de CD/DVD). En caso de detectar algún problema en ellos, lo informa al usuario, ya sea por pantalla, por medio de sonidos o a través de los LEDs del equipo.

Software

El software se almacena en un chip **EEPROM** (*Electrically Erasable Programmable Read-Only Memory*) que tiene la característica principal de ser no volátil, es decir que no se borra al desconectarle la energía, sin importar cuánto tiempo permanezca apagado. La pila que poseen los motherboards (habitualmente, una CR2032) tiene la función de mantener las configuraciones y la hora almacenadas en el CMOS, pero no es necesaria para mantener el BIOS en sí mismo, ya que, como mencionamos anteriormente, este no se borra por falta de energía.

UEFI SE PROPONE PARA REEMPLAZAR AL BIOS; MANTIENE LA COMPATIBILIDAD, INTRODUCIENDO VARIAS MEJORAS.

CMOS

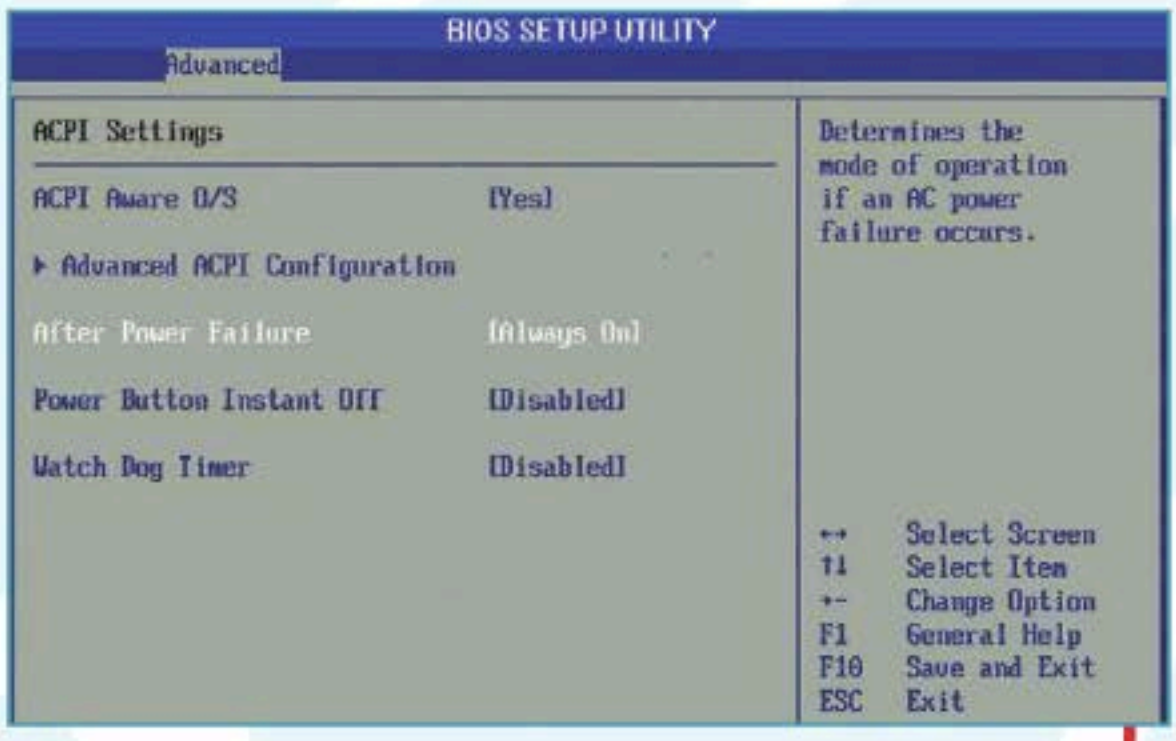
El **CMOS** (*Complementary Metal Oxide Semiconductor*) es una antigua tecnología utilizada en la construcción de circuitos integrados. Se usa para almacenar las configuraciones del BIOS, ya que su simple diseño consume poca energía, emite poco calor y es inmune al ruido. La manera tradicional de restablecer la configuración predefinida del BIOS es, justamente, desconectando la pila o utilizando un jumper destinado a tal fin.
La memoria EEPROM permite que el software sea fácilmente actualizado, sin necesidad de abrir el gabinete del equipo o retirar el chip. Los fabricantes de servidores recomiendan mantener actualizado el BIOS porque periódicamente se aplican mejoras o se corrigen errores. Incluso, en algunos casos se pueden realizar mejoras que influyen en la performance del servidor de modo significativo.

Servidores

El BIOS presente en un servidor posee funcionalidades más amplias que las de una estación de trabajo. Debido a su criticidad y al hecho de que debe permanecer encendido durante la mayor parte de su vida útil, el BIOS monitorea todos los dispositivos a fin de resguardar información útil. Así como las computadoras de a bordo de los automóviles miden el consumo y las velocidades desarrolladas, el BIOS almacena información histórica sobre uso de la CPU y memoria, eventos de apagado y encendido, temperatura, fallas, y más. Definitivamente, esta funcionalidad afecta en cierta medida la performance del equipo, porque genera interrupciones en el trabajo del procesador. Según la funcionalidad que se habilite, por ejemplo, para monitorear el uso y consumo del procesador, puede generar 8 interrupciones por segundo.
Los sistemas operativos modernos operan en modo protegido, y no utilizan el BIOS ni las interrupciones que este genera para acceder a los dispositivos, ya que implementan sus propios mecanismos de acceso al hardware.
Si bien el BIOS de los equipos x86 es un estándar de hecho que se mantuvo y fue evolucionando a lo largo de los años, algunos fabricantes de servidores desarrollaron otros estándares que

El chip Fujitsu FRAM mejora el desempeño y el consumo eléctrico de las tradicionales memorias EEPROM.

tienen la misma funcionalidad, pero de forma diferente. Es el caso de los equipos Sun (actualmente, Oracle), que implementan el sistema **Open Boot**, también aplicado por IBM y Apple.
Otra alternativa al BIOS, pero compatible con él, es la iniciativa **UEFI**. Esta interfaz elimina alguna de las limitaciones del antiguo BIOS, como el modo de 16 bits de arranque y la limitación de 1 MB de direccionamiento, entre otras.
En un principio, la configuración del BIOS y el hardware se realizaba mediante jumpers, pero en la actualidad se lleva a cabo por software desde un menú de configuración. Para acceder a este menú, podemos hacerlo localmente por teclado y video, o en forma remota. La combinación de teclas para acceder al menú puede ser diferente en uno u otro modo. ■



Menú de configuración del BIOS de un servidor con ACPI habilitado.

Tecnología EFI y UEFI

Se trata de una tecnología que va reemplazando la obsoleta plataforma BIOS, tanto en servidores de red, como en equipos portátiles y de escritorio. Conoceremos aquí sus características y ventajas.

El BIOS es el componente de la PC que menos evolución tuvo a lo largo de estos más de 30 años, comparándolo con otros como el procesador, la memoria o las placas de video.
El proceso de bootstrap, o interacción con el arranque del sistema operativo, tampoco cambió demasiado.
Si bien **EFI** (*Extensible Firmware Interface*) fue desarrollado y estandarizado por Intel hace años, todavía no ha llegado a todos los equipos, ya que algunos de gama baja aún continúan utilizando el obsoleto BIOS. Este aspecto cambiará en el corto plazo, para lograr una implementación absoluta.

EFI fue desarrollada a principios de siglo, siendo **IBI** (*Intel Boot Initiative*) su sigla y nombre originales. La idea era suplir las necesidades de los más importantes desarrolladores de sistemas operativos y de hardware, tal como la plataforma Itanium, que rechazaban al clásico BIOS como base de firmware. En 2005, se creó la fundación **Unified EFI**, para dar difusión a la plataforma EFI entre los fabricantes de hardware. Fue así que **UEFI** quedó como nuevo nombre de la plataforma, utilizada no solo para procesadores Itanium, sino también para todo el abanico de la arquitectura x86 y x64.

Sistemas operativos que lo soportan

La finalidad del estándar UEFI es suplantar la forma en que se inicia un sistema operativo y, por lo tanto, la manera en que este o el software booteable accede a los dispositivos. Ningún sistema operativo de Microsoft de 32 bits soporta ni soportará UEFI. Según un comunicado de la compañía de Redmond, esto se debe a la inminente migración de las plataformas de 32 a 64 bits, por considerar que los sistemas operativos de 32 bits son prácticamente obsoletos. Windows 7 x64 tiene un soporte básico para UEFI, mientras que Windows 8 x64 ofrece un soporte completo para esta tecnología, y lo mismo ocurre con Windows Server 2012. En el universo GNU/Linux, tenemos a Elilo, un bootloader UEFI para Linux que soporta plataformas UEFI tanto IA-64 como IA-32 (x86).

¿Qué es UEFI?

A modo de introducción, podemos decir que UEFI es un sistema operativo en miniatura, encargado de encender el equipo; se ubica entre el firmware del equipo y el sistema operativo propiamente dicho.

Menú gráfico UEFI del motherboard de un servidor. Intel llamó a este panel de configuración Visual BIOS.

Las ventajas que brinda este nuevo método son la rapidez en el arranque de los equipos (del orden de la mitad de lo que demoran los basados en BIOS), la seguridad y una mayor adaptabilidad a los cambios de hardware por parte de los fabricantes.
Otro de los beneficios que podemos mencionar es la capacidad de UEFI para gestionar ciertos parámetros en el hardware, incluso, de forma remota (o sea, desde otros equipos), por medio de una interfaz gráfica. Al ser un "mini sistema operativo", una porción de UEFI se alberga en el disco duro y se comunica con el firmware en sí. Uno de los puntos más criticados de este sistema es el hecho de que promueve y permite el uso de la tecnología Trusted Computing, empleada para controlar y comprobar firmas de aplicaciones y drivers, eliminando así la posibilidad de desarrollar programas usando ingeniería inversa.

Más en profundidad

Esta interfaz especifica un modelo para la interacción entre el firmware de un equipo y los sistemas operativos. Consiste en un grupo de tablas que contienen datos relativos a la plataforma, además de llamadas a los servicios de runtime y de booteo disponibles para el sistema operativo y su bootloader. Todo el conjunto de tablas de datos proporciona un entorno estandarizado que permite iniciar un sistema operativo y ejecutar programas previos al inicio. La arquitectura IA-64 define las tres capas de firmware siguientes:

- Capa de abstracción del procesador
- Capa de abstracción del sistema
- UEFI (interfaz de firmware extensible unificada)

Las tres funcionan en conjunto para proporcionar la inicialización del sistema y del procesador durante el booteo del sistema operativo. La capa de abstracción del sistema es una capa de firmware que aísla el sistema operativo y otro software de nivel superior, teniendo en cuenta las maneras de implementar las diferentes plataformas. Por otra parte, la capa de abstracción del procesador es la capa de firmware que se encarga de la implementación del microprocesador.
El entorno de inicio UEFI está formado por dos interfaces principales. La primera es el **UEFI Boot Manager Administrator**, una interfaz basada en menús que permite configurar y seleccionar las opciones de inicio. Desde el administrador UEFI Boot Manager, se puede cargar un sistema operativo, reiniciar la partición y configurar distintas opciones de la consola e inicio de sistema. La segunda es el shell UEFI, una interfaz de inicio de sistema, del tipo consola, a la cual se puede ingresar desde el UEFI Boot Manager.

Ventajas de UEFI

Las ventajas de UEFI son variadas; a continuación, listamos algunas de las más importantes:

- El firmware se programa en C, no en Assembler.
- No requiere trabajar en modo real.

Menú gráfico de un motherboard que soporta la tecnología UEFI, para reemplazar la anticuada apariencia del Setup del BIOS, basada en texto.

- Soporta UGA.
- Soporta GPT.
- Mejor soporte para PXE, Serial ATA 3, SCSI y USB 2.0 y 3.0.
- Todas las direcciones de memoria son accesibles.
- Su preinicio posee un servicio para acceder a una red TCP/IP.

UGA

El BIOS se basa en el estándar VGA para mostrar gráficos en la fase preboot y en el Setup del BIOS, con las consiguientes desventajas, como resoluciones de hasta 640x480, paletas de color limitadas, el anticuado modo texto, etc. En cambio, UEFI se basa en UGA (*Universal Graphics Adapter*), una nueva especificación para mostrar gráficos en entornos preboot. Podría decirse que UGA viene a reemplazar a un estándar tan obsoleto como lo es VESA. Además, el menú del Setup de UEFI soporta en forma nativa el uso del mouse, además del teclado.

GPT

UEFI especifica un nuevo esquema de particionamiento llamado **GTP** (*GUID Partition Table*), que utiliza identificadores para las particiones a nivel global (algo así como una **MAC Address** para los dispositivos de red). Este tipo de tabla de particiones es utilizado por las mencionadas versiones de Windows de 64 bits, y ofrece algunas ventajas sobre el clásico método basado en MBR:

- LBA de 64 bits (por lo tanto, el tamaño máximo de partición supera los 2 TB).
- Nombre de particiones de hasta 36 caracteres Unicode.
- Soporte para múltiples particiones.
- Presenta una doble tabla redundante.
- Futuras expansiones fácilmente aplicables.
- Se encarga de emplear una comprobación denominada CRC32 para mejorar la integridad de la información. ■

Seguridad aplicada a servidores de red

En estas páginas revisaremos la seguridad física del servidor y su entorno. También repasaremos los circuitos de alimentación y refrigeración que soportan la infraestructura.

Teniendo acceso físico a un servidor, es posible, por ejemplo, bootear con un CD, DVD o USB drive, y forzar una nueva contraseña de administrador para acceder al sistema. Es importante tener en cuenta que este es uno de los motivos por los cuales la seguridad física del servidor resulta casi tan importante como la seguridad lógica.

Algunas herramientas que realizan esta tarea en ambientes Windows son **Offline NT Contraseña & Registry Editor**, **ERD Commander** y **MS-DaRT** (*Microsoft Diagnostics and Recovery Toolset*), entre otras. Para Linux, por ejemplo, booteando en modo single user, es posible resetear la contraseña de root. Muchas de estas herramientas fueron pensadas en un principio para ser utilizadas por administradores que necesitaban resolver un problema. Pero, naturalmente, también pueden ser utilizadas por usuarios malintencionados, con el fin de realizar "hacking". Es importante conocer estas herramientas porque, de esta manera, podremos proteger los activos de un modo más consciente.

Seguridad perimetral

La primera medida que debemos considerar es la seguridad perimetral de los servidores. Es recomendable que estos se encuentren en un cuarto exclusivo de acceso restringido, al que denominaremos **server room**.
Este lugar no debe tener ventanas que puedan abrirse, ni tampoco paredes lindantes con el exterior. Es preciso llevar un registro de las personas que acceden a este recinto, ya sean empleados, visitas, proveedores o terceros en general. Para hacerlo, existen distintas herramientas de control de acceso que podemos usar, como las tradicionales cerraduras de llave, tarjetas magnéticas, de proximidad o autenticación biométrica. Seleccionemos el método que mejor se adecue a nuestras posibilidades y necesidades.

Con servidores cerrados, tenemos seguridad de acceso granular.

LAS CINTAS O MEDIOS QUE CONTIENEN LOS BACKUPS NO DEBEN PERMANECER EN EL MISMO RECINTO QUE LOS SERVIDORES.

Infraestructura necesaria

El estándar **TIA-942**, ampliamente aceptado en el mercado, define la infraestructura para un data center: establece la organización del espacio y la disposición de los elementos, la infraestructura del cableado, los niveles de confiabilidad y redundancia, y las consideraciones ambientales a considerar. Existen cuatro tipos de data centers: TIER-1, TIER-2, TIER-3 y TIER-4. La diferencia radica en el nivel de redundancia. Un data center TIER-1 carece de redundancia, en tanto que uno TIER-4 es redundante. Un data center TIER-4 requiere de un edificio independiente y no conectado con otras estructuras; tampoco puede lindar con la vía pública.

Racks

Una vez dentro del server room o data center, debemos considerar que los servidores estén instalados en racks con puerta y cerradura, con los tres paneles (los dos laterales y el posterior) instalados y asegurados; solo deberían abrirse los racks sobre los cuales se va a trabajar. Existen dos tipos básicos de racks: abiertos (bastidores) y cerrados. En caso de que un tercero deba realizar una instalación o tarea específica sobre un equipo dentro del server room, podremos asegurar que el resto de los equipos y su información permanezcan protegidos. A su vez, cada servidor puede tener un cierre propio que protege el acceso al frente del equipo, para impedir el apagado no autorizado o el acceso a la lectora de CD/DVD o puertos USB. En el caso de equipos que estén fuera de un cuarto restringido, ya sean servidores o estaciones de trabajo, es recomendable utilizar tornillos de seguridad o candado para proteger los componentes internos de robo o alteración. Cuando los equipos no están rackeados, también se recomienda utilizar una linga de seguridad, con el fin de anclar el equipo a un punto fijo y, así, dificultar su robo.

Aun cuando los servidores se encuentren en racks cerrados, deben requerir autenticación para el acceso a la consola, así como también bloqueo por inactividad.

Detección de intrusión

Como medida adicional de seguridad, es posible habilitar la detección de intrusión de chasis desde la configuración del BIOS. En caso de que el chasis sea abierto, se generará un evento DMI, que se registrará en el CMOS, y alertará cada vez que el equipo se encienda, hasta que el evento sea borrado. Este tipo de eventos también puede ser monitoreado en forma remota.

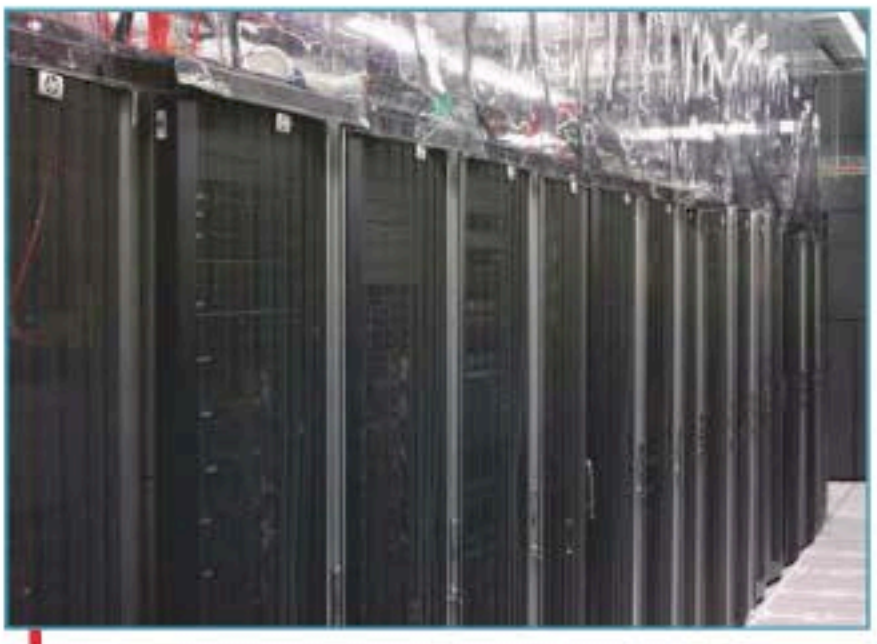
Es recomendable definir un proceso que recopile los eventos y notifique a los administradores para su revisión.

Los switches y patcheras, ya sea dentro o fuera del data center, también deben protegerse dentro de gabinetes cerrados, para evitar que usuarios malintencionados se conecten a los puertos de administración y alteren la configuración o ganen acceso a segmentos de red restringidos. La implementación de NAC (*Network Access Control*) permite detectar, evaluar y remediar la configuración de los equipos que se conectan a la red. Es posible validar si poseen antivirus actualizado, fixes de seguridad y otros requisitos necesarios para garantizar el estado de la red. Si no se llega a cumplir alguno de estos requisitos, puede denegarse el privilegio de conexión a la red o corregir en forma automatizada, según las políticas definidas.

Dado el caso de proceder a la remediación del equipo, el proceso se realiza en una red independiente para tal fin, hasta que

Tipos de control de acceso

El método DAC (Discretionary Access Control) **otorga al dueño del objeto el poder de permitir el acceso a otros individuos. El método** NDAC (Nondiscretionary Access Control) **establece reglas que no son implementadas por el usuario, sino por una entidad administrativa. En** MAC (Mandatory Access Control) **las reglas son establecidas por una entidad centralizada. Según** RBAC (Role Based Access Control)**, las decisiones sobre niveles de acceso se basan en los roles que los usuarios individuales tienen en la organización. El método de etiquetado permite identificar los niveles de seguridad definidos y los métodos de control de acceso permitidos.**



Data center con separación de pasillos fríos y calientes; la refrigeración está optimizada.

Los HVAC para data centers succionan el aire caliente por el techo, lo enfrían y lo envían por debajo del piso técnico.

se corrijan todos los desvíos y pueda conectarse a la red correspondiente.
Los servidores en ambientes inseguros (sucursales, áreas de tránsito, pequeños negocios u oficinas) deben contar con *Full Disk Encryption*. De esta forma, y en caso de robo del equipo, podremos garantizar la confidencialidad de la información contenida. Para esto existen distintas tecnologías, como Bitlocker para Windows Server, o dm-crypt para Linux.

CCTV

Los **CCTV** (circuito cerrado de TV) cumplen una doble función. Por un lado, disuaden el vandalismo o el robo del equipamiento; y por otro, lo evidencian una vez realizado. Existen equipos especialmente diseñados para el data center que tienen sensores para medición de temperatura, humedad y capacidad infrarroja para visión en la oscuridad, cuando las luces están apagadas. Algunas aplicaciones de CCTV incluyen la funcionalidad de detección facial, para permitir el acceso a áreas restringidas. Estas requieren cámaras de mayor fidelidad de imagen, pero brindan una funcionalidad que puede ser complementaria a las tarjetas tradicionales, con lo cual otorgan un nivel de seguridad adicional.
Es posible integrar el CCTV con el sistema de control de acceso. Esto permite asociar rápidamente una imagen de una persona con la información de la tarjeta o huella digital presentada ante el lector de esa zona. Habitualmente, la grabación de video se realiza solo cuando hay detección de movimiento, de modo que se reduce el espacio total de almacenamiento utilizado, y esto aumenta la cantidad de horas de grabación disponible.

UPS Eaton 9390IT para data centers de tres fases. Utiliza procesos de doble conversión.

HVAC

Los circuitos HVAC de data centers tienen la particularidad de que, además de enfriar el aire, regulan la humedad del ambiente y filtran las partículas de polvo. La **ASHRAE** (*American Society of Heating, Refrigerating and Air-Conditioning Engineers*) recomienda un rango de temperatura de entre 16 y 24° C, con una humedad de entre 40 y 55%.
La humedad por encima de estos valores puede generar condensación, y por debajo de ellos, producir estática en los componentes electrónicos.
La norma TIA-942 define cómo debe ser la circulación del aire: pasillos fríos por donde los servidores toman el aire y pasillos calientes por donde lo expulsan. El aire frío circula por debajo del piso técnico y sale por los orificios frente a los racks. El aire caliente sube por detrás de los racks y es succionado por el aire acondicionado, que lo enfría y envía otra vez por debajo del piso técnico. Esta forma de separar los pasillos fríos y los calientes optimiza el flujo de aire, y así genera un ahorro en la energía necesaria para mantener las temperaturas recomendadas.

Incendios

La detección temprana de humo es clave para reducir los daños al equipamiento. Por lo tanto, es importante colocar sensores debajo del piso técnico, en los racks y en el techo. Si solo existieran sensores en el techo y el fuego se originara debajo del piso técnico, donde existe gran cantidad de cableado, este sería detectado una vez que estuviera en una etapa muy avanzada, y entonces habría dañado gran parte del equipamiento.
La metodología de supresión de incendios utilizando **gas Inergen** es la preferida. Este gas es un compuesto de nitrógeno, argón y dióxido de carbono que extingue el fuego al suprimir el oxígeno, uno de los tres elementos necesarios para que exista combustión. La ventaja es que no causa ningún tipo de daño en los equipos, como sí ocurre con el agua o el polvo. Así, no es necesario realizar una limpieza luego de utilizarlo, por lo que permite retornar rápidamente a la actividad normal.
El compuesto Inergen no es nocivo para los humanos, y por este motivo reemplazó al CO^2, que sí lo es.

Alimentación eléctrica

Los data centers deben contar con circuitos de alimentación independientes para poder energizar de manera correcta a los equipos que poseen fuentes redundantes. Dado el caso de que exista un corto o salte una térmica en un circuito, el servicio no se interrumpirá. Los sistemas **UPS** (*Uninterruptible Power Supply*) proveen energía de emergencia. Su objetivo es mantener el suministro eléctrico luego de un corte de la energía de la red hasta que los generadores entran en funcionamiento. Las baterías soportan algunos minutos, que son los necesarios para que la corriente generada por los motores sea estable y, por lo tanto, apropiada para los equipos.

Respaldos

Las cintas o medios que contienen los backups o respaldos no deben permanecer en el mismo recinto donde se encuentran los servidores, ni tampoco en forma contigua. El BCRA (Banco Central de la República Argentina) establece en la comunicación "A" 4609:

General Electric Spectra Series Power otorga protección eléctrica y permite cambiar las líneas.

Tubos de **gas Inergen** para extinción de incendios en data centers. Este no daña los equipos ni afecta a las personas.

"Los procedimientos para el resguardo de datos, programas y todo otro componente de información deben prever, como mínimo, la generación de 2 (dos) copias de resguardo sincronizadas, manteniendo el almacenamiento de una de ellas en una localización distinta a la primaria, ubicada a una distancia determinada de acuerdo con el análisis de riesgos simultáneos que la entidad haya formalmente realizado".

ASHRAE RECOMIENDA QUE LOS DATA CENTERS TRABAJEN EN UN RANGO DE TEMPERATURAS DE ENTRE 16 Y 24° C, CON UNA HUMEDAD DE ENTRE 40 Y 55%.

EPO

En circunstancias extremas, puede ser necesario realizar un **EPO** (*Emergency Power Off*) de un data center. Si bien es un recurso útil, implica que es un único punto de falla. Debe ser protegido para evitar que una persona malintencionada lo accione. Por otro lado, existen situaciones críticas en las que se cuenta con una ventana de tiempo que permite el apagado ordenado de los equipos, por lo que es necesario tener un plan de apagado de emergencia detallado y actualizado. Este tiene que estar organizado, de forma que un operador pueda ejecutarlo paso por paso sin necesidad de recurrir a su memoria o su juicio. Un ejemplo simple consiste en apagar primero las bases de datos, luego las aplicaciones, y por último, los DNS y LDAP, que permiten autenticarnos en los equipos. Después de apagar los servidores, continuamos con los dispositivos de comunicación y, al final, con los HVAC. Es posible desarrollar un script que permita realizar el apagado ordenado de todo el equipamiento en el data center en forma veloz.

Monitoreo

El monitoreo del buen funcionamiento de los servicios es fundamental. Para determinar qué debemos monitorear se aconseja aplicar el método **Whatif?** Por ejemplo: **Pregunta 1:** ¿Qué pasa si se descompone el aire acondicionado? **Respuesta 1:** Todo el ambiente se recalienta. **Pregunta 2:** ¿Qué pasa si el ambiente se recalienta? **Respuesta 2:** Los servidores podrían fallar o reiniciarse. **Pregunta 3:** ¿Qué pasa si los servidores se apagan? **Respuesta 3:** La empresa se demoraría o paralizaría. **Conclusión:** el mal funcionamiento del aire acondicionado del data center puede afectar de manera significativa al negocio. Por lo tanto, utilizando esta metodología de análisis podemos:

- Identificar riesgos.
- Evaluarlos y valorarlos.
- Desarrollar controles o implementar salvaguardas. ■

El backup a disco

El **backup** a disco está ganando mercado por ser un económico y muy efectivo método para reducir las ventanas de backup y mejorar los tiempos de restauración. La velocidad de los discos aumenta permanentemente, y las tecnologías SAS y SATA han reducido sus costos. Los discos permiten acceso aleatorio, lo que posibilita varias sesiones concurrentes de backup. Pero la cinta aún no puede ser completamente reemplazada cuando se trata de retención y archivo offsite.

Hardware management

Conoceremos diversos estándares y cuestiones de interoperabilidad y gestión. Veremos la administración remota y automatizada del hardware.

Cada vez más, los sistemas se multiplican y abarcan todos los órdenes de la vida. Desde un simple kiosco hasta una gran multinacional, todo es regido por los sistemas. Esto lleva a que los data centers crezcan en forma exponencial, y que los administradores cada vez tengan que administrar más y más equipos. La administración artesanal y dedicada para cada servidor va quedando en el pasado, y cada vez está más automatizada y requiere menor intervención por parte de los técnicos. Los servidores no suelen ser fácilmente accesibles para los administradores, que muchas veces pueden estar a kilómetros de ellos. Por este motivo, existen facilidades para administrarlos a distancia, con herramientas de *Remote Management Support*. Intel ha desarrollado **IPMI** (*Intelligent Platform Management Interface*) con el fin de estandarizar y unificar las distintas implementaciones existentes para administración independiente de servidores (*Out of Band Management*).

Intel Active System Console, para pequeñas empresas, ofrece monitoreo de servidores individuales mediante una consola simple.

Implementaciones

Como sabemos, cada fabricante realiza su propia implementaciónde IPMI. HP desarrolla su tecnología **ILO** (*Integrated Lights Out*); **Oracle** tiene **ILOM** (*Integrated Lights Out Manager*); **IBM**, **RAS** (*Remote Supervisor Adapter*); **Dell**, **DRAC** (*Dell Remote Access Controller*), y **Cisco**, **CIMC** (*Cisco Integrated Management Controller*), solo por nombrar algunos de los casi 200 suscriptores de IPMI.

IBM Hardware Management Console

HMC es una tecnología desarrollada por IBM para permitir la configuración de LPARs (máquinas virtuales) en sistemas IBM p5, i5 y OpenPower. Se basa en un simple kernel Linux, un entorno gráfico X y aplicaciones Java. Un administrador, utilizando IBM HMC, puede identificar problemas de hardware, monitorear y configurar las LPARs. También puede asignar hardware (memoria, procesadores, etc.) a una LPAR dinámicamente. La administración se realiza desde la interfaz gráfica o por línea de comandos. Un HMC es capaz de controlar hasta 32 sistemas.

Belkin OmniView SMB KVM-over-IP Switch. Permite acceder a 256 servidores a nivel de BIOS, para un usuario remoto y uno local.

Las implementaciones de IPMI típicamente permiten realizar algunas de las siguientes funciones en forma remota: monitoreo del hardware, monitoreo del estado del sistema y log de eventos, administración de errores y fallas, generación de reportes ambientales y eléctricos, generación de alertas, visualización de LEDs e indicadores, consulta de SNMP traps, generación de inventario, visualización de direcciones de red IP y MAC, visualización de números de parte y de serie, auditoría de usuarios administradores, administración de cuentas de usuarios, y monitoreo de BIOS y POST. Posee, además, las siguientes características: puede ser accedido desde el sistema operativo; cuenta con RKVMS (Remote Keyboard, Video, Mouse and Storage); permite bootear desde un DVD local, remoto o una imagen ISO; soporta WS-MAN, IPv6, SSH 2.0, LDAP, Microsoft Active Directory y Radius; y permite enviar alertas vía SMTP y configurar un Remote Syslog Server.

BMC

BMC (*Baseboard Management Controller*) forma parte de IPMI. Es un microcontrolador embebido en el motherboard que comunica el hardware con el software. Los sensores reportan al sistema operativo la temperatura, la velocidad de los ventiladores, la alimentación, etc. BMC puede enviar alertas a través de la red si cualquier parámetro se aleja de los límites definidos. Un administrador también puede acceder de manera remota a la información de BMC y tomar una acción correctiva, como reiniciar, apagar y encender el equipo. La tecnología ILO, desarrollada por HP, es una de las más difundidas. Permite ver los eventos que acontecieron en el servidor, como el reinicio del equipo, el cambio de partes, etc. También, ver e interactuar con la pantalla como si estuviéramos delante del servidor. A su vez, es posible forzar el reinicio o el apagado del servidor de la misma manera que si oprimiéramos los botones del equipo. Esta facilidad puede ser utilizada independientemente de que el servidor tenga o no un sistema operativo instalado o el equipo esté apagado.

Intel vPro

Intel vPro agrupa un conjunto de tecnologías desarrolladas por Intel para la administración de computadoras de escritorio y notebooks, sin importar su sistema operativo o aunque no tenga uno instalado. Sus funciones son monitorear, actualizar, encender y conectarse remotamente a un equipo. Esta tecnología funciona con procesadores Intel Core 2 Duo o superiores. vPro utiliza Intel Active Management Technology (AMT) para la conexión remota al equipo mediante el protocolo VNC que tiene embebido. Esta funcionalidad puede ser utilizada estando el equipo con conexión Ethernet o wireless. HECI (*Host Embedded Controller Interface*) es una funcionalidad que forma parte de AMT y que permite que el sistema operativo se comunique con el chipset del motherboard para intercambiar mensajes con comandos o información como: estado de la batería, velocidad de los ventiladores, habilitación o deshabilitación de dispositivos, apagado del equipo, cambio del dispositivo de booteo, etc.

SMBus

SMBus (*System Management Bus*) fue creado por Intel como método de comunicación entre dispositivos (slave y

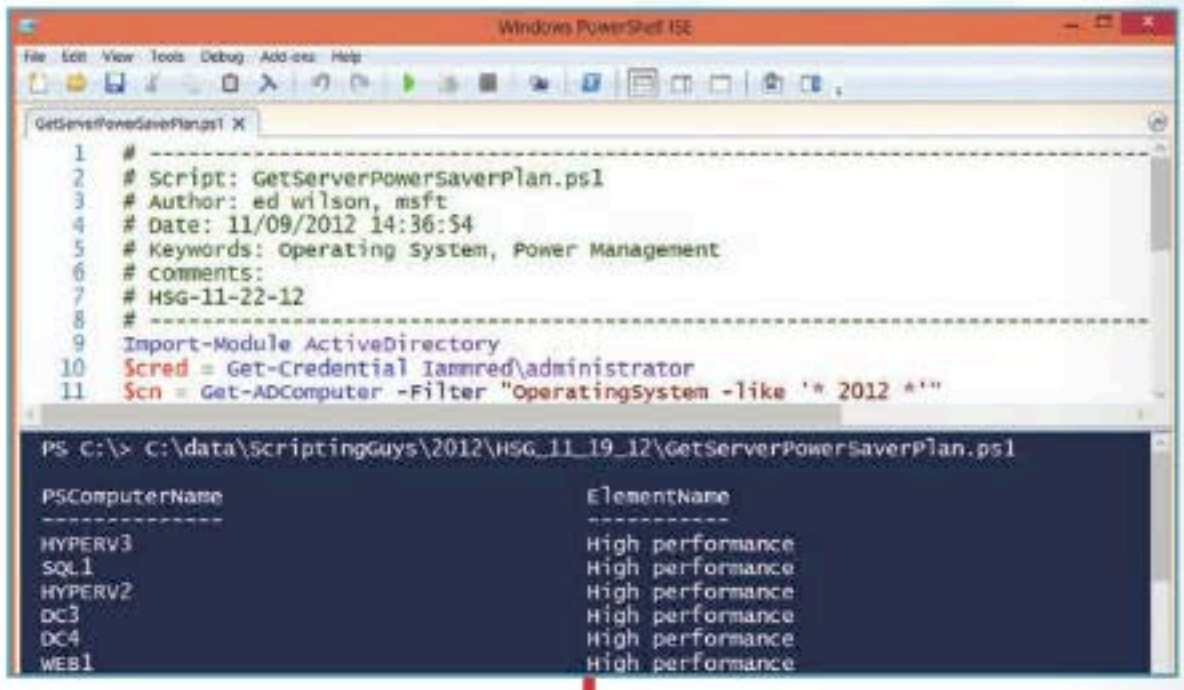
Oracle Integrated Lights Out Manager. Aun estando el equipo apagado, es posible acceder a la configuración del sistema.

master). Un dispositivo slave puede recibir una orden de un master y responder con la información solicitada, como: datos del fabricante, número de serie, temperatura, velocidad del ventilador, reporte de errores e, incluso, apagado o encendido del equipo. A diferencia de SMBus, PMBus (*Power Management Bus*) define un lenguaje de comandos que facilita la comunicación entre dispositivos, porque solo define timeouts y formatos, pero no, el contenido de los mensajes. Este protocolo se monta sobre SMBus, y permite la programación, el control y el monitoreo en tiempo real; además de la comunicación entre dispositivos basados en tecnologías analógicas y digitales; y la interoperabilidad, que permite que los dispositivos de distintos fabricantes se comuniquen entre sí.

ILOM FACILITA LA ADMINISTRACIÓN REMOTA DE SERVIDORES AUN CUANDO EL SISTEMA OPERATIVO NO RESPONDA O NO ESTÉ INSTALADO.

DMTF

El *Distributed Management TaskForce* (**DMTF**) es un grupo integrado por 160 compañías que desarrolla estándares para la administración de sistemas orientado, principalmente, a servidores. Está compuesto por actores como Intel, AMD, Microsoft, HP, Cisco y Oracle, por lo que busca desarrollar estándares independientes del sistema operativo y que permitan la interoperabilidad. Algunas de las iniciativas desarrolladas son:



Uso de **Powershell 3.0** para configurar el plan de energía de un servidor Windows 2012.

- **Systems Management Architecture for Server Hardware** (**SMASH**): es un conjunto de especificaciones para unificar la administración de data centers, que facilita la administración local y remota.
- **Alert Standard Format** (**ASF**): es una especificación que define sistemas de alerta para mejorar la experiencia de usuario y minimizar la carga administrativa del sistema.
- **Desktop Management Interface** (**DMI**): es un estándar discontinuado que permite llevar el control de los componentes en una PC.
- **Common Information Model** (**CIM**): evolucionó a partir de DMI, y permite gestionar y controlar la información de redes, aplicaciones, servicios y sistemas.
- **Web Services Management** (**WS-MAN**): establece un método común para acceder e intercambiar información a lo largo de la infraestructura mediante el uso de web services.

Conclusión

Todas estas iniciativas carecerían de sentido si los desarrolladores no las implementaran. No necesariamente las implementaciones hacen referencia a los estándares que aplican, ya que, en general, utilizan nombres comerciales para nombrarlos. Otro ejemplo de una implementación realizada por Microsoft de los estándares desarrollados por **DMTF** se encuentra en Powershell con el agregado de los **CIM cmdlets**. ■

PRÓXIMA ENTREGA

15

ADMINISTRACIÓN DE WINDOWS SERVER

En el próximo número veremos las características del sistema para servidores de Microsoft. Analizaremos las opciones de Active Directory y la administración de directivas de grupo en forma avanzada.

Técnico en
REDES &SEGURIDAD

PROFESORES EN LÍNEA
profesor@redusers.com

SERVICIOS PARA LECTORES
usershop@redusers.com

SOBRE LA COLECCIÓN

CURSO VISUAL Y PRÁCTICO QUE APORTA LOS SABERES NECESARIOS PARA FORMAR TÉCNICOS EXPERTOS EN REDES Y SEGURIDAD. INCLUYE UNA GRAN CANTIDAD DE RECURSOS DIDÁCTICOS COMO INFOGRAFÍAS, GUÍAS VISUALES Y PROCEDIMIENTOS REALIZADOS PASO A PASO.

Con la mejor metodología para llevar adelante el montaje y mantenimiento de las redes informáticas y con los aspectos clave para brindarles la protección necesaria, esta obra es ideal para aquellos aficionados que deseen profundizar sus conocimientos y para quienes quieran profesionalizar su actividad.

REDES &SEGURIDAD 00014
9 789871 857784

CONTENIDO DE LA OBRA