Administración de servidores

Jordi Serra Ruiz

PID_00200513

UOC
Universitat Oberta de Catalunya

Índice

Introducción

Lo primero que hay que hacer para hablar de seguridad en un sistema informático es decidir qué sistema operativo instalamos en la máquina, ya sea en una nueva o en una en la que se haya decidido cambiar las funciones. Debemos pensar si va a ser un servidor de ficheros, de sitios web o de impresión, por ejemplo.

En este módulo, describimos todo lo que hace falta para preparar un sistema informático para la instalación de un servidor, por ejemplo, cómo se tiene que hacer la partición del disco adecuadamente para cada uno de los sistemas operativos o dónde se tiene que instalar el software del servidor. No iniciaremos aquí una discusión sobre qué sistema operativo se tiene que instalar en un servidor, ya que eso depende mucho de la política de cada una de las empresas y, en definitiva, de la experiencia de cada administrador de sistemas, que es quien lo instala y después lo tiene que mantener. Así pues, se describe qué hay que tener en cuenta para instalar un servidor basado en GNU/Linux y, después, en Windows Server 2012.

Cuando tengamos claras las consideraciones preliminares, describiremos la instalación y configuración de los servidores para acabar describiendo la administración, así como el mantenimiento de estos servidores. La seguridad en los sistemas, ya sean servidores, dispositivos de red, móviles o cualquier otro sistema, no se acaba en la instalación, puesto que, como se puede ver todos los días, los ataques son continuos y con unas técnicas nuevas cada día. Por lo tanto, la actualización y el mantenimiento de los sistemas es lo más importante que hay en ese sentido.

Objetivos

Este módulo tiene los siguientes objetivos:

1. Analizar los requisitos necesarios para dimensionar un servidor que se tiene que implantar en una empresa, ya sea esta una pyme o una gran corporación.

2. Planificar la instalación de una máquina ponderando los sistemas de archivos, haciendo la partición de los discos y dimensionando las particiones que formarán el servidor.

3. Instalar un servidor mediante el sistema operativo, activar los protocolos de red necesarios y los mecanismos de autenticación que vamos a utilizar en el servidor.

4. Conocer las herramientas básicas que nos pueden ser útiles a la hora de administrar un servidor.

1. Análisis de requisitos

1.1. GNU/Linux

Lo primero que debemos considerar en la instalación de un servidor es saber qué tipo de servidor queremos instalar. Para hacerlo, tenemos que pensar previamente en una serie de puntos muy importantes:

- Cuántos usuarios habrá en el sistema, en valor absoluto. No hay que saberlo de manera exacta, pero sí en una magnitud bastante aproximada, ya que más adelante nos va a ser muy difícil redimensionar todo el sistema si, por ejemplo, se ha calculado para 20 empleados y resulta que hay 200.

- Qué servicios se tienen que ofrecer dentro del sistema informático.

- Cuántos usuarios estarán conectados de manera simultánea, lo que nos marcará mucho el tipo de red y las conexiones.

- Cómo serán las conexiones de los usuarios: la duración, el tipo (interactiva, remota, pasiva, *batch*, por ejemplo).

Una vez hemos resuelto estos requisitos, los tenemos que analizar para dimensionar el servidor de manera correcta; para hacerlo, hay que prever, también, la escalabilidad del servidor, tener prevista una posible ampliación del negocio y, por lo tanto, de las necesidades que requerirán los servidores.

Hay que tener presente que, para dimensionar bien los sistemas, debemos tener en cuenta todos los factores, así como las combinaciones posibles de estos. Es decir, si ofrecemos correo electrónico, tenemos que considerar que hoy en día los correos gratuitos ya ofrecen una capacidad superior a unas decenas de gigabytes de espacio por usuario, y si además ofrecemos un espacio para que los usuarios cuelguen su sitio web, hablamos de 250 MB más. Si a estos dos servicios añadimos el de disco de red, donde los usuarios guardan los documentos, y suponiendo que les ofrezcamos 500 MB de espacio, nos encontramos que un usuario puede llegar a ocupar 5 GB fácilmente. Y para dimensionar de manera correcta siempre va bien prever el peor caso.

Una vez tenemos una idea de la cantidad de disco que necesitamos por usuario, lo tenemos que multiplicar por el número de usuarios que tendremos. Sin embargo, antes de efecturar esta operación, tenemos que prever el crecimiento. Es decir, cuando el servidor haga poco que está instalado tendremos 150

usuarios, pero al cabo de cinco o seis años (que es más o menos la esperanza de vida de un servidor), tendremos un crecimiento de diez usuarios por año. Esto hace 210 usuarios en total.

Si multiplicamos los usuarios por la cantidad de espacio que van a necesitar (210 x 5 GB), nos sale poco más de 1.050 GB de disco. A esta cantidad tenemos que añadir un 15 o 20% para que el disco esté saneado. Así, vemos que, solo para los usuarios, necesitamos más de 1 terabyte de espacio de disco. Debemos tener presente que a esta cantidad hay que añadir el espacio que ocupa el sistema para fijar de manera concreta la cantidad de disco duro.

Otro aspecto que tenemos que considerar es que necesitaremos un terabyte y medio útiles (imaginemos que solo necesitamos 250 GB para el sistema y todas las aplicaciones). Es decir, si finalmente adoptamos un sistema de redundancia de disco (del tipo RAID), a la cantidad útil que obtenemos habrá que añadir la parte de redundancia.

Esta parte depende del sistema redundante que tengamos. Si es RAID 1 (*mirror*), tenemos que multiplicar esta cantidad por 2. Si es RAID 5 (como mínimo tres discos del mismo tamaño), tenemos que añadir un tercio del espacio útil. Por lo tanto, incluso antes de comprar los equipos, los discos y la circuitería de red, se tiene que pensar muy bien lo que vamos a poner y cuánto nos va a durar, ya que si ponemos la cantidad de espacio justa para los requisitos de hoy, mañana seguro que tendremos un problema.

Hay razonamientos parecidos que nos llevarán a valorar la memoria RAM, la red o la velocidad de proceso. Sin embargo, hay que destacar que a veces llegaremos a algunos un poco inverosímiles, como por ejemplo que nuestro servidor solo necesitará una velocidad de proceso de 400 MHz. ¿Esto quiere decir que tenemos que poner como servidor un Pentium II? No. ¿Esta conclusión nos invalida el razonamiento? No. ¿Para eso estamos dimensionando, para obtener resultados que no nos sirven? No. Esta conclusión solo muestra que la velocidad de proceso no es un factor crítico para nuestro servidor.

Para evaluar cuántos usuarios estarán conectados de manera simultánea, otra vez tenemos que saber el entorno en el que va a estar ubicado el servidor o conjunto de servidores. No es lo mismo que los ordenadores tengan todo el software en local y los usuarios se conecten a una intranet para compartir ficheros, que los ordenadores tengan el software instalado de manera administrativa y con los datos en el servidor. En el primer caso, los usuarios se conectarán de manera puntual con el servidor, mientras que en el segundo los usuarios estarán casi siempre conectados.

En el caso concreto de Ubuntu, que es el sistema GNU/Linux del que en capítulos posteriores explicaremos cómo se tiene que instalar, los requisitos del sistema recomendados son los siguientes:

- Intel-compatible CPU (i486 o superior).
- 256 MB de RAM utilizando el modo gráfico, que permite el uso de aplicaciones ofimáticas.
- Disco duro de 3 GB como mínimo.
- Unidad de CD-ROM o unidad de disco y CD-ROM (IDE/ATAPI o SCSI) normal.
- Tarjeta compatible con SVGA.
- Ratones serie o PS/2 o compatible con IMPS/2 o USB.

1.1.1. Configuraciones de hardware recomendadas

Los sistemas operativos son, *a priori*, independientes del hardware en el que se ejecutan, a pesar de que siempre hay excepciones. Sin embargo, para que el sistema operativo (SO) se entienda con el hardware se necesitan los programas controladores o *drivers* específicos de cada hardware. Los controladores son programas que dependen del sistema operativo y que interactúan directamente con el hardware, ya que son responsables de la comunicación entre el SO y el hardware.

Nos podemos encontrar con cierto hardware que no puede funcionar con GNU/Linux, ya que no existe ningún controlador compatible para este sistema operativo. Una manera sencilla de saber si el hardware que queremos comprar es compatible es buscando el logotipo de TUX (el pingüino) en la caja[1], a pesar de que algunas veces puede serlo sin que el fabricante lo indique.

(1)Si no tenemos la caja del software, lo podemos consultar en Internet mediante la URL: http://www.tldp.org/howto/hardware-howto/index.html.

1.1.2. Consideraciones del software

Uno de los posibles servicios de un servidor es el de proporcionar software a los usuarios conectados. Este software seguramente tiene también unos requisitos mínimos que hay que considerar; si a estos requisitos añadimos el hecho de dar servicio a los usuarios, nos encontramos con que también tenemos que dimensionar el servidor según el software que queremos proporcionar.

Podemos tener un servidor de ficheros que necesita poca RAM, poca CPU o GPU pero necesita una muy buena tarjeta de red para servir los ficheros, aunque también podemos necesitar un servidor en el que se ejecute un programa de cálculo o diseño gráfico y, por lo tanto, la red no será crítica, pero la RAM y la CPU y GPU sí. Las aplicaciones que se ejecutan en los servidores a veces también pueden condicionar el tipo de servidor que se tiene que instalar.

1.2. Windows Server 2012

1.2.1. Diferentes versiones de Windows Server 2012

- **Foundation:** Esta versión está pensada para pequeñas empresas, ya que no tiene posibilidades de realizar virtualización con el Hyper-V y solo dispone de quince usuarios como mucho dentro del directorio activo. Claramente, está pensada para una muy pequeña empresa de pocos usuarios.

- **Essentials:** Del mismo modo que la anterior, no dispone de virtualización de máquinas, no se pueden tener máquinas virtuales con Hyper-V, pero se pueden tener hasta veinticinco usuarios en el directorio activo de la empresa. Está pensada para pequeñas empresas pero que necesiten algo más que la Foundation. Y es que hay algunos temas dentro de los roles de los servidores que varían un poco, como por ejemplo los escritorios remotos, o la preconfiguración del acceso a la nube Internet.

- **Standar:** En este caso, tenemos usuarios ilimitados pero únicamente se pueden tener dos máquinas virtuales por cada licencia de Windows Server 2012, podríamos tener por lo tanto más de una licencia para poder disponer de más máquinas virtuales dentro del mismo servidor. Cada usuario que queramos que se conecte a este servidor tendrá que tener una licencia CAL de conexión al servidor.

- **Datacenter:** Esta versión dispone de todo incluido, usuarios ilimitados y máquinas virtuales como se quiera y cuantas se quieran. Es evidente que es una versión para grandes compañías que necesitan muchos usuarios y máquinas virtuales y que permite crear una nube virtual privada dentro de la misma empresa; también cabe decir que es la más cara con diferencia. Como en el caso anterior, habrá que disponer de las licencias CAL para cada cliente que se quiera conectar al servidor.

Nombre versión	Licencias / Usuarios	Precio aproximado
Foundation	1 servidor / 15 usuarios	OEM (preinstalado)
Essentials	1 servidor / 25 usuarios	400 €
Standard	por procesador / ilimitado + CAL	800 €
Datacenter	por procesador / ilimitado + CAL	4.000 €

Estas licencias CAL que se necesitan son las correspondientes a los clientes de Windows que hay que instalar en el servidor, además del cliente, para que puedan conectarse y trabajar con el servidor. Uno de los temas interesantes que gestionan las cuatro versiones son las actualizaciones de los sistemas clientes, ya que incorporan WSUS, que es el sistema de actualización automática de Windows. Por lo tanto, desde el servidor se podrá controlar completamente qué y cuándo se instalan las actualizaciones en los servidores y ordenadores clientes que hay en la empresa, dentro de la red local.

Antes de decidirse por una licencia, se tienen que consultar en este caso las páginas web del fabricante donde se especifican todas las posibilidades de cada una de las versiones, ya que quizás necesitemos una versión que permita acceder a ficheros compartidos o al escritorio remoto en una pequeña empresa, pero la versión Foundation no lo permite, por lo tanto se tendrá que optar por una versión más amplia, como podría ser la estándar.

En este material nos vamos a centrar en la versión estándar, ya que es la más común y la de propósito más general. Así pues, cuando hablemos de Windows Server 2012, nos referiremos a la versión Standard Edition.

1.2.2. Requisitos mínimos de hardware para Windows Server 2012

Los requisitos de hardware necesarios para un rendimiento adecuado del sistema operativo Windows Server 2012 son los siguientes:

1) Un procesador a 1,4 GHz de 64 bits. Solo hay versión para 64 bits.

2) 512 MB de memoria RAM.

3) El espacio de disco duro libre necesario para la instalación es de 32 GB, a pesar de que este tamaño puede variar según el número de componentes que se quieren instalar y otros factores, como por ejemplo:

- El método utilizado para la instalación (la instalación mediante una red necesita más espacio que si se instala desde el disco compacto).

- El tamaño del archivo de paginación. En equipos con más de 16 GB de memoria RAM se necesita más espacio de disco duro para almacenar este fichero de paginación, la hibernación y posibles volcados de memoria.

4) El espacio de disco duro ocupado al final de la instalación es más pequeño que el tamaño necesario durante el proceso de la instalación y depende del número de componentes instalados.

5) Un monitor VGA o de más resolución.

6) Un teclado.

7) Un ratón.

8) Una unidad de DVD, si se tiene que hacer la instalación desde el DVD.

9) Un adaptador o unos cuantos adaptadores de red compatibles con Windows y los cables correspondientes, así como un servidor desde el que se pueda ofrecer acceso a la Red, si se tiene que hacer la instalación desde esta.

1.2.3. Listas de compatibilidad de hardware con Windows Server 2012

La lista de compatibilidad de hardware de Windows Server 2012 indica qué componentes de hardware son compatibles (es decir, que funcionan correctamente) con Windows Server 2012. Si hay un hardware que no sale en esta lista, no está garantizado el buen funcionamiento en Windows Server 2012.

Página web

La lista de compatibilidad de hardware se puede consultar en la web de Microsoft.

1.2.4. Consideraciones de software en Windows Server 2012

Del mismo modo que para el caso anterior, hay una lista de compatibilidad de software con Windows Server 2012, análoga a la lista de compatibilidad de hardware. Antes de comprar e instalar un determinado software, es conveniente comprobar que es compatible con Windows Server 2012. Si el software no se encuentra en la lista de compatibilidad, no está garantizado que funcione correctamente.

El propio sistema ya avisa de los problemas que puede haber en el momento de instalar los nuevos softwares, pero hay algunas herramientas de Microsoft que diagnostican y resuelven algunos problemas de compatibilidad. En concreto, Windows Application Compatibility Toolkit[2] proporciona herramientas como Application Verifier, que comprueba si una aplicación determinada cumple o no los requisitos para ser compatible, o Application Compatibility Analyzer, que hace una comprobación de compatibilidad para todos los programas instalados en un ordenador o en más de uno.

(2)Este paquete de herramientas se puede bajar gratuitamente en la URL: http://www.microsoft.com/en-us/download/details.aspx?id=7352.

2. Instalación del servidor GNU/Linux

2.1. Planificación de la instalación del sistema operativo

Antes de empezar a instalar un servidor de cualquier fabricante, se tienen que tomar unas cuantas decisiones que nos marcarán la elección del que instalaremos en la máquina. La mayoría de estas decisiones afectan a los discos, ya que debemos decidir dónde se tiene que instalar el sistema, qué espacio necesitamos y qué tipo de sistema de ficheros utilizaremos. Estas decisiones las tenemos que tomar con la ayuda del análisis de requisitos que hemos hecho del sistema.

Así pues, en un sistema basado en GNU/Linux, una de las primeras decisiones, y de las más importantes, que nos podemos encontrar es que el sistema no funcione correctamente, y debemos decidir dónde pondremos el espacio de intercambio o *swap* y cómo lo haremos. Al poner el espacio de intercambio en una partición separada, se consigue más eficiencia de uso. A pesar de que podemos forzar a Linux a usar como espacio de intercambio un fichero regular, no es recomendable hacerlo.

Que es el *swap*

El *swap* es un espacio físico dentro del disco duro del equipo informático de uso temporal para un sistema operativo, que permite utilizar el espacio de disco duro como memoria virtual. Cuando el sistema trabaja, utiliza la memoria RAM para acceder a los datos que usa de una manera más rápida que si los va a buscar al disco.

Si la máquina requiere más información de la que cabe en la RAM, entonces utiliza el espacio reservado como *swap*. Por lo tanto, el *swap* nos permite ampliar la memoria RAM, pero a cambio de perder velocidad (puesto que el espacio de intercambio está en el disco). Debemos tener presente que el *swap* tiene un uso esporádico; si la máquina trabaja mucho en modo *swap*, nos tendremos que plantear ampliar la memoria RAM, ya que se ganará en velocidad y en fiabilidad del disco, puesto que el acceso de la memoria *swap* al disco hace que el disco quede muy dañado.

Una vez hemos decidido que pondremos el espacio de intercambio, *swap*, en una partición separada del sistema, tenemos que decidir el tamaño de esta partición. Es aconsejable que el tamaño final dependa de la memoria RAM que tiene el servidor. Si tenemos un servidor con poca memoria RAM, es recomendable poner como espacio de intercambio el doble de la memoria del sistema. Si tenemos un servidor con mucha memoria, tenemos que poner como tamaño de la partición de *swap* la misma cantidad de RAM. Hay que tener en cuenta que en arquitecturas de 32 bits (i386) el tamaño máximo para un espacio de intercambio es de 2 GB. Una cuestión que debemos plantearnos, tanto en el caso de los servidores como en el caso de los ordenadores de los clientes, es que para poder hibernar el sistema se necesitará más memoria *swap* de la que se disponga en realidad; en caso contrario, el sistema no podrá copiar la

memoria real en el fichero o partición *swap*. Eso se debe tener muy en cuenta si se dispone de portátiles, a pesar de que en el caso de un servidor no tiene mucho sentido poder hibernarlo.

Si estamos en un entorno doméstico con estas dos particiones, la de intercambio (*swap*) y la de sistema, llamada raíz (/), ya podemos empezar la instalación del sistema. Sin embargo, en la mayoría de los entornos multiusuario se recomienda dar al GNU/Linux más que el número mínimo de particiones.

Hay dos motivos principales para aumentar el número de particiones, y los dos hacen referencia a la seguridad. El primer motivo es que, si se deteriora el sistema, siempre es más fácil recuperar una partición que recuperar todo el disco. Además, si se deteriora cualquier otra partición que no sea la del sistema, el servidor se sigue pudiendo inicializar y se puede intentar solucionar el problema. El segundo motivo es por una cuestión de recursos. Imaginemos que se pierde el control de una aplicación. Si esta aplicación se ejecuta en modo de usuario privilegiado, irá escribiendo en el disco hasta agotar todo el espacio. El hecho de no tener espacio en el disco no es bueno para un sistema operativo basado en GNU/Linux, ya que, aparte del espacio de intercambio, el sistema necesita utilizar ficheros reales para funcionar.

El correo basura

Si el servidor recibe mucho correo basura (*spam*), o se trabaja con muchos ficheros que no se van borrando y por lo tanto van ocupando cada vez más espacio de disco, puede llegar a saturarlo y, por lo tanto, si el disco no tiene particiones que separen el sistema operativo de los datos que pueden crecer sin conductor, cuando se sature puede colapsar el sistema.

Antes de dar paso a las particiones que utilizaremos, debemos tener presente que el hecho de hacer particiones nos hipoteca. Si hacemos particiones demasiado pequeñas, tendremos que reinstalar el sistema o mover datos continuamente para obtener espacio; si hacemos particiones demasiado grandes, tendremos mucho espacio no utilizado en cada partición. La recomendación de particiones para sistemas multiusuario es poner los directorios *usr*, *var* y *home* en particiones separadas de la partición raíz. La partición raíz (/) siempre tiene que contener físicamente los directorios `etc`, `bin`, `sbin`, `lib` y `dev` o, en caso contrario, no se podrá arrancar. Estas particiones tienen que estar forzosamente en la raíz del sistema de ficheros de GNU/Linux. Hay distribuciones que recomiendan la separación del directorio raíz en una partición diferente de la partición raíz. Si hacemos esta partición, el espacio destinado a la partición raíz puede ser que no necesite más de 50 MB. Usualmente basta con un tamaño de la partición raíz de 2 GB.

La partición `usr` contiene todos los programas, todas las librerías y toda la documentación de usuario, y se encuentran respectivamente en los directorios `bin, lib` y `share`. Esta parte del sistema de archivos es la que necesita mayor espacio. Si se quieren instalar más paquetes, se tiene que incrementar la cantidad de espacio que se da a esta partición.

Todos los usuarios del sistema que tengan espacio de disco tendrán un directorio personal en la partición `home`. El tamaño de esta partición depende de cuántos usuarios van a utilizar el sistema y de qué archivos se almacenarán en los directorios. En el análisis de requisitos, ya hemos tenido que calcular este espacio.

En la partición `var` están los datos variables, como los sitios web, los correos electrónicos, los ficheros de *log*, la memoria caché o la caché de APT. El tamaño de esta partición depende mucho del uso del ordenador. Por lo tanto, esta partición, a pesar de que no es muy importante, la debemos tener siempre controlada porque es la que *a priori* tiene más probabilidades de que se desborde y provoque problemas.

2.1.1. Sistema de archivos

En el apartado anterior hemos hablado de la manera como tienen que ser las particiones que se tienen que definir en el disco duro, pero estas particiones las tiene que gestionar un sistema de archivos. Esta es la manera que tiene el sistema operativo de gestionar, organizar y mantener la jerarquía de ficheros en los dispositivos de almacenamiento, normalmente discos duros. Si hacemos una abstracción del sistema de archivos, lo podemos llegar a interpretar como un sistema orientado a objetos, donde los objetos son construcciones de software (estructura de datos y funciones y métodos asociados) de los tipos siguientes:

- **Superbloque:** Mantiene información relacionada con los sistemas de archivos montados. Lo representa un bloque de control de sistema almacenado en el disco (para sistemas basados en disco).

- ***inode*:** Mantiene información relacionada con un archivo individual. Cada *inode* contiene la metainformación del fichero (propietario, grupo, fecha y hora de creación, modificación y último acceso), más un conjunto de punteros en los bloques del disco que almacenan los datos del archivo. Almacena toda la información sobre el archivo excepto el archivo en sí.

- **Fichero:** Mantiene la información relacionada con la interacción de un archivo abierto y un proceso. Este objeto está solo cuando un proceso interactúa con el archivo.

- ***Dentry*:** Enlaza una entrada de directorio (*pathname*) con el archivo correspondiente. Los objetos *dentry* usados recientemente se almacenan en una memoria caché (*dentry cache*) para acelerar la traslación desde un nombre de archivo al *inode* correspondiente.

El sistema de archivos por defecto del sistema GNU/Linux es el llamado ext3 o, incluso últimamente, el ext4. Sin embargo, no es el único sistema de archivos que hay en un entorno en GNU/Linux. De hecho, en Linux distinguimos entre tres grandes grupos de sistemas de archivos: los de disco, los de red y

los dispositivos especiales. De todos los sistemas de archivos, en este apartado vamos a comentar dos: el ext2, que está quedando en desuso en favor de su sucesor el ext3, y el ext4, precisamente otro del que vamos a hablar. Estos dos sistemas pertenecen a la categoría de sistemas de archivos de disco.

El ext2 es el sistema de archivos que se extendió más internamente en el GNU/Linux. Lo diseñó Wayne Davidson con la colaboración de Stephen Tweedie y Theodore Ts'o. El ext2 está basado en *inodes* (asignación indexada). Cada *inode* mantiene la metainformación del archivo y los punteros en los bloques con los datos reales.

El sistema de ficheros ext3 es una extensión con *journaling* del sistema de archivos ext2. Un sistema con *journaling* es un sistema de archivos tolerante a fallos en el que la integridad de los datos está asegurada porque las modificaciones de la metainformación de los archivos se graban primero en un registro cronológico (*log* o *journal*, que implementa una lista de transacciones) antes de que se modifiquen los bloques originales. Si hay un fallo del sistema, un sistema con *journaling* asegura que se recupere la consistencia del sistema de archivos. El método más común es el de grabar previamente cualquier modificación de la metainformación en una área especial del disco; el sistema grabará realmente los datos cuando se haya completado la actualización de los registros.

En el caso del ext4, se trata de un conjunto de extensiones compatibles hacia atrás que no se quisieron incorporar en el ext3 para evitar problemas de inestabilidad. Principalmente, extiende los límites del sistema de archivos y añade mejoras de rendimiento. Una mejora muy destacada en ese sentido es la mejora del tiempo de comprobación del sistema de archivos. Los bloques libres se marcan como tales y permiten a la utilidad `e2fsck` poder ignorarlos.

Un caso especial de sistema de archivos es el *swap*. Si hemos decidido que nuestro sistema tenga una partición de intercambio, debemos asignar a esa partición el sistema de archivos de tipo *Linux swap*. Si no marcamos la partición con este sistema de archivos, el sistema no tendrá una partición de intercambio. Hay que destacar que esta partición no es directamente visible ni desde GNU/Linux ni desde Windows, es decir, que no veremos nunca el contenido (los archivos y directorios) de esta partición.

2.1.2. Montaje de las particiones

En este apartado, vamos a ver en qué consiste la operación de montaje y cómo se hace, en las diferentes maneras que hay de hacerlo. En sistemas basados en Windows, el modo de acceder a las particiones es entrando a cada una de las unidades que hay (A:, C:, D:, E:, F:, entre otras). En cambio, en los sistemas basados en GNU/Linux, tratan todos los dispositivos, los discos, como si fueran ficheros. Este simple hecho aporta mucha flexibilidad al sistema, ya que nos permite usar todos los mecanismos destinados a ficheros en los dispositivos.

Para acceder a cualquier dispositivo de almacenamiento, tenemos que hacer primero una operación de montaje de esta unidad. Esta idea de montar un dispositivo no queda clara si no se entiende cómo está estructurado el árbol de directorios de un sistema basado en GNU/Linux.

El árbol de las carpetas tiene un directorio raíz que se representa con el símbolo (/); dentro están los directorios `etc, bin, usr, var, sbin boot, dev, lib, mnt, opt, proc, home` propios del sistema operativo. Esta estructura aparece del mismo modo, independientemente de las particiones que hacemos o de dónde se encuentren esas particiones. Esto ofrece una gran ventaja, ya que una vez están montados los dispositivos (USB, CD-ROM, particiones del disco duro), tenemos un único árbol de directorios y nos podemos desplazar por ese árbol de manera independiente a los dispositivos, ya que nos es completamente innecesario conocer en qué dispositivo estamos. La desventaja de tener este tipo de estructura es que cada vez que, por ejemplo, queremos copiar un fichero ubicado en una memoria USB en el disco o en otro lugar, como puede ser a través de la Red, tenemos que seguir los pasos siguientes en el orden indicado:

- Insertar el USB.
- Montar el USB.
- Copiar los ficheros.
- Desmontar el USB.
- Retirar el USB.

Hay dos maneras de montar un dispositivo. La primera es de modo explícito con la orden `mount`. Esta orden se utiliza de la forma siguiente:

```
mount -t tipo_sistema dispositivo punto_montaje
```

Un ejemplo de ejecución de esta orden, para montar una partición, es el siguiente:

```
mount -t ext4 /dev/hda2 /usr
```

Esta orden monta el dispositivo `/dev/hda2` en el punto de montaje `/usr`, y utiliza ext4 como sistema de archivos. Para hacerlo, previamente debemos tener formateado el dispositivo `/dev/hda2` como un sistema ext4.

Las particiones son un caso particular de montaje, ya que debemos saber cuál es el dispositivo que queremos montar. Hay otros sistemas de almacenamiento, como el disquete o el CD, ya que el dispositivo es común para todos los sistemas operativos basados en GNU/Linux. El disquete es el dispositivo `/`

`dev/fd0` y el CD-ROM (si es IDE) está en `/dev/cdrom` (normalmente sale este enlace). No obstante, la gran diferencia respecto a un sistema basado en Windows es que, una vez montado el dispositivo, no podemos retirar el CD, USB o el disquete hasta que no hayamos desmontado ese dispositivo. Para desmontar un dispositivo usamos la orden `umount`.

Por ejemplo, si ahora queremos desmontar la partición que antes hemos montado, debemos ejecutar:

```
umount dispositivo
umount punto de montaje
```

En caso de querer desmontar el dispositivo del ejemplo anterior, debemos ejecutar:

```
umount /dev/hda2
```

o

```
umount /usr
```

Con cualquiera de estas dos órdenes conseguimos desmontar la partición, ya que da igual si desmontamos el sistema de almacenamiento por el dispositivo o por el punto de montaje. Si lo que nos interesa es ver qué ha montado en el sistema en un momento concreto, utilizamos la orden `mount` sin ningún argumento y obtenemos como salida del sistema una tabla de los dispositivos montados y los puntos de montaje. Veamos a continuación un ejemplo de ejecución de la orden `mount`.

```
/dev/hda5 on / type ext3(rw,errores=remount-ro)
proc on /proc type proc (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/hda1 on /boot type ext3 (rw)
/dev/hda6 on /usr type ext3 (rw)
/dev/hda7 on /var type ext3 (rw)
/dev/hda9 on /home type ext3 (rw)
```

La segunda opción que hay para montar dispositivos en GNU/Linux es con el fichero `/etc/fstab`. Este fichero se lee en tiempo de arranque y, si tenemos muy definidos los dispositivos, los tipos y los puntos de montaje, se montarán todos en tiempo de arranque.

```
# <Sis. ficheros> <Punto montaje> <Tipo> <Opciones> <volcado> <pasada>
/dev/hda5 / ext3 errors=remount-ro 0 1
/dev/hda8 none swap sw 0 0
proc /proc proc defaults 0 0
```

```
/dev/fd0 /mount/floppy auto user,noauto 0 0
/dev/sda /mount/usb vfat rw,user,noauto 0 0
/dev/cdrom /cdrom iso9660 ro,user,noauto 0 0
/dev/hda1 /boot ext3 defaults 0 2
/dev/hda6 /usr ext3 defaults 0 2
/dev/hda7 /var ext3 defaults 0 2
/dev/hda9 /home ext3 defaults 0 0
```

De este fichero hay varias cosas que cabe destacar.

- La partición de *swap* no tiene punto de montaje, algo normal, puesto que esta partición solo es accesible en el sistema de archivos, para utilizarla como partición de intercambio con la memoria.

- Los dispositivos `/dev/fd0` (disquetes), `/dev/sda` (USB) y `/dev/cdrom` (CD-ROM), a pesar de que aparecen en este archivo, no se montan hasta que introducimos un CD, un USB o un disquete en las ranuras correspondientes. Debemos tener en cuenta que, aunque introduzcamos un CD (o DVD), un USB o un disquete, no se nos montarán estos sistemas de almacenamiento salvo que el sistema esté configurado para el automontaje. Por eso recomendamos que aprendáis a montar estos dispositivos de manera manual. A pesar de que las memorias USB ya se montan en casi todos los casos de modo automático, esto se debe tener en cuenta en los casos de los servidores en los que sea peligrosa la ejecución de programas no controlados a través de un dispositivo USB, ya que no hay que estar en `root` para montar estos dispositivos.

- El dispositivo `proc`. Este dispositivo tiene un significado especial. Lo que hay en este directorio no son archivos, sino el valor de muchas de las variables que utiliza el núcleo o *kernel* del sistema durante la ejecución del sistema operativo.

- Si os habéis fijado en el ejemplo del archivo `/etc/fstab`, habréis visto que algunas particiones tienen como opciones `defaults`. Esta opción nos configura la partición como `rw`, `exec`, `nouser`, `suid`, `async`, `dev` y `auto`.

Tanto en el fichero de ejemplo `/etc/fstab` como intermediando la opción `-t` del `mount` nos obligan a poner el tipo de sistema de archivos que queremos montar. Si no lo hacemos, toma por defecto el ext3. Para montar dispositivos de almacenamiento del tipo `vfat`, `hado32`, `NTFS`, es poco probable hoy en día que tengamos que compilar el núcleo del sistema para que reconozca estos tipos de sistemas de archivos, ya que son los más utilizados en todos los sistemas.

El paquete de GNU/Linux llamado `autofs`, que detecta automáticamente la inserción de algún dispositivo en el sistema y lo monta sin tener que ejecutar ninguna orden, ya viene por defecto en casi todas las distribuciones, pero es importante conocer cuál es el paquete que nos hará montar todos estos dispositivos para incluirlo o incluso para desinstalarlo si es necesario.

2.1.3. Administración de discos

Los discos, igual que la mayoría de los servicios de un servidor, se tienen que administrar. En este apartado, vamos a explicar cómo se hace esta administración y en qué consiste. Si lo que queremos es visualizar el espacio usado y el libre de cada partición, lo tenemos que hacer con la orden `df` (*disc free*), que nos muestra los resultados en bytes, pero como actualmente los discos son muy grandes, puede resultar dificultoso ver estas cantidades expresadas en bytes. Si queremos visualizar con más comodidad estos resultados, podemos usar las opciones `-k`, `-m` o `-h`, que muestran los resultados en kilobytes, megabytes o de manera humana, respectivamente.

Un ejemplo de visualización de la orden `df -h` es el siguiente:

```
S.ficheros Medida Usado Disp Uso% Montaje en
/dev/hda5 4,0G 277M 3,5G 8% /
Tmpfs 125M 0 125M 0% /dev/shm
/dev/hda1 198M 13M 176M 7% /boot
/dev/hda6 4,0G 1,8G 2,0G 48% /usr
/dev/hda7 4,0G 1,7G 2,2G 44% /var
/dev/hda9 25G 19G 5,0G 79% /home
```

Una de las tareas más básicas desde el punto de vista de la seguridad es controlar que no se agoten los recursos de las máquinas, es decir, que el equipo deje de dar servicio porque se ha agotado algún recurso, como puede ser la memoria o el disco duro. Para ello, debemos usar la orden `df` para ver el estado de los discos. Una partición o disco saneado es aquella que tiene menos de un 85 o 90% de uso. Este parámetro depende del tamaño de esta partición, ya que no es lo mismo un 90% de 10 GB que de 800 GB. El margen tiene que ser más grande en la partición raíz del sistema, ya que si esta partición se satura, el servidor no va a arrancar.

A continuación, vamos a enumerar unas tareas que pueden ayudar a mantener los discos saneados. Algunas de estas tareas son físicas (hacer algo) y otras son políticas de buen uso del sistema que tenemos que aprender nosotros y hacer aprender a los usuarios:

1) Los directorios `/tmp` y `/var/tmp` suelen estar a disposición de muchos procesos en los que se escribe mucha información temporal. Estos directorios se tienen que limpiar periódicamente. Hay muchas distribuciones que ya disponen de tamaños para estos casos, como eliminar los contenidos de estos di-

rectorios durante el arranque de la máquina, pero hay algunos de esos tamaños que están enfocados a tener GNU/Linux como estación de trabajo y no como un servidor. Si utilizamos GNU/Linux para nuestro servidor, como nos interesa que las máquinas estén todo el tiempo en servicio y limpiamos estos ficheros solo en los tiempos de arranque y no detenemos el servidor durante unos cuantos meses, podemos llegar igualmente a la saturación. Una manera más práctica de solucionar este problema es borrarlos todos los días. Para hacerlo, se tiene que utilizar el `crontab` del sistema. El `crontab` es la aplicación que tiene el sistema para ejecutar de manera periódica (cada hora, cada día, cada mes, cada miércoles, por ejemplo) alguna tarea, orden o *shell script*. Para acceder al `crontab` desde el usuario raíz, hay que ejecutar la orden `crontab -e` y añadir las líneas siguientes:

```
05 04 * * * /bin/rm -rf /var/tmp/*
10 04 * * * /bin/rm -rf /tmp/*
```

Con estas dos líneas conseguimos que todos los días a las 4.05 y a las 4.10 de la madrugada se borren los contenidos de estos directorios.

2) Tenemos que controlar el tamaño de los *logs* para evitar un desbordamiento. Los *logs* están, normalmente, en `/var/log` o en `/var/adm/log` y en este tipo de ficheros, según el sistema, pueden llegar a ser muy grandes. Como en los *logs* se guardan todos los acontecimientos del sistema, no es aconsejable eliminarlos. Una tarea que tiene que hacer el administrador de manera periódica es revisar los *logs*, ya que nos dan información sobre todos los hechos que ha habido en el servidor. Lo que sí podemos hacer es guardarlos periódicamente (por ejemplo, todas las semanas) de manera comprimida y eliminar los que sean anteriores a un periodo de dos meses. También podemos guardar todos los *logs* en dispositivos extraíbles.

3) Otro punto en el que se puede desbordar el sistema es en el espacio de los usuarios. Algunos de estos casos son los siguientes:

- Los correos electrónicos. Los podemos alentar para que borren periódicamente los mensajes o bien podemos poner un sistema de cuotas de correo. Más adelante veremos cómo se tienen que configurar las cuotas de correo.

- El espacio de disco de los usuarios propios. Podemos volver a pedir a los usuarios que borren periódicamente lo que no se necesite o podemos poner un sistema de cuotas de disco.

- La memoria caché de los navegadores también es un espacio donde se puede llegar a escribir mucha información. Es recomendable borrarla con periodicidad; para hacerlo, o educamos a los usuarios a hacer esta tarea de manera periódica o la hacemos nosotros mediante un *shell script* que recorra todos los usuarios buscando estas carpetas y eliminando su contenido.

- Si los usuarios utilizan herramientas de compilación, los archivos *core* suelen tener tamaños muy grandes. Los podemos eliminar de manera periódica mediante una búsqueda por el espacio de usuarios.

Otra instrucción que nos puede ser útil es la orden `e2fsck`, que hace una revisión médica del disco y comprueba la integridad de los datos. Se ejecuta de la manera siguiente:

```
e2fsck -t tipo_sistema dispositivo [opciones]
```

Un dato muy importante es que, para ejecutar esta orden sobre un dispositivo, este dispositivo tiene que estar desmontado. Si no, puede dañar el sistema.

2.2. Instalación del servidor

En este apartado, vamos a detallar cómo se instala un servidor Linux. Para hacerlo, utilizaremos la distribución para servidor de GNU/Linux, Debian, en la versión 6, última versión en el momento de imprimir estos materiales. Hay diferentes maneras de ejecutar esta instalación, pero la más sencilla es bajar de la página web de Debian la instalación por red (*netinst*), ya que esto hará que con un CD y con poco tiempo podamos instalar el sistema. Con esta instalación, únicamente se bajarán aquellas partes del sistema operativo que se quiere instalar realmente, así reducimos el tamaño de la descarga total y, por lo tanto, no agotamos el ancho de banda de la red.

El documento básico que nos proporciona Debian para su instalación se encuentra directamente en la página web de Debian. Cada distribución tendrá su documento de instalación. En el caso de la distribución que se usa en este taller, se puede encontrar en la dirección `http://www.debian.org/releases/stable/installmanual`, donde están los enlaces a todas las arquitecturas e idiomas posibles. Podemos encontrar soluciones a, por ejemplo, no disponer de una unidad de DVD-ROM *bootable*.

Esta instalación se llevará a cabo en un ordenador estándar sobre un disco duro SATA pequeño. En cuanto a controladoras y discos SCSI, si estos son medianamente estándares, serán detectados sin ningún problema durante el proceso de arranque, igual que los discos IDE. Antes de hacer la instalación tenemos que asegurarnos de que el CD-ROM del servidor es la primera opción en tiempo de arranque. Una vez tengamos el CD-ROM como primera opción, introducimos el CD de Debian e inicializamos la máquina.

2.2.1. Antes de empezar la instalación

Es muy importante que, antes de iniciar la instalación, nos aseguremos de disponer de un espacio mínimo en el disco duro donde hacerla (se recomienda disponer, como mínimo, de entre veinte y treinta gigabytes de espacio libre solo para el sistema). Podría darse el caso de que otro sistema operativo ya esté

en el disco duro, ocupe ya casi todo el disco y no deje nada de espacio para el nuevo sistema. Pero si el disco es nuevo, podemos empezar directamente con la instalación, a pesar de que pensamos instalar también otro sistema operativo (bastará con que reservemos el espacio que consideremos para este con el tipo de partición que necesite).

Si disponemos de un espacio que previamente habíamos reservado, porque ya teníamos en mente instalar GNU/Linux, o tenemos una partición de cualquier otro sistema operativo donde lo queramos instalar, también podemos proseguir con la instalación, es decir, arrancar desde el DVD-ROM.

Pero si tenemos todo el disco duro ocupado en una sola partición dedicada a otro sistema operativo (cosa muy poco recomendable, ya que en general hace disminuir el rendimiento de cualquier sistema operativo y, en especial, de aquellos con sistemas de archivos poco consistentes), tenemos que liberar espacio para poder instalar Debian GNU/Linux en el caso de querer disponer de los dos sistemas, a pesar de que nunca serán simultáneos. La dificultad de ejecutar esta operación dependerá estrictamente de qué sistema de archivos sea el que contiene esta partición.

Con probabilidad, el sistema operativo en cuestión es de la familia de productos de Microsoft™; si el sistema de archivos es de tipo FAT o FAT32 (utilizados por las antiguas versiones MSDOS™, Windows95™ y Windows98™) el problema es relativamente sencillo de resolver, ya que con la misma distribución se nos facilita una aplicación llamada `fips20.exe` que nos ayudará en la repartición del disco duro y en la creación de espacio para instalar GNU/Linux. En el caso de los sistemas de archivos FAT o FAT32, no hay ningún problema de interpretación desde GNU/Linux, por lo tanto, podremos encontrar también otras herramientas de repartición del disco libres en la Red.

Si ya tuviéramos instalado un sistema operativo GNU/Linux, podemos utilizar una de las muchas aplicaciones que hay para redimensionar particiones de discos duros y crear otras nuevas, como por ejemplo, `partman` (herramienta original de GNU/Linux), `cfdisk` o los editores gráficos `gparted` (escritorio Gnome) o `qtparted` (escritorio KDE). Estas aplicaciones gestionan tanto sistemas de archivos de tipo FAT o FAT32 como NTFS.

Si no se dispone de ningún sistema operativo GNU/Linux ya instalado en el disco, podemos utilizar el Gparted Live-CD, que es un *live-CD* que contiene un sistema operativo GNU/Linux pequeño y básico, que se ejecuta directamente desde el CD-ROM y que contiene la aplicación `Gparted`. Nos tendría que permitir poder reparticionar y, por lo tanto, crear una partición nueva para el nuevo sistema operativo en el disco donde haya también un Windows™XP,

Vista, 7 o 8, con NTFS como sistema de archivos. A pesar de que no siempre funcionarán correctamente, pueden dar problemas y no permitir este reparticionado en algunos tipos de discos duros.

Como última opción, siempre podemos recurrir a aplicaciones comerciales. Pero en todos los casos es muy importante hacer una copia de todos los datos que sea importante conservar (a pesar de que ya se tendría que haber hecho antes), ya que estamos accediendo y moviendo datos de los discos y siempre pueden fallar los discos o la electricidad. Por lo tanto, no daremos este paso sin tener copiados todos los datos necesarios para poder volver a tener el sistema inicial otra vez operativo en el mismo punto donde estaba antes.

Con independencia de la aplicación que utilicemos para crear la partición, antes siempre hay que desfragmentar el disco. El desfragmentador de disco es una utilidad que permite analizar discos locales y encontrar y consolidar carpetas y archivos fragmentados (separados en el espacio). También se pueden desfragmentar discos desde una línea de órdenes mediante la orden `defrag`. Con esto evitaremos problemas, ya que podemos tener archivos fragmentados y una parte de ellos tenerlos al final de la partición. Por lo tanto, al redimensionar y tomar espacio en esta parte final, nos cargaríamos estos ficheros y, dependiendo del tipo, en el mejor de los casos, perderíamos la información, pero si son del sistema, podríamos inutilizar el sistema operativo.

Otra opción, de hecho sería la mejor, es disponer de un disco duro pequeño y nuevo (o formateado) al que no haga falta reparticionar puesto que podremos disponer de todo el disco. En este caso, no tendremos ningún problema con los datos o sistemas operativos anteriores, ya que el sistema se instalará en el nuevo disco y no se tocará el anterior en absoluto.

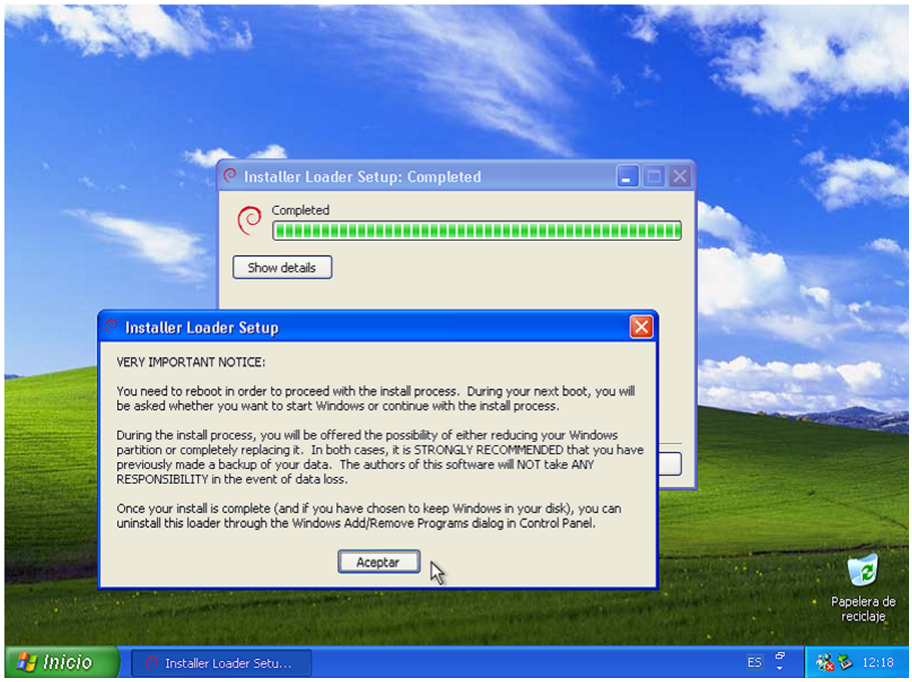
2.2.2. Arranque del sistema de instalación

Llegados a este punto, podemos empezar la instalación propiamente dicha. Para ello, arrancaremos el ordenador, nos aseguraremos de que el primer dispositivo a la hora de arrancar (*boot*) sea la unidad de DVD-ROM (entrando en la BIOS) y pondremos el CD que hemos bajado y quemado en un CD. Al cabo de un momento, aparecerá una pantalla de bienvenida como la de la figura siguiente:

Inicio de instalación Debian

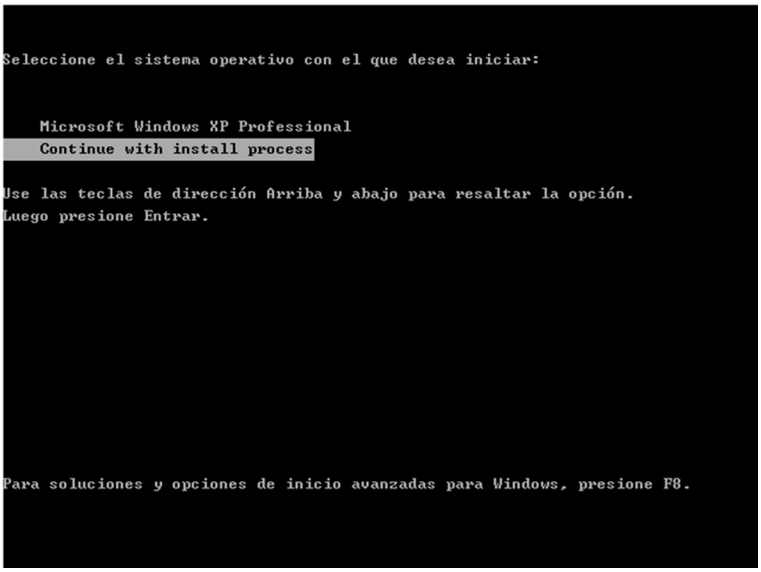
También se puede iniciar la instalación desde el sistema operativo que ya está instalado en el ordenador, simplemente introduciendo el CD de instalación de Debian y ejecutando el fichero setup.exe; así nos aparecerá una ventana en la que nos pedirá el idioma en el que queremos seguir el proceso de instalación y empezará a copiar archivos en el disco duro para volver a reiniciar el sistema y arrancar con el CD de Debian, sin tocar por lo tanto la BIOS del sistema. Una vez acabado el proceso, se tendrá que reiniciar el ordenador.

Instalación desde Windows



Y en el momento de arranque nos pedirá si se quiere continuar con la instalación o arrancar con el antiguo sistema operativo ya instalado en el disco.

Arranque del sistema



A partir de aquí, nos saldrá la misma pantalla de inicio de la instalación del sistema GNU/Linux como si se hubiera hecho cambiando la BIOS para arrancar con la lectora de CD/DVD.

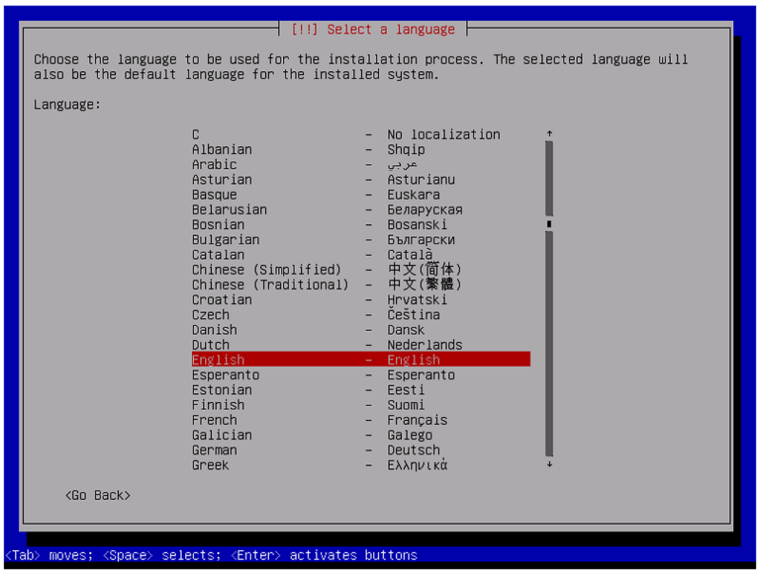
En las opciones avanzadas de la primera pantalla de instalación, encontraremos otro menú que nos permitirá realizar la instalación de diferentes maneras, pudiendo cambiar el escritorio que se use, la instalación en modo experto, donde se puede configurar con más cuidado todo el sistema. También se puede hacer una recuperación del sistema a partir de arrancar el CD con la opción de recuperación (*rescue mode*). Pero esta parte queda fuera de la introducción al sistema operativo que se quiere dar en estos materiales. En todos los casos y, como antes, existe la posibilidad de hacer la instalación dentro de un entorno gráfico o en una consola; los resultados finales serán idénticos, aunque en el caso de usar el entorno gráfico el proceso será más sencillo.

Pantalla de inicio

2.2.3. Configuraciones básicas para ejecutar la instalación

Si entramos en el enlace de instalación de la primera figura veremos la siguiente pantalla en la que se inicia el proceso de instalación, donde nos pide con qué idioma se quiere hacer la instalación del sistema operativo en el disco duro.

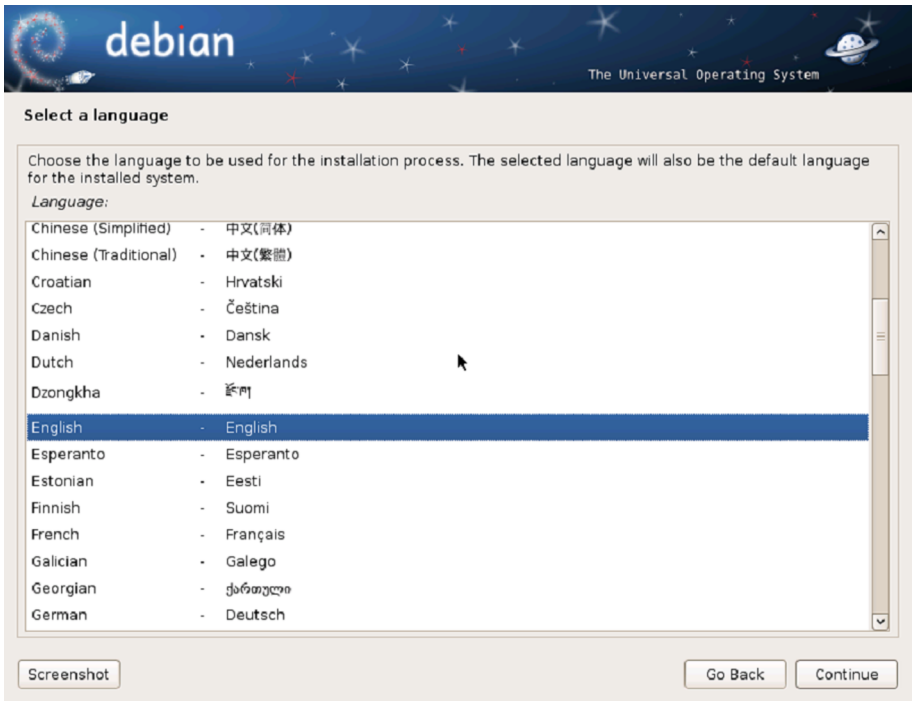
Primeras configuraciones



Sin embargo, si entramos en la instalación gráfica veremos que se accede a las mismas pantallas pero en este caso el ratón también funcionará y será mucho más cómoda la instalación. El proceso es idéntico en ambos casos, aunque varía un poco en el de la instalación del sistema en modo experto, que nos pedirá algunos parámetros de configuración adicionales.

Así pues, volvamos a iniciar el proceso de instalación, pero en este caso con la opción gráfica y la instalación normal. Lo primero que se tiene que decidir es el lenguaje de la instalación. Podemos optar por muchos idiomas, escogeremos el más adecuado.

Selección del idioma



A partir de aquí nos va pidiendo el tipo de teclado que se usa, donde seleccionaremos el teclado español, la zona horaria donde estamos y la localización de los locales que las configuraciones especifican para cada región y teclado. A partir de este momento ya se puede acceder a una *shell* del sistema por si acaso hiciera falta una, se accede a esta con la combinación de las teclas Crtl + Alt + F2 y, cuando nos lo diga, la tecla Enter. Esta *shell* será muy básica, pero nos permitirá hacer alguna que otra prueba.

En la TTY1 (Crtl + Alt + F1) el sistema va dejando los mensajes de los eventos que va haciendo, mostrará los *logs* del sistema, que también se pueden encontrar en el fichero `/var/log/messages`. Para volver otra vez a la sesión gráfica, se tiene que cambiar a la TTY5 (Crtl + Alt + F5). Estas TTY podrían cambiar en las diferentes distribuciones y posiblemente en versiones diferentes de la misma distribución, pero seguro que existen en alguna sesión.

El paso siguiente es la configuración de la red de comunicaciones, que en el supuesto de que Debian tenga los controladores del dispositivo de red y encuentre un servidor de direcciones y por DHCP pueda obtener una, no nos preguntará nada y por lo tanto, no hará falta configurar nada ni darle ningún tipo de dato respecto de la red.

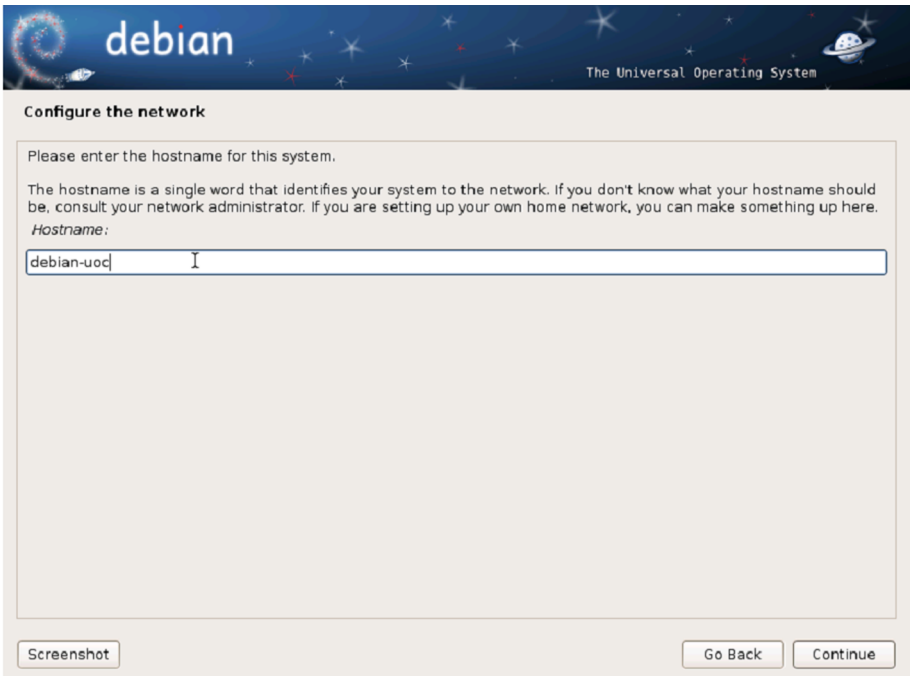
Normalmente los *routers* que las operadoras de telecomunicaciones proporcionan ya tienen activado este servidor de direcciones, por lo que no deberíamos tener problemas, pero si no lo tienen activado y no se puede o no se quiere activar, tendremos que introducir todos los datos relativos a la red local, como la dirección IP del sistema que estamos instalando, la máscara de red, la puerta de enlace y los servidores de nombres que se tienen que usar. Todo esto

se puede encontrar mirando las configuraciones de otros equipos de la red y cambiando la dirección IP en cada equipo o en la configuración del *router* que se disponga.

Este paso es importante que se haga bien, ya que al ser una instalación a través de la red, si no se dispone de esta, no se podrá acabar correctamente, lo que va a impedir que se pueda instalar todo el software necesario para el funcionamiento del sistema y sus aplicaciones. Por lo tanto, antes de iniciar la configuración de la red, si no está activado el DHCP en el *router* o en un servidor propio, debemos tener a mano los números relativos a la red para no tener que detener la instalación a medias.

Lo siguiente que se tiene que configurar es el nombre del equipo, cada uno tiene un nombre diferente para poder identificarlo dentro de una red. Se puede poner el que se quiera, pero es preferible poner alguno que nos haga fácil identificar su propósito. En el caso de tener un sistema único por casa, cualquier nombre servirá, pero para una empresa en la que puede haber miles de ordenadores, una mínima política de nombres facilitará mucho el trabajo a la hora de localizar un ordenador que dé problemas y se tenga que hacer alguna tarea de mantenimiento, cambiarlo o reinstalarlo, por ejemplo.

Nombre del equipo



En la parte de la configuración de la red ya solo queda enmarcar el sistema en un dominio, en un grupo de ordenadores que comparten una misma sala dentro de la red, ya que todos aquellos ordenadores que estén dentro del mismo dominio no tendrán problemas para verse entre sí y, así, poder compartir con mucha más facilidad la información. Podemos dejar por defecto esta

información para ordenadores domésticos, si solo tenemos uno, o poner el nombre del dominio que haya en casa o en la empresa donde se tenga que instalar el sistema.

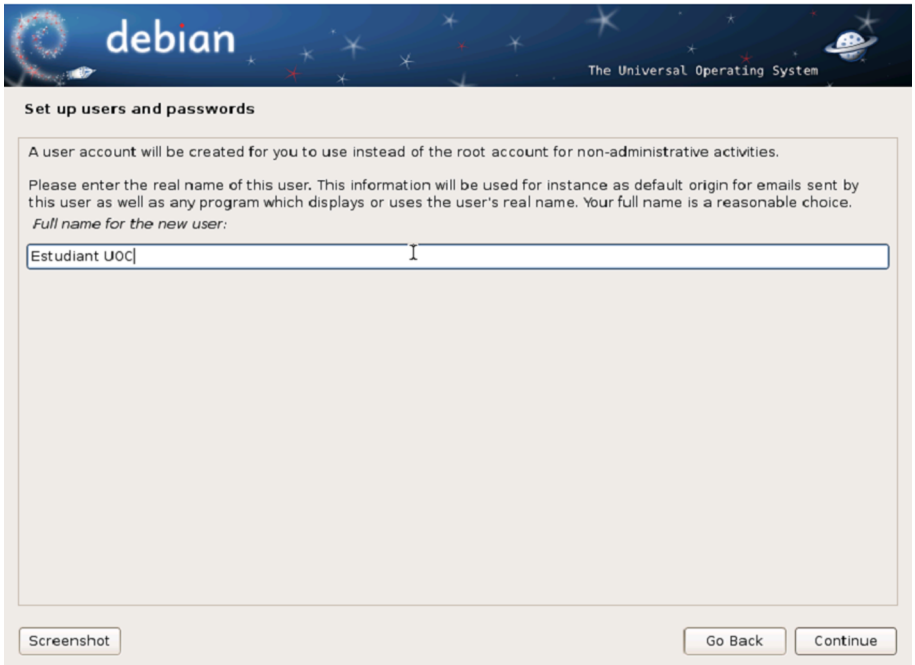
2.2.4. Usuarios y contraseñas

Los pasos siguientes son la configuración de los usuarios iniciales del sistema. Lo primero que se tiene que hacer es decidir la contraseña del usuario con permisos de administración del sistema, el *root*. Esta contraseña debe ser lo bastante complicada como para que otra persona no la pueda reproducir con facilidad sin que la conozca previamente. Hoy en día, los ordenadores están todos conectados a Internet y, por lo tanto, están expuestos a los ataques de las personas que quieren obtener acceso a todas las máquinas para poder, como mínimo, tener el control y poder atacar a otros desde la nuestra.

Una buena contraseña es la que dispone de letras, números y signos de puntuación como @, !, $, +, =, . (punto) o , (coma), entre otros. En el caso de tener un teclado español, también es recomendable usar letras que no estén en otros teclados o abecedarios, como la ç o la ñ. Otra cuestión muy importante es que el usuario *root* se deshabilitará en la entrada y no se podrá entrar al sistema como *root*, por lo que será necesario entrar al sistema como un usuario normal y hacer los pedidos que se desee en la *root* con el comando *sudo*, que permite ejecutar comandos desde los usuarios normales con privilegios de *root*, siempre y cuando se haya habilitado al usuario para hacerlo.

Lo siguiente que se tiene que hacer es la configuración del primer usuario del sistema, que usará todo lo que no sean tareas de administración del mismo. Opcionalmente se puede dar un nombre completo y después el nombre que se quiere que use como usuario.

Usuario del sistema



En el caso de la instalación, si no ponemos contraseña al usuario *root*, este primer usuario que se crea en la instalación tendrá automáticamente los derechos de poder usar el comando *sudo* para poder ejecutar tareas administrativas, puesto que el usuario *root* no existirá.

2.2.5. Reloj del sistema

Queda configurar el reloj del sistema, diciendo en qué franja horaria estamos con la que se quiere configurar el sistema operativo. En el caso de no tener problemas, simplemente pide a partir de la configuración del "locales" que se le ha dicho al principio, qué franja horaria queremos. Hay que tener en cuenta que hay países que tienen más de una, como por ejemplo España, en la que hay una diferente para las islas Canarias.

2.2.6. Partición del disco duro

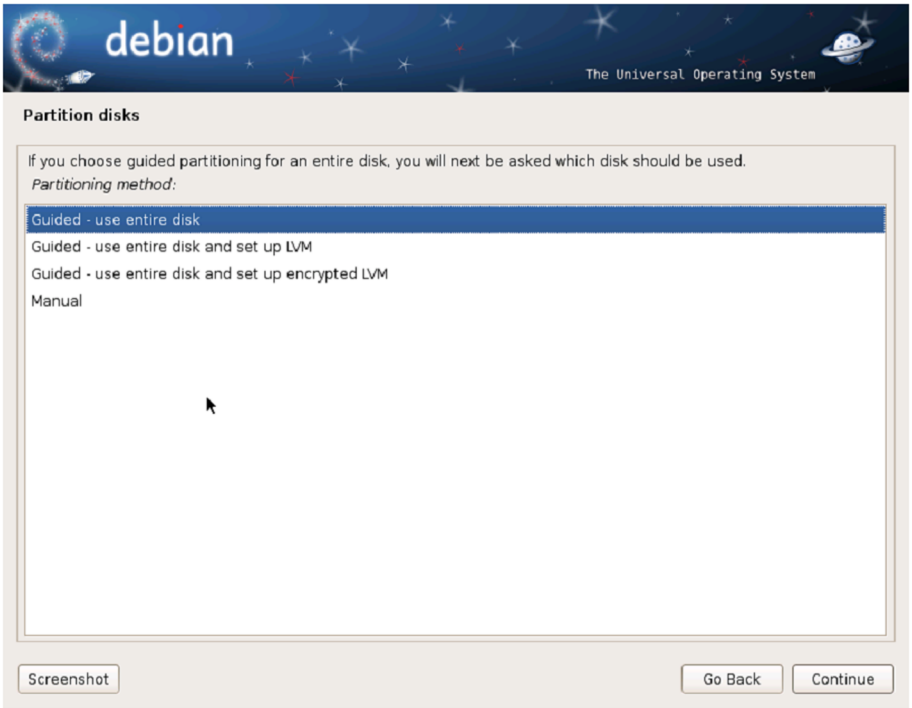
A partir de aquí ya empiezan a complicarse las decisiones y a haber más problemas en las repercusiones que podemos tener, ya que ahora se tiene que afrontar el particionado del disco. Se pide qué disco queremos usar para instalar el sistema y si queremos o no hacer particiones en ese disco.

A la hora de particionar los discos, el tamaño, las características y el número de particiones dependen en gran manera del tipo de uso y de la cantidad de disco duro de la que se disponga. Al tratarse de una instalación con finalidades educativas, se facilita a continuación la información sobre las particiones que se crearán suponiendo que se trabaje sobre un espacio de entre los veinte y los treinta gigabytes destinados a la nueva instalación.

Como mínimo, hay que crear dos particiones: una primera para montar el sistema y la otra de *swap* o intercambio de memoria. Para aumentar la eficiencia del sistema, nosotros crearemos seis particiones, de este modo el sistema será más flexible y mucho más eficiente, ya que se separarán por completo los programas, el sistema y los archivos de usuario, por ejemplo.

Lo primero que se debe decidir es en qué disco se va a instalar el sistema y, si solo tenemos uno, podemos ir directamente al enlace de particionado guiado o seleccionamos uno de los discos de los que se dispone para ejecutar allí la instalación. En ambos casos, vamos a llegar a la configuración del particionado guiado, donde seleccionaremos este, ya que otros tipos de configuraciones, como el RAID de los discos o la configuración en LVM de los discos, quedan fuera del alcance de estos materiales.

Particionado del disco



Discos RAID y LVM

La configuración en RAID de los discos implica tener más de dos discos en el ordenador que configuraremos para poder tener tolerancia a fallos en uno de los discos. Hay varias configuraciones posibles, dependiendo de cada configuración.

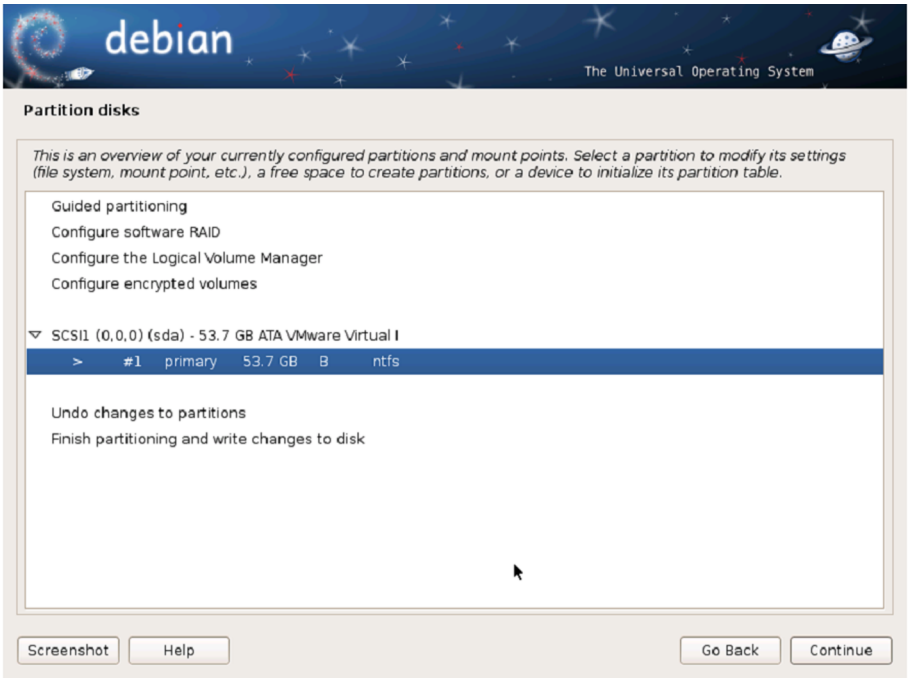
La configuración *LVM* (*logical volume manager*) permite tener más de dos discos configurados para que el sistema y el usuario los vea como uno solo mucho más grande, con la capacidad de todos los discos juntos. Esta configuración no permite tolerancia a fallos y, si se rompe un disco, se pierde toda la información.

En el caso de tener otro sistema operativo en el disco, se tiene que ir con más cuidado con lo que se está haciendo, ya que si seleccionamos el proceso guiado de todo el disco se borrará todo el contenido, puesto que lo estamos haciendo sobre el disco entero. Por lo tanto, lo que se debe hacer antes de ejecutar las particiones en el nuevo sistema es dividir el disco en dos, una parte para el sistema antiguo y otra para el nuevo GNU/Linux, que después volveremos

a partir. Por lo tanto, en este momento se tendrá que seleccionar el proceso manual para partir el disco. Como se ha dicho, en el caso de disponer de un disco separado para poder instalar el nuevo sistema operativo, este problema no lo tendremos, se podrá realizar el particionado guiado directamente.

El siguiente paso, la figura siguiente, es seleccionar el disco que queremos partir en dos y después hacer clic en la opción de cambiar de tamaño la partición.

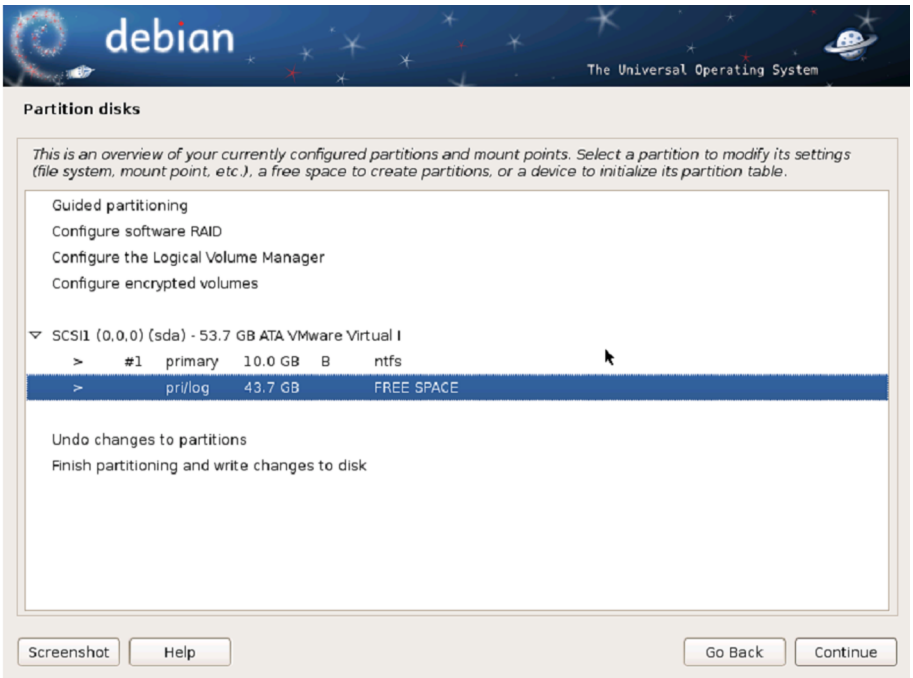
Partición por instalar



Una vez dentro de la opción, se tiene que indicar cómo se hacen las dos partes. Se puede indicar la capacidad de la primera, en gigabytes por ejemplo, o indicando el porcentaje que se quiere para la primera partición sobre el total del disco.

Una vez acabado el proceso de división del disco duro, que dependiendo de la capacidad del disco puede tardar bastante, el proceso de instalación volverá a la pantalla de realizar las particiones, pero ahora veremos que han aparecido dos particiones grandes del disco que teníamos antes, una con el sistema de archivos del sistema operativo antiguo y otra nueva con todo el espacio libre y sin sistema de archivos.

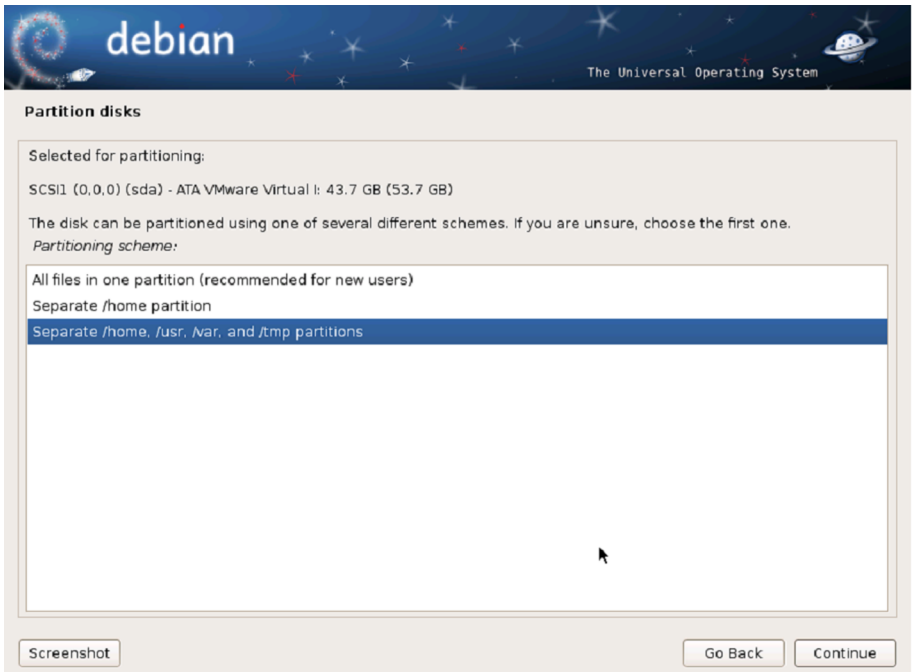
Particiones creadas al instalar Debian



Seleccionaremos la parte nueva que se ha creado para instalar el sistema y crearemos la partición de esta parte que todavía no está creada en el disco, simplemente dejando que se haga la partición automáticamente sobre todo el espacio libre de que disponemos en este momento en el disco. Ahora ya tenemos dos grandes particiones, una para el sistema operativo antiguo, el que había en el disco duro, y la otra para el nuevo, pero en una sola parte. Recordemos que esta se tiene que volver a dividir, al menos para poder hacer el área del sistema operativo y la de intercambio (a pesar de que en realidad no sería necesario, pero el rendimiento del sistema bajaría considerablemente). Este proceso sería idéntico en el caso de tener dos discos, donde, en lugar de seleccionar la segunda parte libre del disco, seleccionaríamos el segundo disco duro. Y el proceso a partir de aquí sería idéntico.

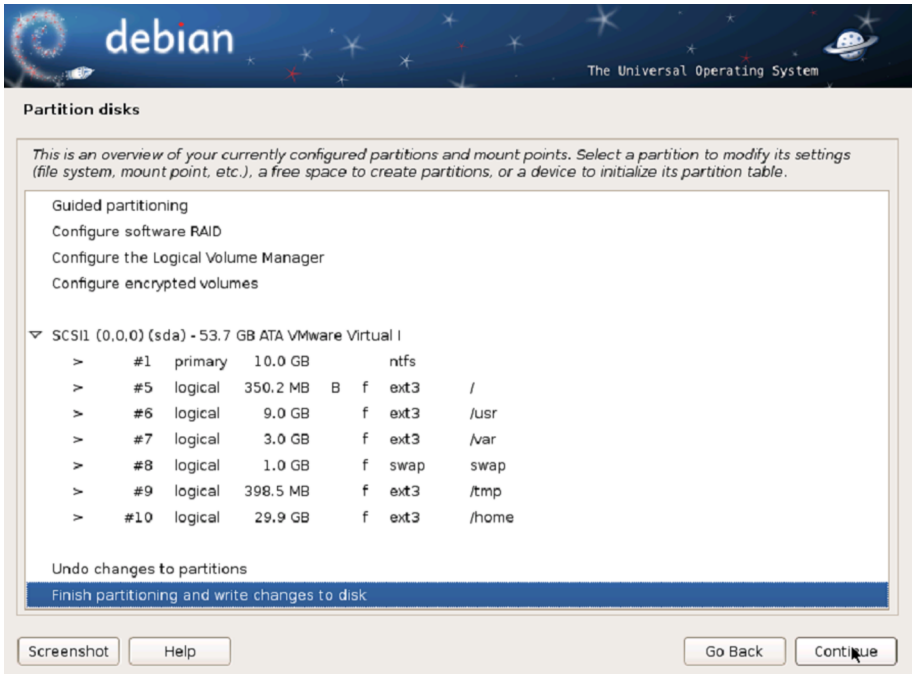
Lo más recomendable es dividir los datos de usuario, los de las aplicaciones y el sistema, ya que esto permite actualizar el sistema e, incluso, cambiar de distribución sin perder nunca los datos de usuario. Se podría formatear la parte del sistema sin perder nunca los datos. Por lo tanto, en el paso de particionar el disco de forma guiada seleccionaremos que se separe el `/home`, `/usr`, `/var` y `/tmp`.

Creación de las particiones del sistema



Finalmente, el proceso acaba con la escritura en el disco de todas las nuevas particiones, en las que se han creado seis nuevas partes aparte de la inicial con el sistema operativo antiguo. Podemos ver que se ha dividido ya con los tamaños que el propio sistema necesita. Estos tamaños serán diferentes teniendo en cuenta la capacidad de la partición, o el disco entero, que se asigna para hacer la instalación del nuevo sistema operativo. Por lo tanto, solo queda finalizar y escribir los cambios en el disco duro.

Particiones creadas



También se puede hacer este proceso manualmente, creando las particiones una a una y especificando el tamaño, el punto de montaje y el tipo de fichero, entre otros.

Para crear una nueva partición, hay que seleccionar la opción adecuada y a continuación, si todavía se pueden crear particiones primarias (hay que tener en cuenta que el número máximo son cuatro), se nos preguntará si la queremos crear como partición primaria o lógica; después tenemos que especificar el tamaño de la partición, y, finalmente, su ubicación física en el disco (es recomendable que antes de empezar a fraccionar el disco hagamos un pequeño esquema de cómo lo queremos hacer y, a continuación, creemos las particiones a partir de esta última partición hecha). Además, es importante tener este esquema para ver qué tamaños tendrán cada una antes de empezar y no tener que volver a borrar particiones por no tener claros los tamaños.

La primera partición es la destinada a alojar la raíz (`/`); esta no tiene que ser muy grande y por eso se destinará menos de un 10% del disco duro (o partición dedicada al GNU/Linux), preferentemente en una partición primaria, pero si no disponemos de ella la podemos crear como partición lógica sin dar más importancia. Le indicamos que la partición estará al principio del espacio libre y que el tipo de sistema de archivos elegido para la partición es ext3.

La segunda se destinará a la partición de intercambio (*swap*). Se recomienda que esta tenga, como mínimo, un tamaño igual al de la memoria RAM (512 Mb o 1.024, Mb, por ejemplo). A pesar de que para sistemas con menos de 1 Gb de memoria tendría que ser algo más del doble, en sistemas con mucha más memoria no hay que tener el mismo, aunque sea recomendable. En el caso de querer hibernar el sistema, sobre todo en instalaciones en portátiles, es importante tener como mínimo el doble de la memoria física asignada a la partición de *swap*, ya que, para hibernar, GNU/Linux hace una copia de la memoria real en el área de *swap* y si no cabe, o ya está bastante ocupada por datos debido a que la memoria física está saturada, no se podrá hibernar el sistema. Esta partición también es preferible que sea primaria, pero si tiene que ser lógica tampoco repercutirá en el rendimiento del sistema. Si tenemos más de una instalación de GNU/Linux en el mismo ordenador, se puede utilizar la misma partición *swap* para todas ellas, ya que la información que se pueda almacenar durante el funcionamiento del sistema es totalmente volátil. El tipo de sistema de archivos para la partición *swap* será de intercambio (*swap area*).

La tercera partición será para el directorio usr (`/usr`). Hay que tener presente que esta partición incluirá gran parte del software que se instale, por lo que deberá tener un tamaño significativo, en torno a un 40% del disco. Su sistema de archivos será ext3. La cuarta partición se destinará al directorio var (`/var`), donde se alojan bibliotecas y ficheros de log, entre otros. Igual que las anteriores, también será ext3. Y no hace falta que tenga un tamaño grande.

La quinta partición estará destinada a alojar los directorios personales de los usuarios (`/home`), cuya finalidad es almacenar los datos de los usuarios y, dependiendo del tamaño del disco duro, se le puede asignar el resto del tamaño del disco duro, en función del número de usuarios y del uso que se hizo del sistema; no es lo mismo tener un equipo dedicado a edición de vídeo que uno para tratar documentos de ofimática o para navegar por Internet, los datos que se han de almacenar afectarán bastante a esta partición de datos de usuarios. Esta partición también estará en ext3.

El espacio restante, la sexta partición, se destinará al directorio de ficheros temporales (`/tmp`) y su sistema de archivos también será ext3, con un tamaño relativamente pequeño, ya que son ficheros temporales que se pueden ir borrando.

La distribución de particiones anterior es solo una propuesta que tiene dos objetivos. Por un lado, pretende mejorar el rendimiento que ofrece una instalación basada únicamente en una o dos particiones y, por otro lado, da más robustez al sistema. Entre otras ventajas, tener los datos repartidos entre diferentes particiones provoca que la corrupción de una de ellas no implique automáticamente la pérdida de toda la información del sistema. Es obvio que se pueden crear otras particiones u omitir algunas de las propuestas (el orden de las particiones no afecta al comportamiento del sistema).

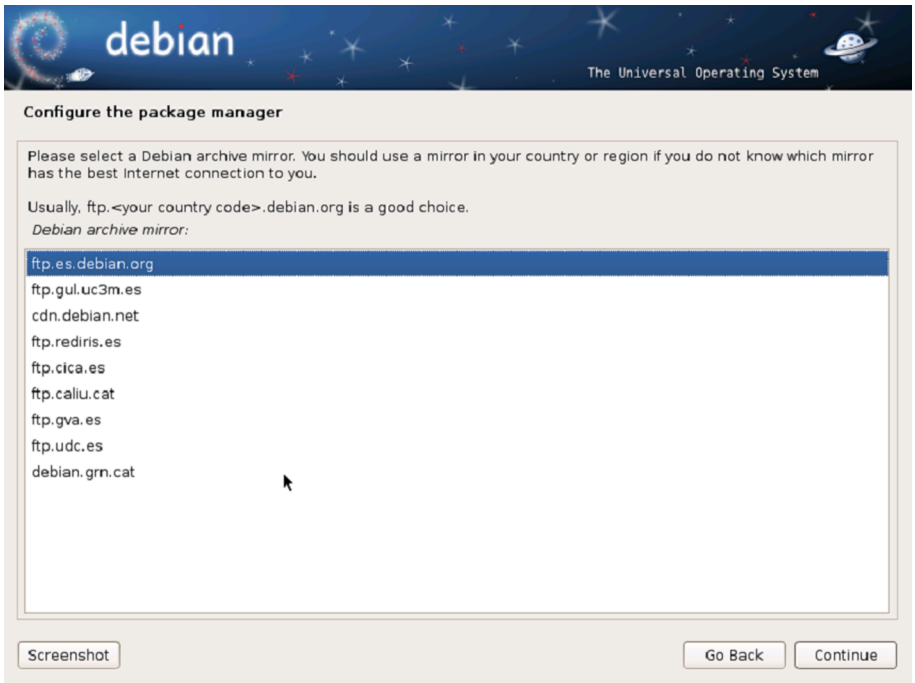
2.2.7. Instalación del sistema base

Ahora el instalador empezará a copiar en el disco duro el sistema base que nos permitirá después seleccionar lo que se quiere instalar y acceder a la red para acabar de obtener e instalar las aplicaciones necesarias y tener todo el sistema a punto.

Para poder seleccionar después los paquetes, debemos escoger un *mirror* de los muchos que tiene Debian por todo el mundo. Se recomienda por temas de tiempo escoger el que está en el mismo país o el más cercano, ya que así la latencia será mucho menor. También se puede seleccionar el *mirror* que creemos o sabemos que tiene más ancho de banda, y por lo tanto tardaremos menos tiempo en bajarnos de Internet las aplicaciones. Pero en principio todo está replicado en todos los *mirrors* y no tenemos que tener ningún problema en la elección más allá del tiempo de bajada de los ficheros.

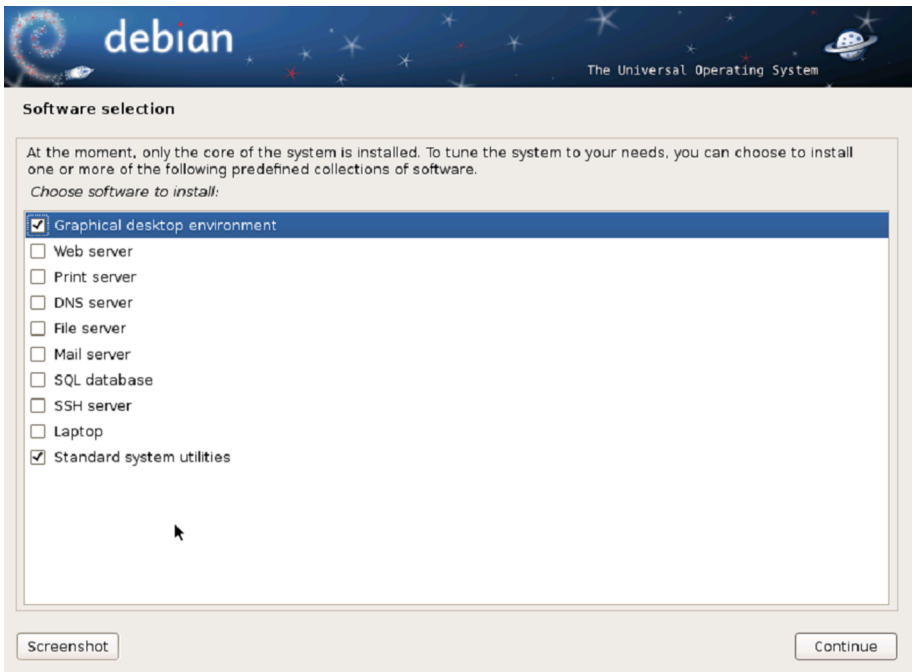
En el caso de necesitar un *proxy* para tener acceso a Internet desde el ordenador en el que se está ejecutando la instalación, se tendrá que especificar antes de poder acceder a los *mirror*; en caso de tener acceso directo, no hay que indicar nada en el campo de la configuración del *proxy*.

Configuración de los espejos del software



2.2.8. Instalación de programas

Selección del software



A partir de la utilidad que se quiera dar al sistema operativo, se seleccionarán las diferentes utilidades y herramientas que se requieran. En el caso de tener un sistema básico para empezar a trabajar con el GNU/Linux, solo hay que tener el entorno gráfico y las utilidades básicas del sistema, dejando todos los programas y utilidades de los servidores para cuando se disponga de más conocimiento del sistema. En el caso de tener un servidor, en este paso ya será posible instalar todos aquellos componentes que sean necesarios, como el servidor de archivos, el de páginas web o el servidor SSH, por ejemplo. Este

proceso puede ser bastante largo dependiendo de la velocidad de bajada de la conexión a Internet que se tenga, ya que ahora se bajarán todos los ficheros de las aplicaciones que se están instalando en el disco duro.

Una vez acabado, instalará el sistema de arranque en el caso de tener otro sistema operativo antes, indicando qué se ha encontrado y si realmente se quiere instalar este gestor; se podría optar por usar algún otro o no instalar ninguno en ese momento. Para poder acceder a los dos sistemas operativos, es necesario tener un gestor de arranque para las particiones de los discos duros. Se recomienda instalar este que ya configura solo el propio programa de instalación de GNU/Linux. Si todo ha ido de manera correcta, finalmente aparece la pantalla en la que nos dice que ya se ha completado toda la instalación y, por lo tanto, ya podemos iniciar el sistema.

Para poder utilizar el usuario con el que normalmente se va a trabajar, el que se da de alta en el momento de la instalación, en tareas de administración hay que darle acceso al comando `sudo`, y esto se hace con el comando `visudo`, en el que podemos añadir los usuarios a la lista de admitidos a usar el comando `sudo` y por lo tanto a operar como *root* en el sistema.

Finalmente, para tener acceso a un número más grande de paquetes, se tiene que activar el repositorio *non-free*. Para hacerlo, hay que iniciar la sesión en la máquina y abrir un terminal desde el usuario de acceso, cambiarse a usuario *root* con el comando `sudo` y, por último, editar el fichero `/etc/apt/sources.list` con cualquier editor de texto (como `vi` o `gedit`).

```
# sudo root
Password: *****
# vi /etc/apt/sources.list
...
deb http://ftp.es.debian.org/debian/ squeeze non-free
deb-src http://ftp.es.debian.org/debian/ squeeze non-free
...
```

También se puede hacer de manera gráfica con la aplicación de fuentes del software, dentro del menú de sistema, donde directamente se puede seleccionar el software no libre.

2.2.9. Activación de servicios y protocolos de red

En este apartado, vamos a mostrar cómo se instala y se configura la red en un sistema operativo basado en GNU/Linux. Un requisito para la instalación es tener una tarjeta de red, no un módem, ya que con el módem no tenemos un acceso a una red propiamente dicha, sino solo a un ordenador, que recibe

nuestra llamada y hace de puente hacia Internet. Hoy en día, la mayoría de las grandes distribuciones de GNU/Linux ya se instalan con la opción de trabajo en red activada, pero antes no era así.

A pesar de que esté activado el trabajo en red, es posible que tengamos que compilar el núcleo. Esto se debe al hecho de que en el núcleo hay definidos los tipos de tarjetas de red, conocidas también como *NIC* (*network interface card*), compatibles directamente con el sistema. Si usamos un tipo de tarjeta muy específico, tenemos que compilar el núcleo y añadir a este núcleo nuestra tarjeta de red. Para hacerlo, debemos seleccionar el tipo de tarjeta de la lista de dispositivos compatibles, guardar la configuración y ejecutar las órdenes que compilan el núcleo. Si usamos tarjetas de red conocidas (como 3Com, Intel o Ne2000) y una distribución de las más utilizadas (RedHat, Suse, Debian, Ubuntu), nos ahorraremos tener que compilar el núcleo, ya que la gran mayoría de tarjetas están soportadas.

Debemos saber qué dispositivo utiliza la tarjeta de red. Si solo tenemos una tarjeta de red, es muy probable que el dispositivo sea el `/dev/eth0`, pero para asegurarnos debemos ejecutar la orden `dmesg` y buscar el dispositivo de red en la lista de dispositivos que devuelve este comando. Podremos ver si está en eth0, en wlan0 o cuál es el dispositivo donde está conectado.

Con `dmesg | grep eth0` podremos saber si nos dice algo que es el dispositivo eth0, en caso contrario podemos buscar por wlan0 o algún otro.

Antes de configurar el protocolo IP, es muy importante tener los datos de configuración de la red. Estos datos los tiene que facilitar el proveedor de servicio ISP o el administrador de la red a la que se quiere conectar la máquina. En estos datos debe constar:

- la dirección IP;
- la máscara de red;
- la pasarela predeterminada (*gateway*);
- el servidor de nombres (DNS) primario y, opcionalmente, el secundario;
- el tipo de dirección (estática o dinámica).

En el caso de un servidor, es importante tener direcciones fijadas desde la misma máquina y no usar clientes de DHCP que nos podrían dar direcciones diferentes dependiendo de las circunstancias. Así, nos aseguramos de que siempre tendrá la misma IP y, por lo tanto, los ordenadores conectados no tendrán que cambiar nunca la dirección. Ahora que tenemos todos los datos necesarios podemos empezar a configurar la red.

La orden ifconfig

Una instrucción básica a la hora de configurar la red es la orden `ifconfig`. Si la ejecutamos sin ningún parámetro, nos muestra la configuración actual. Pero si, por ejemplo, queremos configurar un dispositivo de red eth0 con dirección IP dinámica, tenemos que ejecutar desde *root* # `ifconfig eth0 up`.

Hay otros muchos parámetros de configuración, como la dirección IP, la máscara de esta dirección o la pasarela. Para más información, consultad el manual (`man`). La configuración que obtenemos mediante la ejecución de esta orden es una configuración temporal y, cuando volvamos a arrancar la máquina, la configuración se habrá perdido. Según la distribución GNU/Linux que tengamos, es posible que al arrancar nos detecte la red y, si la red se configura mediante DHCP, el sistema ya nos la configura de manera automática.

¿Qué es el `man`?

El `man` es una ayuda que nos ofrece el sistema sobre las órdenes y los parámetros de estas órdenes. Para consultar esta ayuda tenemos que ejecutar `man comanda`, donde `comanda` es la orden que queremos consultar.

Si la red no utiliza DHCP o el sistema no nos configura la red en tiempo de arranque, lo debemos configurar nosotros mismos para que funcione de modo permanente. La manera de configurar la red en permanente tiene ligeras modificaciones según la distribución de GNU/Linux que utilicemos. En el caso concreto de Debian se configura del modo siguiente:

1) Editar el fichero `/etc/network/interfaces`.

2) Añadir a la línea auto el nuevo dispositivo.

3) Si configuramos con una dirección IP dinámica, tenemos que añadir:

```
iface eth0 inet dhcp
```

4) Si configuramos con una dirección IP estática, tenemos que añadir:

```
iface eth0 inet static address vuestra_direccion_IP netmask
vuestra_mascara_IP gateway vuestra_gateway_IP
```

Llegados a este punto ya tenemos dirección IP; ahora nos falta configurar el servidor de nombres de dominio (DNS) y las rutas. Para más información sobre el archivo `interfaces`, consultad el `man` (`man 5 interfaces`). Para configurar el DNS tenemos que editar el fichero `/etc/resolv.conf` y añadir una línea con la información siguiente.

```
nameserver vuestro_servidor_DNS
```

Si tenemos servidor secundario de DNS, debemos añadir una segunda línea con los datos de este servidor secundario. Si la dirección IP es de asignación dinámica, el DNS es un parámetro que recibiremos por DHCP; por lo tanto, no tenemos que configurar nada.

En la mayoría de las distribuciones, cuando se configura una interfaz de red con su dirección IP, normalmente ya se añade la ruta estándar correspondiente. Sin embargo, si no se ha añadido o no tenemos bastante con la ruta estándar, debemos configurar las rutas. Para configurar las rutas de encaminamiento (*routing*), es necesario que esté configurado como mínimo un dispositivo de red. La orden que se utiliza en este caso es `route`.

La orden `route`

La orden `route` sin ningún parámetro nos muestra la tabla de encaminamiento que está activa en aquel momento. Para añadir una ruta, tenemos que usar los parámetros `route add options` y, para borrar una, `route del options`. Para más información sobre estas opciones, consultad el `man`.

2.2.10. Protocolos y sistemas de autenticación de usuarios

Hay varios métodos de autenticación de los usuarios en sistemas basados en GNU/Linux. Los métodos que vamos a comentar a continuación son, o han sido, muy comunes. El primer método y el más simple es la autenticación mediante el archivo `/etc/passwd`. Cada línea de este archivo contiene toda la información de un usuario. Los campos están separados por el signo (:). El primer registro de la línea es el identificador de usuario. El segundo registro es la contraseña o *password*.

```
jordi: abcfl3yjFYN4Q:1000:1000:Jordi Serra:/home/jordi:/bin/bash
```

La contraseña se encontraba en texto plano (a principios de la era Unix) o cifrada, mediante la codificación *crypt* (como en el ejemplo superior). La segunda manera de autenticar es mediante el fichero `/etc/shadow`. Es una versión mejorada del método anterior. En el registro *password* (el segundo campo) del `/etc/passwd` se pone la letra `x`; entonces el sistema busca la contraseña en el fichero `/etc/shadow`. Este archivo tiene un formato parecido al archivo `/etc/passwd` pero cambian los valores de la mayoría de los registros. Como en el caso anterior, el primer campo es el usuario y el segundo –separado por (:)–, la contraseña codificada mediante *crypt* o MD5. La ventaja de este método respecto al anterior es que nadie (excepto el usuario *root*) tiene acceso a este fichero, ni de lectura. Por lo tanto, se vuelve más difícil poder acceder a esta información.

Los métodos que vamos a comentar a partir de ahora son métodos que requieren la instalación de un programa llamado Pluggable Authentication Module (PAM). El PAM es un juego de bibliotecas compartidas que habilitan al administrador local del sistema a elegir la manera como los programas van a autenticar a los usuarios. Dicho de otro modo, es posible intercambiar los métodos de autenticación que usa una aplicación que funcione con el PAM sin tener que compilar (o reescribir) la configuración de esta aplicación. Todavía más, se puede actualizar el sistema de autenticación local sin tocar las aplicaciones en sí. Esta aplicación da mucha flexibilidad al administrador a la hora de configurar y garantizar los privilegios de su sistema.

Otro método de autenticación es mediante la base de datos. Hay que disponer de una base de datos, ya sea local o remota, con una tabla donde estén los usuarios. Esta tabla debe contener como mínimo el campo del usuario y la contraseña. Para autenticar de este modo tenemos que configurar los PAM

indicando dónde está la base de datos, qué usuario es necesario para acceder a la base de datos, qué tabla tenemos que usar y qué campos contienen la información de usuario y contraseña.

Una versión mejorada de este último método es el llamado Lightweight Directory Access Protocol (LDAP). Tal como indica el nombre, se trata de un cliente muy "ligero" para acceder a servicios de directorio. Un directorio es parecido a una base de datos, pero tiende a contener información más descriptiva de los atributos. En un directorio, la información se lee mucho más de lo que se escribe. Hay muchas maneras de configurar un servidor LDAP; una es usando el PAM. Para configurar el PAM con el LDAP, tenemos que saber dónde está el directorio (el nombre de la máquina que ofrece el servicio de LDAP y el puerto por donde habla el servidor), si es necesario un usuario para acceder al directorio y qué atributos necesitamos para autenticar (usuario y contraseña). Aunque parezca una contradicción, a veces se necesita un usuario y una contraseña válidos para autenticar los usuarios. Es decir, que solo hay determinados usuarios que tengan el privilegio de autenticar a los usuarios. A veces, este tipo de doble autenticación es más perjudicial que beneficiosa.

Usurpadores de autenticidad

Imaginemos que un pirata informático es capaz de capturar una petición LDAP de autenticación normal. Está en posesión de un usuario sin privilegios. Ahora imaginemos que captura una petición LDAP de autenticación con un usuario con privilegios de autenticar. La captura de esta petición tiene mucho más valor, ya que además de un usuario normal tiene en su poder un usuario con privilegios sobre el directorio.

La última manera de autenticar que vamos a tratar en este apartado (hay muchas más, pero aquí solo comentamos algunas de las más habituales) se denomina Remote Authentication Dial In-User Service (RADIUS). El método de autenticación RADIUS también tiene asociada una base de datos detrás. Lo que lo hace diferente de los demás métodos es que es compatible con muchos protocolos de autenticación (PAP, CHAP, EAP, MD5) y, aparte de tener la capacidad de *accounting*, es capaz de determinar a cada usuario el tipo de servicio que se tiene que ofrecer. Hasta ahora, lo han usado mucho los ISP para dar servicio a sus usuarios de *dial-up*. Hoy en día, también se utiliza mucho para autenticar a los usuarios de redes inalámbricas. Esta nueva aplicación de RADIUS se debe al hecho de que se han desarrollado una serie de protocolos seguros (cifrados) a nivel dos para dar servicio a redes tradicionalmente inseguras (redes inalámbricas).

Para elegir un protocolo de autenticación para nuestra máquina, debemos tener presentes dos aspectos: el entorno y la seguridad. El entorno nos marca qué tipo de necesidades tenemos. No es lo mismo tener una máquina con todos los servicios de usuario que tener una máquina para cada servicio y los usuarios accediendo a todas esas máquinas. En el primer caso, basta con el `/etc/shadow` y la codificación MD5. En el segundo, es recomendable tener un servidor dedicado a autenticar y que todos los servidores acudan para dar acceso a los usuarios. En este caso, desde el punto de vista de la seguridad, es recomendable usar LDAP o RADIUS.

3. Instalación del servidor Windows Server 2012

3.1. Instalación

Antes de instalar Windows Server 2012, hay unos cuantos parámetros que se deben decidir sobre el proceso de instalación. A continuación, repasamos los más importantes.

3.1.1. Elegir el origen de la instalación

Windows Server 2012 se puede instalar desde el CD-ROM/DVD si el BIOS del ordenador admite el arranque desde una unidad de disco compacto. En caso contrario, hay que iniciar la instalación desde los disquetes de arranque. Otra posibilidad de hacer la instalación es por la red, aunque será considerablemente más lenta, ya que se tienen que pasar todos los archivos por la red, que en algunos casos podría estar en producción y por lo tanto dando servicio a otros servidores y clientes.

3.1.2. Proceso de instalación

Con esta versión del sistema operativo de Windows se ha minimizado mucho la interacción con el proceso de instalación. Básicamente, ahora el proceso pide el idioma en el que se quiere instalar el sistema, en el caso de tener una versión multiidioma, y el tipo de teclado que se tiene instalado en la máquina, para entrar ya directamente en el proceso de instalación propiamente de todos los ficheros necesarios. Una vez se haya introducido el número de licencia correspondiente a la versión que se quiere instalar, de las cuatro en las que se distribuye el sistema operativo se pasa a la primera decisión más importante que se tiene que tomar, ya que se puede instalar el sistema operativo Windows Server 2012 de dos modos muy diferentes, a pesar de que *a posteriori* se pueden cambiar y pasar de uno al otro con cierta facilidad. Así pues, tenemos dos posibilidades:

1) Windows Server 2012 Standard (Server Core Installation)

2) Windows Server 2012 Standard (Server with a GUI)

Describiremos ahora de modo muy breve las diferencias más importantes que hay entre las dos instalaciones.

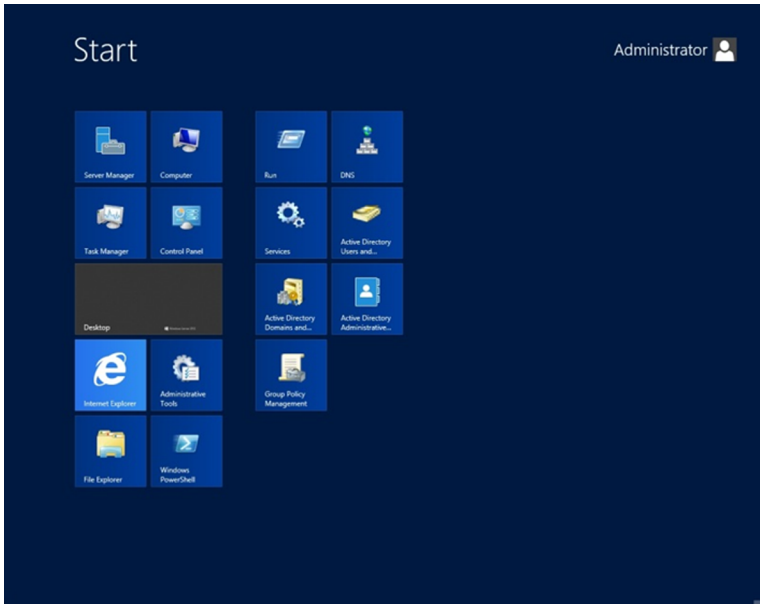
3.1.3. Server Core Installation

En este caso, el sistema que se acaba instalando no dispone de ninguna interfaz gráfica, una vez se entra al sistema para trabajar con él se abre una consola y todo se tiene que hacer desde la línea de pedidos con el nuevo intérprete PowerShell. Esta modalidad permite disponer de sistemas que ocupan muy poco disco, la instalación del sistema operativo no tiene nada más que lo necesario para funcionar y dar servicio a todo lo que se vaya configurando. En un principio, no hay ningún servicio o programa complementario al sistema operativo, es decir, que se tendrá que incluir todo lo que sea necesario para trabajar con este servidor. Aparte de la localización del disco donde se quiere hacer la instalación, no se pide nada más, y se obtiene una instalación muy rápida y sencilla completamente funcional.

3.1.4. Server with GUI

Por el contrario, en el segundo caso, la instalación también introduce en el sistema toda la interfaz gráfica a la que se está más acostumbrado con todos los sistemas operativos de la familia Windows. Más en concreto, la nueva interfaz llamada Metro, que se inició en los dispositivos móviles que llevaban Windows Phone 7. La figura siguiente muestra un ejemplo de cómo queda tras instalar el sistema y alguna aplicación.

Nueva interfaz Metro de Windows



3.1.5. Planear particiones de discos

Durante el proceso de instalación de Windows Server 2012, aparte del idioma en el que se quiere configurar el teclado y el propio sistema, se puede seleccionar dónde se quiere instalar el Windows Server 2012. Esto quiere decir que se pueden crear particiones específicas para instalarlo en un disco más grande, con otros sistemas o directamente en todo el disco duro. El instalador creará una partición pequeña, de unos cuantos megabytes, por temas de administración del sistema, que será inaccesible desde el propio sistema operativo. Por lo tanto, a la hora de ejecutar la instalación, se debe tener en cuenta que en el tamaño que se le ponga, se verá un poco afectado, aunque con los discos de que actualmente se dispone no afectará casi nada a la capacidad. Es recomendable usar una partición relativamente pequeña para instalar el sistema operativo y las pocas aplicaciones que se pueden usar desde el servidor y dejar una partición mucho más grande para usarla de disco de usuario si es un servidor dedicado a hacer de servidor de archivos o para tener los archivos de una página web, por ejemplo. De este modo, será mucho más fácil la administración de todo el servidor, ya que se dispondrán completamente separados los datos y el sistema. Desde el proceso de instalación, se puede asignar una pequeña parte para el sistema, hacer una partición e instalar el sistema en ella y luego desde el administrador de discos que dispone el Windows Server 2012 configurar el resto de particiones que sean necesarias. El funcionamiento de este particionador del disco duro y el administrador de discos es bastante sencillo e intuitivo y queda fuera del contenido de estos materiales.

Web recomendada

En la página siguiente, hay más información sobre planificación de particiones y sobre la instalación del sistema operativo de Windows.

http://technet.microsoft.com/es-es/library/jj134246.aspx

3.1.6. Sistema de archivos

Ya desde la versión Windows Server 2008, el sistema de archivos que implementan estos sistemas operativos es el NTFS, que deja a un lado los FAT y FAT32 como nativos para poder instalar el sistema. No obstante, dispone de soporte para poder leer los discos externos portátiles y las memorias USB que se puedan usar, ya que seguro que estos formatos se siguen usando en algunas de estas memorias externas. Esta decisión ya comportó un gran salto en temas de seguridad, sin permitir que un servidor tuviera un sistema de archivos sin seguridad como son FAT y FAT32, pero que por compatibilidad con un sistema ya muy antiguo en las versiones anteriores se permitía poder usar estos sistemas de archivos.

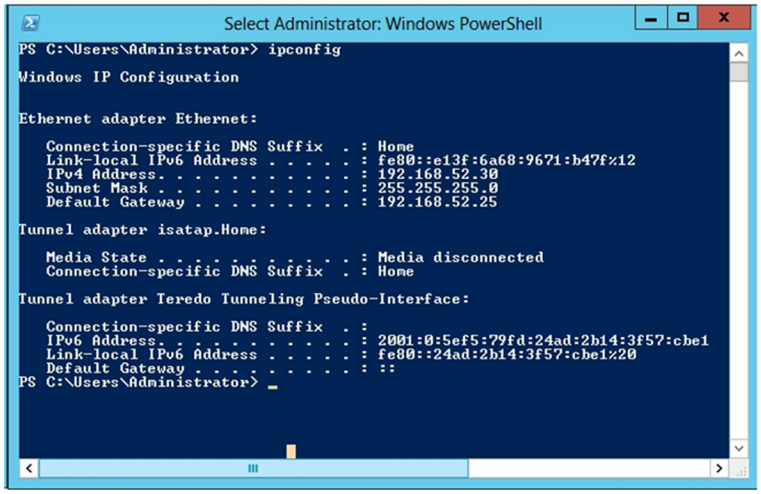
El proceso de instalación sigue formateando la partición si fuera necesario, es decir, en el supuesto de que se haya hecho una nueva partición, y copia los archivos necesarios para la instalación en el disco. Una vez acabadas estas operaciones, el programa de instalación reinicia por primera vez el servidor para acabar definitivamente la instalación. Tras reiniciar por primera vez, se lanza la instalación en el modo gráfico para ultimar las tareas de instalación y por último, sin más preguntas, tendremos ya instalado el sistema.

3.1.7. Primeras modificaciones

Una vez reiniciado el sistema, ya es completamente operativo, a pesar de que no dispondrá de ningún rol de servidor, pues por defecto no lleva ninguno preinstalado. Lo primero que tenemos que hacer es configurar los parámetros de la red que, por defecto, los cogerá por DHCP y en un servidor esto no es lo más adecuado, ya que podríamos tener problemas a la larga si el servidor de direcciones IP cambia por algún motivo la dirección del servidor. Todos los clientes dejarían de tener acceso al servidor automáticamente.

Para cambiar la dirección IP del servidor, basta con abrir el panel de control y configurar de manera correcta los parámetros del protocolo IPv4 o IPv6 dependiendo de la configuración de red que se tenga en cada institución. En este caso, justo es decir que, a pesar de que no se asigne una IP al protocolo IPv, Windows Server 2012 convertirá la dirección que se introduzca en el protocolo de IPv4 a IPv6. De forma que, sobre la red interna, se trabajará siempre sobre IPv6. Esto lo podemos ver a través del comando `ipconfig`, figura siguiente, y ahí se puede ver que, a pesar de tener solo asignada la dirección de IPv4, también tiene una configurada para IPv6 que usa la red Microsoft para que pueda crear dentro de la organización.

Configuración IPv4 e IPv6



La siguiente cosa importante que se debe ejecutar es cambiar el nombre del servidor y ponerlo en un dominio si hace falta, ya que por defecto el proceso de instalación dará uno aleatorio que no servirá para poder identificar con rapidez el servidor dentro de la organización.

El nombre y el dominio se pueden cambiar en el panel de control, dentro de la categoría de propiedades del sistema. Ahora se tiene que elegir el nombre del equipo, que es una secuencia de caracteres que identifica al servidor dentro de un dominio o grupo de trabajo. Es importante, por lo tanto, no utilizar ningún nombre de equipo que ya se use. Es útil asignar nombres a los equipos que nos recuerden la funcionalidad que tienen. Por ejemplo, BD_Central o BD puede

ser el nombre de equipo para el servidor que almacene las bases de datos de la organización, y Website puede ser el servidor que contenga el sitio web de la organización.

En el caso de que el servidor que estamos instalando tenga, ya que lo instalamos con posterioridad, el rol de servidor de dominio, no es necesario que se le asigne un nombre de dominio de la red, puesto que lo tomará directamente del rol que se configure posteriormente. En el caso de pertenecer a una red ya establecida, sí se tendrá que incluir en la red reescribiendo el nombre del dominio.

Por otro lado, la contraseña del administrador es un punto importante en orden a la seguridad del servidor. A veces, cuando se hacen pruebas en un ordenador personal, se suele omitir esta contraseña por comodidad, pero un servidor en producción tiene que tener asignada una contraseña de administrador para evitar intrusiones en el sistema. Y esta contraseña solo la tienen que saber las personas que tengan derechos de administración sobre este servidor.

Otro factor que se debe tener en cuenta a la hora de establecer una contraseña, ya sea de administrador o de usuario corriente, es que sea una cadena de letras y números sin sentido, que no estén relacionados con ningún dato personal, como la fecha de nacimiento o el nombre y apellidos, por ejemplo. Además, es recomendable no apuntar la contraseña en ningún papel o medio digital y cambiarla a menudo para evitar que la descubran.

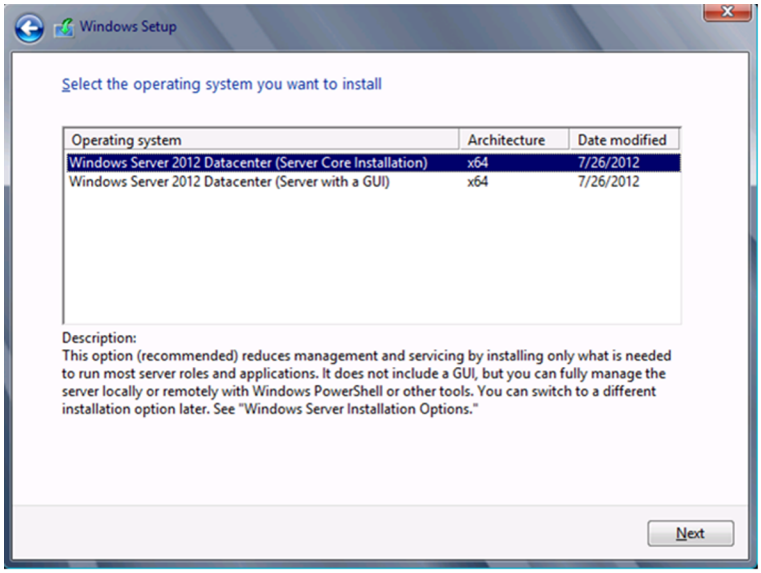
Windows Server 2012 introduce un sistema de calidad de contraseña por defecto, que nos avisa en caso de que la que hemos establecido sea débil. Si así es, nos informa de que hay que elegir una más segura y nos da indicaciones sobre qué criterios tiene que cumplir esta contraseña: al menos los dos primeros y, como mínimo, tres de los siguientes:

- debe tener más de ocho caracteres;
- no debe tener partes del nombre de usuario al que pertenece;
- debe tener alguna letra en mayúscula;
- debe tener alguna letra en minúscula;
- debe tener algún número;
- debe tener algún carácter no alfanumérico (como $, & o #).

3.1.8. Instalación del sistema Core

Una de las nuevas características que tiene Windows Server 2012 es que permite la instalación de todo el sistema en una versión muy reducida y que, una vez instalada, consume los mínimos recursos en el sistema operativo.

Tipos de instalaciones de Windows Server 2012



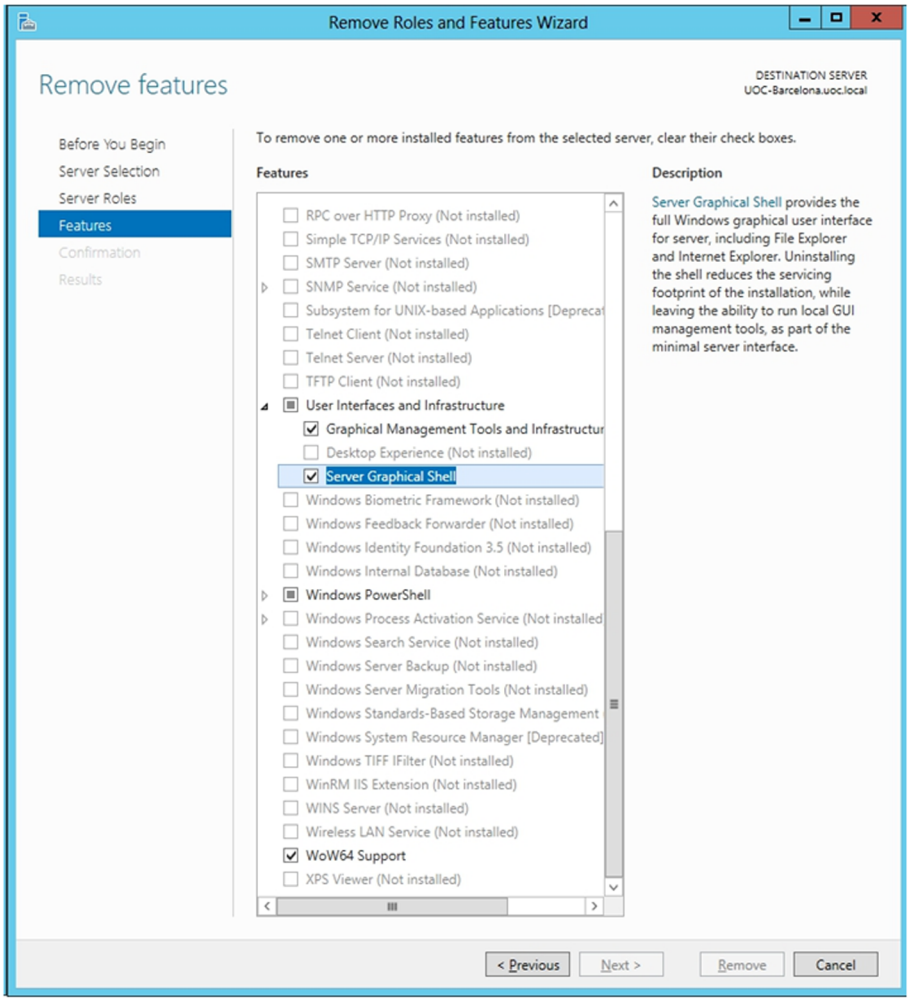
Para hacerlo, únicamente será necesario seleccionar la opción de la instalación del Server Core Installation para tener al final un sistema lo más pequeño posible. Tan solo dispondrá una consola de comandos para interactuar con el administrador, a pesar de que desde esta se puede llamar a la nueva *shell* llamada PowerShell, donde se pueden hacer muchas más cosas que con la antigua consola de comandos y que además nos permitirá configurar por completo todo el sistema, mostrada en la figura siguiente. Permite configurar la red, instalar nuevos roles y configurarlos, entre otros.

Consola de comandos y PowerShell

También se puede pasar de un sistema a otro una vez instalado y configurado, por lo que siempre será más cómodo instalar la versión completa, con la interfaz gráfica, configurarlo todo, instalar todos los roles, características, usuarios, políticas de seguridad y después pasar a la versión Core para hacer el sistema mucho más rápido y seguro.

Para pasar de la versión GUI a la versión Core, hay que desinstalar una de las características que se instalan por defecto en esta versión. Para hacerlo, habrá que abrir el administrador del servidor y en la configuración entrar en la herramienta de desinstalar roles y características. Aquí hay que eliminar del sistema la característica de infraestructura e interfaz de usuario, tal y como muestra la figura siguiente. Se tendrán que eliminar por completo todas las subccaracterísticas que tiene.

Característica de infraestructura e interfaz de usuario



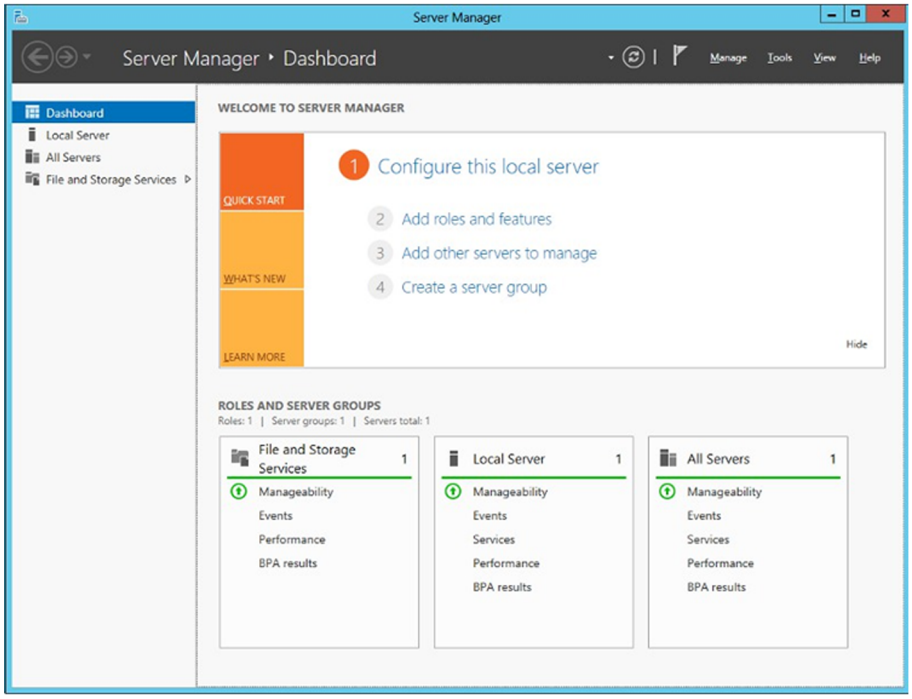
Al reiniciar el sistema, ya no aparecerá la interfaz de usuario que aparece por defecto, y el sistema será únicamente accesible mediante la consola de comandos. Podemos tener una versión intermedia entre la versión Core y la GUI, donde se dispondrá de la versión Core, pero con una mínima interfaz gráfica para algunas herramientas del sistema. Esto lo conseguiremos eliminando únicamente el servidor de comandos gráficos que está seleccionado en la figura anterior.

También se puede pasar de la versión Core a la versión GUI instalando en paso la interfaz a partir del disco de instalación de Windows Server 2012 y la línea de comandos. Estos pasos se pueden encontrar en la dirección http://technet.microsoft.com/en-us/library/hh831786.

3.2. Configuración del servidor

Una vez instalado el sistema operativo, podemos cambiar algunos parámetros de los diferentes servicios del servidor para configurar el comportamiento. Al arrancar el sistema, el propio Windows Server 2012 ya nos abre una ventana donde podemos configurar todo lo necesario e, incluso, hay una guía inicial sobre lo que se tiene que hacer.

Tareas iniciales de administración



Desde esta pantalla se puede ir al primer *link*, donde está la configuración inicial del servidor, y desde donde se podrán tener todas las características del servidor completamente controladas. Desde esta misma pantalla se puede crear un grupo de servidores que estén todos en la misma empresa y que formarán parte del directorio activo del servidor. De este modo, se podrán gestionar en remoto todos los servidores, sin tener que ir físicamente o mediante el protocolo RDP (el escritorio remoto) a estos servidores. Así, desde este administrador podemos gestionar toda la red de servidores a la vez y, por lo tanto, tener una visión mucho más cuidadosa de lo que está pasando en toda la red. Iremos añadiendo los roles y las características a los diferentes servidores desde un único punto de gestión.

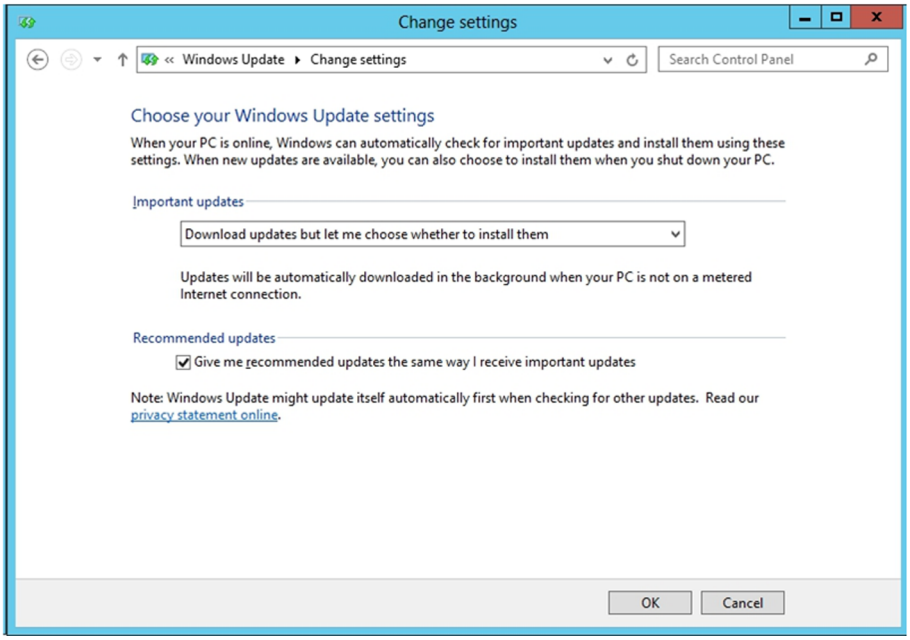
Otra de las cosas que se tienen que hacer desde buen principio es configurar el servidor para actualizarse correctamente. Y esto se lleva a cabo mediante las actualizaciones periódicas que hace Microsoft y que cada segundo martes de

mes envía las correcciones a través del sistema de actualizaciones automáticas. Es importante tener una buena política de actualizaciones y saber en todo momento qué es lo que se quiere actualizar. En sistemas en los que puede haber software de terceros o es muy crítico el funcionamiento de los servidores, antes de aplicar una actualización es importante documentarse sobre a qué puede afectar, a qué otros programas afecta y lo que hace en el sistema. Nos podríamos encontrar con actualizaciones que hacen que un software hecho a medida que accede a una DLL, o API del sistema, sea modificado por la actualización y por lo tanto deje de funcionar el software de terceros.

En algunos casos en los que el funcionamiento del sistema es muy importante, las actualizaciones se hacen en horario fuera de la jornada normal de trabajo para poder volver atrás en el supuesto de que pase lo que se ha indicado antes. O, si es el caso, que una actualización pida reiniciar el servidor.

Por lo tanto, es importante configurar el sistema de actualizaciones para que no instale los nuevos componentes cuando el sistema quiera sino que sea el propio administrador quien decida cuándo y qué actualizaciones se hacen. La mejor opción es configurarlo de forma que nos pregunte qué actualizaciones se quieren bajar si tenemos software que interactúa con las API del sistema que se pueden cambiar, y que podamos decir cuándo se instalan y poder reiniciar el sistema cuando sea más adecuado. La figura siguiente muestra una configuración típica de estas políticas de actualizaciones.

Configuración de Windows Update



3.2.1. Cambio del nombre

Lo primero que habrá que hacer al arrancar por primera vez el sistema después de la instalación es cambiarle el nombre, ya que pone uno aleatorio. Esto se hace en el panel de control y, dentro de "Sistema y seguridad", se encuentra el enlace donde poder ejecutar el cambio de la configuración del nombre.

En este paso, se tiene que decidir qué política de nombres se usa, ya que el nombre de cada equipo tendría que diferenciarlo e identificarlo con rapidez. Un nombre como servidor1 no nos aportará información si desde la red vemos este nombre, pero si le ponemos un nombre como `S1DNS`, `S1HTTP` o `S1Files` sabremos con rapidez que se trata del servidor 1 y que está dedicado a las tareas de resolución de nombres, de páginas web o de servidor de ficheros, por ejemplo. Esto, que puede ser útil para los administradores de sistemas, se puede volver en contra en el caso de la seguridad, ya que con rapidez un atacante (interno o externo) sabrá qué IP están asignadas a los servidores más importantes. Por lo tanto, lo que parece más razonable es tener una codificación propia a la hora de asignar los nombres y que si se conoce esta codificación sea rápido saber qué hace cada servidor.

3.2.2. Activación de servicios y protocolos de red

Una vez tenemos el nombre asignado al nuevo servidor, basta con hacer la configuración de los parámetros de red. Podemos configurar los parámetros de red mediante la opción "Conexiones de red" del panel de control. Aquí será importante dar una IP fija al servidor, puesto que podríamos tener problemas después si la tenemos por defecto, tal y como se queda después de la instalación, y usar el *dynamic host configuration protocol* (*DHCP*). En la ventana de conexiones de red están todas las conexiones configuradas en el sistema. Además, podemos añadir conexiones nuevas o eliminar algunas de las que ya hay. Para configurar una conexión de red, podemos utilizar la opción "Propiedades" del menú contextual que sale al hacer clic con el botón secundario del ratón encima del icono de la conexión. Al abrir la ventana de propiedades de la conexión, vemos los diferentes servicios y protocolos instalados. Para instalar y configurar otros servicios o protocolos, hacemos clic sobre "Instalar" y nos salen los protocolos disponibles. Rara vez se tendrá que incluir un nuevo protocolo de comunicación, pero en redes antiguas sí podría darse el caso. También podemos configurar un protocolo o servicio que ya ha instalado mediante el botón "Propiedades". Por ejemplo, para configurar el acceso a Internet del servidor, tenemos que modificar las propiedades del protocolo TCP/IP. En la ventana de propiedades de TCP/IP, podemos modificar la IP del servidor, de forma que quede fijada, y las IP de los servidores de DNS (nombres de dominio). En este caso, de los DNS y para poder después configurar el servidor como servidor de dominio y poder tener el Active Directory, tendremos que

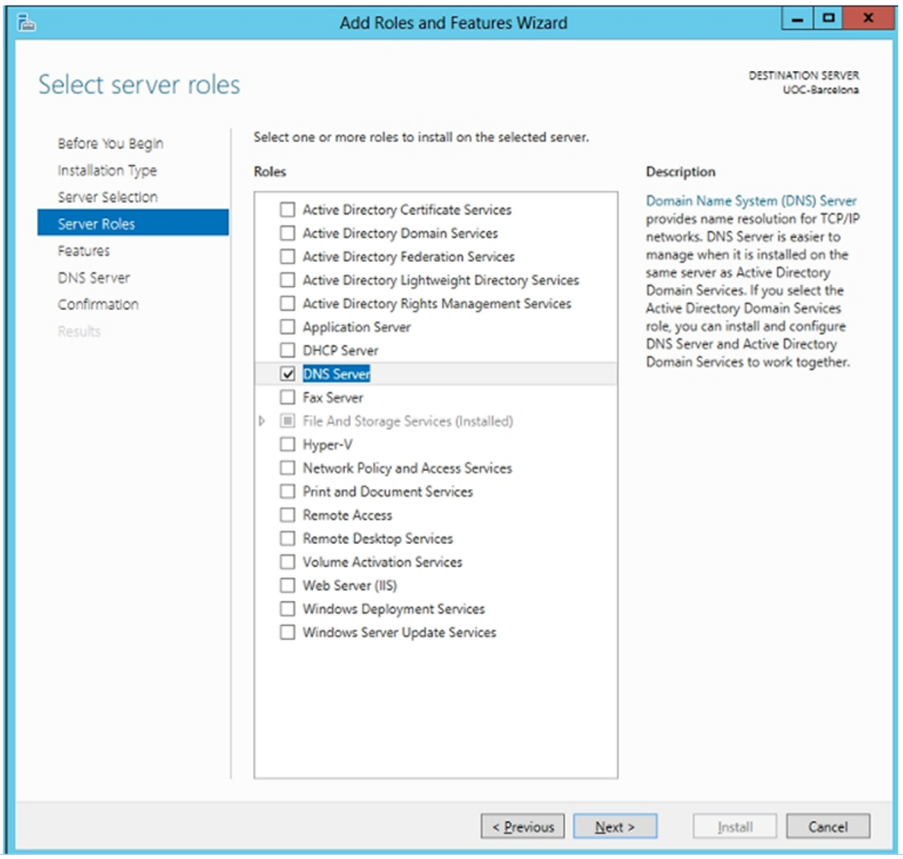
poner en el DNS primario la *localhost*, es decir, la dirección 127.0.0.1, y como secundario otro servidor DNS de apoyo del que se disponga o los DNS que haya suministrado el proveedor de Internet que se tenga contratado.

3.2.3. Roles del servidor

Como ya se introdujo en el Windows Server 2008, el sistema operativo Windows Server 2012 está formado por roles que se tienen que ir seleccionando e instalando en el sistema. Estos roles son las funcionalidades que se quiere dar al sistema, ya que por defecto, tras la instalación, el sistema no será nada más que un sistema escritorio, puesto que no tiene ninguna característica adicional instalada.

Algunos de estos roles se mostrarán luego, pero los más usuales son el del AD (*active directory*), el DNS (*domain name server*) y el de *web server* (IIS). La figura siguiente muestra los posibles roles que se pueden instalar en el sistema.

Listado de los roles de Windows Server 2012



Lo primero que se tiene que hacer es instalar el servidor de DNS para poder después hacer la resolución interna de nombres dentro de la red de ordenadores clientes que se conectarán al servidor de dominio; sin este DNS no se podría hacer el resto de cosas y configurar y securizar el entorno de una manera centralizada y segura. Solo hay que instalar el rol, seguir las instrucciones

y ya se dispone de un DNS local. Aparecerá en la interfaz Metro el enlace a la configuración del DNS. Ahora tendremos que crear en el administrador de DNS una nueva zona para poder incluirla después en el directorio activo.

3.2.4. Protocolos y sistemas de autenticación de usuarios

Windows Server 2012 tiene un sistema de inicio de sesión único, donde el usuario inicia la sesión en el dominio una sola vez mediante una única contraseña o tarjeta inteligente y después puede acceder a todos los recursos a los que tiene acceso sin tener que reescribir la contraseña o requerir una diferente para cada equipo del dominio. La autenticación de usuarios en Windows Server 2012 consta de dos fases: el inicio de sesión interactivo y la autenticación de red.

1) Inicio de sesión interactivo

Kerberos V5-1.11 constituye el protocolo de seguridad principal para la autenticación dentro de un dominio. El protocolo Kerberos V5 comprueba la identidad del usuario y los servicios de red. El inicio de sesión interactivo comprueba los datos de identificación del usuario en una cuenta de dominio (acceso a cualquier recurso del dominio) o en un equipo local (acceso solamente a los recursos del equipo local). Al iniciar sesión, el usuario introduce sus credenciales o utiliza una tarjeta inteligente para tener acceso al sistema. Si la cuenta es de dominio, se usa el protocolo Kerberos V5 para la autenticación, o Kerberos V5 con certificados si se utiliza una tarjeta inteligente. En el caso de inicio de sesión en una cuenta local, las credenciales del usuario se comprueban con los datos almacenados en el administrador de cuentas de seguridad (SAM).

2) Autenticación de red

Mediante la autenticación de red se identifica a un usuario en cualquier servicio de red al que intente acceder. En este proceso de autenticación, se utilizan protocolos como Kerberos V5, nivel seguro de *sockets* o seguridad del nivel de transporte (SSL/TLS). Para los usuarios de una cuenta de dominio, el proceso de autenticación es automático (inicio de sesión único). En cambio, los usuarios de cuentas locales (usuarios de la máquina local, no del dominio) tienen que proporcionar las credenciales cada vez que quieren tener acceso a un recurso de red.

Web recomendada

Encontraréis más información sobre protocolos de autenticación de usuarios de Windows Server 2012 en la dirección http://technet.microsoft.com/en-us/library/hh831747.aspx.

3.2.5. Configuración de un servidor de dominio Windows. Rol active directory

Un servidor de dominio consiste en un servidor de la red que permite controlar todos los equipos y dispositivos que forman parte de esta red, de forma que un usuario pueda acceder al dominio y entrar en los equipos a los que está autorizado, introduciendo la contraseña una sola vez. El controlador de dominio permite centralizar la administración y seguridad de una red.

¿Qué es un dominio?

Un dominio consiste en un grupo de equipos que forman parte de una red y comparten una base de datos de directorio común. Los dominios se organizan en niveles y se administran como unidades con reglas y procedimientos comunes. Cada dominio tiene un nombre único.

Para configurar el servidor como un controlador de dominio, hay que instalar el rol de *active directory*, que almacena información sobre los objetos de la red y facilita la busca y utilización de esta información para los usuarios y administradores.

El *active directory* utiliza un almacén de datos estructurado como base para una organización lógica y jerárquica de la información del directorio. Este almacén de datos, denominado también directorio, contiene información sobre los objetos del *active directory*, que suelen incluir recursos compartidos como servidores, volúmenes, impresoras, cuentas de usuario de red o cuentas de equipo, al mismo tiempo que permiten a los usuarios y a las aplicaciones acceder a los recursos. A la vez, proporciona una manera coherente de asignar nombres, de describir, localizar, obtener acceso, administrar y proteger la información de estos recursos.

El *active directory* es una implementación de los protocolos de nombres y directorios estándar de Internet (X.500 y LDAP). Utiliza un motor de bases de datos para procesar las transacciones y, además, es compatible con varios estándares de interfaces de programación de aplicaciones.

La seguridad está integrada en *active directory* mediante la autenticación del inicio de sesión y el control de acceso a los objetos del directorio. Con un único inicio de sesión a la red, los administradores pueden administrar datos del directorio y de la organización en cualquier punto de la red, y los usuarios autorizados de la red pueden tener acceso a recursos en cualquier lugar de la misma. La administración basada en directivas facilita la tarea del administrador incluso en las redes más complejas.

Web recomendada

En la URL siguiente hay información extensa sobre el *active directory*, las funcionalidades que tiene, cómo está organizado o la seguridad, entre otros:

http://technet.microsoft.com/en-us/library/hh831484.aspx.

1) Configuración de DNS

De manera predeterminada, y en el caso de que no se deba instalar previamente, el asistente para instalación del *active directory* intenta situar un servidor DNS autorizado en el nuevo dominio, a partir de la lista de servidores DNS configurados que admitirán una actualización dinámica de un registro de recursos de servicio (SRV). Si lo encuentra, todos los registros adecuados para el controlador de dominio se registran automáticamente con el servidor DNS, una vez reiniciado el controlador de dominio. Si no encuentra ningún servidor DNS que acepte actualizaciones dinámicas, ya sea porque el servidor DNS

no está compatible o porque no están habilitadas para el dominio, el asistente para instalación del *active directory* sigue los pasos siguientes para asegurar que el proceso de instalación se completa con el registro necesario de los registros de recursos SRV:

- El servicio DNS se instala en el controlador de dominio y se configura automáticamente con una zona basada en el dominio del *active directory*. Es decir, si no está instalado previamente lo instala en el proceso de la instalación del directorio activo.

- Por ejemplo, si el dominio que eligió para el primer dominio del bosque de los directorios activos (ya se verá qué quiere decir en el momento de instalar el directorio activo) era ejemplo.microsoft.com, se agrega una zona cuya raíz está en el nombre de dominio DNS de ejemplo.microsoft.com y se configura para utilizar el servicio de servidor DNS en el nuevo controlador de dominio.

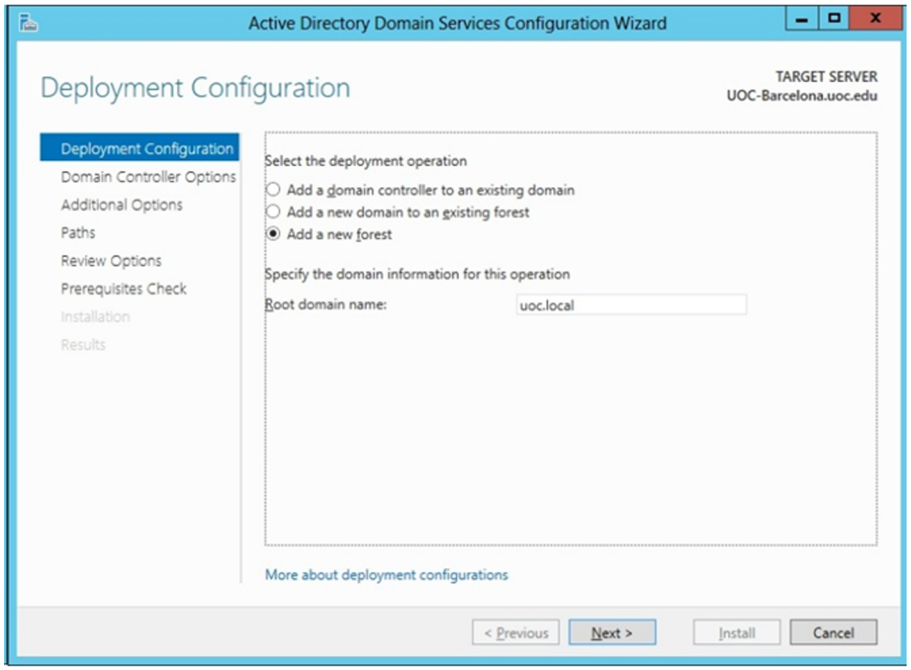
- Se crea un archivo de texto que contiene los registros de recursos DNS adecuados para el controlador de dominio. El archivo `Netlogon.dns` se crea en la carpeta `arrelSistema\System32\Config` y contiene todos los registros necesarios para guardar los registros de recursos del controlador de dominio. El servicio NetLogon utiliza `Netlogon.dns`, que admite *active directory* en los servidores DNS que no ejecutan Windows Server 2012. Si utiliza un servidor DNS que admite el registro de recursos SRV pero que no admite actualizaciones dinámicas, puede importar los registros de `Netlogon.dns` al archivo de la zona principal adecuada con el fin de configurar manualmente la zona principal en este servidor para que admita Active Directory.

Si no hay servidores DNS disponibles en la red, se puede optar por instalar y configurar de modo manual un servidor DNS local, cuando se instale *active directory* con el asistente para instalación d*e active directory*. O instalarlo antes y configurarlo para que funcione después correctamente con el directorio activo. El servidor DNS se instala en el servidor donde se ejecuta el asistente y las opciones del servidor DNS preferido se configuran para que utilice el nuevo servidor DNS local. Se debe tener en cuenta que más adelante tendremos que configurar todas las estaciones de trabajo y servidores miembros del dominio con el cliente de DNS configurado contra nuestro nuevo servidor de DNS. En caso contrario, no seremos capaces de encontrar el dominio ni los recursos que tiene. A continuación, es recomendable configurar los reenviadores o *forwarders* del servidor de DNS con los servidores DNS de nuestro proveedor de Internet.

2) Instalación de *active directory*

Podemos instalar ahora *active directory* desde la ventana de configuración del servidor, incluyendo el nuevo rol en este. Así pues, basta con seleccionar el nuevo rol e instalarlo en el sistema. Una vez hecho todo el proceso, el propio administrador del servidor avisa con una notificación de que se tiene que promover el nuevo rol de directorio activo controlador de dominio. Entrando directamente al enlace se abrirá el administrador, donde podremos dar un nombre al controlador de dominio, en este caso `uoc.local`, tal como se puede ver en la figura siguiente.

Nuevo bosque de directorio activo



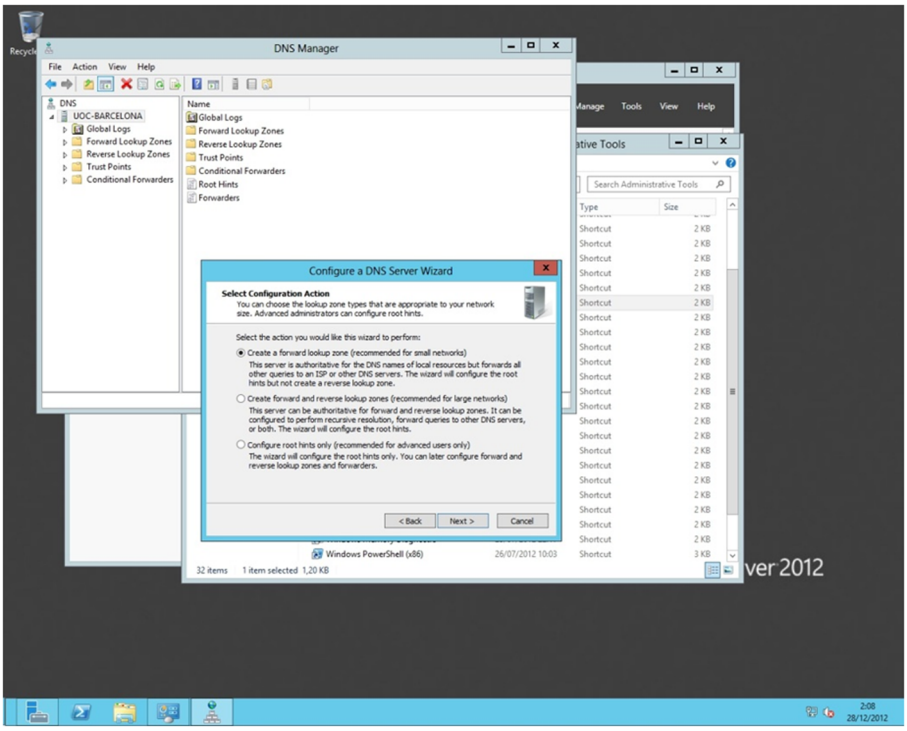
Sigue la instalación con la contraseña del dominio y la compatibilidad que se quiere tener. Si se quiere más compatibilidad con otros sistemas operativos de Microsoft más antiguos, se tendrá que seleccionar o Windows 2003 Server o 2008 Server. Es evidente que, en cuanto a seguridad se refiere, lo mejor es seleccionar el último, el Windows Server 2012, ya que tiene las últimas características que se han diseñado específicamente para este último sistema y dispone de mayor seguridad que el resto de posibles configuraciones. Continúa con algunas características más sobre ubicaciones de archivos y opciones, contraseña del administrador del dominio, que puede ser diferente de la contraseña del administrador local del Windows Server 2012.

Una vez tenemos ya acabada la configuración del directorio activo, se reiniciará la máquina y ya se puede ver la pantalla de entrada, ahora mediante el nuevo dominio, puesto que nos pide un usuario legítimo del dominio, en el caso del administrador sería UOC\administrador.

El siguiente paso que hay que dar es la vinculación del servidor DNS con el directorio activo, y así hacer que los ordenadores cliente de la red puedan ver y vincularse al servidor del directorio activo y por lo tanto validarse contra

el dominio nuevo que se ha creado. Esto se hace rápidamente abriendo el administrador del servicio de DNS y ejecutando el asistente de configuración. Para una empresa pequeña la primera opción ya es suficiente, figura siguiente.

Configuración DNS con asistente



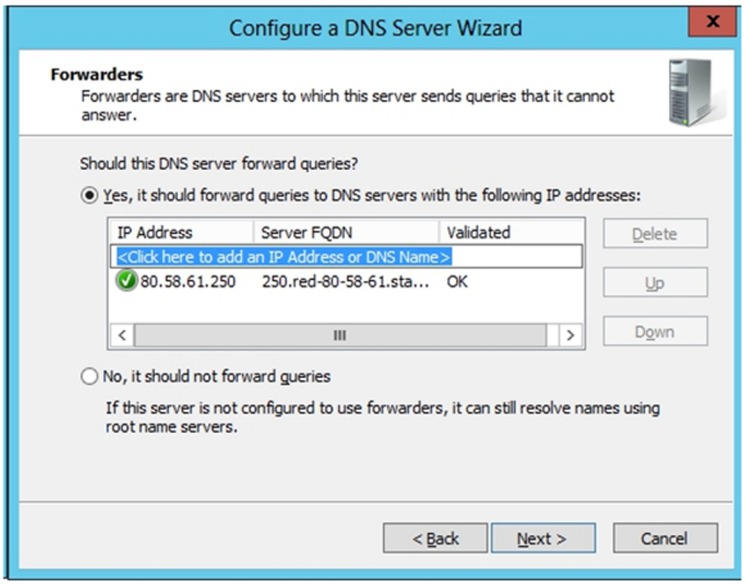
Acto seguido nos pedirá un nombre para el servicio, donde le podemos poner uno parecido a `dns.uoc.local`, que es el que teníamos ya asignado al dominio del directorio activo como `uoc.local`. Con posterioridad, solo hay que seleccionar la opción de actualización segura a partir del propio directorio activo, así nos aseguraremos de que no se actualiza el DNS de fuentes inseguras y será más difícil poder iniciar un ataque de *DNS spoofing*.

Para acabar, solo hay que indicarle dónde tiene que formular las consultas en el supuesto de que no pueda resolver por sí mismo la dirección real de Internet. Solo habrá que indicarle un servidor de DNS que la propia ISP nos haya dado como válido para la conexión a Internet que se tenga contratada.

DNS spoofing

Se trata de una técnica relativamente nueva, en la que un atacante envía al servidor de nombres una relación de nombre de dominio-IP falsa. Así, hace que una petición al nombre del dominio en el navegador de Internet haga que, en lugar de ir a la dirección IP real de la página web, vaya a una falseada preparada por el atacante y que es idéntica a la página buena. El ataque se puede llevar a cabo al hacer estas actualizaciones si permitimos que el servidor se actualice desde sistemas no controlados.

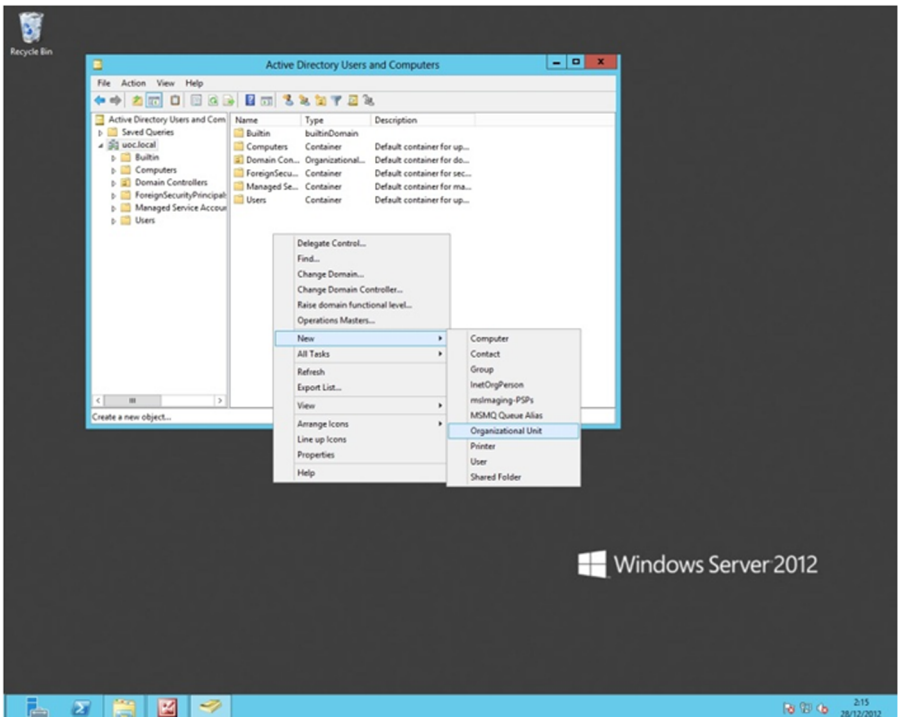
Configuración del DNS



Con esto finaliza la instalación de los servidores de manera funcional. A partir de aquí, es necesario ir llenando el directorio activo con las unidades organizativas que se quiera tener definidas, los usuarios que pueden o no estar dentro de estas unidades, los grupos, los ordenadores, entre otros.

Las unidades organizativas las podemos asimilar a los departamentos, edificios o secciones, entre otros; nos ayudarán a crear una copia de la organización para poder diferenciar o encontrar con más rapidez a los usuarios. Por ejemplo, una organización con dos sedes, una en Barcelona y otra en Madrid, dispondría de dos unidades organizativas separadas para cada sede, así podremos incluir a los usuarios y grupos, si se quiere, en cada una de estas. Esto facilita el cambio en las reglas de los ordenadores, ya que si asignamos reglas generales a las diferentes unidades, todos los usuarios, grupos y ordenadores se verán afectados, sin tener que introducir los cambios uno a uno.

Estructura del directorio activo, creación de una unidad organizativa



Los grupos permitirán que los diferentes usuarios de la organización, a pesar de estar en diferentes unidades organizativas, puedan estar agrupados en un grupo y tener todos los privilegios que se les puedan asignar a un grupo concreto. Por ejemplo, se pueden crear grupos para acceder a diferentes discos o particiones, así cada grupo puede tener un área de archivos completamente diferente del resto y no ver la información más allá de lo que le corresponde.

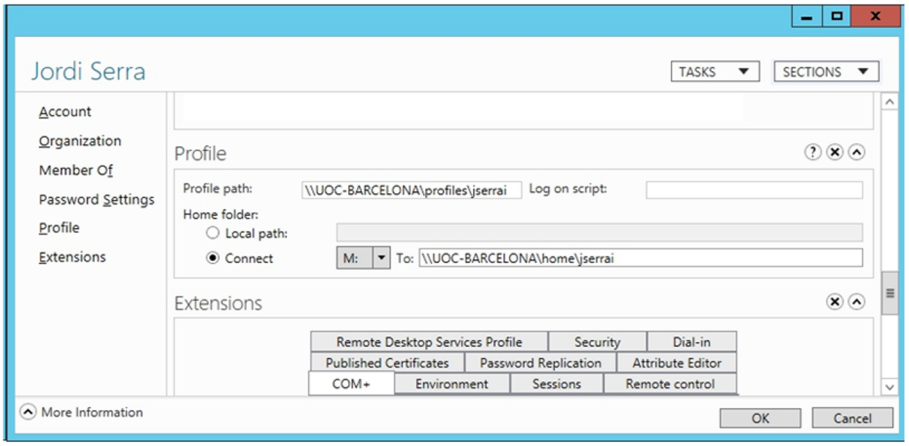
Si ya tuviéramos un servidor de dominio en la red, se podría añadir otro controlador al propio dominio. En el caso del esquema de directorio activo y de los dominios Windows 2012, todos los controladores de dominio son multimáster, que quiere decir que todos pueden escribir en el directorio y crear, actualizar o borrar datos a la vez. Así pues, no hay ningún controlador de dominio en un dominio Windows que sea más importante que otro; todos comparten y mantienen replicada la información del directorio, y ofrecen así redundancia y tolerancia a fallos, además de balanceo de carga en las operaciones de dominio.

La organización de dominios Windows Server 2012 es jerárquica y podemos tener un esquema lógico de todos los dominios y subdominios en forma de árbol. El conjunto de árboles de dominio recibe el nombre de bosque de dominios; por lo tanto, este nuevo servidor de dominio que se puede instalar se tendrá que añadir al bosque de dominios que se ha iniciado con la instalación del primer servidor de dominio en la red de la organización.

Para poder conectar y ordenar los archivos de usuario y los archivos de los perfiles, hay que crear y compartir dos carpetas en algún lugar del sistema de archivos. Podemos crear las dos carpetas dentro del directorio c:\users que crea

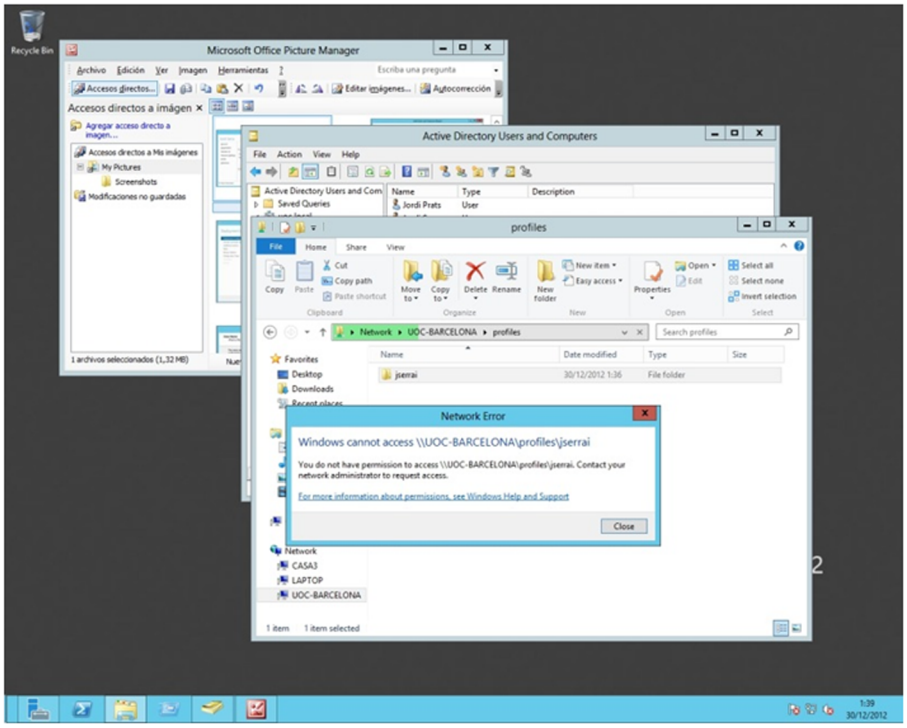
el sistema y compartirlas con todos los permisos abiertos por todo el mundo, después ya se cerrarán los directorios internos de cada usuario para que nadie más pueda tener acceso a esos directorios personales. Por defecto, los perfiles no se guardan en el servidor, sino que son locales en las máquinas donde se crean, lo que insta a no poder hacer con facilidad las copias de seguridad de los perfiles de cada usuario y que cada usuario esté más ligado a un único puesto de trabajo. Así, para cada usuario se tendrá que definir dónde tiene cada carpeta personal dentro de las propiedades de los usuarios. La figura siguiente muestra un ejemplo.

Configuración de la ruta del perfil y de la carpeta personal



Como vamos a ver más adelante, es importante poder hacer copias de seguridad de todo lo que sea importante para la empresa –y en casi todos los casos, los documentos creados por todos los usuarios lo serán– y tenerlos dispersos por los diferentes equipos no ayudará a un buen mantenimiento de estos.

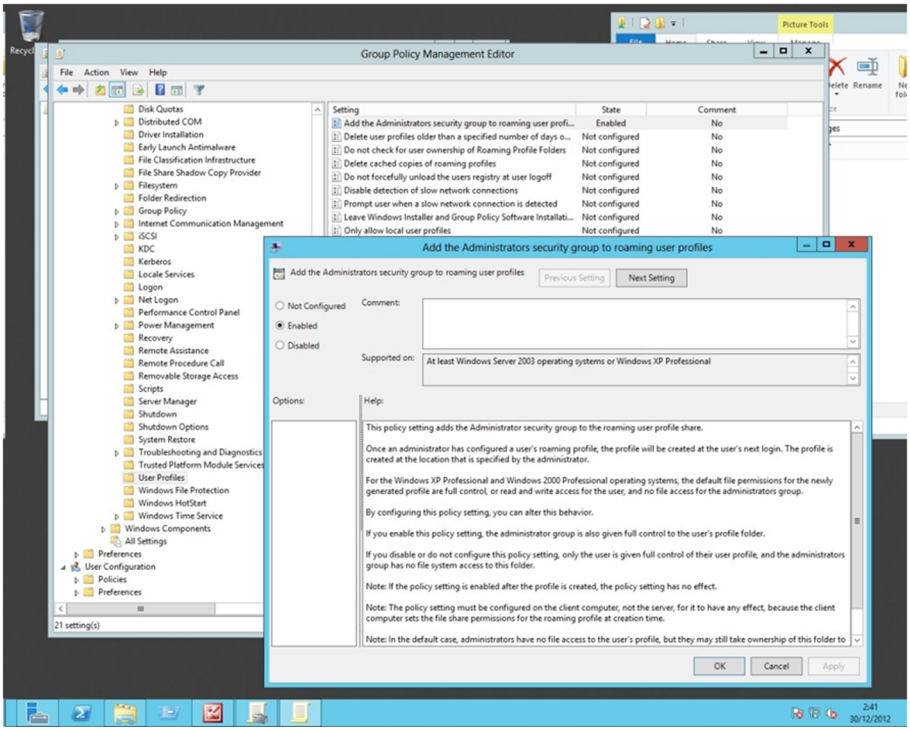
Error al acceder en la carpeta de los perfiles de usuarios



Por defecto, los directorios de cada perfil de usuario no son accesibles por ningún otro usuario que no sea el propio usuario y, por lo tanto, no se pueden hacer copias de seguridad de estos ficheros a menos que se cambie la política de acceso a estas carpetas. La figura anterior muestra un ejemplo del error que devuelve el sistema.

Para poder cambiar esta política es importante que antes de promocionar el servidor de dominio, y por lo tanto antes de definir los usuarios, se configure el acceso a las carpetas de los perfiles de usuario o no se podrá hacer *a posteriori* y se tendrá que desinstalar el servidor de dominio para poder otorgar este privilegio al administrador. La figura siguiente muestra cómo se tienen que cambiar las políticas de grupo para que el administrador pueda entrar en los directorios de los perfiles y así poder hacer copias de seguridad de estos archivos.

Configuración del acceso a los ficheros del perfil



3) Servicios de certificado

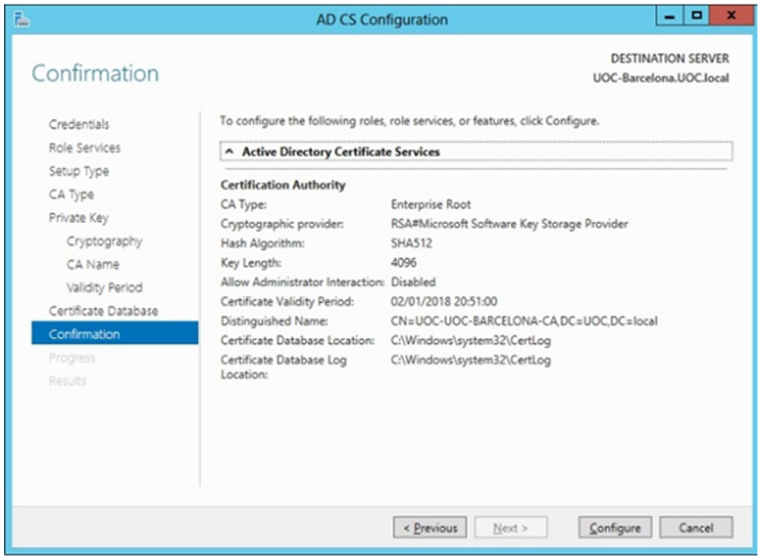
Otro de los roles interesantes que se pueden incluir en el servidor son los servicios de certificado, que es uno de los roles que tiene el Windows Server 2012. Se puede instalar en el servidor y nos permitirá emitir y administrar certificados de infraestructura de clave pública PKI. Así pues, podremos establecer identificaciones, firmas digitales y hacer transacciones seguras.

Una vez instalado nos pide que se configure correctamente con las credenciales del propio administrador y continúa con la configuración de la entidad de certificación que se tiene que crear dentro de los servidores. La primera será de tipo *root* y le tenemos que decir que es la primera y, por lo tanto, se tiene que crear una clave privada nueva.

El siguiente paso es seleccionar las características criptográficas, que por defecto ya funcionarán bien, a pesar de que se pueden mejorar cambiando a SHA512. Aquí nunca cogeremos MD5 o menor que este y no es recomendable usar SHA1, ya que podría ser inseguro. La longitud de la clave también nos aportará más seguridad cuanto más grande sea.

La figura siguiente muestra la configuración final que se aplicará al nuevo rol.

Configuración del servidor de certificados



4) Servicios de gestión de derechos (RMS)

Además de poder proteger los documentos con los permisos asociados a los archivos, en las carpetas, a los usuarios y a los grupos, el Windows Server 2012 puede gestionar otro servicio que va algo más allá en la gestión de los documentos y de los permisos que se dan a los usuarios para poder acceder. Podemos tener la necesidad de proteger la información de la empresa de forma que no se pueda manipular de manera intencionada o para que no sea visible por los usuarios que no la tienen que ver. Así, el servicio de gestión de derechos añade una manera de proteger los ficheros todavía más fuerte que los permisos que ya tiene el servidor.

Simplemente se tendrá que añadir este rol, y todas sus dependencias al servidor y configurarlo cuando lo pida para que gestione los usuarios del directorio activo ya creado. Este servicio añadirá a cada fichero unos permisos especiales que siempre estarán ligados al archivo; de este modo, aunque se cambie de carpeta, se envíe por e-mail, lo abra o lo copie otro usuario, siempre tendrá los mismos permisos y, por lo tanto, no lo podrán abrir quienes no estén autorizados. Además, estos permisos pueden ser temporales al asignar una fecha de caducidad al acceso de un determinado fichero, y al caducar el usuario dejará de tener los permisos automáticamente y no lo podrá abrir, copiar o imprimir, por ejemplo. Esto añade mucha más seguridad al sistema, a pesar de que requiere tener instalados más roles y características, como el servidor de páginas web.

5) Configuración de un cliente del dominio

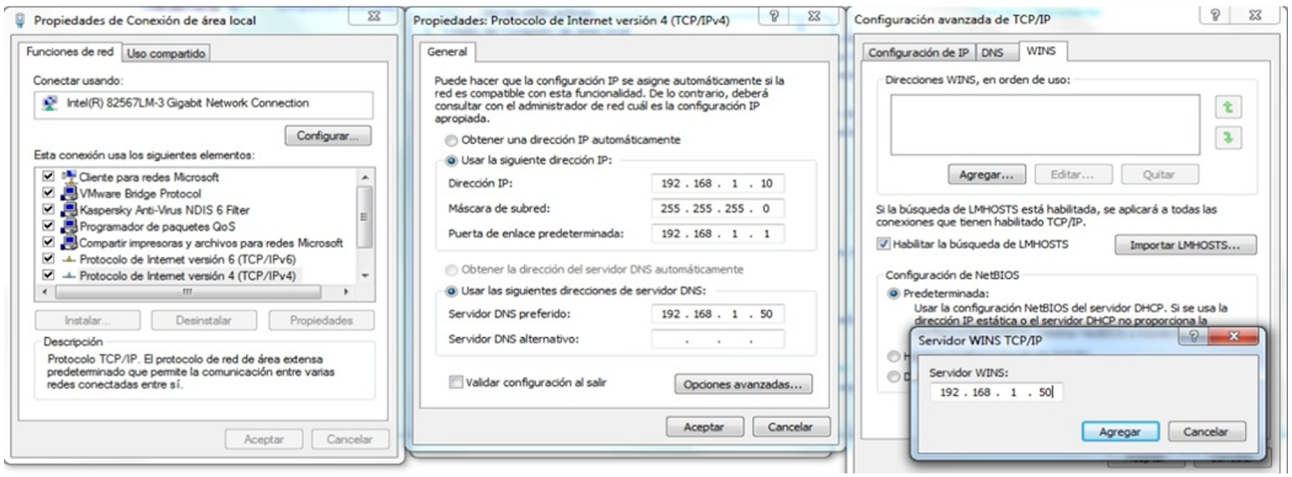
Lo primero que se tiene que hacer a la hora de incluir un nuevo equipo en el dominio, y por lo tanto en la red que se quiere crear, es indicar el DNS que debe usar para poder encontrar los nombres de los servidores y el resto de equipos de la propia red. Por eso, en el servidor, se ha instalado el servidor de

nombres (DNS) para que el mismo servidor haga la traducción de nombres de máquinas a IP reales. Por lo tanto, ahora en los clientes, como dirección de servidor DNS se tiene que configurar y poner la misma que tiene el servidor DNS mencionado. No hace falta incorporar ninguno más, ya que se encargará el servidor de nombres propios de cambiar los nombres de páginas web por las IP reales de Internet a la hora de formular las peticiones para navegar por Internet.

En el caso de disponer todavía de clientes con el sistema operativo Windows XP más antiguos u otros sistemas operativos de otro tipo, se tendrá que instalar en el servidor de dominio donde hemos configurado antes la característica WINS, que es un servidor de nombres de red que usan las versiones antiguas de Windows y que será necesario para poder juntar estos sistemas con el nuevo sistema Windows Server 2012.

Para hacerlo, basta con abrir el administrador del servidor e instalar la característica WINS (Windows Internet Name Server), que usará los nombres NetBIOS de los equipos de la red informática en direcciones IP reales. De este modo, se podrán incluir todos aquellos equipos que trabajen únicamente con las direcciones NetBIOS dentro de la red Ethernet. Por lo tanto, en los equipos cliente se tendrá que configurar para que vaya a buscar el servidor WINS a la dirección del servidor donde se haya instalado esta característica, tal y como muestra la figura siguiente.

Configuración del WINS en el cliente



El siguiente paso es cambiar el grupo de trabajo por el dominio que se ha creado. Esto dependerá de cada sistema, pero en general, para la familia Windows, se puede hacer a partir del panel de control, sistema y seguridad y sistema. Ahí se podrá cambiar la configuración del grupo de trabajo predeterminado por el nuevo dominio.

A continuación, incluimos la lista de una serie de referencias en las que se explica cómo se tienen que configurar diferentes sistemas operativos cliente con dominios Windows:

1) Windows XP, Vista, 7 y 8:
http://www.wown.com/articles_tutorials/wxpjoind.html

2) Windows 95 o 98:
http://www.wown.com/articles_tutorials/w2ksvw9x.html

3) Windows NT 4:
http://www.wown.com/articles_tutorials/nt4jw2kd.html

4) Linux:
http://www.wown.com/articles_tutorials/
authenticating-linux-active-directory.html

Con esto ya habremos conseguido tener el sistema cliente y servidor configurado. En el momento de volver a iniciar el cliente, se verá que, por ejemplo, se pide un nombre de usuario y contraseña, pero esta vez pedirá los usuarios del dominio, y solo podrán entrar aquellos usuarios que el administrador haya configurado previamente. En las carpetas configuradas dentro del servidor para guardar los perfiles, se irán creando las nuevas carpetas a medida que se vayan abriendo las sesiones de los usuarios en los ordenadores clientes.

4. Administración y mantenimiento del servidor GNU/Linux

La informática no es muy diferente de la mayoría de las cosas que pasan en el mundo; lo fácil es instalar un sistema, lo difícil es mantenerlo. El administrador de sistemas normalmente tiene que ejecutar varias tareas de manera periódica y repetitiva. La lista siguiente nos muestra algunas de las tareas del administrador de sistemas, puesto que, según como sea el sistema o el entorno, puede hacer unas u otras.

La lista solo muestra las más conocidas sin ningún orden concreto:

- **Gestión de usuarios y grupos:** Dar de alta y de baja a los usuarios constituye una de las principales tareas de cualquier administrador. Tenemos que destacar que las políticas de dar de alta o de baja a un usuario normalmente son responsabilidad de los directivos de la empresa o del área de informática. Esta tarea tiene una importancia especial y, por eso, vamos a dedicar un apartado más adelante a explicar cómo se hace.

- **Gestión de recursos del sistema:** Tenemos que estar atentos a qué servicios ofrecemos, cómo los ofrecemos y a quiénes damos acceso a determinados recursos. Cualquier recurso compartido tiene que ser administrado. Esto se debe a que o bien los usuarios no son conscientes de que los recursos que hay a su disposición son compartidos con otros usuarios o bien abusan de estos recursos. Para gestionarlos de manera correcta, hay muchos recursos que aceptan cuotas de usuario (como CPU, memoria o disco). Un caso particular de esta gestión lo constituyen las cuotas del sistema de archivos. Igual que la gestión de usuarios, esta tarea la vamos a ver con más detenimiento en un apartado posterior.

- **Gestión de los sistemas de ficheros:** La gestión de los sistemas de archivos constituye otro de los puntos principales del administrador. En el apartado dedicado a administrar los discos, hemos comentado las tareas del administrador respecto a esta gestión.

- **Arranque y apagado del sistema:** Cualquier sistema basado en Unix puede configurar el sistema de arranque y apagado. De este modo, podemos configurar qué servicios ofrecemos en el arranque de la máquina y cuándo hay que detenerlos.

- **Seguridad del sistema:** Seguridad local del mismo sistema, es decir, que cada usuario tenga acceso a todo lo que necesita pero no a recursos que no tiene asignados.

- **Copia de seguridad y restauración del sistema:** Hoy en día es imprescindible tener una política de copias de seguridad. El administrador tiene la responsabilidad de definir esta política y llevarla a cabo. Debido a la importancia de esta tarea dedicaremos un módulo más adelante a hablar de ello.

- **Gestión de impresión y colas:** Los sistemas Unix se pueden utilizar como sistemas de impresión para controlar una impresora o más de una conectadas al sistema, así como para gestionar las colas de trabajo que los usuarios o las aplicaciones usen.

- ***Accounting* (o *log*) de sistema:** En los *logs* del sistema es donde se escriben todas las incidencias que hay. El administrador tiene la tarea de revisar estos *logs* y ver si los servicios funcionan de manera correcta o si hay anomalías. En el caso de una intrusión en la máquina, guardamos estos *logs* en un lugar seguro para tener pruebas del delito.

- **Personalización del sistema:** El núcleo del sistema es un paquete abierto altamente configurable. El administrador tiene la tarea de tener un núcleo adecuado y optimizado para el servidor que gestiona. También es importante, para mantenerlo tan actualizado y seguro como se pueda, incluir las actualizaciones que van saliendo, sobre todo las de seguridad.

- **Automatización de tareas rutinarias:** Muchas de las tareas del administrador son rutinarias o fáciles de automatizar. El administrador es quien decide qué tarea automatiza y cómo la lleva a cabo.

4.1. Permisos de archivos y directorios

Un tema sobre el que el administrador tiene que estar muy pendiente son los permisos de los dispositivos, archivos y directorios. Todos los recursos del sistema tienen el mismo tipo de permisos. Lo que cambia es el significado que tienen según si es un archivo o un directorio.

La propiedad de que todos los recursos tengan el mismo tipo de permisos nos la da el sistema de archivos. Tal como hemos visto antes, el sistema de archivos trata todos los recursos del sistema como si fueran archivos. Hay tres grupos de permisos. El primer grupo hace referencia a los permisos del propietario, el segundo indica los permisos del grupo y el tercero lo componen los permisos del mundo (todos los usuarios que no son ni propietarios ni forman parte del grupo). Cada uno de los grupos tiene tres tipos de permisos, esto es, lectura, escritura y ejecución, que se simbolizan con una `r`, una `w` y una `x`, respectivamente. Si, por ejemplo, el propietario tiene permiso de lectura sobre un archivo, aparece una r; si no tiene, aparece un (`-`). Para ver los permisos de los archivos del directorio donde estamos debemos ejecutar la orden `ls -l`.

La asignación de permisos a un usuario se hace del modo siguiente:

1) Se le aplican los permisos de propietario cuando es propietario de un archivo.

2) Se le aplican los permisos de grupo cuando pertenece al grupo correspondiente al archivo.

3) Se le aplican los permisos del resto cuando no es ninguno de los casos anteriores.

La asignación de permisos se hace en este orden secuencial; por lo tanto, si a un usuario, para un archivo cualquiera, se le aplican los permisos de propietario, los otros dos grupos de permisos no tienen relevancia para este usuario respecto al fichero en cuestión. La única excepción a este método la constituye el usuario *root*. A este usuario solo le afectan los permisos cuando es el propietario de los archivos o directorios; si no es el caso, se puede leer, modificar y borrar cualquier archivo en cualquier directorio.

Un ejemplo de los permisos de unos archivos es este:

```
Nombre de fichero        Propietario    Grupo     Permisos
/home/jordi/test.txt     jordi          uoc       rwxrwxrwx
/home/jordi/readme.txt   jordi          uoc       rw-rw----
/home/jordi/documentos   jordi          uoc       rw-rw----
/home/jordi/temp         jordi          uoc       drwx------
```

Debemos tener presente el significado de cada uno de los permisos, ya que la interpretación es diferente según si es un archivo o un directorio. En un archivo, el permiso de lectura permite editar el archivo, el permiso de escritura permite modificar el archivo y el permiso de ejecución permite ejecutar el archivo. En un directorio, el significado es diferente: el de lectura permite ver el contenido del directorio, el de escritura permite crear y borrar archivos y el de ejecución permite atravesar el directorio.

Un factor muy importante para los directorios es que los permisos se aplican cada vez que el usuario se mueve por el árbol de directorios. Por lo tanto, un usuario, para llegar a su directorio raíz, por ejemplo, debe tener los permisos de ejecución en todos los directorios que tiene que atravesar; si no, este usuario no puede almacenar los archivos en su directorio raíz, aunque en este directorio tuviera todos los permisos y fuera el propietario. En el caso del ejemplo anterior, el usuario `jordi` debe tener permisos de ejecución en los directorios (`/`) y `/home`.

El administrador tiene la tarea de asegurarse de que todos los usuarios tengan los permisos correctos para acceder a todo lo que tienen que acceder, y no acceder a nada más.

Una cosa que hay que destacar es que, para cambiar los permisos de un archivo, debemos ser propietarios de este archivo o directorio (o ejecutar este cambio de permisos como usuario *root*). Para cambiar los permisos de los archivos o directorios tenemos que utilizar las órdenes que mostramos a continuación:

- `chmod`: esta orden cambia los permisos específicos (`rwx`) de un archivo o directorio.

- `chown`: esta orden cambia el propietario de un archivo o directorio.

- `chgrp`: esta orden cambia el grupo de un archivo o directorio.

4.2. Altas, bajas y modificaciones de usuarios

GNU/Linux, igual que la mayoría de los sistemas operativos, está pensado para apoyar a los usuarios. Los usuarios, por defecto en Linux, sí tienen una cuenta (con sus datos) junto con el espacio de disco asignado para que puedan almacenar los archivos o directorios. Este espacio de disco, en principio, solo lo puede utilizar el usuario en cuestión, pero se puede cambiar mediante los permisos del directorio.

Un sistema operativo basado en GNU/Linux tiene tres tipos de cuentas diferentes:

1) La del administrador, con identificador *root*. Esta cuenta, para evitar problemas de seguridad, solamente se tiene que utilizar para las operaciones de administración. Debemos tener presente que la mayoría de los permisos de archivo no afectan al usuario *root*, de modo que este usuario es el que tiene más permisos y más acceso completo a la máquina y a los archivos de configuración. En consecuencia, también es la que puede causar más daño por errores u omisiones. Un buen administrador tiene que evitar usar la cuenta de *root* como si fuera un usuario más, de modo que se recomienda dejarla solo para operaciones de administración. Los intrusos intentarán acceder a la máquina por agujeros o por las cuentas de usuario y, una vez dentro, tratarán de cambiarse a administradores para tener todos los privilegios posibles sobre la máquina.

2) Cuentas normales de usuarios. Lo normal es que estas cuentas tengan permisos restringidos en su espacio de disco y en algunas zonas particulares (por ejemplo, el directorio temporal `/tmp`). Estas cuentas también pueden usar todos los dispositivos para los que tienen permisos.

3) Cuentas especiales de los servicios, por ejemplo `www-data`, `lp`. En Linux, hay varios servicios que se ejecutan con un usuario concreto. No hay ningún usuario que utilice estas cuentas, sino que las usa el sistema de manera interna. Así, evita que servicios poco seguros se ejecuten con privilegios de *root*. Todos los servicios que están en ejecución pertenecen a un usuario. Hay determinados procesos que permiten la configuración del usuario propietario. La mayoría de estos procesos tienen asociada una cuenta especial que no permite la entrada interactiva de este usuario a la máquina, pero permite que estos procesos tengan un propietario diferente de *root*. Desde el punto de vista de la seguridad, va bien que usemos estas cuentas para ejecutar los procesos asociados, ya que si este proceso tiene vulnerabilidades es mejor que los usuarios que lo ejecutan no tengan demasiados privilegios en la máquina.

Se crea normalmente un usuario mediante la especificación de un nombre (identificador de usuario, que debe ser único en el sistema), una contraseña, un directorio personal que está asociado (para almacenar la información) y un tipo de *shell*. La información de los usuarios del sistema está incluida en los archivos siguientes:

```
/etc/group
```

Veamos a continuación unas líneas, por ejemplo, del archivo `/etc/passwd`:

```
root:x:0:0:root:/root:/bin/bash
jordi:x:1000:1000:Jordi Serra:/home/jordi:/bin/bash
```

En el que (`:`) es el separador de cada uno de los campos. Si salen dos (`:`) seguidos, indica que este campo está vacío:

- `jordi`: identificador de usuario en el sistema; debe ser un identificador único.

- `x`: contraseña del usuario codificada; si hay una x quiere decir que está en el archivo `/etc/shadow`.

- `1000`: código del usuario. En inglés, de este campo se llama *user ID* (*UID*); lo usa el sistema como código de identidad del usuario. Igual que el nombre, este número debe ser único en el sistema. Lo asigna el sistema mismo por defecto.

- `1000`: código del grupo principal al que pertenece. En inglés, este campo se llama *group ID* (*GID*); la información del grupo está en el fichero `/etc/group`.

- `Jordi Serra`: este campo es un comentario; se suele poner el nombre completo del usuario, el documento de identidad o cualquier otra información que ayude al administrador.

- `/home/jordi`: directorio personal asociado a su cuenta; se debe poner el camino absoluto desde el directorio raíz.

- `/bin/bash`: *shell* interactivo que utilizará el usuario cuando interactúe con el sistema, en modo texto, o por *shell* gráfico.

En versiones anteriores de GNU/Linux, el archivo `/etc/passwd` solía contener las contraseñas de los usuarios de manera cifrada, pero el problema era que cualquier usuario podía ver el archivo. En el momento en el que se diseñaron los *cracks* que intentaban encontrar mediante la fuerza bruta la contraseña usando la contraseña cifrada como punto de partida (codificada con el sistema *crypt*), se modificó el archivo `/etc/passwd` para que no saliera la palabra clave codificada. Por eso, hoy en día ya no se ponen las contraseñas en este archivo y solo hay una x, que indica que están en otro fichero, que es solo de lectura para el usuario raíz. Este otro archivo donde están las palabras clave cifradas es el archivo `/etc/shadow`, cuyo contenido puede ser algo parecido a lo siguiente:

```
jordi:2n26TS47RxagQ:12440:0:99999:7:::
```

Aquí está el identificador del usuario junto con la contraseña cifrada. Además, salen como campos separados por (`:`):

- Días desde el 1 de enero de 1970 en los que la contraseña se cambió por última vez.

- Días que faltan para que se cambie (0 no hay que cambiarla).

- Días al cabo de los cuales hay que cambiarla (o sea, plazo de cambio).

- Días en los que se avisará al usuario antes de que le expire el plazo.

- Días al cabo de los cuales, una vez expirado el plazo, se le deshabilitará la cuenta.

- Días desde el 1 enero de 1970 en los que la cuenta está deshabilitada.

- Y un campo reservado.

Si queremos seguir una política de cambio de contraseñas, es decir, obligar a los usuarios a hacer que cambien la contraseña algunas veces al año, tenemos que poner un valor diferente a cero en los campos segundo, tercero, cuarto y quinto, o hacerlo con la aplicación gráfica de gestión de usuarios y grupos.

En `/etc/group` está la información de los grupos de usuarios:

```
root::0:
uoc::1000:
```

Donde tenemos que el primer campo es el nombre del grupo (identificador), que debe ser único. Entre los grupos, no puede haber dos con el mismo nombre, a pesar de que puede haber un usuario y un grupo con el mismo nombre. El segundo campo es la contraseña del grupo (este campo no es de uso común). El último campo es el identificador numérico del grupo; este número debe ser único (entre los diferentes grupos).

Hay dos maneras de vincular un usuario a un grupo. La primera es mediante el `/etc/passwd`: se pone, en el campo correspondiente al identificador de grupo, el grupo al que pertenece el usuario. La segunda manera de vincular usuarios a grupos consiste en añadir al final de la línea del grupo los usuarios que pertenecen a este grupo separados por comas.

Veamos a continuación una serie de órdenes útiles para esta administración de usuarios:

- `adduser`: añadir un usuario al sistema.

- `deluser`: borrar un usuario del sistema.

- `addgroup, delgroup`: lo mismo para grupos.

- `passwd`: cambia la contraseña de un usuario. Esta orden se puede ejecutar como usuario y, entonces, nos pide primero la contraseña vieja y después que pongamos la nueva (esta petición la hace por duplicado para asegurarse de que se ha puesto de manera correcta). En caso de ejecutar esta orden como usuario administrador, se debe especificar el usuario al que cambiará la contraseña (si no, cambiaría su propia contraseña) y no tiene que poner la contraseña antigua de este usuario. Es quizás la orden que usa más el *root*, pensando en los usuarios, cuando se les olvida la contraseña antigua.

- `su`: una manera de cambiar de identidad. La utilizan tanto los usuarios como el *root* para cambiar el usuario actual. En el caso del administrador, se utiliza mucho para verificar que la cuenta del usuario funciona correctamente. Hay diferentes variantes: `su` (sin parámetros, sirve para pasar a usuario *root* y, siempre que se tenga el *password* de *root*, nos permite, cuando estamos en una cuenta de usuario, pasar a *root* para hacer alguna tarea).

La sentencia `su iduser` cambia el usuario a `iduser`, pero deja el entorno tal como está, es decir, en el mismo directorio. La instrucción `su - iduser` lleva a cabo una sustitución total, como si el otro usuario hubiera entrado en el sistema haciendo un login.

Como administradores, va bien que no usemos el usuario *root* como nuestro usuario habitual de trabajo. Ahora bien, si el usuario de trabajo no tiene privilegios para hacer nada, a largo plazo dejaremos de usar el usuario para utilizar el de *root*. Para que no pase esto va bien poner que el usuario pertenece al grupo de *root*. De este modo, el usuario tendrá algunos privilegios y no habrá que utilizar tan a menudo el de *root*. Igual que el grupo de *root*, hay otros grupos que se crean por defecto al instalar la máquina. Hay muchos de estos grupos que afectan a servicios de la Red (como correo electrónico, *news*, servidor intermediario o *proxy*, fax), los hay que se refieren a diferentes servicios que se pueden instalar (por ejemplo, impresoras, cintas, disquetes o *floppys*, CD-ROM, audio) y, finalmente, hay otro que hace referencia a los procesos de la máquina (demonio o *daemon*, *root*, *adm*, entre otros).

Debemos tener presente que todos los archivos y órdenes que hemos comentado hacen referencia a la administración de una única máquina. Si nuestro sistema consta de más de una máquina que comparten los usuarios, se suelen usar aplicaciones de gestión de los usuarios (como LDAP, NIS o RADIUS).

4.2.1. Cómo debe ser una contraseña

La política de seguridad que hay en cada organización debe fijar los requisitos para que una contraseña se considere aceptable dentro del ámbito de aquella organización. Sin embargo, hay algunas consideraciones aceptadas comúnmente:

- Todas las cuentas de usuario, sin excepción, deben tener asociada una contraseña. Si hay usuarios que no se utilizan (como *nobody*, correo electrónico), deben tener la cuenta deshabilitada.

- En la primera conexión a la Red, se debe obligar al usuario a cambiar de contraseña.

- La longitud de las contraseñas no tiene que ser inferior a siete caracteres.

- Las contraseñas no deben ser palabras simples que encontraríamos en un diccionario.

- La contraseña no tiene que ser el nombre de los hijos ni ningún nombre de ningún personaje (ya sea de cine, de literatura, real o de ficción).

- La contraseña no debe contener el identificador o el nombre del usuario.

- Las contraseñas deben caducar, como máximo, cada seis meses. El periodo mínimo de validez de una contraseña tiene que ser de un día. Dependiendo del tipo de organización, se podría reducir este tiempo en el que la contraseña es válida.

- Cuando se haga un cambio de contraseña, la nueva debe ser diferente a las que ha utilizado antes el usuario. En algunos sistemas, incluso se comprueba que sea sustancialmente diferente a las demás contraseñas utilizadas. Es decir, si hasta ahora teníamos como contraseña `ePFeter1`, no aceptará que la nueva sea `ePFeter2`.

- Periódicamente, se debe hacer una auditoría para verificar que se cumplen los requisitos de la política de seguridad.

Si no podemos poner nada de esto, ¿qué podemos poner en la contraseña? Una contraseña tiene que estar formada por caracteres alfanuméricos (números y letras) y tiene que ser *key sensitive*, es decir, que podamos poner minúsculas y mayúsculas. Entonces el problema es cómo lo tenemos que hacer para recordar la propia contraseña.

Un método para poner buenas contraseñas y para que las podamos recordar es que formen parte de una frase. Por ejemplo, pongamos la frase *Anyone who has never made a mistake has never tried anything new* (Albert Einstein). Si tomamos la primera letra de cada palabra tenemos `Awhnmamhntan`. Ahora, por similitud, convertimos la letra A en el número 4 y tenemos `4whnmamhntan`. Si somos unos románticos, diremos que la palabra más importante de esta frase es *new* y, por lo tanto, la pondremos en mayúscula, de forma que la contraseña nos quedará finalmente así: `4whnmamhntaN`. Esta contraseña cumple todas las especificaciones y, además, es fácil de recordar.

4.2.2. Desencriptador de contraseñas

Hay muchas herramientas en la Red cuya finalidad es obtener tantas parejas de usuario/contraseña como se pueda para acceder a la máquina, y tienen como objetivo principal conseguir una cuenta con privilegios (si puede ser *root*). Una de las herramientas más extendidas que desempeña esta función es la llamada John The Ripper. Para instalar esta herramienta en la máquina, tenemos que ejecutar la orden:

```
Root# apt-get install john
```

Las versiones antiguas de esta herramienta tratan de descifrar las contraseñas de todos los usuarios. Esto solo es cuestión de tiempo y de recursos. Usando un ataque de fuerza bruta podemos llegar a descifrar todas las contraseñas de la máquina.

Un ataque de fuerza bruta

Un ataque de fuerza bruta es el ataque en el que se van probando todas las combinaciones posibles hasta encontrar la correcta.

Debido a problemas de compatibilidad con la ley de protección de datos, es decir, que no es legal que un administrador sepa las contraseñas de sus usuarios, las versiones modernas de esta herramienta solo intentan descrifrar la contraseña del administrador.

4.3. Cuotas de disco

Una tarea importante para el administrador de la máquina es mantener el sistema de archivos. En un apartado anterior, hemos visto cómo se tiene que hacer para mantener los discos para que se conserven saneados. Mantener los discos saneados implica que haya bastante espacio para que todo el mundo pueda trabajar, incluso el mismo sistema operativo. Para que todos podamos trabajar es imprescindible que nadie abuse de los recursos que nos ofrece el sistema de archivos. Uno de los métodos para evitar que nadie abuse del espacio libre del sistema de archivos es asignar cuotas a los usuarios.

Hay un paquete a GNU/Linux que nos permite asignar cuotas a los usuarios. En la mayoría de las distribuciones, si queremos que el sistema sea compatible con las cuotas, debemos seguir dos pasos. Por un lado, instalar los paquetes `cuota` y `quotatool`, que nos permiten tener cuotas. Para instalar estos paquetes, tenemos que ejecutar las órdenes siguientes:

```
Root# apt-get install quota
Root# apt-get install quotatool
```

La aplicación de cuotas nos permite especificar límites en dos aspectos del almacenamiento de información: el número de *inodes* que puede tener un usuario y el número de bloques que también puede tener asignados un usuario. Las cuotas también tienen dos tipos de límite, que son el límite software y el límite hardware. El primer tipo nos indica la máxima cantidad de espacio de disco que puede tener un usuario en una partición, que, combinado con el tiempo máximo permitido de superar el límite, actúa como un tope en el que el usuario recibe avisos que le notifican que ha superado el margen que establece el sistema. El segundo tipo de límite, el hardware, especifica el límite absoluto que no puede superar un usuario bajo ningún concepto. El periodo de gracia es el tiempo que pasa entre que el usuario viola el límite software y recibe la notificación de que lo ha superado.

Las órdenes que intervienen en la asignación de cuotas son las siguientes:

1) `edquota`: nos permite crear y modificar la cuota de un usuario.

2) `quotachek`: se utiliza para escanear las cuotas de un sistema y actualizar las cuotas de los usuarios.

3) `repquota`: elabora un informe sobre los usuarios del sistema y su cuota.

4) `quotaon`: activa las cuotas de un sistema de archivos.

5) `quotaoff`: desactiva las cuotas de un sistema de archivos.

Web recomendada

Si queréis profundizar en la manera de habilitar las cuotas en un sistema basado en GNU/Linux, consultad la dirección http://www.tldp.org/howto/quota.html.

4.4. Herramientas básicas

El administrador de sistemas GNU/Linux se tiene que enfrentar a diario con una gran cantidad de tareas. En general, en la filosofía Unix no suele haber una única herramienta para cada tarea o una sola manera de hacer las cosas. Lo común es que los sistemas Unix proporcionen una gran cantidad de herramientas más o menos simples para afrontar las tareas. Para ello, es muy recomendable saber usar las herramientas que el sistema pone a nuestro alcance.

4.4.1. Documentación

El primer gran bloque de herramientas que tenemos que saber utilizar lo constituye la documentación que el sistema, o las aplicaciones, ponen a nuestra disposición. Hay muchas fuentes de información dentro del sistema, pero vamos a destacar las más importantes:

- `man`: es la ayuda básica y más utilizada de todas las que mostraremos. Nos permite consultar el manual de GNU/Linux. Este manual está agrupado en varias secciones. Para obtener la ayuda que está asociada al mismo, tenemos suficiente con `man ordre`. Cada página nos describe la orden, las opciones que tiene, a veces algunos ejemplos, y órdenes que están relacionadas. Como el `man` tiene varias secciones, es posible que nos encontremos con que una determinada página esté disponible en varias secciones (cada una de estas secciones muestra información diferente); en este caso, hay que especificar qué sección queremos visualizar mediante la línea de órdenes: `man n ordre` (donde *n* es el número de sección). Una orden interesante que está relacionada con la orden `man` es `apropos ordre`, que nos puede servir para localizar páginas `man` que hablen de un tema determinado (asociado con la palabra buscada).

- Documentación de las aplicaciones: hay muchas aplicaciones que, además de mostrar mucha información en el `man`, nos proporcionan una información adicional que encontraremos en `/usr/doc/`, donde se crea un directorio para cada paquete de aplicación.

4.4.2. *Shell*

Otro gran bloque de herramientas básicas lo constituyen los *shells*. El término *shell* se utiliza para denominar un programa que sirve de interfaz entre el usuario y el núcleo del sistema. Estas interfaces pueden estar en modo texto o en modo gráfico.

El *shell* en modo texto es una herramienta que permite a los usuarios comunicarse con el sistema mediante órdenes, que los usuarios introducen en el *shell* y que el sistema interpreta. Esta interfaz en modo texto también llama línea de órdenes. El *shell* en modo gráfico tiene un gestor de ventanas donde el mismo sistema ofrece que algunas aplicaciones (del sistema) se ejecuten en modo gráfico. Sin embargo, a pesar de disponer de ventanas, hay algunas órdenes del sistema que todavía se tienen que introducir por línea de órdenes. Los entornos gráficos tienen emuladores de terminales con esta finalidad.

Hay dos maneras de acceder a un *shell*, ya sea texto o gráfico, y es en consola o remoto. El acceso en consola se hace cuando un usuario tiene acceso (físico) a la máquina. El usuario se sienta ante el sistema e introduce las órdenes. El acceso remoto se produce cuando el usuario accede a la máquina mediante una red. En ese caso, el sistema debe tener instalados sistemas de consola remota (como rlogin, Telnet, SSH, Xwindows).

Una de las herramientas más interesantes y potentes, pensando en el administrador de una máquina, que nos ofrecen los *shells* son los *shell scripts*, archivos de texto que contienen secuencias de órdenes de sistema, más una serie de órdenes propias del *shell* interactivo, más las estructuras de control necesarias para procesar el flujo del programa (de los tipos `while`, `for`, por ejemplo).

Los *shell scripts* son muy importantes dentro de un sistema. Los motivos principales de esta importancia los resumimos en las dos razones siguientes:

- La manera principal de automatizar procesos es la que lleva a cabo el administrador creando *shell scripts*.

- La configuración del sistema y de la mayoría de los servicios se hace mediante herramientas proporcionadas en forma de *shell scripts*.

4.4.3. Procesos

El sistema operativo basado en GNU/Linux es un sistema llamado multiproceso. Esto quiere decir que es capaz de ejecutar de manera simultánea más de un proceso. Hay varios tipos de procesos:

- Procesos de sistema: son los procesos asociados al funcionamiento local de la máquina, del núcleo o de los servicios. Este último tipo de proceso también se llama demonio o *daemon*. La mayoría de los procesos de sistema están asociados al usuario *root*, a pesar de que este usuario no tiene ninguna consola abierta en el sistema (ya sea remota o interactiva). Hay determinados servicios que se ejecutan asociados a usuarios virtuales, que solo existen en el sistema para facilitar la ejecución de un determinado servicio (como lp, www-data, correo electrónico).

- Procesos de usuarios del sistema: los procesos asociados a la ejecución de las aplicaciones de usuario, tanto si se trata de tareas interactivas en modo texto como de tareas interactivas en modo gráfico. Un caso especial de los procesos de usuario es el caso del *root*, donde todos los procesos que ejecuta el *root* (que no sean de sistema) son procesos del usuario administrador.

La gestión de los procesos de una máquina la podemos hacer mediante las órdenes siguientes:

- `ps`: el resultado de la ejecución de esta orden es una lista con los procesos que hay en ejecución en aquel momento. Por defecto, muestra los procesos del usuario que ha ejecutado la orden. Hay muchas opciones disponibles (ved `man`), pero una de las que usa más el administrador es `ps aux`.

- `top`: es una orden que nos muestra los procesos en ejecución pero ordenados por consumo de CPU. Esta lista se actualiza a intervalos.

- `kill`: tiene la función de eliminar procesos, tanto si son de usuario como de sistema. Solo se pueden "matar" los procesos de los que somos propietarios (o de los que somos *root*). El modo de ejecución más común para el administrador es `kill -9 PID`. El *PID* (*process identifier*) lo obtenemos ejecutando el `ps`.

4.4.4. El editor `vi`

Hay muchos editores de archivos. Los hay que utilizan entornos gráficos y los hay que usan modo texto. Ahora, el editor que se instala con el sistema operativo y, salvo que lo primero que hagamos sea instalar un editor de archivos, el que tenemos para modificar los archivos de configuración se llama `vi`.

El editor `vi`, a pesar de que es un editor muy potente, tiene una interacción con el usuario muy difícil. Si no se está acostumbrado a usarlo, modificar unas letras de un archivo puede resultar una tarea muy complicada. Sin embargo, es necesario que aprendamos a usarlo porque nos podemos encontrar máquinas que solo tienen este editor. Este tiene dos modos de operación: el modo insertar y el modo orden. Para entrar al modo insertar tenemos que pulsar la tecla `i`; a partir de ahí podemos introducir texto en el archivo. Para pasar a modo orden tenemos que pulsar CTRL + F3 o ESC. En modo orden nos permite grabar y ejecutar las operaciones de copiar y pegar o salir. Para salir grabando del editor tenemos que estar en modo orden y pulsar `:wq`.

5. Administración y mantenimiento del servidor Windows Server 2012

Windows Server 2012 incorpora muchas herramientas para administrar los servidores que utilizan un entorno o una interfaz gráfica comunes, denominado Microsoft Management Console (MMC). El MMC es extensible y hay herramientas de otras empresas que lo utilizan para añadir herramientas de administración al sistema. Varios fabricantes han creado herramientas que se ayudan de esta consola y del directorio activo para facilitar la gestión de los usuarios y de la seguridad con mucha más facilidad. Además, podemos crear consolas MMC a la medida de nuestras necesidades, e incluso confeccionarlas para distribuirlas después con el fin de que haya determinadas gestiones que las ejecuten usuarios en los que delegamos alguna tarea administrativa, como por ejemplo el cambio de contraseña de los usuarios del dominio.

Dispone también del administrador del servidor, donde tenemos todos los roles que hay instalados en la máquina en esta aplicación, que permite configurar con rapidez y de modo sencillo estos roles. Además, da una visión rápida de los problemas que puedan tener. Para cada uno de los roles, Windows Server 2012 incorporará las herramientas necesarias para la administración y configuración propias, como el servidor de nombres DNS. En el momento de instalar el servidor también se instala la herramienta de configuración y se incorpora al resto de herramientas de las que ya dispone el servidor.

5.1. Gestión de usuarios

En Windows Server 2012, podemos gestionar los usuarios que tienen acceso al sistema, así como los privilegios que tiene cada uno de estos usuarios. Para gestionarlos mejor, estos usuarios se pueden organizar por grupos o, incluso, dentro de unidades organizativas o entidades con un rol determinado. Así, a la hora de otorgar un privilegio, se suele otorgar a un determinado grupo o entidad, en lugar de hacerlo a todos los usuarios que lo componen uno por uno. Esto comporta una seguridad añadida, ya que, en el caso de que un usuario con privilegios elevados por estar en una posición de la empresa que lo requiera se cambia de responsabilidades, solo hay que cambiarlo de grupo y, por lo tanto, se le cambiarán todos los privilegios automáticamente, sin tener que pensar en qué privilegios debe seguir teniendo y cuáles no, y sobre todo dejar de retirar privilegios importantes que ya no tendría que tener.

Los privilegios, aparte del acceso al sistema, se configuran desde el mismo servicio que requiere seguridad. A continuación, exponemos una lista de algunos servicios que permiten indicar los usuarios autorizados:

- acceso a carpetas archivos, impresoras;
- uso de conexiones de red;
- acceso a bases de datos;
- tareas de administración.

Es conveniente, para mejorar la seguridad, repasar las cuentas de usuario que ha creado automáticamente el sistema durante el proceso de instalación para eliminar las que no son necesarias o protegerlas con alguna contraseña conocida. Muchas veces, hay usuarios invitados o usuarios que se crean automáticamente para desempeñar tareas que después dejan de tener sentido, pero no se bloquean o se eliminan y pueden ser un posible punto de entrada al sistema.

5.1.1. Gestión de usuarios sin Active Directory

Si no se ha instalado Active Directory en el servidor, utilizamos la herramienta Administración de equipos que hay dentro de la carpeta Herramientas administrativas para crear y gestionar usuarios. Dentro de esta herramienta, vemos que hay varias utilidades para gestionar el equipo, organizadas en forma de árbol. Entre estas utilidades encontramos la opción Usuarios locales y grupos, donde se muestran dos carpetas en las que se almacenan los usuarios del equipo y los grupos, respectivamente.

Para crear usuarios o grupos, debemos hacer clic con el botón secundario del ratón sobre la carpeta correspondiente y seleccionar la opción Usuario nuevo o Grupo nuevo. Al crear un usuario nuevo, nos sale la ventana de creación de usuarios, donde nos piden los datos del usuario y la contraseña. Aparte del nombre de usuario y la contraseña inicial, podemos establecer algunas de las opciones siguientes:

- El usuario tiene que cambiar la contraseña en el inicio de sesión siguiente. Por defecto, se tiene que usar para que el usuario tenga que cambiarla y configurar una propia y más segura.
- El usuario no puede cambiar la contraseña. Pensando en la seguridad vale más desactivar esta opción, puesto que, cuanto más tiempo se esté sin cambiar una contraseña, más probabilidades hay de que un usuario no autorizado lo descubra.
- La contraseña no caduca nunca. Igual que la opción anterior, vale más mantenerla deshabilitada pensando en la seguridad.
- Cuenta deshabilitada. Si se selecciona esta opción, se deniega el acceso del usuario al sistema, pero se guarda su información por si más adelante se le vuelve a habilitar. Es útil para cuentas que tienen que estar un tiempo

deshabilitadas y no hace falta que estén activas y, por lo tanto, poder ser focos de ataques.

Una vez creado un usuario, podemos visualizar sus propiedades mediante la opción Propiedades del menú Acción o del menú contextual del usuario en la lista de usuarios de la derecha. También es posible modificar la contraseña de un usuario mediante la opción Establecer contraseña del menú Acción o del menú contextual.

Al pulsar Crear, la ventana se mantiene abierta como la ventana de creación de usuarios. Una vez creado el grupo, podemos visualizar sus propiedades mediante la opción Propiedades del menú Acción o del menú contextual del grupo en la lista de grupos de la derecha. Para añadir usuarios a los grupos utilizamos la opción Agregar a grupo del menú Acción o del menú contextual del grupo. En la ventana de selección de usuarios que forman parte del grupo podemos seleccionar los usuarios o grupos que ya hay y añadirlos mediante el botón Agregar. En la parte inferior, sale una lista de todos los usuarios o grupos añadidos al grupo actual.

Los grupos se crearán de modo similar, basta con hacer Crear el grupo y darle un nombre. Como vemos, Windows Server 2012 crea algunos grupos predefinidos, como por ejemplo, el grupo de administradores, que tiene permisos para ejecutar tareas de administración del sistema y tiene acceso a todos los directorios del sistema de archivos. Hay que destacar que todas las opciones descritas en este apartado solo se aplican a servidores que no sean controladores de dominio, ya que estos controladores tienen instalado Active Directory y, por lo tanto, no tienen SAM local con usuarios y grupos locales.

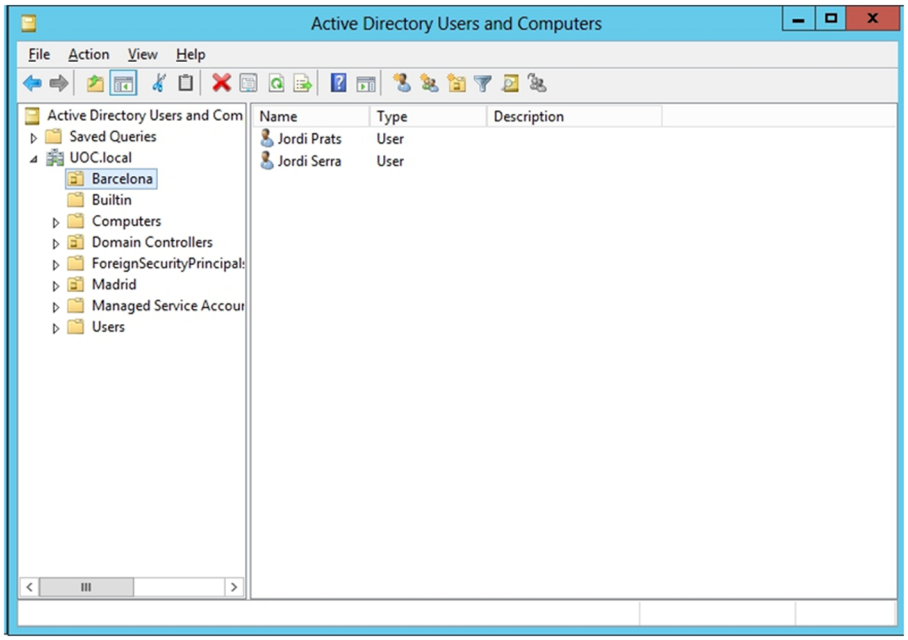
5.1.2. Gestión de usuarios con Active Directory

Si se ha instalado Active Directory para configurar el servidor como controlador de dominio, al acceder a la herramienta anterior veremos que ya no se muestra la gestión de usuarios y grupos. Las cuentas de usuarios se tienen que gestionar con el complemento de usuarios de Active Directory, de modo que tenemos que utilizar esta herramienta para crear o modificar usuarios o grupos. Un servidor de dominio solo permite gestionar cuentas de dominio, por lo tanto no permite usuarios locales. Esta herramienta o complemento del directorio activo se denomina Usuarios y equipos de Active Directory y también está en la carpeta Herramientas administrativas.

Al hacer clic con el botón secundario del ratón sobre una de las carpetas del árbol de la izquierda, sale un menú contextual con las diferentes opciones, entre las que están las opciones para crear nuevos grupos o usuarios. Al crear un nuevo usuario, hay que introducir sus datos personales, así como el nombre de inicio de sesión asignado (*login*). También hay que establecer una contraseña

y las características que tiene (si se tiene que cambiar la contraseña en el inicio siguiente de sesión, si la contraseña no caduca, si se puede no cambiar o si la cuenta de usuario está deshabilitada inicialmente).

Herramienta de creación y configuración de usuarios y equipos



Al crear un nuevo grupo, hay que introducir el nombre, el ámbito y el tipo de grupo, que podrán ser de seguridad o distribución. También se puede introducir el nombre del grupo compatible con versiones del sistema anteriores a Windows 2000, aunque se debe tener en cuenta que mantener compatibilidad con sistemas anteriores puede comportar problemas de seguridad. El tipo de un grupo puede ser de seguridad o de distribución. Los grupos de seguridad se muestran en las listas de control de acceso discrecional (*discretionary access control list* o *DACL*), que definen los permisos sobre recursos y objetos. Además, se pueden utilizar como entidades de correo electrónico, de forma que, al mandar un mensaje al grupo, este mensaje se envía a todos los miembros del mismo. En cambio, los grupos de distribución no salen en las listas DACL. Estos grupos son preferibles si no se requiere dar permisos directamente al grupo, o utilizarlo como entidad de correo electrónico.

El ámbito del grupo identifica el alcance de aplicación del grupo en el árbol o en el bosque de dominios. Hay tres ámbitos diferentes:

- **Universal:** Pueden tener como miembros grupos y cuentas de cualquier dominio de Windows 200x en el árbol o el bosque de dominios y se pueden conceder permisos en cualquier dominio del árbol o el bosque de dominios. Solo se pueden utilizar cuando hemos elevado el nivel funcional del dominio a modo nativo.

Web recomendada

Encontraréis más información sobre gestión de usuarios y grupos con Active Directory en la dirección http://technet.microsoft.com/en-us/library/hh801901.aspx.

- **Global:** Pueden tener como miembros grupos y cuentas solo del dominio en el que se ha definido el grupo y se pueden conceder permisos en cualquier dominio del bosque.

- **Local:** Pueden tener como miembros los grupos y las cuentas de un dominio de Windows 200x o Windows NT, y solo se pueden utilizar para conceder permisos en un dominio

5.2. Cuotas de disco

Las cuotas de disco definen la cantidad de espacio en el disco duro que puede ocupar una determinada cuenta de usuario. Para habilitar cuotas de disco, accedemos a las propiedades del disco donde las queremos activar, mediante la opción Propiedades del menú contextual. Dentro de esa ventana de propiedades, entramos a la pestaña Cuota.

Desde la pestaña Cuota podemos habilitar las cuotas en el disco y configurar otras propiedades de cuotas como denegar espacio de disco a cuentas que excedan la cuota o no, establecer el límite de cuota de disco para usuarios nuevos y el nivel de advertencia a partir del cual se avisa al usuario de que está a punto de exceder la cuota disponible o, finalmente, activar el registro de los excesos de cuota producidos. También se puede configurar la cuota permitida para cada usuario o grupo de usuarios. Para lograrlo, hacemos clic sobre el botón Valores de cuota... y nos sale la ventana de configuración de cuotas para cada usuario. Para añadir una restricción de cuota seleccionamos la opción Nueva entrada de cuota del menú Cuota.

A continuación, añadimos a la lista de la parte inferior los usuarios afectados por la cuota que definiremos. Por último, especificamos los límites de la cuota. Al aceptar estos límites, salen en la lista de entradas de cuota los nuevos usuarios con sus respectivas restricciones.

Desde el servidor y mediante el directorio activo también se puede imponer a todos los usuarios, estén en el equipo que sea, una cuota de disco local. Esto lo podemos hacer abriendo el gestor de políticas de grupo, buscando la política que hace referencia a las cuotas de disco y forzando a que los usuarios tengan una cantidad fija de espacio en disco. Lo encontraremos en la siguiente rama de las políticas de grupo:

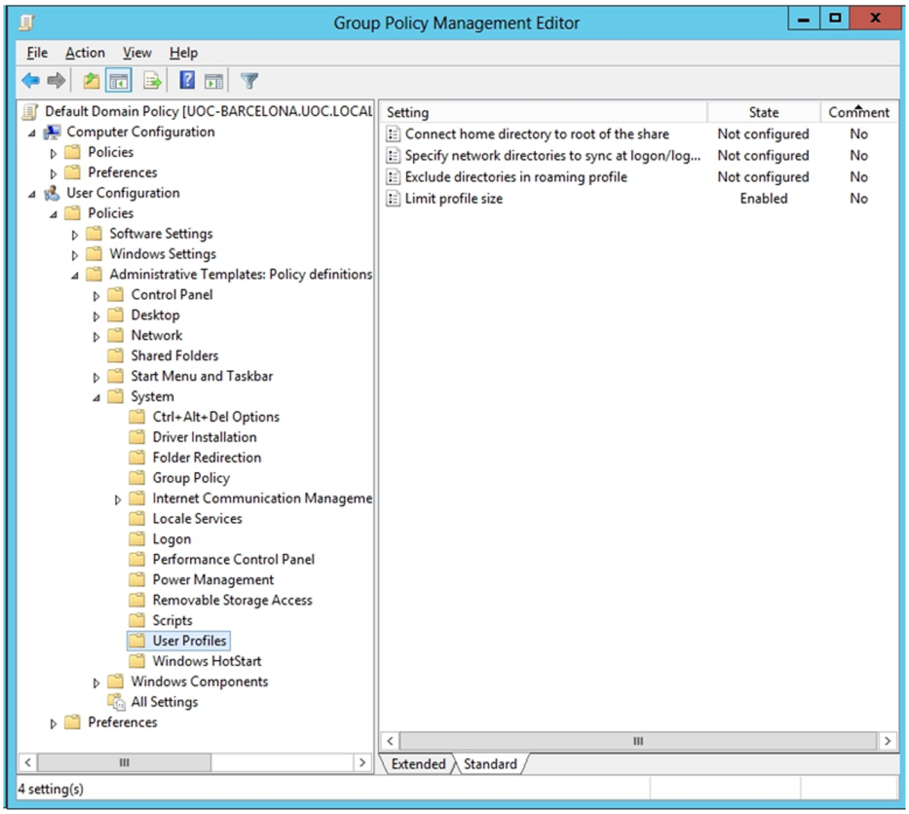
Configuración del PC -> políticas -> plantillas administrativas -> sistema -> cuota de disco.

Ahí se puede habilitar y marcar el máximo y el umbral para enviar un aviso de superación de la cuota de disco. Del mismo modo, podemos limitar el tamaño del perfil móvil de cada usuario para que no se puedan tener perfiles demasiado grandes que pueden hacer que la red se sature en los momentos de entrada y

salida de la entidad. Además, tendremos más controlado el espacio de disco del servidor donde se guardan los perfiles de cada usuario. Esto lo haremos a partir de la política de grupo siguiente:

Configuración de usuario -> políticas -> plantillas administrativas -> sistema -> perfil de usuario

Editor de políticas de grupo para los perfiles de usuario



5.3. Herramientas básicas

Las herramientas básicas de administración del sistema operativo a escala local, en el servidor, están en la carpeta Herramientas administrativas, que podemos encontrar en la interfaz Metro. A continuación, vamos a ver algunas de las más importantes.

5.3.1. Servicios

Los servicios son aplicaciones o procesos que se ejecutan en segundo plano y que no tienen interfaz gráfica de usuario. Estos servicios llevan a cabo una serie de tareas que no requieren interacción con el usuario o que reciben peticiones de otras aplicaciones para ejecutar una tarea u otra. En la ventana de servicios, vemos los servicios instalados en el sistema, como la cola de impresión o el coordinador de transacciones. Vemos también el estado de cada uno de estos servicios, activar o desactivar servicios o configurar servicios para que se inicien automáticamente al iniciar Windows o de manera manual.

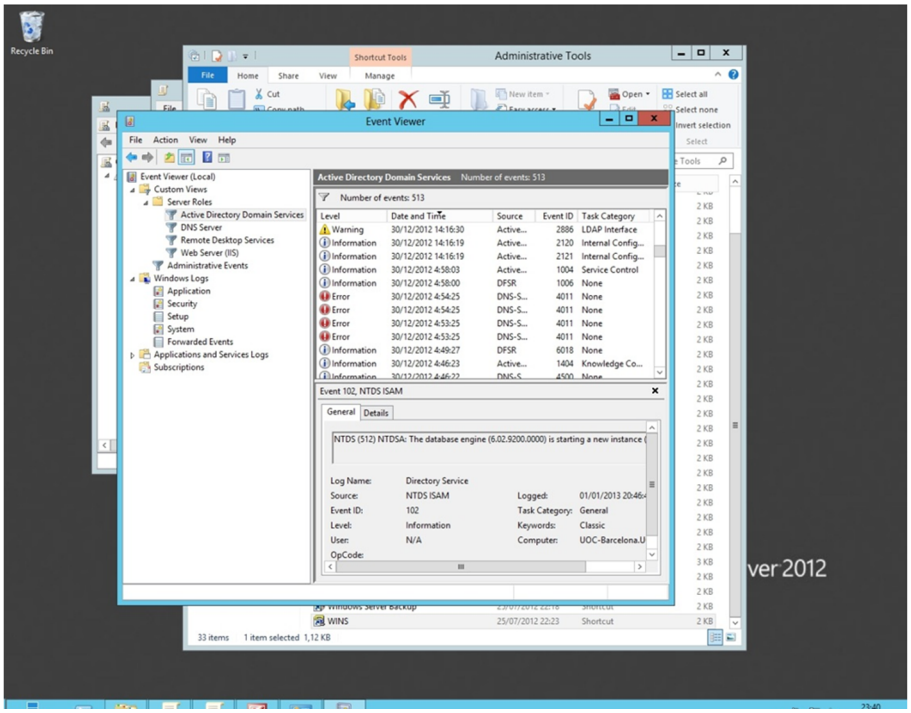
5.3.2. Configuración del servidor

Existe la herramienta Administración del servidor que sale la primera vez que se inicia el sistema después de la instalación y que no desaparecerá hasta que no se configure de otro modo en las propiedades de esta herramienta. También la podemos iniciar manualmente cuando sea necesario. Esta ventana permite configurar varios aspectos del servidor para configurarlo como controlador de dominio (instalando Active Directory), como servidor de archivos o de impresión, como servidor web o servidor de aplicaciones, entre otros. Es donde se tienen que ir añadiendo y retirando todos los roles y características que se quiera dar al servidor. Además, cuando hay un error en el sistema que está relacionado con alguno de los roles o características, aquí es donde el sistema avisa de manera visual de que hay un error. Se puede ver con rapidez qué error se ha producido.

5.3.3. Visor de incidencias

Cuando se produce algún error, ya sea en uno de los roles, características o en el propio sistema operativo, se guarda en un archivo de *logs* del sistema. De este modo, el sistema se comunica con los administradores y estos son los que tienen que ir a visualizar estos archivos de registro. Desde el visor de incidencias (o visor de eventos) vemos los errores o problemas que se han producido en el sistema, así como información adicional sobre el error. Estos informes de error nos permiten ver si hay algún fallo en alguna aplicación o en la seguridad del sistema y dan información adicional para poder buscar información, ya esté en la web de Microsoft o en foros especializados. Los eventos están divididos en categorías y grupos. Así, podemos encontrar los registros de evento del sistema operativos, de los servidores instalados, entre otros, separados en los apartados que muestra la figura siguiente.

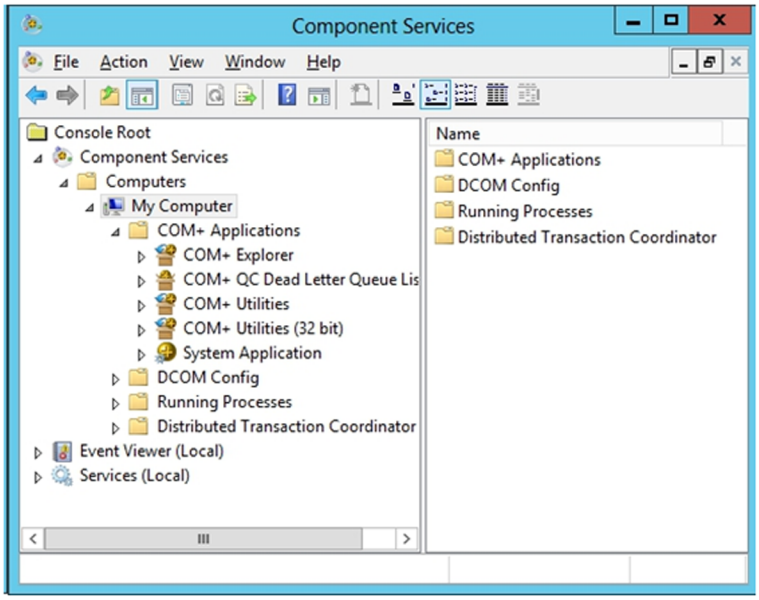
Ejemplo del visor de eventos



5.3.4. Servicios de componentes (COM)

Los componentes *COM* (*common object model*) son componentes de software situados en el registro del sistema que los pueden utilizar otras aplicaciones. La ventana de servicios de componentes muestra los componentes COM instalados en el sistema. También muestra información sobre el controlador de transacciones distribuidas. Tenemos un ejemplo en la figura siguiente.

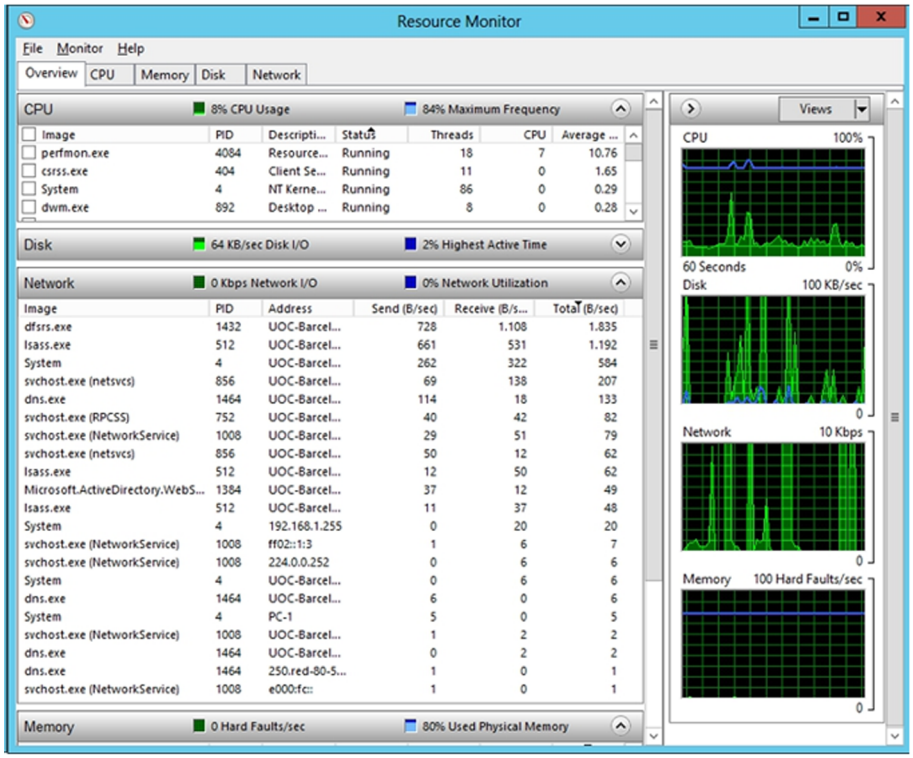
Componentes COM



5.3.5. Rendimiento

El monitor de rendimiento permite ejercer un control sobre el rendimiento del sistema. Ofrece la posibilidad de seleccionar entre muchos contadores de rendimiento (como memoria, uso del procesador, uso en disco o red) y forma un gráfico de los valores de los contadores seleccionados a lo largo del tiempo. En esta versión del sistema operativo, la herramienta de control del rendimiento del servidor da mucha información adicional al rendimiento y se puede ver cómo, por ejemplo, consumen el ancho de banda las diferentes aplicaciones que hay en cada momento ejecutándose, con lo que se puede ver si hay alguna aplicación maliciosa que está usando la red y, por lo tanto, encontrar con rapidez qué aplicación está usando la red para comunicarse, enviar *spam* o bajando algún otro programa, entre otros. La figura siguiente muestra un ejemplo de las aplicaciones que están usando la red Ethernet.

Rendimiento de la red de comunicaciones del servidor



5.3.6. Administración de equipos

Algunas de las consolas de herramientas anteriores y algunas otras más se agrupan en la consola predeterminada que viene en el sistema operativo "Administración de equipos". A continuación, vamos a describir con brevedad las diferentes herramientas de "Administración de equipos":

- **Visor de incidencias:** Muestra las incidencias o los errores producidos en el sistema.

- **Información del sistema:** Proporciona datos sobre el sistema, como hardware, componentes y software instalado.

- **Registros y alertas de rendimiento:** Muestra y configura las alertas de rendimiento del sistema.

- **Carpetas compartidas:** Permite configurar las carpetas compartidas con otros equipos.

- **Administración de dispositivos:** Permite configurar los dispositivos de hardware.

- **Usuarios locales y grupos:** Gestiona usuarios y grupos del equipo.

- **Administración de discos:** Permite gestionar los diferentes volúmenes de discos disponibles, hacer particiones de discos, formatear o cambiar la letra de acceso a una unidad, entre otros.

- **Compactador de disco:** Optimiza el emplazamiento de los archivos en disco para mejorar el acceso.

- **Unidades lógicas:** Gestiona las unidades lógicas definidas en el equipo.

- **Medios de almacenamiento:** Controla los dispositivos de almacenamiento extraíbles e intercambiables.

- **Servicios y aplicaciones:** Contiene otra serie de herramientas para controlar servicios y aplicaciones del sistema (como DHCP, WMI, Index Server, IIS, WINS, DNS).

Si tenemos un controlador de dominio, podemos administrar los diferentes equipos del dominio con la herramienta Usuarios y equipos de Active Directory, seleccionando el equipo que se tiene que administrar y haciendo clic en la opción Administrar.

5.4. Herramientas de protección de Windows Server 2012

5.4.1. *Security configuration wizard* de Microsoft

El asistente de configuración de la seguridad o *security configuration wizard* (*SCW*) es una herramienta de reducción de superficie de ataque para servidores de la familia Microsoft Windows Server. El SCW determina el nivel de funcionalidad mínima que requiere el servidor para funcionar y proporcionar los servicios correctamente, al mismo tiempo que deshabilita las funcionalidades que no son necesarias.

Webs recomendadas

Para más información sobre el SCW, consultad "Security Configuration Wizard for Windows Server 2012" en el sitio web de Microsoft Windows Server 2012:

http://technet.microsoft.com/en-us/library/cc754997.aspx

http://technet.microsoft.com/en-us/windowsserver/hh534429

http://technet.microsoft.com/en-us/library/hh831360.aspx

Pasos que sigue el SCW

1) Deshabilita los servicios innecesarios.

2) Bloquea los puertos que no se utilizan.

3) Permite la configuración específica de seguridad en los puertos que quedan abiertos.

4) Prohíbe las extensiones de la IIS que no son necesarias, si es aplicable.

5) Reduce la exposición a riesgos de los protocolos SMB, Lanman y LDAP.

6) Define una política de auditoría de alta seguridad.

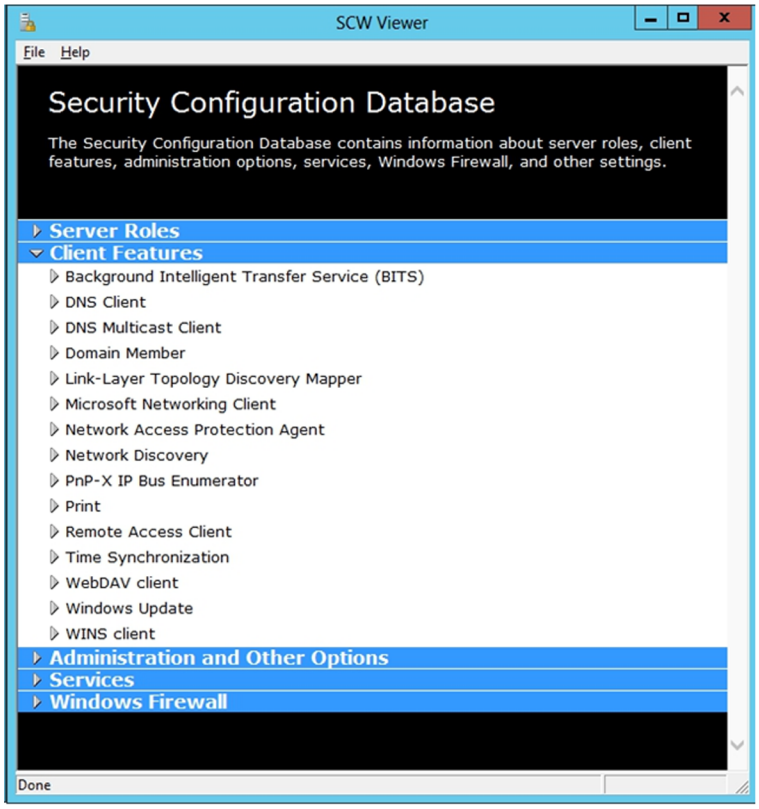
7) El SCW guía en el proceso de crear, editar, aplicar o retirar una política de seguridad basada en los roles seleccionados del servidor. Las políticas de seguridad creadas con el SCW son archivos XML que, cuando se aplican, configuran servicios, la seguridad de la red, valores específicos de registro, políticas de auditores y, si es aplicable, el servicio de información de Internet.

El procedimiento de protección de los servidores se basa en ejecutar el software de Security Configuration Wizard de Microsoft. Además, se comprueban y se revisan mediante la *Microsoft Security Guide* todos los puntos débiles que aconseja revisar. Después, se lleva a cabo la comprobación de que los servicios funcionan correctamente y de que la protección es correcta.

Iniciamos el SCW, desde la interfaz Metro o desde las herramientas administrativas, y seguimos hasta la siguiente pantalla, donde se pueden seleccionar diferentes opciones: crear una nueva política de seguridad, editar una existente, aplicar una política ya existente o deshacer los cambios de una política que ya se aplicó con anterioridad. Al ser la primera vez que se hace una política, crearemos una nueva sobre el mismo servidor que estamos configurando, se podría hacer sobre otro de manera remota, pero no será este el caso. Empieza a procesar y a analizar la política aplicada actualmente en el servidor y extrae

un registro muy completo. Podemos ver este registro con el botón *View Configuration Database*. La figura muestra un ejemplo de esta recopilación inicial de todos los parámetros de seguridad que ha encontrado ya configurados en el sistema.

Visor SCW; configuración inicial



A continuación, el asistente se divide en cuatro grandes partes:

1) Configuración basada en los roles Microsoft que tiene el servidor.

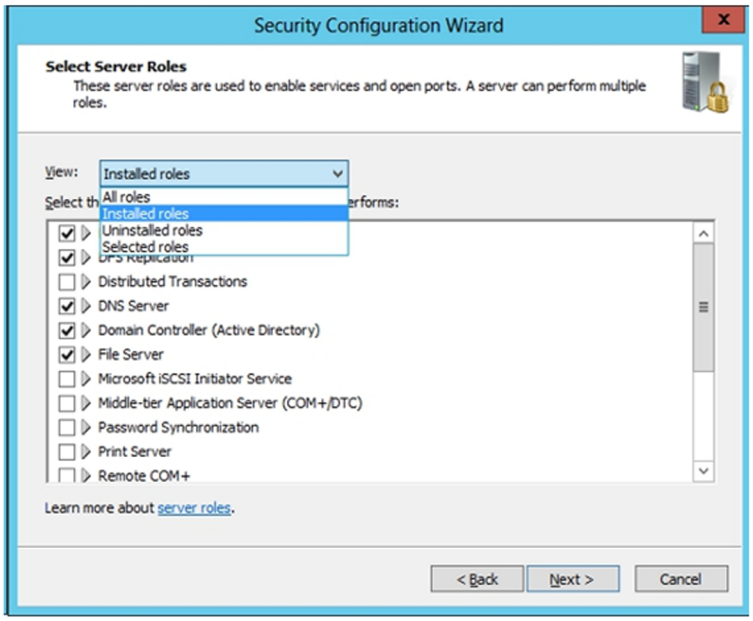
2) Configuración de seguridad de la red.

3) Configuración del registro.

4) Políticas de auditoría.

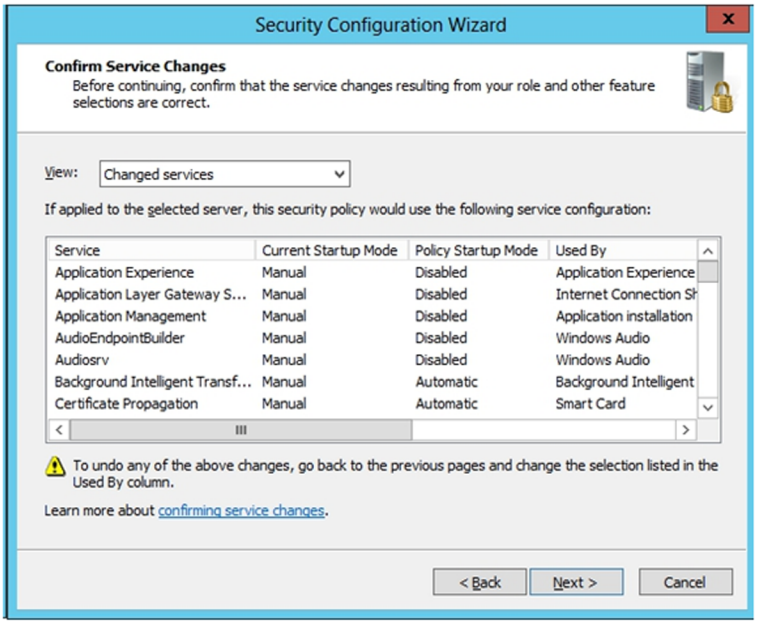
La figura siguiente nos muestra los roles que el asistente ha detectado que tiene nuestro servidor. Si queremos, añadimos los que nosotros consideramos necesarios. Se puede ver que elabora un listado de los que encuentra que están instalados y de los que se pueden configurar.

Selección de roles por securizar



Lo siguiente que nos muestra el asistente es qué características y programas cliente ha detectado que utiliza el servidor para acceder a otros servicios de otras máquinas; tenemos que elegir los que nos parece que necesitará el servidor. A la vez, nos enseña qué programas destinados a la administración del servidor, como el RPC, los servicios de copia de seguridad que abren puertos o la aplicación de políticas de grupos, utiliza nuestro servidor. Además, nos muestra qué servicios ajenos al sistema operativo y a las herramientas Microsoft tenemos en el servidor y nos permite elegir cuáles son válidos y cuáles no. Finalmente, muestra un resumen de las acciones que tomará dependiendo de los datos que acabamos de introducir.

Cambios que aplicará el SCW



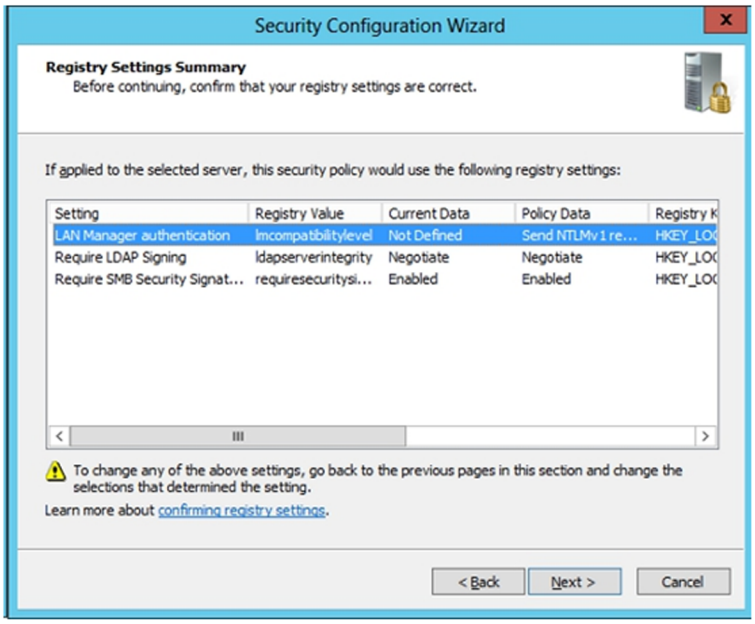
Como vemos en la figura anterior, apaga y deshabilita los servicios que ha detectado que no son necesarios para el funcionamiento correcto del servidor, y deja los que son necesarios y los que le hemos nombrado específicamente.

A continuación, vamos a configurar la parte de la configuración de seguridad de la red de una manera muy similar a la anterior. Nos muestra las reglas a partir de los protocolos que usan los roles y aplicaciones que usan la red y, por lo tanto, podemos aquí bloquear los protocolos y reglas para que no puedan tener acceso a la red.

El punto siguiente consiste en proteger la configuración específica de seguridad del registro. Básicamente, estas configuraciones sirven para proteger la manera como se comunican entre sí los servidores NT y posteriores y para que lo hagan de manera segura. La primera que nos muestra consiste en forzar a que las comunicaciones por SMB (NetBIOS) se firmen. La siguiente pantalla pregunta por las comunicaciones contra la LDAP del Active Directory si también tienen que estar firmadas. La siguiente es la manera como debe comportarse la autenticación de dominios Windows desde nuestro servidor hacia máquinas externas.

Al final, nos muestra un resumen de los cambios que se harán en el registro según los datos suministrados.

Cambios en el registro



El último punto del asistente lo constituye la configuración de la política de auditorías, que sirven para mantener un control exhaustivo de los accesos al servidor, tanto de la red como de archivos. Lo configuramos para que se auditen las actividades que han tenido éxito y las que no lo han hecho. Así se podrá controlar mucho más los posibles ataques o manipulaciones al sistema

que hayan funcionado y los que no. Finalmente, se guarda la configuración de la política en un directorio para poder recuperarla con posterioridad y se aplica para que tenga efecto sobre el servidor en el mismo instante.

Hay que comprobar que los servicios de la máquina no han quedado afectados y que continúan funcionando correctamente. Todos aquellos servicios que antes funcionaban se tienen que revisar por si se ha seleccionado algún protocolo mal y se ha bloqueado el servicio. Se debe destacar que, como protegemos la red, se cambia la configuración del cortafuegos de la máquina del servidor, lo que hay que tener en cuenta a partir del momento en el que se inicia por si queremos añadir nuevos servicios o programas que accedan al exterior. Si no queremos que arranque el cortafuegos de estación, se tiene que hacer un *skip* del apartado de protección de la red y no configurar este punto del asistente. A pesar de que es muy aconsejable configurar de manera correcta este punto, siempre será mejor configurar correctamente el cortafuegos con los protocolos o puertos que se tienen que usar desde el exterior, que no tener ninguno y dejar el servidor completamente vulnerable a los ataques de red.

5.4.2. Política de aplicación de parches de seguridad críticos de Microsoft

Tan importante como la protección del sistema es la actualización sistemática de todo el sistema operativo de Windows con los parches de seguridad críticos que publica periódicamente Microsoft. Se recomienda que, aunque sea después de un cortafuegos, o que estén incomunicados del exterior, se haga esta actualización del sistema de manera automática, mediante las actualizaciones automáticas.

Lo más recomendable es configurarlo para bajar las actualizaciones automáticas del sitio web de Microsoft y que nos permita elegir cuándo las queremos instalar. Aunque automatizar todo el proceso en un servidor puede ser peligroso, ya que si la instalación de un parche requiere reiniciar la máquina, se hará de manera automática a la hora especificada. Esta opción puede ser buena en estaciones de trabajo, pero para servidores es recomendable ser algo más conservadores y poder decidir cuándo queremos actualizar el sistema operativo. Podemos hacer que las actualizaciones se apliquen en el momento en el que el servidor no está en uso y en el momento de hacer un reinicio de la máquina. El sistema avisará de que tiene tareas de mantenimiento pendientes y que se tiene que reiniciar para hacer efectivas las actualizaciones.

También se puede añadir al servidor el rol del Windows Server Update Services (WSUS), que proporcionará un servidor de actualizaciones de parches para todos los ordenadores de la empresa. Pueden hacer un filtrado de los que se considere que no hay que instalar o, lo que es más importante, reduciendo el uso de la red a Internet, ya que ahora las actualizaciones, en lugar de ir al servidor de Microsoft a través del *router* y el IPS, irán únicamente mediante la red local Ethernet al servidor WSUS acabado de instalar. En el caso de tener

una pequeña empresa con diez ordenadores, no nos hará falta hacer esta instalación, pero para empresas grandes con centenares o miles de PC sí resulta una ganancia considerable en el ancho de banda tener un punto interno de actualizaciones, ya que solo hay que bajar los programas y servirlos a todos los demás ordenadores cliente de la red. Estos ordenadores se tendrán que configurar para que vayan a buscar las actualizaciones al servidor interno de la organización y no a los servidores de Microsoft.