



Índice

Módulo 1: Sistemas Operativos de Red.....	3
1 Fundamentos de sistemas operativos	3
1.1 Introducción	3
1.2 Sistemas operativos de escritorio.....	3
1.3 Sistemas operativos de red.....	4
1.4 El modelo cliente/servidor	4
1.5 Servicios de red	5
2 Hardware de servidores.....	5
2.1 Servidores de red.....	5
2.2 Hardware especial	5
2.3 Procesadores múltiples.....	10
2.4 RAID	10
3 Instalación de un sistema operativo de red	13
3.1 Introducción	13
3.2 Planeamiento del sistema	14
3.3 Planeamiento de la instalación.....	15
3.4 Listas de compatibilidad de hardware	16
4 Proceso de instalación	17
4.1 Medio de instalación	17
4.2 Programa de instalación.....	18
4.3 Partición de disco.....	19
4.4 Herramientas de particionado	22
4.5 Archivos/particiones swap.....	23
4.6 Formateo	25
4.7 Cuenta del administrador	25
5 Instalación de Windows 2000.....	26
5.1 Instalación del sistema operativo	26
5.2 Interfaz de usuario/administrador.....	29
6 Administración de usuarios en Windows 2000.....	31
6.1 Usuarios.....	31
6.2 Creación de Grupos/Agregado de Usuarios.....	32
6.3 Administración de las Cuentas de Usuario	32
6.4 Passwords y Permisos.....	33
6.5 Tipos de permisos.....	33
7 Active Directory.....	34
7.1 Introducción	34
7.2 Estructura de la base de datos del Active Directory	34
7.3 Dominios del Windows 2000	34
7.4 Unidades Organizativas (OUs) de Windows 2000.....	34
7.5 El Active Directory y el DNS.....	34
7.6 Servidores de Active Directory	35
7.7 Reproducción del Active Directory	35
7.8 Seguridad del Active Directory	35
7.9 Compatibilidad del Active Directory.....	36
8 Instalación de un sistema operativo Linux	36
8.1 Selección de los parámetros apropiados para la instalación	36
8.2 Creación de un sistema de archivos Linux	37
8.3 Selección de paquetes para la instalación	37





8.4	Instalación y configuración de Linux.....	38
8.5	Configuración de la Seguridad Apropriada	38
8.6	Configuración de los Datos de Red.....	39
8.7	Otras Configuraciones y Datos.....	40
8.8	Opciones de Inicio.....	40
9	Administración de Linux	41
9.1	Interfaz de usuario	41
9.2	Interfase GUI.....	41
9.3	Interface CLI	43
9.4	Cuentas de usuario y grupos	44
9.5	Permisos.....	49
9.6	Gestión del sistema de archivos.....	50
9.7	Demonios.....	53



Módulo 1: Sistemas Operativos de Red

1 Fundamentos de sistemas operativos

1.1 Introducción

En el origen de la historia de las computadoras (hace unos cuarenta años), los sistemas operativos no existían y la introducción de un programa para ser ejecutado se convertía en un increíble esfuerzo que solo podía ser llevado a cabo por muy pocos expertos. Esto hacía que las computadoras fueran muy complicadas de usar y que se requiriera tener altos conocimientos técnicos para operarlas. Era tan complejo su manejo, que en algunos casos el resultado llegaba a ser desastroso.

Además, el tiempo requerido para introducir un programa en aquellas grandes máquinas de lento proceso superaba por mucho el de ejecución y resultaba poco provechosa la utilización de computadoras para resolución de problemas prácticos.

Se buscaron medios más elaborados para manipular la computadora, pero que a su vez simplificaran la labor del operador o el usuario. Es entonces cuando surge la idea de crear un medio para que el usuario pueda operar la computadora con un entorno, lenguaje y operación bien definido para hacer un verdadero uso y explotación de esta. De esta forma, surgen los sistemas operativos.

Un sistema operativo es el encargado de brindar al usuario una forma amigable y sencilla de operar, interpretar, codificar y emitir las ordenes al procesador central para que este realice las tareas necesarias y específicas para completar una orden.

El sistema operativo, es el instrumento indispensable para hacer de la computadora un objeto útil. Bajo este nombre se agrupan todos aquellos programas que permiten a los usuarios la utilización de este enredo de cables y circuitos, que de otra manera serían difíciles de controlar. Un sistema operativo se define como un conjunto de procedimientos manuales y automáticos, que permiten a un grupo de usuarios compartir una instalación de computadora eficazmente.

1.2 Sistemas operativos de escritorio

La función de un Sistema Operativo es controlar el hardware de una computadora, el entorno de ejecución de los programas, y la interfase del usuario. El Sistema Operativo ejecuta estas funciones para un usuario único o para una cantidad de usuarios que comparten la máquina en forma serial en lugar de concurrente. Un administrador puede crear cuentas para más de un usuario, pero los usuarios no pueden ingresar al sistema al mismo tiempo.

Las computadoras personales (PC) funcionan como clientes en un entorno de Sistema Operativo de Red (Network Operating Systems – NOS). Al usar las funciones del Sistema Operativo nativo de la PC, el usuario puede acceder a los recursos que son locales a la PC. Estos incluyen aplicaciones, archivos, y dispositivos que están conectados directamente como las impresoras. Cuando una PC se convierte en un cliente en un entorno NOS, el software adicional especializado permite que el usuario local acceda a recursos no locales, o remotos como si estos recursos fueran parte del sistema local. El NOS aumenta el alcance de la PC cliente haciendo disponibles los servicios remotos como extensiones del sistema operativo nativo local.





Aunque una cantidad de usuarios pueden tener cuentas en una PC, sólo una cuenta está activa en el sistema en un momento determinado.

1.3 Sistemas operativos de red

Los Sistemas Operativos de Red (Network Operating Systems – NOS) distribuyen sus funciones sobre una cantidad de computadoras en red. Un NOS depende del sistema operativo nativo en cada computadora individual. Luego agrega funciones que permiten el acceso de una cantidad de usuarios a los recursos compartidos en forma concurrente.

Las computadoras con NOS toman roles especializados para llevar a cabo el acceso concurrente a los recursos compartidos. Los sistemas clientes contienen un software especializado que les permite solicitar recursos compartidos controlados por los sistemas servidores que responden a las solicitudes de los clientes.

Un NOS soporta múltiples cuentas de usuarios al mismo tiempo y permite el acceso concurrente a los recursos compartidos por múltiples clientes. Los servidores deben dar soporte a múltiples usuarios y actuar como repositorios de los recursos que son compartidos por muchos clientes. Los servidores requieren un software especializado y un hardware adicional. Los servidores deben contener varias cuentas de usuarios y deben poder permitir que más de un usuario acceda a los recursos de la red en un mismo momento.

1.4 El modelo cliente/servidor

En un arreglo cliente/servidor, los servicios de red están ubicados en una computadora dedicada llamada servidor, que responde a las solicitudes de los clientes. El servidor es una computadora central que está continuamente disponible para responder a las solicitudes de un cliente por archivos, impresión, aplicaciones, y otros servicios. La mayoría de los sistemas operativos de red adoptan la forma de relaciones cliente/servidor. Normalmente, las computadoras de escritorio funcionan como clientes y una o más computadoras con poder de procesamiento, memoria y software especializado adicional funcionan como servidores.

Los servidores están diseñados para manipular solicitudes de muchos clientes simultáneamente. Antes de que un cliente pueda acceder a los recursos de un servidor, debe identificarse a sí mismo y ser autorizado para utilizar el recurso. Esto se hace asignando a cada cliente un nombre y clave de cuenta que es verificado por un servicio de autenticación que actúa como un guardia para cuidar el acceso a la red. Al centralizar las cuentas de los usuarios, la seguridad, y el control de acceso, las redes basadas en servidor simplifican la tarea de administración de la red.

La concentración de recursos de red (archivos, impresoras y aplicaciones) en varios servidores también hace que los datos que generan sean más fáciles de mantener y de copiar para respaldo. En lugar de tener a estos recursos esparcidos por máquinas individuales, pueden ser localizados en servidores especializados y dedicados para un acceso más fácil. La mayoría de los sistemas cliente/servidor también incluyen facilidades para mejorar la red agregando nuevos servicios que extienden la utilidad de la red.

La distribución de funciones en las redes cliente/servidor brinda ventajas sustanciales, pero también incurre en algunos costos. Aunque la centralización de recursos en los sistemas servidores proporciona mayor seguridad, acceso más sencillo y control coordinado, el servidor introduce un punto único de falla dentro de la red. Sin un



servidor operativo, la red no puede funcionar. Los servidores requieren un personal entrenado y experto para que lo administre y mantenga. Esto aumenta el costo de operar la red. Los sistemas servidores también requieren hardware adicional y software especializado que se suma al costo.

1.5 Servicios de red

Los Sistemas Operativos de Red (Networking Operating Systems – NOS) están diseñados para proporcionar procesos de red a los clientes y pares. Los servicios de red incluyen la World Wide Web (WWW), compartir archivos, intercambio de correo, servicios de directorio, administración remota y servicios de impresión.

La administración remota es un poderoso servicio que permite que los administradores configuren los sistemas en red que están a gran distancia. Es importante entender que estos procesos de red son llamados "Servicios" en Windows 2000 y "Demonios (Daemons)" en Linux. En esencia todos proporcionan las mismas funciones pero la forma en que interactúan con el NOS será diferente en cada sistema operativo. Los servicios y daemons serán tratados con más detalle en capítulos posteriores.

Dependiendo del NOS, algunos de estos procesos de red claves pueden ser activados durante una instalación por defecto. Los procesos de red más populares dependen de la suite de protocolos TCP/IP. Como TCP/IP es un conjunto de protocolos abierto y bien conocido, los servicios basados en TCP/IP son especialmente vulnerables a rastreos no autorizados y a ataques maliciosos. Los ataques de Negación de Servicio (Denial of Service – DoS), virus de computadora y "gusanos" de Internet de expansión rápida han forzado a los diseñadores de NOS a reconsiderar cuáles servicios de red son iniciados automáticamente.

Versiones recientes de Sistemas Operativos de Red populares, como Windows 2000 y Red Hat Linux, restringen la cantidad de servicios de red que son activados por defecto. Cuando se instala un NOS, los servicios de red claves necesitarán ser activados en forma manual.

2 Hardware de servidores

2.1 Servidores de red

Un servidor de red es una computadora en una red que es compartida por múltiples usuarios. Un servidor puede tener teclado, monitor, y mouse conectados directamente a él, o un teclado, monitor y mouse pueden estar conectados a una cantidad de servidores a través de un conmutador Teclado Video Mouse (Keyboard Video Mouse – KVM). Los servidores también pueden ser accedidos a través de una conexión de red. El término "servidor" puede referirse tanto al hardware y al software o sólo al software que realiza el servicio.

2.2 Hardware especial

En un entorno NOS, muchos sistemas clientes acceden y comparten los recursos de uno o más servidores. Los sistemas clientes de escritorio están equipados con sus propias memorias y dispositivos periféricos como un teclado, monitor, y disco. Para soportar el procesamiento local, los sistemas servidores deben estar equipados para soportar múltiples usuarios concurrentes y múltiples tareas ya que los clientes hacen pedidos de recursos remotos al servidor.



Los servidores NOS, por lo tanto, son sistemas más grandes con memoria adicional para soportar las múltiples tareas que están todas activas, o residentes, en memoria al mismo tiempo. También se necesita en los servidores espacio adicional de disco para albergar los archivos compartidos y para que funcionen como una extensión de la memoria interna del sistema. Además, los servidores por lo general requieren slots de expansión extras en sus placas de sistema para conectar dispositivos compartidos, como impresoras, y múltiples interfaces de red. En los servidores de multiprocesador, las CPUs adicionales aumentan el poder de procesamiento.

Como los servidores NOS funcionan como repositorios centrales de recursos que son vitales para la operación de los sistemas clientes, los servidores no sólo deben ser eficientes sino también robustos. "Robusto" indica que los sistemas servidores tienen que poder funcionar en forma efectiva bajo una carga pesada y sobrevivir a la falla de uno o más procesos o componentes sin experimentar una falla general del sistema. Este objetivo es logrado construyendo redundancia en los sistemas servidores. La redundancia es la inclusión de componentes de hardware adicionales que pueden tomar el control si otros componentes fallan. La redundancia es una característica de los sistemas tolerantes a fallos que son diseñados para sobrevivir a las fallas e incluso para ser reparados sin interrupción mientras están encendidos y funcionando. Como un NOS depende de la operación continua de sus servidores, los componentes extra de hardware justifican el costo adicional.

Gabinete del servidor

Se debe verificar que el gabinete del servidor es del modelo correcto que fue pedido y con el factor de formato correcto. La mayoría de los gabinetes de servidor son de configuración tower, wide o fat (ancha) tower, o de montura en rack. Asegúrese de que si se pidió un modelo X en configuración tower, fue enviado eso y no un modelo X en una configuración de montura en rack. Cuál es el mejor depende de varias cosas, incluido el espacio disponible para el servidor.

Rack de servidor

Un gabinete de servidor de montura en rack debe ser montado en un rack de equipo diseñado para hardware de montura en rack. La mayoría de los fabricantes de servidores que venden servidores en un gabinete de montura en rack también venden el rack de servidores. Los racks de servidores generalmente vienen en varios tamaños (alturas). El tamaño del rack de servidores se mide en unidades de rack (U). Una unidad de rack estándar es 1,75 pulgadas. Un servidor de red nuevo será instalado en un rack de servidores existente o se deberá comprar un nuevo rack para el nuevo servidor de red. Los racks de servidores por lo general tienen puertas delanteras y traseras y paneles laterales para formar una unidad completamente cerrada. Las puertas y paneles laterales ayudan a asegurar el entorno y también están diseñados para ayudar a la refrigeración del equipo en el rack controlando los patrones de flujo de aire. En la mayoría de los casos se pueden unir varios racks de servidores para formar un espacio de instalación para una gran cantidad de servidores

Una instalación de servidores montados en racks ahorra espacio en la habitación donde residen los servidores. Si se decidió usar una configuración de montura en rack, por lo general todo el equipo debe estar diseñado para encajar en el rack de servidores. Esto incluye la UPS, el teclado/mouse, y el monitor (LCD o CRT) para el servidor. La instalación del equipo en el rack de servidores debería realizarse con las especificaciones del fabricante del servidor. Varios fabricantes de servidores ofrecen ayuda en la colocación apropiada del equipo en el rack de servidores. Por ejemplo, todos los fabricantes de servidores recomiendan que la UPS sea instalada en la parte inferior del rack. Esto es así por varias razones, incluyendo el peso de la UPS montada



en el rack y la necesidad de evitar el posible daño a un servidor de red causado por una filtración de la batería de la UPS.

Procesador(es)

Los servidores de red comúnmente tienen más de un procesador. Se debe verificar que la cantidad correcta y tipo de procesadores están disponibles para el servidor de red. Algunos fabricantes de servidores instalan todos los procesadores que fueron pedidos. Otros suministran el servidor sin procesador o con uno instalado, y el administrador de red debe instalar los procesadores adicionales. Hay que verificar que los procesadores sean del mismo tipo, velocidad y stepping (versión). También verificar que cada procesador tiene el mismo tamaño de cache L2. Se deben seguir estrictamente las instrucciones del fabricante de servidores de red para instalar los procesadores adicionales.

Memoria

Los servidores de red generalmente necesitan una considerable cantidad de memoria para que realicen adecuadamente sus funciones. Algunos fabricantes de servidores instalan toda la memoria que fue pedida. Sin embargo, otros fabricantes de servidores entregan el servidor con una cantidad de memoria estándar, y el administrador de red debe instalar la memoria por encima de la cantidad estándar. Es necesario verificar que el servidor tenga la cantidad de memoria solicitada. Si se debe instalar memoria, hay que verificar que la memoria es del tipo correcto para el servidor y seguir las instrucciones del fabricante de hardware de servidor para instalar la memoria adicional. Este es un paso crítico. Algunos servidores requieren que la memoria sea instalada en grupos de 2 o 4 módulos de memoria (es de suma importancia revisar la documentación del fabricante del servidor para ver si los módulos de memoria deben ser instalados en grupos de 2 o 4, en lugar de por separado). El no instalar la memoria correctamente provocará que el servidor no reconozca toda la memoria instalada o que el servidor no logre encender.

Unidades de disco

Muchas configuraciones de servidor de red requieren que una gran cantidad de almacenamiento en disco esté disponible en el servidor. Es importante que las unidades de disco tengan el tamaño, velocidad y tipo correcto (IDE/ATA, EIDE/ATA-2, SCSI, SCSI-2, SCSI-3, SAS). Las unidades de disco pueden venir instaladas en el gabinete del servidor o pueden ser entregadas por separado en cajas acolchadas para evitar ser dañadas. El plan de instalación especificará cuáles unidades de disco (tamaño, velocidad y tipo) deberían ser instaladas en el servidor de red.

Monitor, teclado y mouse

Verifique que el monitor para el servidor de red es el que se pidió. En general el monitor debería soportar una resolución VGA de al menos 1024 por 768 puntos por pulgada (dpi). El monitor puede ser del tipo CRT tradicional o uno de los más nuevos monitores LCD de pantalla plana. Si el monitor va a ser montado en un rack, será necesario comprar un estante especial para monitor. Hay disponibles monitores LCD de pantalla plana especiales para montura en rack. Estos a menudo incluyen una combinación de teclado/trackball o touch pad (sustituto del mouse) en un único cajón de rack.

Fuente de Alimentación Ininterrumpida (Uninterruptible Power Supply – UPS)

Es necesario comprobar que esté disponible una UPS para el servidor de red. La UPS debería ser del tamaño adecuado para soportar al nuevo servidor por un corto tiempo, lo que permitirá un apagado correcto del servidor. Las UPSs para montura en rack están disponibles para las instalaciones de servidores de red montados en racks.





Todas las UPSs deberían poder ser supervisadas por el servidor de red, a través de un cable USB o de comunicaciones serial. Si la UPS va a ser supervisada por medio de una conexión serial, asegúrese de que está disponible una conexión serial en el servidor de red. A través de la compra de hardware adicional para la UPS, el administrador de red puede normalmente supervisar una UPS a través de la red. Las UPSs de alta línea a menudo permiten que el administrador de red las supervise a través de una consola de administración SNMP o de una interfase web incorporada. Esto permitirá que el administrador de red revise la UPS desde cualquier conexión a Internet, una característica superior para un administrador.

Sistema de copia de respaldo

Verifique que el sistema de copia de respaldo es el especificado en el plan de instalación y que sea adecuado para soportar la copia de respaldo del servidor de red. El sistema de respaldo es generalmente una unidad de cinta magnética de un formato u otro. La unidad de cinta debería poder hacer una copia de respaldo del contenido de las unidades de disco en el servidor de red en forma periódica. La capacidad de la unidad de cinta y la velocidad con que los datos pueden ser transferidos a la unidad de cinta son ambas de importancia crítica. Si el administrador de red determina que dadas las especificaciones de la unidad de cinta, una copia de respaldo completa del servidor de red tarda 10 horas y el administrador de red sólo tiene 4 horas para realizar la copia, por ejemplo, la unidad de cinta es inadecuada para la tarea. El administrador de red también puede hacer copia de respaldo a otros dispositivos, como unidades de disco rígido, dispositivos CD-R, y dispositivos CD-RW. Los dispositivos de copia de respaldo deberían ser instalados en una controladora separada de las unidades de disco del servidor de red, para proporcionar un rendimiento óptimo durante el proceso de copiado.

Cables SCSI

Se deben controlar los cables correctos para conectar la controladora de canal SCSI a los dispositivos SCSI (unidades de disco). Los cables SCSI difieren mucho entre sí (por ejemplo, SCSI-1, SCSI-2 y SCSI-3). Las versiones más anchas de SCSI-2 y SCSI-3 utilizan diferentes cables. Los cables SCSI internos son generalmente cables de cinta, con el pin 1 identificado por una cinta de color (normalmente rojo) en el borde del cable de cinta. Los cables SCSI externos son por lo general un manojo redondo. Es necesario controlar que los cables SCSI tengan la cantidad correcta de conectores para la configuración del servidor de red y asegurarse de que los cables SCSI no excedan la longitud máxima del canal SCSI. También hay que asegurarse de que los cables SCSI tienen suficientes conectores para permitir que todos los dispositivos SCSI sean conectados a él. Si el administrador de red necesita conectar cuatro unidades de disco SCSI a un canal SCSI, por ejemplo, el cable SCSI necesita al menos cuatro conectores para las unidades de disco, más uno donde puede ser conectado al adaptador SCSI.

Adaptador(es) SCSI

Verificar que esté disponible el adaptador SCSI correcto. Muchos servidores de red tienen uno o más adaptadores SCSI incorporados. Pueden ser necesarios adaptadores SCSI adicionales para soportar la cantidad de dispositivos SCSI que serán usados con el servidor de red. Asegurarse de que el adaptador SCSI y los dispositivos SCSI son del mismo tipo de SCSI (SCSI-1, SCSI-2, SCSI-3, etc.).

También verificar de que la interfase del adaptador SCSI concuerda con el bus que está en el servidor de red, por ejemplo, EISA, PCI o PCI-64.



Controladora(s) de Matriz Redundante de Discos Económicos (Redundant Array of Inexpensive Disks – RAID)

Si el servidor de red va a utilizar la versión de hardware RAID, verifique que la controladora RAID esté disponible. La controladora RAID debería ser entregada con el software de configuración. La controladora RAID debe ser configurada antes de instalar el sistema operativo. La mayoría de las controladoras RAID están diseñadas para soportar algunas versiones de unidades de disco SCSI. Asegúrese de que la controladora RAID concuerda con el bus que está en el servidor de red, por ejemplo, EISA, PCI o PCI-64.

Tarjeta(s) de interfase de red

Verifique que la tarjeta de interfase de red (NIC) para el servidor de red esté disponible. Algunos servidores de red tienen la NIC incorporada al servidor de red. Si son necesarias NICs redundantes para el servidor de red, verifique que todas las NICs están disponibles. Asegúrese de que la NIC soporta el tipo de red donde el servidor de red va a ser instalado (Ethernet, Token Ring, etc). También se podrían instalar NICs múltiples en un único servidor de red si va a ser conectado a múltiples redes.

Hardware adicional

Podría ser necesario otro hardware para el servidor de red. El servidor de red requiere un adaptador de video que soporte el monitor del servidor de red. No hay razón para gastar mucho dinero en un adaptador de video de lujo que tenga una gran cantidad de memoria de video para soportar resoluciones de video extremadamente altas y millones de colores. El monitor de video en un servidor de red es por lo general usado sólo para realizar funciones administrativas en el servidor de red. Un adaptador de video que puede soportar resolución VGA de hasta 1024 por 768 y 65.536 colores debería ser adecuado para la mayoría de los servidores.

Muchos fabricantes de hardware de servidor tienen un adaptador de administración de servidor especializado que puede ser comprado e instalado en sus servidores de red. Estos dispositivos generalmente supervisan la salud del hardware del servidor y pueden ser usados por el software de administración del servidor que corre en una computadora designada de administración. Algunos de estos dispositivos tienen un modem incorporado, lo que permite supervisar el hardware del servidor a través de una conexión de discado.

Un servidor de red montado en rack podría incluir un switch de teclado/video/mouse (KVM) para permitir que un teclado, una pantalla de video y un mouse sean utilizados por los múltiples servidores de red que están en un solo rack. El switch KVM permite que el teclado, el mouse y la pantalla de video cambien (normalmente desde el teclado) entre los servidores de red en el rack. Esto ahorra espacio en el rack, porque cada servidor de red no necesitará su propio teclado, mouse y monitor. Algo de dinero también se ahorra al compartir el teclado, el mouse y el monitor, porque el administrador de red no tiene que comprarlos para cada servidor.

Un servidor de red también debería tener algunos dispositivos encontrados comúnmente en la mayoría de los sistemas de computación de escritorio, como diskettera de 3,5 pulgadas y una unidad de CD-ROM y una unidad de DVD-ROM. Estos dispositivos son necesarios para instalar el software del sistema operativo, los drivers del hardware y otro software en el servidor de red.





2.3 Procesadores múltiples

Otra característica de los sistemas capaces de actuar como servidores NOS es el poder de procesamiento. Comúnmente, las computadoras tienen una única Unidad Central de Proceso (CPU), que ejecuta las instrucciones que realizan las tareas o procesos dados. Para que funcione en forma eficiente y emita respuestas rápidas a las solicitudes de los clientes, un sistema operativo que funciona como un servidor NOS requiere una poderosa CPU para ejecutar sus tareas o programas. Los sistemas de procesador único con una CPU pueden cumplir con las necesidades de la mayoría de los servidores NOS si tienen la velocidad necesaria. Para lograr velocidades de ejecución mayores, algunos sistemas están equipados con más de un procesador.

Tales sistemas son llamados sistemas de multiprocesamiento. Son capaces de ejecutar múltiples tareas en paralelo asignando cada tarea a un procesador diferente. La cantidad de trabajo total que el servidor puede realizar en un tiempo dado está aumentada enormemente en los sistemas de multiprocesador. Los servidores de esta naturaleza a veces son llamados servidores empresariales a causa de su capacidad para manipular grandes y múltiples servicios. Los servidores empresariales también son capaces de ejecutar copias concurrentes de un comando en particular. Esto les permite ejecutar múltiples instancias del mismo servicio o threads de llamadas a programas. Un thread es un término de programación de computadoras que describe a un programa que se puede ejecutar en forma independiente de otras partes. Los sistemas operativos que soportan multithreading permiten que los programadores diseñen programas cuyas partes se pueden ejecutar simultáneamente.

2.4 RAID

La Matriz Redundante de Discos Económicos (Redundant Array of Inexpensive Disks – RAID) está diseñada para permitir cierta tolerancia a fallos que evite la pérdida de datos en el caso de una falla de disco rígido en un servidor de red. Un disco rígido es un dispositivo mecánico. Por lo tanto, la cuestión no es si el disco fallará, sino cuándo fallará. RAID brinda esta tolerancia a fallos o redundancia a través de la paridad de almacenamiento de discos rígidos o la misma información en dos discos rígidos diferentes.

El nivel 1 de RAID utiliza la duplicación de los datos para proporcionar tolerancia a fallos.

Los niveles 3, 4 y 5 usan información "de paridad" que es calculada con los patrones de bits de los datos grabados en la matriz RAID para proporcionar tolerancia a fallos. Cuando un disco rígido falla en el RAID 3, 4 o 5, la información de paridad puede ser usada junto con los datos en los discos restantes en la matriz para calcular los datos que estaban en el disco que falló. Esto permite que el subsistema de discos y el servidor de red sigan funcionando, aunque serán un poco más lentos debido a los cálculos requeridos para recrear los datos perdidos.

El nivel 2 del RAID es estructuralmente diferente ya que no utiliza duplicación o paridad para proporcionar tolerancia a fallos. RAID 2 utiliza en cambio un "código hamming" especial.

Controladoras RAID

Las controladoras RAID son controladoras de disco especializadas que utilizan tecnologías ATA o SCSI. Las controladoras RAID ATA están limitadas en la cantidad de discos que pueden ser conectados a ellas debido a las limitaciones del canal ATA, que tiene un máximo de dos canales con un máximo de dos discos por canal (lo que





da un total de cuatros discos). Las controladoras RAID SCSI tienen múltiples canales. Las de dos canales son comunes. Las controladoras RAID con tres, cuatro y cinco canales están disponibles. Las controladoras RAID son generalmente costosas debido a la sofisticación que deben contener.

Las controladoras RAID a menudo tienen una memoria cache onboard que va de los 4 MB a los 256 MB. Esta memoria cache onboard a menudo tiene un sistema de copia de respaldo a batería para evitar la pérdida de datos en el caso de una pérdida de energía repentina en el servidor de la red. Esto es crítico porque los datos grabados desde la memoria del sistema hasta la controladora RAID son grabados primero en la cache onboard y podrían pasar varios segundos antes de que los datos sean realmente grabados en el disco. Sin la batería que suministre energía a la controladora RAID, la memoria cache onboard podría ocasionar que los datos en el disco no sean actualizados con los datos actuales. Esto podría fácilmente provocar la pérdida de la integridad de los datos.

La memoria cache en la controladora RAID puede normalmente ser configurada como una cache de lectura, una cache de escritura, o una combinación de ambos. La cache de lectura mejorará el rendimiento de la lectura. La cache de escritura permitirá que el procesador continúe con otras tareas en lugar de esperar que los datos sean grabados en el disco.

Las siguientes características deberían ser consideradas cuando se evalúen las controladoras RAID:

- Cantidad de canales
- Velocidad de los canales
- Cache onboard cache (lectura, grabación, combinación, y opción de copia de respaldo a batería)
- Adaptador de host rápido (PCI)
- Ancho del bus (16 bit, 32 bit, y 64 bit)

RAID basado en hardware

RAID normalmente se implementa usando una controladora de disco RAID. Sin embargo, las controladoras de disco RAID son bastante costosas. RAID también puede ser implementado con software por varios sistemas operativos, incluyendo Novell NetWare, Linux Red Hat, Microsoft Windows NT, y Microsoft Windows 2000.

Cuando se utiliza la versión de RAID de Windows 2000, el disco rígido debe ser convertido en un disco dinámico para que las opciones de RAID estén disponibles para su implementación.

RAID basado en software

Los sistemas de RAID de software normalmente soportan RAID 0, 1 y 5. El RAID de software normalmente se implementa a nivel de partición de disco en lugar de a nivel de disco físico (el disco completo) como en el RAID de hardware. La desventaja del RAID de software es que necesita al procesador del servidor de red para realizar el trabajo que normalmente haría la controladora RAID en el RAID de hardware. El RAID 5 implementado en software necesita que el procesador calcule toda la información de paridad cuando graba los datos en la matriz de discos de RAID 5. El RAID 1 implementado en software pone una cantidad mínima de carga sobre el procesador del servidor de red.

El RAID basado en software tiene una ventaja sobre el RAID basado en hardware. En el RAID basado en software, la implementación de RAID puede estar basada en



particiones de discos en lugar de en discos completos. Por ejemplo, tres particiones de 10 GB en tres discos diferentes pueden ser usadas para crear una matriz RAID 5 de software. Podría haber espacio en diferentes particiones en cada uno de estos discos que podría utilizarse para algún otro propósito.

En casi todos los casos, el RAID basado en hardware es mejor que en RAID basado en software. Sin embargo, el implementar el RAID en software es mucho mejor que no tener ninguna tolerancia a fallos.

RAID 0

RAID 0, en realidad, no es un RAID en absoluto, ya que no proporciona ninguna redundancia. RAID 0 es sólo una matriz (o grupo) de discos usados como un único disco. Los datos son grabados en pedazos o tiras en todos los discos de la matriz. Esto mejora el rendimiento de entrada/salida del disco porque varios pedazos de datos se pueden escribir o leer simultáneamente. Si un disco en la matriz de RAID 0 falla, se pierden todos los datos en la matriz RAID 0. El nivel 0 del RAID también se llama a menudo striping de disco sin paridas.

RAID 1

RAID 1 necesita un mínimo de dos discos (todos los otros niveles de RAID, excepto el nivel 0, necesitan al menos tres discos) para implementarse. RAID 1 graba todos los datos en dos lugares separados. Para almacenar 20 gigabytes (GB) de datos usando RAID 1, se necesitan dos discos de 20 GB. Esto es una pérdida del 50% de la capacidad de disco.

Hay dos formas de implementar el RAID 1:

- Espejado (mirroring) de disco
- Duplexado (duplexing) de disco

En el espejado de disco, los dos discos son conectados a la misma controladora. El único problema con el espejado de disco es que si la controladora falla, no hay acceso a los datos espejados. Para eliminar este punto único de falla, se utiliza el duplexado de disco en lugar del espejado de disco.

En el duplexado de disco, cada disco en el conjunto espejado está conectado a una controladora diferente. Esto elimina el punto único de falla en el espejado de disco puro. El único costo adicional es el agregado de la controladora de disco.

RAID 2

RAID 2 utiliza un código hamming para crear un Código de Corrección de Error (Error Correcting Code – ECC) para que todos los datos almacenados en la matriz de RAID 2. El ECC puede detectar y corregir errores de bit único y detectar errores de bit doble. El código ECC tiene que ser leído y decodificado cada vez que los datos son leídos del disco. RAID 2 es muy difícil y costoso para implementar y tiene una sobrecarga muy alta (por ejemplo, 3 bits de paridad por cada 4 bits de datos).

Un código hamming es un método de corrección de errores que mezcla tres bits de chequeo al final de cada cuatro bits de datos. Cuando se reciben estos bits de chequeo, son utilizados para detectar y corregir errores de un bit automáticamente.

RAID 2 no tiene implementaciones comerciales debido a lo costosa y difícil que es su implementación. Requiere un mínimo de tres discos para implementarlo.



RAID 3

RAID 3 utiliza la paridad a nivel de bit con un único disco de paridad para proporcionar tolerancia a fallos a los datos almacenados en la matriz de RAID 3 en el caso que falle un disco de la matriz. RAID 3 requiere que todos los discos en la matriz estén sincronizados entre sí. Los bits de datos y la información de paridad calculada de los datos son grabados en todos los discos de la matriz simultáneamente. RAID 3 requiere un mínimo de 3 discos para crear una matriz.

RAID 4

RAID 4 utiliza la paridad a nivel de bloque con un único disco de paridad para proporcionar tolerancia a fallos a la matriz de RAID 4 en el caso de falla de un disco en la matriz. En una matriz de RAID 4, los datos y la información de paridad calculada de los datos son grabados en los discos en forma de bloques. No hay necesidad de que los discos estén sincronizados, y los discos pueden ser accedidos en forma independiente. Se necesita un mínimo de tres discos para crear la matriz. El problema con RAID 4 es que el disco de paridad es accedido en cada operación de grabación de la matriz RAID. Esto provocará un uso pesado del disco de paridad, el que probablemente falle antes que los otros discos en la matriz.

RAID 5

RAID 5 utiliza paridad a nivel de bloque, pero distribuye la información de paridad entre todos los discos de la matriz. Esto elimina la falla de paridad de disco común en los sistemas RAID 4. La pérdida de capacidad de almacenamiento en los sistemas RAID 5 es equivalente a la capacidad de almacenamiento de uno de los discos. Si hay tres discos de 10 GB en una matriz RAID 5, la capacidad de almacenamiento de la matriz será de 20 GB (una pérdida de 1/3, o 33%). En otro ejemplo, si hay siete discos de 10 GB en una matriz RAID 5, la capacidad de almacenamiento total de la matriz será de 60 GB (una pérdida de 1/6, o 16,67%).

RAID 0/1

RAID 0/1 también se conoce como RAID 0+1 y a veces es llamada RAID 10. Esta combinación de RAIDs proporciona lo mejor de ambos mundos. Tiene la performance de RAID 0 y la redundancia de RAID 1. RAID 0/1 necesita al menos cuatro discos para su implementación. En RAID 0/1, hay dos conjuntos stripe de RAID 0 (usados para proporcionar alto rendimiento de entrada/salida) que son espejados (lo que proporciona tolerancia a fallos).

3 Instalación de un sistema operativo de red

3.1 Introducción

La instalación de un Sistema Operativo de Red (NOS) hace referencia al proceso de creación y copiado de los archivos del sistema NOS en un disco rígido. Los archivos del sistema son los archivos que permiten que el sistema operativo funcione. Muchos fabricantes venden las computadoras con el sistema operativo ya instalado. Esto es especialmente cierto con las computadoras de escritorio.

Los Sistemas Operativos (OS) o software de NOS pre-instalados tienen varias ventajas. Al comprar una PC o servidor con un OS pre-instalado, un cliente evita el proceso complejo de instalación y configuración. Además, un OS que está pre-cargado en un sistema normalmente está optimizado para esa configuración de hardware en particular.





La desventaja de la pre-instalación es que un cliente puede no poder controlar las características, paquetes y configuraciones exactas del OS o NOS. Mientras que es posible hacer cambios a un OS después del proceso de instalación, hay algunas configuraciones que no pueden deshacerse o que sólo pueden ser modificadas con extrema dificultad.

A pesar de estas desventajas, algunos clientes pueden querer que el fabricante del servidor instale un NOS antes de vender el sistema. Sin embargo, la mayoría de las organizaciones instalan los NOS ellas mismas. La instalación en casa asegura que el servidor está optimizado para las funciones específicas de la organización. Además, los administradores del NOS normalmente prefieren tener un control directo de las versiones, actualizaciones y patches del software instalados en el sistema.

3.2 Planeamiento del sistema

La instalación del NOS debería ser preparada con cuidado. Primero, el inventario del hardware del sistema. No hay un NOS que funcione con todo el hardware de computadora, por lo que debe determinar si el hardware actualmente disponible funcionará con el NOS. Segundo, determine si el NOS soporta o no todo el software de aplicación que será cargado en el sistema. Tercero, familiarícese con el NOS mismo. Como parte del proceso de instalación, tendrá que tomar decisiones de configuraciones importantes (y a veces irreversibles).

Cada fabricante de NOS fija lo que se llama "requisitos mínimos de hardware" para su software. Los requisitos mínimos de hardware normalmente apuntan al tipo y velocidad de la Unidad Central de Proceso (Central Processing Unit – CPU), cantidad de RAM, y la cantidad de espacio en disco disponible.

Es relativamente fácil determinar si un sistema concuerda o no con los requisitos mínimos del NOS. También determine si el NOS puede soportar los periféricos de hardware del sistema. Esto es especialmente importante para periféricos costosos o de misión crítica como equipo de video alto perfil o hardware de almacenamiento de alta capacidad.

Cuando planifique instalar un NOS, realice un inventario completo del hardware. En entornos de producción, se debería reunir un inventario formal y escrito. Una vez terminado, revise los sitios web de fabricantes, personal de soporte e incluso grupos de noticias para determinar si el hardware inventariado es soportado. Puede ser necesario bajar e instalar actualizaciones de firmware o drivers de software antes de que el hardware funcione correctamente con el NOS.

Realice un inventario de todas las aplicaciones que funcionarán en el servidor mismo. Si la organización depende de software personalizado o software heredado, consulte a los fabricantes para asegurar la compatibilidad. El software es considerado heredado si es viejo y no puede ser actualizado, pero aun está en uso porque algunos componentes de la red necesitan los servicios que este software proporciona. La mayoría de los administradores eligen cargar y probar las aplicaciones en el NOS antes de introducir un NOS en una red.

Finalmente, conozca lo básico acerca de un NOS en particular antes de instalarlo. Por ejemplo, sepa cómo un NOS en particular manipula la partición de las unidades, el formateo de los discos, y las cuentas administrativas.





Lo que sigue es una lista de la planificación de un sistema:

- Realice el inventario del hardware del sistema y determine la compatibilidad con el NOS.
- Verifique que todas las aplicaciones de software deseadas sean soportadas por el NOS.
- Investigue el NOS y familiarícese con el procedimiento de instalación antes de instalarlo realmente.

3.3 Planeamiento de la instalación

El primer paso que el especialista en hardware de servidor debería realizar es verificar que todo lo especificado en el plan de instalación esté listo y disponible antes de comenzar la instalación.

Las actividades de verificación son las siguientes:

- Verificar que el lugar donde el servidor será instalado está listo para la instalación.
- Verificar que el conector de electricidad para el servidor de red está disponible y activo. (Revíselo con un voltímetro.)
- Verifique que la conexión de red está disponible y activa.
- Verifique que todo el hardware para el servidor de red ha llegado y que el hardware es el especificado en el plan de instalación.
- Verificación del sitio de la instalación

Después de leer y verificar el plan de instalación, el especialista de hardware de servidor debería visitar el sitio de la instalación y verificar que esté preparado. Una de las primeras cosas a observar es la habitación misma. La habitación necesita ser modificada para asegurar que la vida del servidor no sea limitada. Las dos cosas que tienen el mayor impacto en el servidor son la humedad y la temperatura. La disponibilidad de energía, el espacio en el piso y las medidas contra inundación e incendio son algunos otros elementos que necesitan ser revisados antes de comenzar.

Verificación de la energía

El especialista en hardware de servidor debería verificar que la energía necesaria para el servidor de red está realmente disponible y viva. Asegúrese de revisar que el voltaje para la fuente de energía es el correcto usando un voltímetro o un multímetro digital. La fuente de energía también debería estar en un circuito de energía en sí misma. También revise que la fuente de energía tenga el tipo de amperaje correcto y que el conector tenga la configuración correcta. Como la fuente de energía ininterrumpida (uninterruptible power supply – UPS) es el componente que va a ser conectado a la fuente de energía, esta información puede encontrarse en la documentación de la UPS. La UPS puede necesitar un circuito de 20 A o 30 A, en lugar del circuito más común de 15 A. La UPS también puede tener un conector de energía especial, el que por supuesto requerirá un socket de energía especial.

Verificación del tamaño de la UPS

La UPS debería tener un tamaño adecuado para mantener al servidor de red funcionando lo suficiente como para que realice un apagado normal. Este tiempo es normalmente de 5 a 10 minutos. Una UPS de menor tamaño mantendrá al servidor funcionando sólo un tiempo muy corto. Una UPS de tamaño mayor no sólo mantendrá al servidor de red operativo por un tiempo mayor durante un corte de energía sino que también permitirá el crecimiento del servidor de red (el agregado de componentes al servidor de red con el paso del tiempo). La UPS debería ser lo bastante grande como





para soportar a todos los componentes del servidor de red que están conectados a la UPS. El tamaño de una UPS está especificado con una clasificación de volt-amp (VA). Cuanto más grande es la clasificación VA de la UPS, por más tiempo puede mantener funcionando al servidor de red en el caso de una falla de energía. Una gran cantidad de VA también permite que se agreguen componentes adicionales al servidor de red.

Temperatura adecuada en una habitación de servidor

El lugar debería tener una capacidad adecuada de acondicionamiento del aire para soportar al servidor de red a ser instalado. El plan de instalación debería indicar la salida de calor de los dispositivos que serán parte de la instalación del servidor de red (chasis, monitor, UPS, etc). Puede ser difícil averiguar la carga de calor real (medida en Unidades Térmicas Británicas – British Thermal Units – BTUs) de la habitación donde el servidor de red será instalado. Un indicador adecuado de la capacidad de refrigeración disponible de la habitación donde será instalado el servidor de red es la temperatura de la habitación. Si la temperatura de la habitación es mayor a 22 grados Celsius sin el servidor de red a instalar, es dudoso que haya una refrigeración adecuada para el servidor de red. Por esto que es una buena idea tener una unidad de aire acondicionado dedicada sólo para la habitación del servidor.

La mayoría de los servidores de red utilizan ventiladores internos para la refrigeración. Para que estos ventiladores funcionen adecuadamente y proporcionen una refrigeración correcta tiene que haber un espacio despejado alrededor del servidor para el flujo de aire apropiado. De acuerdo con la mayoría de las especificaciones, un área de 90 centímetros adelante y atrás del servidor proporcionará una refrigeración adecuada. Esto permitirá que el flujo de aire apropiado y la temperatura pasen a través del servidor.

Verificación de la conexión de red

El tipo y velocidad correctos de la conexión al servidor necesitan ser determinados antes de la instalación real del servidor. El usuario puede revisar esto usando otra computadora con el adaptador de red apropiado instalado para ver si la conexión de red que utilizará el servidor de red está funcionando y es la correcta.

3.4 Listas de compatibilidad de hardware

El inventario de hardware debería ser creado antes de ejecutar cualquier programa de instalación o antes de intentar preparar el disco rígido para la instalación. Si es necesario, abra el gabinete del sistema y examine las tarjetas de expansión para determinar el fabricante y el chipset usado. Si el sistema trajo manuales, consúltelos también. Finalmente, si otro sistema operativo ya está instalado en el sistema, utilice los utilitarios de sistema, como el Administrador de Dispositivos de Windows, para obtener información sobre el hardware instalado.

El inventario de hardware debería incluir la siguiente información para cada dispositivo:

- Tipo de dispositivo
- Fabricante
- Número de modelo
- Versión del driver de dispositivo
- Número de revisión del BIOS

Un inventario de hardware también contiene una lista de todas las tarjetas de expansión y dispositivos periféricos conectados al sistema.



Algunas instalaciones pueden necesitar más detalles sobre el hardware, como el slot donde se ubica una tarjeta de expansión, o incluso la configuración de los jumpers en una tarjeta en particular. La mayor parte de esta información puede ser obtenida usando un utilitario como el Administrador de Dispositivos.

Las últimas versiones de la mayor parte del hardware y NOSs utilizan diferentes métodos para detectar y configurar automáticamente el hardware. Sin embargo, las tarjetas de expansión y el software viejos pueden no ser compatibles con estos métodos de detección automática, como Plug and Play. En algunos casos, será necesario inspeccionar físicamente la tarjeta de expansión para registrar su configuración de jumpers y número de slot.

Después de terminar el inventario del hardware, compárelo con el NOS y los fabricantes de hardware para verificar que el hardware es compatible con el NOS. Aunque los manuales del hardware y el software pueden tener información de compatibilidad, la fuente más actualizada para esta información es la World Wide Web.

El sitio web del fabricante del hardware proporciona la última información sobre una tarjeta de expansión o periférico en particular. Estos sitios web normalmente incluyen drivers de software, actualizaciones de firmware y, si es aplicable, información sobre la configuración de los jumpers.

4 Proceso de instalación

4.1 Medio de instalación

Después de seleccionar el NOS que concuerda con los requisitos de red y de hardware, se debe determinar el medio de instalación, como un CD-ROM, la red, o diskettes. Normalmente, un NOS se instala usando un CD-ROM que contiene los archivos de sistema y un programa de instalación. En algunos casos, un NOS se instala por medio de diskettes. La instalación usando diskettes se ha convertido en algo cada vez menos frecuente a medida en que los sistemas operativos han crecido en tamaño y que las unidades de CD-ROM se han convertido en un estándar de prácticamente todos los modelos de PC.

Si está disponible una conexión a Internet de alta velocidad, puede ser posible instalar una versión de Windows, UNIX o Linux sobre una red. Con una conexión LAN, es posible instalar la mayoría de los NOS usando la red local.

A continuación se resumen los métodos de instalación más comunes.

CD ROMs de inicio

Si el sistema tiene una unidad de CD-ROM y puede ser iniciado desde el CD, se puede realizar una instalación desde el CD-ROM local. Este método es relativamente rápido y es el método de instalación más simple. Puede ser necesario bajar patches y otras actualizaciones desde el sitio web del fabricante antes de colocar a la computadora en funcionamiento.

Diskette de inicio y CD-ROM

Si el sistema tiene una unidad de CD-ROM pero no puede ser iniciado desde el CD, aun se puede realizar una instalación desde el CD-ROM local después de iniciar desde un diskette (o, en algunos casos, desde un disco rígido). Cuando inicia desde un diskette, asegúrese de que los drivers del CD-ROM son cargados desde el disco de inicio o desde alguna otra fuente. Sin los drivers de software, no se puede acceder al





CD-ROM. El inicio desde un diskette y luego la instalación desde un CD-ROM tiene las mismas ventajas y desventajas de iniciar directamente desde el CD, con la complicación agregada de la necesidad de crear el disco de inicio. La mayoría de los fabricantes de NOS proporcionan programas que crean los diskettes de instalación apropiados.

Sólo diskettes

Algunos de los NOSs más viejos o muy pequeños pueden ser cargados por completo desde una serie de diskettes. Una ventaja de este método es que no se requiere un CD-ROM. La desventaja obvia es que la copia de archivos desde múltiples diskettes es increíblemente lenta.

Diskette/Disco rígido/CD de inicio e instalación de red

En este caso, el sistema es iniciado por medio de un diskettes y el NOS es instalado luego desde un servidor de red local. Este método también puede ser usado cuando se inicia desde un disco rígido o CD. Las instalaciones de red pueden ser rápidas y convenientes, pero requieren una configuración y prueba compleja. Para que este método funcione, un administrador debe cargar una copia o imagen del NOS en un servidor y configurar el servidor para permitir el acceso del cliente. Normalmente, las instalaciones de red dependen de uno de los siguientes protocolos: Sistema de Archivos de Red (Network File System – NFS) o Procolo de Transferencia de Archivos (File Transfer Protocol – FTP). Unos pocos NOS tienen la opción de iniciar por medio de un diskette (o incluso de un CD-ROM) e instalar la última versión del NOS a través de Internet. La ventaja de este método es que se instala la última versión del NOS. Otra ventaja menor es que la instalación puede ser realizada aun si el sistema no tiene una unidad de CD-ROM. Sin embargo, este método requiere una conexión a Internet de velocidad relativamente alta. Además, la instalación a través de la Internet es normalmente compleja y no confiable.

Configuración de la BIOS

En especial con los motherboards más viejos y con los sistemas operativos más viejos, la configuración del Sistema Básico de Entrada y Salida (Basic Input Output System – BIOS) es una parte muy importante en el proceso de instalación. El sistema BIOS normalmente reside en la ROM del motherboard y es el primer programa ejecutado cuando se enciende una computadora. Es responsable de chequear los dispositivos de hardware usando un proceso llamado Autoprueba de Encendido (Power-On Self Test – POST). El BIOS también carga el sistema operativo desde varios medios, incluyendo disco rígido, diskettes y normalmente CD-ROMs.

Cuando se configuran sistemas viejos, la información sobre cada una de las unidades de disco se debe ingresar manualmente en el utilitario de configuración del BIOS. Con el hardware y los sistemas operativos que son nuevos o tienen sólo unos años, el sistema BIOS es capaz de detectar en forma automática las unidades de disco y otro hardware.

Para las instalaciones basadas en CD sobre estos sistemas nuevos, sólo una configuración del BIOS es importante: la que permite que el sistema se inicie desde el CD-ROM.

4.2 Programa de instalación

Un programa de instalación controla y simplifica el proceso de instalación.





Dependiendo del NOS, el programa de instalación solicita al usuario la información de configuración. La mayoría de los programas de instalación permiten la partición y el formateo del disco rígido antes de copiar los archivos del sistema.

En Windows, el programa de instalación es llamado setup.exe (instalar.exe). En un sistema Red Hat Linux, el programa de instalación actualmente se llama Anaconda.

Estos programas guían al usuario a través del proceso de instalación del NOS. El programa de instalación le hará al usuario una serie de preguntas, como por ejemplo el idioma y la disposición de teclado que debe usar.

Los programas de instalación también dan al usuario la opción de instalar un conjunto de componentes por defecto o de elegir cada componente en forma manual. El uso de una configuración por defecto simplifica el proceso de instalación y asegura que no se creará un sistema paralizado o que no funciona.

Si el servidor va a ser puesto en funcionamiento en la red, considere muy en especial una configuración personalizada. La elección manual de los componentes y características garantizará que el sistema esté construido para las tareas específicas requeridas en un entorno específico.

4.3 Partición de disco

Para usar en forma eficiente el espacio de almacenamiento de un disco rígido, el disco se divide en secciones llamadas particiones o partes. Cada partición, o parte, es una división lógica del disco rígido. Un disco puede tener una o más particiones.

Normalmente, un servidor de red es configurado con múltiples particiones antes de instalar el NOS. Un sistema con múltiples particiones de disco tiene las siguientes ventajas:

- Se pueden instalar múltiples sistemas operativos en el mismo disco.
- Los datos pueden ser separados físicamente de los archivos del sistema para proporcionar seguridad, administración de archivos y/o tolerancia a fallos.

Una partición específica, llamada partición de intercambio, puede ser creada para suplementar la RAM del sistema y mejorar el rendimiento.

Una vez que el disco está dividido en particiones, cada partición debe ser formateada para que los datos puedan ser almacenados allí. En un sistema Windows, las particiones formateadas en un disco rígido reciben una letra del alfabeto como nombre. La primera partición es nombrada con una C, la segunda partición, si está presente, es nombrada con una D, y así.

Hay tres tipos de particiones que pueden existir en un disco rígido. Una partición primaria es lo mismo que una partición original. Las particiones extendidas son variaciones de una partición primaria, que actúan como un contenedor para las particiones lógicas. Las particiones lógicas son particiones creadas dentro de las particiones extendidas. En cualquier sistema operativo, puede haber hasta cuatro particiones primarias o tres particiones primarias y una partición extendida.

La disposición de las particiones es almacenada en la tabla de particiones. La tabla de particiones está ubicada en el primer sector del disco rígido en el que está instalado el sistema operativo. Este sector del disco rígido se conoce como Registro Maestro de Inicio (Master Boot Record – MBR). Esta sección también contiene ciertos parámetros





y código, que la computadora necesita ejecutar después de que el BIOS se inicializa. Aunque las particiones lógicas están almacenadas dentro de la partición extendida, que está afuera del MBR, aun son consideradas parte de la tabla de particiones porque definen ubicaciones de partición.

Requisitos para las particiones de Linux

Linux manipula el esquema de partición primaria, extendida y lógica de forma un poco diferente que los otros sistemas operativos. Linux numera a sus particiones primaria y extendida del uno al cuatro y las particiones lógicas son numeradas del cinco en adelante. Por ejemplo, si el usuario creó dos particiones primarias y una partición extendida, las particiones primarias tendrán el número uno y dos respectivamente, y la partición extendida tendrá el número cuatro. La partición extendida será numerada cuatro y no tres porque los números uno a tres están reservados para particiones primarias aun si no son utilizados. En el caso anterior, sólo hay dos particiones primarias creadas, por lo que sólo el número tres es omitido. Por otra parte, las particiones lógicas siempre se numeran 5, 6, 7, etc., sin importar la cantidad. Sin embargo las particiones lógicas siempre comenzarán con el cinco.

Linux tiene una partición raíz, que es la partición en la cual se instala el OS y desde la que se inicia la computadora. Como mínimo, Linux necesita tener al menos una partición para que el sistema operativo pueda ser instalado y que pueda iniciarse. La partición raíz también se identifica como /. Esto hace referencia a la partición raíz porque la estructura de archivos completa se identifica por su ubicación relativa a /.

Opciones de Partición

Cuando se particiona un disco en Linux además de en otros sistemas operativos, hay varias opciones y elecciones que están disponibles para el administrador. Hay varias ventajas que surgen de tener un disco rígido partido en lugar de solo una partición raíz gigante.

Discos múltiples

Cuando se instalan múltiples discos, el usuario debe crear por defecto más de una partición. El usuario debe crear al menos una partición en cada disco que está instalado. La ventaja de hacer esto es que la partición raíz puede ser instalada en un disco mientras que otro directorio, como el directorio /home, puede ser instalado en otro disco. Al colocar el directorio /home en otros discos se almacenaría allí todos los datos de los usuarios que son grabados en su directorio home y se lograría que esos datos sean salvados en el caso de que el disco con el directorio raíz falle.

Mejores opciones de seguridad

La partición de un disco rígido puede mejorar también la seguridad en la unidad. La seguridad en el acceso a una partición puede ser mayor o menor que la seguridad de acceso a otra. Por ejemplo, si el directorio /home fue ubicado en su propia partición, el administrador podría tener una seguridad más estricta para acceder a esa partición que contiene los directorios home de los usuarios.

Protección contra el exceso de datos

Cualquiera que utilice un sistema operativo ha aprendido que ocurrirán errores o ataques. A veces uno de estos errores puede causar que un archivo crezca continuamente hasta tamaños enormes tomando así todo el espacio de la partición y causando que el sistema de archivos se paralice o se caiga porque ya no puede crear más archivos o directorios en esa partición. La partición de un disco rígido puede ayudar a reducir la cantidad de daño producido y a veces permite que un administrador solucione el problema antes de que pueda causar mucho más daño.



Esto es porque se reduce la cantidad de espacio de disco rígido que este proceso desbocado puede consumir.

Protección de error de disco

La partición de un disco también puede ayudar en el caso de que un sector del disco rígido se dañe o que un virus corrompa una parte del disco rígido ya que el usuario sólo perderá los datos de ese disco rígido que no hayan tenido una copia de respaldo en algún otro lado. Si el usuario no había particionado el disco rígido entonces podría perder todos los datos del disco completo.

Sistema de archivos ideal

La partición de un disco puede ser útil en el caso en que el usuario necesita usar múltiples sistemas de archivos. El usuario puede tener un sistema de archivos en el cual está instalado el sistema operativo y éste se inicia y luego puede tener otro sistema de archivos en otra partición que podrían ser necesarios para que ciertos archivos o programas funcionen.

Dependiendo del OS, la partición se realiza antes de ejecutar el programa de instalación o desde el programa de instalación mismo. La partición puede realizarse manual o automáticamente. Muchos programas de instalación permiten la partición automática. Aunque esta opción es útil para los administradores novatos, puede no producir un sistema optimizado para necesidades específicas.

Para particionar manualmente un disco en forma efectiva, es importante conocer los tipos de particiones que son necesarios para el NOS. La forma en que el servidor será utilizado también dicta la forma en que el servidor es particionado. Por ejemplo, si se configura un servidor Linux para que sea un servidor de correo, tenga cuidado de asegurar que la partición apropiada sea lo suficientemente grande como para contener el correo no leído de todos los usuarios.

La información sobre la cantidad de particiones, sus tamaños, y sus ubicaciones en el disco es mantenida en el primer sector del disco. Esta información se llama tabla de particiones. Las tablas de particiones pueden tener uno de varios formatos, incluyendo DOS y BSD/Sun.

En sistemas que utilizan una tabla de particiones tipo DOS, como Windows y Linux, el primer sector del disco a veces se llama Registro Maestro de Inicio (Master Boot Record – MBR) o Sector Maestro de Inicio. Las tablas de particiones tipo DOS pueden describir hasta cuatro particiones primarias. En BSD y UNIX de Sun, el primer sector del disco rígido se llama etiqueta de disco o Tabla de Contenidos del Volumen (Volume Table of Contents – VTOC). La tabla de particiones tipo Sun puede describir hasta ocho particiones primarias.

La tabla de particiones incluye información que le dice al OS cuáles particiones son de inicio. Una partición de inicio es una partición que contiene un sistema operativo. Cuando se definen las particiones manualmente, una partición debe ser configurada de inicio para que se pueda iniciar el sistema desde allí. El MBR o etiqueta de disco contiene un programa que localiza el primer sector de un sistema operativo que sea capaz de iniciar y luego le pasa el control del sistema a ese OS.

Si el MBR o etiqueta de disco está corrupto o perdido, el sistema ya no se iniciará correctamente. Por esta razón, se debería mantener una copia del MBR/etiqueta de disco como respaldo en un diskette.





4.4 Herramientas de particionado

Antes de que un sistema operativo pueda ser instalado en un disco rígido éste debe ser correctamente particionado. Hay varias herramientas disponibles que permitirán a un usuario particionar un disco rígido. Sin embargo, sólo hay unas pocas que deberían usarse si el usuario está instalando Linux en el disco rígido.

FDISK

La mayoría de software de instalación de NOS incluye un programa llamado FDISK. FDISK es una abreviatura de disco fijo (fixed disk). Los programas FDISK están diseñados para manipular la tabla de partición de un disco rígido. Un programa FDISK puede ser usado para crear particiones, borrar particiones, y fijar particiones como "activas".

Microsoft proporciona una versión del programa FDISK que está disponible con facilidad. El programa proporciona medios basados en texto para crear particiones en un disco rígido que Linux puede usar.

Linux también proporciona una versión de FDISK. La versión de Linux de fdisk está basada en texto también pero proporciona medios más flexibles para particionar un disco rígido que la versión de Microsoft.

Herramientas de tiempo de instalación de Linux

Linux proporciona sus propias herramientas que pueden ser usadas cuando se instala un sistema sólo de Linux. Estas son herramientas de GUI que son mucho más fáciles de usar que el fdisk. Esta es probablemente la mejor forma y la más fácil de particionar un sistema Linux.

Herramientas de partición de terceros

Hay algunas herramientas de terceros que pueden ser usadas para particionar un sistema Linux. La herramienta más conocida para hacer esto es PartitionMagic de PowerQuest. PartitionMagic es una herramienta basada en GUI que puede ser usada para particionar un disco rígido formateado con una variedad de sistemas de archivos incluyendo FAT, NTFS, HPFS, ext2, y ext3. PartitionMagic está basado en DOS pero viene con un diskette que puede usarse en sistemas operativos que no sean Windows. Proporciona un medio excelente para particionar un disco que tiene más de un tipo de sistemas operativos o sistemas de archivos en él. PartitionMagic también es útil para hacer otras cosas. Puede ser usado para cambiar el tamaño de las particiones sin dañar los archivos dentro de la partición existente.

FIPS

El Primer Divisor de Particiones Interactivo No Destructivo (First Nondestructive Interactive Partitioning Splitting – FIPS) está incluido en el CD de instalación que viene con la mayoría de las distribuciones de Linux. FIPS es una gran herramienta de partición que puede ser usada para dividir una partición FAT en dos particiones. FIPS es más comúnmente usado en los sistemas Windows que necesitan hacer una partición separada para instalar Linux en ella. FIPS hace esto primero dividiendo la partición FAT existente. Luego el usuario puede borrar esa partición e instalar el Linux en esa nueva partición.

Pautas generales para particionar

Hay algunas reglas generales que es importante conocer cuando se particiona un disco rígido. El seguir estas reglas ahorrará mucho tiempo pasado en solucionar errores o reparando un sistema de archivos caído. Por lo general, cualquier OS puede



ser instalado en cualquier partición que sea creada por cualquier herramienta de partición, ya que la herramienta usa la tabla de partición estándar x86. Sin embargo, esto no siempre es así.

Hay dos reglas que se deben seguir cuando se particiona un disco rígido:

- Una buena idea es usar una herramienta de plataforma cruzada como PartitionMagic. Como se describió antes, esta herramienta de partición puede ser usada para partir un disco rígido que se va a usar con casi cualquier sistema operativo.
- Si no puede usar una herramienta de partición de terceros entonces la siguiente mejor idea es usar la herramienta de partición que viene con el OS. Linux y Windows 2000/XP vienen con sus propias herramientas de partición que se pueden usar durante la instalación del OS.

4.5 Archivos/particiones swap

Un archivo de intercambio es un área del disco rígido usada como memoria virtual. La memoria virtual es espacio de disco rígido que se utiliza para suplementar a la RAM. Los datos son grabados en el archivo de intercambio (también llamado archivo de paginación) cuando no hay suficiente RAM disponible. Los datos son luego intercambiados entre la RAM y el archivo de intercambio, como sea necesario. Si el sistema tiene suficiente RAM, el archivo de intercambio puede ser pequeño y no ser utilizado con frecuencia. Si el uso de la RAM aumenta, el archivo de intercambio puede crecer más y el intercambio se produciría con más frecuencia. Esto permite ejecutar programas que de otra forma el sistema no podría soportar.

Aunque Windows utiliza un archivo de intercambio, éste no tiene que ser configurado. El archivo de intercambio es creado como un archivo en la partición del NOS.

Los sistemas UNIX normalmente dedican una partición entera a espacio de intercambio. Esta partición, o parte, se llama partición de intercambio. El tamaño mínimo de la partición de intercambio debería ser igual o el doble que la RAM de la computadora.

Es importante administrar el uso del espacio de intercambio porque si el sistema comienza a agotar el espacio de intercambio el OS puede paralizarse.

Configuración de archivos de intercambio

Los sistemas operativos de red que usan memoria virtual (Windows NT, Windows 2000, UNIX y Linux) tienen un archivo de intercambio en la unidad de disco del servidor de red. Para un óptimo rendimiento, el archivo de intercambio debería ser instalado o movido a un disco físico diferente de la unidad de disco que contiene los archivos del sistema operativo, o los archivos de aplicaciones accedidas con frecuencia (como bases de datos). Las secciones siguientes identifican los nombres de los archivos de intercambio y los tamaños por defecto para varios sistemas operativos de red.

Windows 2000 Server

Los archivos por defecto del Microsoft Windows 2000 Server son los siguientes:

Nombre del archivo de intercambio: C:\PAGEFILE.SYS

Tamaño por defecto: 1,5 veces la cantidad de RAM en el servidor

Se permite un archivo de intercambio por volumen





Para cambiar la cantidad de archivos de paginación o para cambiar el tamaño de un archivo de paginación, seleccione el botón Inicio > Configuración > Panel de Control > Sistema > Avanzado > Opciones de Rendimiento > Cambiar Memoria Virtual

Linux

El uso del comando `free` permitirá al usuario revisar la memoria del sistema. Este comando mostrará el uso de la memoria total del sistema. Hay diferentes opciones que pueden ser usadas junto con este comando para manipular su salida.

Es difícil conseguir un estimado del uso del archivo de intercambio con sólo mirar esta salida por unos segundos. Se necesita hacer una mejor evaluación por un mayor tiempo cuando el sistema está siendo usado con regularidad. Una forma de hacer esto es capturar la salida y grabarla en un archivo de texto que puede ser leído y evaluado más tarde. Para hacer esto el usuario debería usar la opción `-s` junto con el comando > que redirigirá la salida hacia un archivo de texto.

El comando para hacer esto sería:
`free -s 900 > swapeval.txt`

Esto causaría que la salida sea mostrada por 900 segundos y luego la salida del uso del archivo de intercambio por un período de 900 segundos sería dirigida hacia un archivo de texto que podrá ser leído más tarde.

Agregado de un archivo de intercambio

Una forma de agregar espacio de intercambio es agregar un archivo de intercambio. La forma de agregar un archivo de intercambio a un sistema Linux se describe a continuación.

El primer paso que se necesita dar es crear un archivo que tomará el espacio igual al tamaño del archivo de intercambio que se va a crear. Para hacer esto, el usuario necesitará usar el comando `dd`. La salida es la siguiente:

```
# dd if=/dev/zero of=swap.swp bs=1024 count=131072
```

Este comando indica la cantidad de bytes que serán copiados desde `/dev/zero` y luego creará un archivo `swap.swp` que tiene un tamaño de 128 MB.

Luego, el archivo `swap.swp` que fue creado necesitará ser inicializado para que el sistema Linux pueda usarlo para intercambiar memoria al disco. Al usar el comando `mkswap` el usuario puede permitir que Linux utilice el nuevo archivo de intercambio pero no estará activo. La salida para este comando es la siguiente:

```
# mkswap /swap.swp
```

Para activar este archivo de intercambio el usuario necesitará usar el comando `swapon`. Para hacer desactivar este archivo de intercambio simplemente utilice el comando `swapoff` en lugar del comando `swapon`. La salida es:

```
# swapon /swap.swp
```

Este archivo de intercambio que fue recién creado no será usado la próxima vez que el sistema se reinicie a menos que se ingrese en `/etc/fstab`. El usuario necesitará listar en este archivo la ruta completa del lugar donde está ubicado el archivo de intercambio.



El agregado de espacio de intercambio usando este método es definitivamente la forma más rápida y fácil. Sin embargo, tiene algunas desventajas. Al crear este archivo de intercambio en una partición que ya está siendo usada, el archivo puede resultar fragmentado a medida que la partición es usada más y más. Esto causará que el archivo de intercambio se fragmente por toda la partición también, lo que degrada el rendimiento. La única opción alternativa que se puede usar es crear una partición de intercambio completamente nueva. Sin embargo, esto es mucho más complejo y no es recomendable a menos que sea absolutamente necesario.

4.6 Formateo

Después de que las particiones han sido creadas, necesitarán ser formateadas. Normalmente, el programa de instalación brindará las opciones de formato disponibles. Las particiones pueden ser formateadas con distintos utilitarios, como el FORMAT.EXE de Windows.

El proceso de formateo define el sistema de archivos de la partición. Dentro de cada partición, el sistema operativo mantiene un registro de todos los archivos que están almacenados allí. Cada archivo está en realidad almacenado en el disco rígido en uno o más clusters de espacio de disco de un tamaño uniforme predefinido.

Cuando formatee una partición en un NOS Windows, elija entre los siguientes sistemas de archivos:

- NTFS (Sistema de Archivos de Tecnología Nueva – New Technology File System). Recomendado para los servidores de red.
- FAT32
- FAT

Cuando formatee una partición UNIX o Linux, elija entre los siguientes sistemas de archivos:

- UFS (Sistema de Archivos de UNIX – UNIX File System)
- EXT3
- Otros sistemas de archivos importantes incluyen a HFS (Sistema de Archivos H – H File System), que se utiliza con OS/2.

4.7 Cuenta del administrador

Una de las partes más importantes de cualquier instalación de NOS es la creación de la cuenta del usuario administrativo. Como se dijo en capítulos anteriores, un NOS es un sistema multi-usuario. La cuenta administrativa tiene acceso irrestricto para crear y borrar usuarios y archivos. Por esta razón, la cuenta administrativa es llamada "cuenta de super usuario" en algunos sistemas.

Cuando se instala el NOS, el programa de instalación le pedirá al usuario que cree una cuenta administrativa. Como esta cuenta tiene todos los poderes, es crítico que se le asigne una clave "fuerte". Una clave es considerada fuerte cuando contiene ocho caracteres o más y no usa nombres o palabras reconocibles encontradas en un diccionario. Las claves fuertes también utilizan combinaciones de letras en minúscula y mayúscula, números y otros caracteres.



5 Instalación de Windows 2000

5.1 Instalación del sistema operativo

Requisitos para la instalación del Windows 2000

Hay algunas cosas a considerar antes de instalar el Windows 2000. Primero, asegúrese de que el hardware es capaz de ejecutar Windows 2000. Microsoft recomienda los siguientes requisitos antes de instalar el sistema operativo:

- Microprocesador Pentium 133 MHz o superior
- 64 MB de RAM
- Disco rígido de 2 GB o una partición con un mínimo de 1 GB de espacio libre
- Monitor VGA
- CD-ROM de 12X, mínimo
- Tarjeta de red

Microsoft tiene una herramienta llamada Lista de Compatibilidad de Hardware (Hardware Compatibility List – HCL) que se puede usar para verificar que el hardware realmente funcionará con el Windows 2000. Microsoft proporciona drivers probados sólo para los dispositivos que están incluidos en esta lista. El uso de hardware que no esté en la lista HCL podría causar problemas durante y después de la instalación. Esta HCL puede ser vista abriendo el archivo Hcl.txt en la carpeta Support en el CD-ROM del Windows 2000 Professional, o visitando el sitio oficial de la empresa.

Descripción de los pasos en la instalación del Windows 2000

Hay cuatro pasos principales en el proceso de instalación del Windows 2000. La instalación comienza cuando se ejecuta el programa Setup (Instalar). Esto prepara al disco rígido y copia los archivos. Setup luego ejecuta un asistente que proporciona páginas de información, que es usada para completar el resto de la instalación. Los cuatro pasos en el proceso de instalación del Windows 2000 son:

- El programa Setup
- El asistente del Setup
- Instalación del networking de Windows
- Terminación del programa Setup

El programa Setup

El primer paso del proceso de instalación es preparar el disco rígido para las otras etapas de la instalación. Se copian los archivos que son necesarios para ejecutar el asistente del setup y se muestra la parte de texto del setup. Puede comenzar la instalación del Windows 2000 usando los Discos de Inicio del Setup (Setup Boot Disks) o iniciando la máquina desde el CD-ROM.

Si se eligen los Disco de Inicio del Setup, inserte el primer disco en la computadora y enciéndala. Siga los pasos para insertar los otros tres discos para comenzar a copiar los archivos.

Puede ser mucho más fácil usar el CD-ROM del Windows 2000. Después de iniciar desde el CD-ROM, se copia una versión mínima del Windows 2000 en memoria, que es usada para ejecutar el programa Setup.

Aquí es donde comienza la parte basada en texto del Setup. El administrador hará lo siguiente:

- Leer y aceptar el acuerdo de licencia





- Reconfigurar las particiones del disco rígido o borrar una partición si fuera necesario
- Crear y formatear una nueva partición para instalar el Windows 2000 o reformatear una partición existente
- Seleccionar la FAT o la NTFS como el tipo de sistema de archivos

El Setup formateará luego la partición con el sistema de archivos seleccionado. El tipo de sistema de archivos seleccionado puede ser FAT o NTFS. Recuerde que la FAT puede ser convertida a NTFS pero la NTFS no puede ser convertida en FAT sin reinstalar el OS. Esta es una de las características de seguridad que proporciona la NTFS. Cuando instale el OS en una red, prefiera la NTFS a causa de la seguridad del sistema de archivos para el usuario y para el administrador del sistema. Una vez que la partición ha sido formateada, el programa Setup comenzará a copiar los archivos necesarios al disco rígido y grabará la información de configuración. Luego el Setup reiniciará en forma automática la computadora y ejecutará el asistente del Setup del Windows 2000. Por defecto, los archivos del sistema operativo del Windows 2000 son instalados en la carpeta C:\Winnt.

El asistente del Setup

El Asistente del Setup inicia la parte de Interface Gráfica del Usuario (Graphical User Interface – GUI) del proceso de instalación y guía al administrador a través de la siguiente etapa del proceso de instalación. Reúne información sobre el administrador, la organización y la computadora. Este paso instala las características de seguridad y configura los dispositivos del sistema. El administrador entonces será llevado por una serie de pantallas de configuración en las cuales el asistente del Setup del Windows 2000 pedirá la siguiente información:

- Configuración regional – Windows 2000 fue diseñado para ser un sistema operativo global. Aquí es donde se ingresa la información para personalizar el idioma, la ubicación, y la configuración del teclado. Windows 2000 puede ser configurado para utilizar múltiples idiomas y configuraciones regionales.
- Nombre y organización – Ingrese el nombre de la persona que va a ser el usuario de la computadora y la organización para la cual está licenciada esta copia del Windows 2000.
- Clave del Producto – Microsoft distribuye las copias del Windows 2000 con una Clave del Producto específica de 25 caracteres que normalmente se ubica en la parte trasera de la caja del CD.
- Nombre de la computadora – Cuando se conecta la computadora a una red, cada computadora en la red necesitará un nombre único para que pueda ser identificada en la red. Se debe ingresar un nombre de computadora. No puede ser más largo que 15 caracteres. El asistente del Setup de Windows 2000 mostrará un nombre por defecto, usando el nombre de la organización que fue ingresado anteriormente en el proceso del Setup, pero se recomienda cambiarlo.
- Password para la cuenta del Administrador – Windows 2000 tiene la capacidad de tener muchos perfiles diferentes para los usuarios de la computadora. También hay una cuenta administrador incorporada que incluye privilegios para hacer cualquier cambio en la computadora. En este punto el administrador debe suministrar la clave para la cuenta de administrador. Esta clave puede ser cambiada más tarde, pero sólo por el usuario que tiene privilegios administrativos locales al sistema.
- Información de discado de MODEM – Como las redes modernas utilizan LANs y tarjetas de red de alta velocidad, esta opción dependerá primero de si se usará un MODEM. La mayoría de las laptops aun los utilizan, por lo que podría ser necesario ingresar información aquí. Primero seleccione el país o región



donde está ubicada la computadora. A menudo esto ya está completado, en base a la configuración regional seleccionada. El área (o ciudad) de la ubicación de la computadora también debe ser ingresada al igual que el número para obtener una línea externa. Finalmente, seleccione si el sistema telefónico es de discado por pulso o por tono.

- Configuración de fecha y hora – Se debe especificar la fecha y hora además de uso horario. También se debe seleccionar si el Windows 2000 ajustará o no en forma automática el reloj de la computadora para los cambios de hora de verano.
- Instalación del networking de Windows
Como Windows 2000 fue diseñado para ser un Sistema Operativo de Red (NOS), la instalación de la configuración de red es un paso importante en el proceso de instalación. Después de reunir información sobre la computadora, el programa de Setup de Windows 2000 instalará en forma automática el software de red.

Windows 2000 instala los componentes de networking en una serie de pasos:

- Detección de las tarjetas adaptadoras de red – El sistema operativo necesita primero detectar las tarjetas de red. Si no hay tarjetas instaladas, este paso será salteado.
- Instalación de los componentes de networking – Hay archivos necesarios que deben ser instalados para permitir que la computadora se conecte con otras computadoras, redes y con Internet.
- El programa Setup le pide al administrador que elija entre usar una configuración típica o personalizada para configurar los siguientes componentes de networking. Si se elige típica, el sistema instalará la configuración por defecto. Al elegir la opción personalizada, el administrador puede ingresar la información que es específica a la red de la compañía. Por ejemplo, el Cliente para Redes Microsoft permite que la computadora tenga acceso a los recursos de la red. Compartir impresoras y archivos para redes Microsoft permite que otras computadoras tengan acceso a los recursos de archivos y de impresión además de permitir a la computadora local que tenga acceso a los archivos e impresoras compartidos de la red. TCP/IP es el protocolo de networking por defecto que permite que una computadora se conecte a Redes de Área Local (LAN) y a Redes de Área Amplia (WAN). En esta etapa se pueden instalar otros clientes, servicios y protocolos de red, como la Interface de Usuario Mejorada de NetBIOS (NetBEUI), AppleTalk, y el transporte compatible con NWLink IPX/SPX/NetBIOS llamado NWLink) si la red los requiere.
- Ingreso a un grupo de trabajo o dominio – El administrador necesita decidir si la computadora será parte o no de un dominio o grupo de trabajo. Esta información debería ser conocida antes de este paso. Si se crea una cuenta de computadora en el dominio para la computadora durante la instalación, el asistente del Setup de Windows 2000 le pedirá al administrador el nombre y la clave para unirse al dominio.
- Instalación de componentes – El último paso es instalar y configurar los componentes de networking que acaban de ser seleccionados.
- Terminación del programa Setup
Una vez que los componentes de networking han sido instalados, el asistente del Setup copia los archivos adicionales para configurar el Windows 2000. El programa Setup automáticamente iniciará el cuarto paso en el proceso de instalación.

Hay cuatro pasos básicos en la etapa final del proceso de instalación:



- Instalación de los ítems del menú Inicio – Donde se instalan todos los ítems de acceso directo que aparece en el menú Inicio
- Registro de componentes – Windows 2000 comienza a aplicar la configuración que fue especificada en el asistente del Setup de Windows 2000.
- Grabado de la configuración – Después de que se aplicó la configuración, ésta necesita ser grabada en el disco rígido para que sea usada cada vez que la computadora es encendida.
- Borrado de archivos temporales – Mientras el sistema operativo está siendo instalado, muchos archivos necesitaron ser copiados para que ejecuten estos pasos de la instalación. Después de la instalación, los archivos ya no son necesarios. El asistente del Setup borrará automáticamente estos archivos. Después de que este paso esté terminado la computadora se reiniciará automáticamente y el administrador puede entonces ingresar para terminar el procedimiento de instalación.

5.2 Interfaz de usuario/administrador

El primer paso para utilizar cualquier Sistema Operativo de Red (NOS) es ingresar al sistema. Windows 2000 implementa una Interface Gráfica del Usuario (GUI) y permite que un usuario ingrese al sistema usando la pantalla "Ingrese a Windows. Después de iniciar por primera vez la computadora con Windows 2000, puede pedirle al usuario que presione las teclas Ctrl, Alt y Supr simultáneamente para mostrar esta ventana. El nombre de usuario y la password requeridos pueden ingresarse en esta pantalla, además de información más detallada, como el dominio de red asignado al usuario. Por razones de seguridad, los caracteres de la clave son enmascarados con asteriscos (*) a medida que son escritos. Observe que tanto el nombre de usuario como la password son sensibles a las mayúsculas, y ambos deberían ser ingresados en forma exactamente igual a como el administrador del sistema los creó. Si alguno de los dos es incorrecto, el sistema le pedirá al usuario que reingrese la información de la cuenta hasta que sea correcta.

Windows 2000 tiene varios elementos básicos:

- Iconos
La característica más básica de Windows 2000, los iconos, son pequeñas imágenes con nombres de texto que se usan para representar funciones importantes. Al hacer doble click sobre un icono, el usuario invoca la función representada por ese icono. Por ejemplo, al hacer doble click en el icono "Mi PC" se abre una ventana de sistema, mientras que al hacer doble click en el icono "Internet Explorer" se ejecuta el programa Microsoft Internet Explorer. Otros iconos pueden representar archivos o documentos almacenados en la computadora, y al hacer doble click sobre ellos se ejecutará el programa apropiado y mostrará el contenido del archivo.
- Botones
Los botones en Windows 2000 son muy similares a los iconos con unas pocas diferencias importantes. Primero, los botones vienen en una variedad más amplia de formas y tamaños que los iconos estándar. Pueden tener sólo texto, sólo imagen, o texto e imagen. Normalmente están diseñados dentro de la interfase de una aplicación como un control para que el usuario realice una tarea específica. Ejemplos de usos de botones son confirmar una opción con un botón "Aceptar" y grabar un documento con un botón "Guardar".
- Ventanas
En los sistemas GUI más populares, los usuarios interactúan con el sistema a través de visualizaciones conocidas como "ventanas". La importancia de este



concepto (concebido por primera vez por Xerox y usado por Apple durante el principio de los '80) se refleja en el nombre dado a la línea de Microsoft de sistemas operativos. Una ventana funciona en forma muy parecida a su contraparte en el mundo real como un portal para ver otras áreas. En el caso de las GUIs, las ventanas le dan al usuario acceso a los datos y a las funciones programadas del sistema operativo y sus aplicaciones. Si un programa necesita la interacción del usuario, como lo hace la mayoría de las aplicaciones de Windows 2000, normalmente es mostrado en una ventana con controles para el ingreso del usuario. Se pueden ver múltiples ventanas simultáneamente distribuyéndolas y dándoles el tamaño necesario, permitiendo así que el usuario realice multitarea en forma más eficiente. En el caso de Windows 2000, el mismo OS tiene la responsabilidad de crear, administrar y cerrar estas ventanas.

- **Menús**
Una característica muy común de todos los programas que usan ventanas es el "menú". Estos grupos de botones de texto se encuentran normalmente en la parte superior de las ventanas y ofrecen funciones específicas relacionadas con esa ventana en particular. Por ejemplo, un programa procesador de texto puede tener un encabezado de menú llamado "Herramientas", bajo el cual hay una opción de menú llamada "Contar palabras". Las opciones del menú disponibles cambiarán de ventana a ventana además de entre diferentes secciones de la misma ventana. Los encabezados de menú más comunes son "Archivo" y "Edición", donde el usuario puede emitir comandos para abrir, cerrar y grabar documentos además de copiar y pegar datos. Otros menús importantes en Windows 2000 son el "menú Inicio" (haga clic en el botón Inicio ubicado en la barra de tareas) y el "menú de clic derecho" (encontrado haciendo clic derecho con el mouse sobre casi cualquier cosa).
- **Barra de tareas**
Normalmente encontrada en la parte inferior de la pantalla, la barra de tareas del Windows 2000 realiza muchas funciones importantes. El menú Inicio (para ejecutar aplicaciones) y la bandeja del sistema (que muestra los programas que corren en trasfondo y el reloj) están ubicados en la barra de tareas. Pero lo más importante es que la barra de tareas mantiene un registro de todas las ventanas abiertas. Un botón horizontal que muestra el icono y el título de la aplicación representa a cada ventana abierta. Los usuarios pueden hacer clic sobre estos botones para navegar entre las distintas ventanas y restaurar cualquiera de ellas que haya sido minimizada. Esta herramienta es particularmente útil para los usuarios que trabajan con muchas ventanas al mismo tiempo.

La última habilidad básica del Windows 2000 es la capacidad de apagar la PC. Esta opción está disponible bajo el comando "Apagar" del menú Inicio, donde los usuarios pueden también elegir "Cerrar sesión" y "Reiniciar" la computadora.

La interfase de Línea de Comando (Command-Line Interface – CLI) de Windows 2000 está basada en el antes popular sistema operativo MS-DOS de los '80. Ahora se lo llama "intérprete de comandos de Windows 2000" aunque muchos usuarios probablemente aun piensen en él como el clásico MS-DOS. A pesar de todo, su funcionalidad básica es prácticamente idéntica a la del MS-DOS con la excepción de unos pocos comandos nuevos agregados y a una gran cantidad de comandos obsoletos quitados. El intérprete de comandos corre sobre Windows 2000 para proporcionar a los usuarios todos los beneficios de un CLI dentro de la GUI de Windows 2000.



El intérprete de comandos en Windows 2000 puede ser ejecutado de distintas formas.

- En la barra de tareas, seleccione Inicio > Programas > Accesorios > Símbolo del Sistema.
- En la barra de tareas, seleccione Inicio > Ejecutar. En la caja "Abrir" escriba: cmd

Después de abrir una ventana de intérprete de comandos, el usuario recibirá un prompt para ingresar comandos. El prompt de comandos por defecto puede variar dependiendo de cómo es lanzado el intérprete de comandos, pero por lo general se verá similar a esto: C:\>. La apariencia del prompt de comandos puede cambiar, pero su función siempre será la misma. Es simplemente un lugar para que el usuario escriba comandos sobre la pantalla.

El proceso básico de ingresar comandos es muy simple. Escriba el comando en el prompt, presione la tecla ENTER, y vea la salida en la pantalla. Este proceso es el flujo estándar de la actividad del usuario para casi todos los sistemas CLI. Un comando útil para recordar es el comando doskey. No tiene salida, pero una vez que se ejecuta, el usuario puede presionar la flecha arriba en el teclado para desplazarse por los comandos ingresados previamente.

Si un usuario pasa mucho tiempo con el intérprete de comandos, otra herramienta útil es ejecutar la ventana en "modo de pantalla completa". Al presionar ALT + ENTER en el teclado, la ventana se ampliará para llenar toda la pantalla con el CLI de Windows 2000. Esto permite leer mucho mejor la interfase y es una reminiscencia de los días del MS-DOS. Para cerrar el intérprete de comandos de pantalla completa o de ventana, escriba el comando exit. Este comando cerrará de inmediato el intérprete y regresará al usuario a la GUI de Windows 2000 (el cerrar la ventana manualmente con el mouse es considerado inapropiado por el Windows 2000).

6 Administración de usuarios en Windows 2000

6.1 Usuarios

Antes de ingresar a cualquier cliente Windows 2000, se debe crear primero una cuenta de usuario en el servidor de red apropiado. Esta cuenta permitirá que el usuario ingrese a un dominio de red específico usando la información de cuenta creada por el administrador del sistema. La tarea de crear esta cuenta en Windows 2000 se realiza con la herramienta Administración de Equipos. Seleccione Inicio > Programas > Herramientas Administrativas > Administración de Equipos para mostrar esta ventana.

La herramienta Administración de Equipos permite que un administrador de sistemas administre todos los aspectos de una computadora en particular, incluyendo usuarios autorizados, y en el caso de un servidor de red, los usuarios autorizados de un dominio de red. Para crear un nuevo usuario para una máquina local, expanda el árbol de directorio a la izquierda para que aparezca "Herramientas del Sistema", "Usuarios Locales y Grupos". Haga clic sobre el icono Usuarios para mostrar todas las cuentas de usuarios existentes en la mitad derecha de la ventana. Bajo la acción o el menú con clic derecho, seleccione Usuario nuevo... para mostrar una pantalla que pide toda la información necesaria de la cuenta

El "Nombre de usuario" es un campo necesario. No puede tener más de 20 caracteres de largo, y no puede contener los siguientes símbolos:

/ \ [] : | < > + = ; , ? *





Tanto el "Nombre completo" como la "Descripción" son sólo para propósitos informativos y no son necesarios. Después de ingresar toda la información y presionar el botón Crear, el nuevo usuario será creado y puede ingresar inmediatamente a la computadora con el nombre y la clave especificada.

6.2 Creación de Grupos/Agregado de Usuarios

Windows 2000 permite que los administradores de sistemas creen grupos de muchos tipos y usos diferentes. Uno de tales tipos es "grupos locales". Un grupo local existe sólo en una única computadora y está formado por los distintos usuarios de esa computadora. Otros grupos más orientados a red encontrados en Windows 2000 son los "grupos globales", "grupos de dominio local" y "grupos universales". Los diferentes tipos de grupos varían en alcance y funcionalidad y son usados por los administradores de sistemas de Windows 2000 para administrar grandes cantidades de usuarios en una red. En contraste, los grupos locales no son usados en la red pero proporcionan un ejemplo suficiente sobre cómo usar grupos en Windows 2000.

Durante el proceso de instalación, Windows 2000 crea grupos locales por defecto como los grupos "Administrador" y "Usuarios". Cada uno de estos grupos tiene diferentes niveles de control sobre el sistema local. Además, los usuarios pueden crear nuevos grupos locales usando la herramienta Administración de Equipos (que se encuentra seleccionando Inicio > Programas > Herramientas Administrativas). Al expandir el árbol de directorio de la izquierda aparece la herramienta "Usuarios locales y Grupos", donde la carpeta "Grupos" muestra todos los grupos existentes en el sistema. Usando el botón derecho o el menú Acción de esta ventana el usuario podrá seleccionar la opción de menú Grupo Nuevo. Después de especificar un nombre, descripción y miembros, el grupo será agregado al sistema local. Cualquier usuario listado como miembro tendrá los mismos permisos de acceso y restricciones que ese grupo. Para agregar más usuarios, cambiar el nombre o eliminar el grupo, simplemente haga clic derecho sobre el nombre del grupo en la ventana y seleccione la opción de menú apropiada.

6.3 Administración de las Cuentas de Usuario

La herramienta Administración de Equipos es el medio principal por medio del cual un administrador de sistemas agrega y administra usuarios en el Windows 2000. Estas tareas deberían ser mucho más intuitivas en este entorno GUI que en uno CLI como el Linux. En lugar de memorizar nombres de comando, los usuarios de Windows 2000 pueden realizar estas operaciones de muchas formas distintas, desde simples selecciones de menú hasta comandos de teclado.

La técnica más simple de administración de usuarios es hacer clic derecho sobre el nombre de usuario listado en la mitad derecha de la ventana de Administración de Equipos y seleccionar la tarea apropiada en el menú. Desde aquí, el administrador del sistema puede elegir en forma instantánea Establecer contraseña, Eliminar, o Cambiar nombre al usuario. La cuenta también puede ser deshabilitada seleccionando Propiedades y la opción Cuenta deshabilitada. Estas y otras opciones de administración se pueden encontrar navegando por los menús restantes de la ventana.

Se debe ser sumamente cuidadoso cuando utiliza la opción "Eliminar" ya que no hay forma de deshacer ese cambio.





6.4 Passwords y Permisos

El mantenimiento de una red de incontables usuarios puede presentar problemas de seguridad para un administrador de sistemas. Como se mencionó anteriormente, la seguridad es una de las principales consideraciones para todos los administradores de sistemas, y se deben tomar las medidas necesarias para impedir que los usuarios abusen o interfieran accidentalmente con las operaciones de la red. Las herramientas de seguridad básicas relacionadas con los usuarios que están disponibles para el administrador son las claves y los permisos.

En la sociedad basada en Internet de hoy, la mayoría de los usuarios comprenden fácilmente el concepto de password. Una password es un grupo secreto de caracteres que sólo conoce un usuario. Todos los usuarios tienen su propia password, que a menudo es elegida por el mismo usuario para que pueda recordarla fácilmente (en oposición a las passwords generadas en forma aleatoria que pueden ser difíciles de recordar). Las passwords son usadas junto con un nombre de usuario cuando se ingresa a un NOS para verificar la identidad del usuario. Una buena password tendrá al menos cinco caracteres de longitud y será alfanumérica (incluirá una combinación de letras y números o caracteres especiales).

Las passwords no necesitan necesariamente ser únicas entre los usuarios pero deberían mantenerse en secreto para mantener la seguridad de la red. Los administradores de sistemas a menudo necesitan que las passwords sean cambiadas con frecuencia. Sin embargo, si la password de un usuario se hace pública, cualquiera podría usarla para ingresar a la red y operar bajo la identidad de ese usuario y con su nivel de acceso. Este peligro es una gran preocupación para los administradores de sistemas, que intentan controlar tales accesos a través del uso de "permisos".

6.5 Tipos de permisos

Los permisos son restricciones creadas por el administrador del sistema que habilitan y deshabilitan las acciones que un usuario puede ejecutar en la red. Por ejemplo, un administrador de sistemas normalmente tiene todos los permisos, es decir, no tiene restricciones, y conserva el acceso pleno a todas partes de la red. Un ejecutivo financiero puede tener un control total sobre ciertos directorios financieros en un servidor pero no tiene el control sobre los datos de recursos humanos. Esta división del acceso refuerza la seguridad de la red, ya que cada usuario sólo tiene acceso a áreas específicas y necesarias.

Los permisos son asignados a los usuarios durante el proceso de creación de la cuenta y están normalmente divididos en las siguientes categorías:

- Permiso de lectura – La capacidad de leer el contenido de un archivo o directorio.
- Permiso de escritura – También llamado permiso de "cambio" o "modificación". Esto permite al usuario editar y grabar los cambios a un archivo o agregar y borrar archivos de un directorio.
- Permiso de ejecución – Permite que el usuario ejecute un archivo o ingrese a un directorio.

Los permisos de arriba normalmente pueden ser asignados a usuarios individuales o a grupos de usuarios en cualquier combinación. Por ejemplo, un ejecutivo financiero puede tener permitido ingresar y ver el contenido de un directorio de recursos humanos (permisos de ejecución y lectura) pero no puede modificar el directorio o grabar cambios a cualquiera de sus archivos (permiso de escritura). Los permisos





proporcionan una herramienta efectiva a los administradores de sistemas para reforzar la seguridad en la red.

7 Active Directory

7.1 Introducción

Con el lanzamiento del Windows 2000 Servidor, Microsoft realizó cambios fundamentales en sus componentes. El Active Directory es el punto central de estos cambios. El Active Directory de Microsoft funciona como una aplicación que está profundamente integrada con el sistema operativo.

7.2 Estructura de la base de datos del Active Directory

La información del Active Directory está almacenada en tres archivos:

- Base de datos del Active Directory
- Archivos de registro del Active Directory
- Volumen del Sistema Compartido

La base de datos es el directorio. Los archivos de registro guardan los cambios hechos a la base de datos. El Volumen del Sistema Compartido (llamado Sysvol) contiene scripts y objetos de política de grupos sobre los controladores de dominio del Windows 2000. La Política de Grupos es el medio por el cual los administradores de Windows 2000 controlan los escritorios de los usuarios, ejecutan aplicaciones automáticamente, y fijan los derechos de los usuarios.

7.3 Dominios del Windows 2000

La estructura lógica del Active Directory está basada en unidades llamadas dominios. Aunque se utiliza la misma terminología, los dominios en Windows 2000 funcionan en forma diferente a los de Windows NT. Tanto en Windows NT como en Windows 2000, un dominio representa un recinto administrativo asegurado, además de una unidad de reproducción. Sin embargo, Windows NT utiliza una estructura de dominio plana, y Windows 2000 organiza los dominios en árboles de dominios jerárquicos.

Las redes de Windows 2000 pueden tener múltiples dominios, organizados en árboles de dominios. Además, estos árboles pueden ser unidos a otros árboles para formar bosques. Bosque es el término que utiliza Microsoft para llamar a una colección de árboles de dominio diferentes que está incluido en la estructura jerárquica del Active Directory.

7.4 Unidades Organizativas (OUs) de Windows 2000

El Active Directory, utiliza Unidades Organizativas (OUs) para organizar los recursos en dominios. La autoridad administrativa puede ser delegada a OUs individuales. En contraste, el networking de NT permite que los privilegios administrativos sean asignados sólo a nivel de dominio.

7.5 El Active Directory y el DNS

El Active Directory utiliza las convenciones de nombres del Servicio de Nombre de Dominio (Domain Name Services – DNS) y depende del DNS para funcionar. Debe haber un servidor DNS en cada red de Windows 2000. Además, las actualizaciones de información zonal de DNS pueden ser integradas con la reproducción del Active Directory, lo que es más eficiente que los métodos tradicionales de actualización de DNS.



Windows 2000 soporta DNS Dinámica (Dynamic DNS – DDNS), lo que permite la actualización automática de la base de datos DNS.

7.6 Servidores de Active Directory

Para utilizar el Active Directory, se debe configurar al menos un servidor como Controlador de Dominio (Domain Controller – DC). Se recomienda que haya al menos dos DCs en cada dominio, para tolerancia a fallos. La configuración del primer controlador de dominio en la red crea el directorio para ese dominio.

A diferencia de los servidores Windows NT, los Windows 2000 Servers que están ejecutando Active Directory no tienen un controlador de dominio primario (Primary domain controller – PDC) o un controlador de dominio de respaldo (Back-up domain controller – BDC). En los dominios de Windows NT, sólo el PDC contiene una copia completa para lectura/escritura del directorio de las cuentas de usuarios e información de seguridad. El PDC autentica los nombres de usuario y passwords cuando los miembros ingresan a la red. El BDC mantiene una copia de sólo lectura del directorio maestro de PDC y por lo tanto cualquier cambio necesitaría ser hecho en el PDC.

Los servidores de Windows 2000 que están ejecutando Active Directory presentan el concepto de controlador de dominio un poco diferente. A diferencia del Windows NT Server, donde un PDC debe estar accesible para hacer cambios en el directorio, el Windows 2000 Server depende del modelo de reproducción multimaster de Active Directory para actualizar a todos los controladores de dominio dentro del Bosque cuando se hace un cambio en cualquier otro controlador de dominio. No hay PDC ni BDC. Todos los controladores de dominio son iguales. Todos los Controladores de Dominio contienen una copia de lectura/escritura de la partición Active Directory. Esta información es mantenida actualizada y sincronizada a través del proceso de reproducción.

7.7 Reproducción del Active Directory

La reproducción es el proceso de copiar datos de una computadora a una o más computadoras y sincronizar esos datos para que sean idénticos en todos los sistemas. El Active Directory utiliza la reproducción multimaster para copiar información de directorio entre los controladores de dominio en un dominio. Los cambios pueden realizarse en cualquier controlador de dominio, y esos cambios son luego reproducidos en los otros.

Los administradores de Windows 2000 pueden establecer políticas de relaciones que determinan cuándo y cuán a menudo se realizan las reproducciones del directorio. Esto permite un uso óptimo del ancho de banda de la red. El control del esquema de reproducción es especialmente importante cuando los controladores de dominio están ubicados en lados opuestos de un enlace lento, como un enlace WAN de 56K.

7.8 Seguridad del Active Directory

Cada objeto en el Active Directory tiene una Lista de Control de Acceso (Access Control List – ACL) que contiene todos los permisos de acceso asociados con ese objeto. Los permisos pueden ser permitidos o denegados explícitamente, o en una base granular.

Hay dos tipos diferentes de permisos:

- Permisos asignados – Permisos otorgados en forma explícita por un usuario autorizado



- Permisos heredados – Permisos que se aplican a objetos hijos porque fueron heredados de un objeto padre

Los permisos pueden ser asignados a un usuario individual o a un grupo de usuarios. Windows 2000 permite que los administradores controlen este proceso.

7.9 Compatibilidad del Active Directory

El Active Directory es independiente del sistema operativo y corre sólo en los servidores de Windows 2000. Como el Active Directory es compatible con LDAP, los servicios y la información pueden ser accedidos o intercambiados con otros servicios de directorio LDAP.

8 Instalación de un sistema operativo Linux

8.1 Selección de los parámetros apropiados para la instalación

Estos son los primeros pasos que se deben realizar después de que ha sido seleccionado el método de instalación apropiado y de que el sistema ha sido iniciado. Algunas de las primeras pantallas mostradas darán opciones para seleccionar ciertos parámetros para el sistema operativo. Estas opciones incluyen cosas como el idioma que será usado, y la fase de detección de hardware. Todos estos procedimientos proporcionan un medio para aplicar ciertos parámetros que el sistema necesitará saber para que el sistema pueda ser preparado para la fase siguiente, que será seleccionar los paquetes apropiados para instalar.

Idioma

Una de las primeras opciones que se mostrará será la elección del idioma que será utilizado. Este debería ser un paso bastante simple. Obviamente la elección a hacer aquí sería seleccionar el idioma de la persona que estará usando el sistema o el idioma de la persona que está instalando el OS en la computadora.

Términos de la Licencia

Aunque no es tan estricto con Linux como podría ser con otros sistemas operativos como Microsoft, los términos de la licencia son importantes y por eso es importante que la persona que está haciendo la instalación lea estos términos. Aunque Linux es código abierto hay veces en que puede haber software propietario dentro de la distribución. Por lo tanto, si no se siguen los términos de este acuerdo de licencia podría haber la posibilidad de violaciones de copyright.

Clase de instalación

Una vez que los términos de la licencia han sido aceptados, el paso siguiente será seleccionar el tipo de instalación a realizar. Dependiendo de cuál distribución está siendo instalada, esta fase será diferente hasta cierto punto. Algunas distribuciones pedirán seleccionar una instalación recomendada o experta en este punto. Otras distribuciones, como Red Hat, darán la opción de elegir entre una Instalación de Estación de Trabajo, Servidor o Personalizada. Cuando se instala Linux por primera vez, elegir el tipo de instalación recomendado puede ser el método más sencillo. Sin embargo, al optar por este método, no habrá opciones para elegir con respecto al tipo de instalación que se está haciendo. Por ejemplo, si elige la opción de estación de trabajo en Red Hat, entonces éste instalará las características básicas que puede necesitar una estación de trabajo incluyendo el sistema X Window. No instalará características de servidor como daemons FTP, HTTP o Telnet. Si se elige la instalación de servidor, estas características serán instaladas, pero el sistema X



Window no. Esto significa que la línea de comando será la única opción para administrar el servidor. La opción de instalación personalizada permitirá elegir las opciones a ser instaladas. Por ejemplo, puede elegir tener el sistema X Windows instalado además de algunos de los daemons que podría necesitar para un servidor como FTP, HTTP y Telnet.

Mouse y teclado

Después de seleccionar el tipo apropiado de instalación el sistema realizará un paso en el cual detecta los discos rígidos del sistema. Luego detectará el mouse y el teclado del sistema. Linux puede autodetectar el mouse y el teclado y es probable que seleccione los correctos. Se mostrará una ventana para elegir el tipo de mouse y teclado que están conectados a la computadora si no los puede autodetectar. Se pueden seleccionar características tales como la cantidad de botones que tiene el mouse y si tiene una rueda o no. Linux soporta también muchos tipos de teclados y se debería seleccionar la opción correcta.

8.2 Creación de un sistema de archivos Linux

Después de especificar los parámetros apropiados para la instalación, particione el disco rígido y elija el sistema de archivos que va a estar en este sistema Linux. Básicamente cuando Linux crea el sistema de archivos, está formateando la unidad de disco. Este es el proceso en el cual el sistema de archivos ext2 o ext3 será grabado en la partición. Tenga presente que el formateo de la unidad de disco borrará cualquier dato que esté actualmente en la unidad o partición que se está formateando. Por lo tanto, asegúrese de que los datos del disco están copiados en un respaldo o que ya no los necesita.

El formateo del disco rígido no es necesario y puede haber ocasiones en que este no sea un paso necesario. A veces estos sistemas de archivos pueden ya haber sido creados con otra herramienta de partición y formateo como PartitionMagic por ejemplo. Otra situación donde el disco rígido puede no necesitar ser formateado o particionado es cuando se actualiza o se hace un inicio dual con otro OS ya instalado. Si se está haciendo una instalación fresca del Linux, entonces sería deseable formatear el disco rígido.

Una opción que está incluida con la mayoría de las distribuciones de Linux cuando se formatea es la de realizar una "revisión de bloques dañados". Esta es una opción avanzada que puede ser seleccionada para revisar los sectores del disco o partición para asegurarse de que pueden almacenar los datos antes de formatearlos. La realización de esta revisión tomará tiempo adicional en comparación con el formateo regular pero puede ahorrar más tiempo a largo plazo si un sector está malo y no se sabe eso. Si durante la revisión se encuentran bloques dañados, entonces es una buena idea reemplazar el disco porque es un signo de que el disco está comenzando a fallar.

8.3 Selección de paquetes para la instalación

Después de particionar y formatear el disco rígido, será mostrada una lista de paquetes que pueden ser instalados. Hay muchos paquetes para elegir y dependiendo de cuál distribución se está instalando, algunas pueden tener más que otras. Tenga presente que aquí está la cantidad de espacio en disco que está disponible para trabajar. Si instala muchos de estos paquetes consumirá espacio en el disco. Por ejemplo, muchos de estos paquetes en particular de la estación de trabajo KDE o GNOME pueden consumir cientos de megabytes de espacio en disco. Algunas distribuciones mostrarán cuánto espacio será necesario para el paquete en particular



que será instalado, otras no mostrarán esto hasta después de que el paquete haya sido seleccionado y el proceso de instalación haya pasado al paso siguiente.

Algunas distribuciones como Mandrake darán la opción de seleccionar todo o parte de un paquete para instalar. Esto es útil si se desean algunas de las características de un paquete en particular pero no el paquete completo. Si se selecciona esta opción se podrá navegar a través del paquete y seleccionar las características en particular deseadas. Algunas de estas características individuales de los paquetes tienen dependencia, lo que significa que será necesario instalar otros programas o características para que funcionen. La instalación de uno de estos paquetes sin instalar el programa o paquete del que depende el sistema hará que el sistema indique que los otros paquetes también deben ser instalados.

Después de que todos los paquetes a ser instalados fueron seleccionados, el proceso de instalación procederá con el siguiente paso. Este es donde se realiza la instalación real del sistema operativo.

8.4 Instalación y configuración de Linux

La instalación comenzará una vez que el CD sea insertado y la BIOS esté configurada para iniciar desde el CD. Seleccione la configuración para el sistema, por ejemplo, el idioma a ser usado. Luego, elija el tipo de mouse y teclado que se están usando. Se le pedirá al instalador que elija el tipo de instalación, servidor o estación de trabajo. La GUI X Window no estará disponible si se elige la instalación de servidor. La instalación de servidor instalará las diferentes herramientas necesarias para un servidor como las herramientas de archivo y de servidor web. El paso siguiente es particionar el disco rígido.

Después de que el disco es particionado, se debe configurar los datos de red y la zona horaria. En este punto son creadas las cuentas de root y la password además de cualquier otra cuenta que sea necesario instalar en el sistema. Con propósitos de seguridad, la cuenta root no se debería usar. Se recomienda crear una segunda cuenta para administrar Linux. Para una instalación de servidor el próximo paso es instalar el sistema operativo. Si se seleccionó la instalación de estación de trabajo, se le pedirá primero al instalador que configure el Entorno de X-Window antes de que la instalación comience. Este entorno incluye cosas como seleccionar la configuración apropiada de monitor y tarjeta de video, además de la configuración de la resolución y el color del sistema. Cuando el proceso de instalación haya terminado pedirá que se creen discos de inicio. Una vez hecho esto, el proceso de instalación está completo.

8.5 Configuración de la Seguridad Adecuada

Algunas de las configuraciones de seguridad más importantes para seleccionar son la configuración y password de la cuenta usuario y de la cuenta root. Los usuarios que están familiarizados con Windows 2000 saben que para ingresar al sistema debe haber una cuenta de usuario almacenada localmente en la misma computadora o en el Active Directory. Linux funciona de la misma forma en el sentido en que las cuentas de usuario son la característica principal que controla quién puede o no ingresar al sistema. Linux utiliza la cuenta root, que es similar a la cuenta administrador en Windows 2000. La cuenta root tiene privilegios para realizar cualquier tarea en el sistema incluyendo agregar y borrar otras cuentas de usuarios.

Durante el proceso de instalación se pedirá la creación de la password root y luego se dará la opción de crear cuentas de usuarios que van a ser agregadas al sistema en ese momento. Sin embargo, las cuentas de usuario no necesitan ser agregadas en





este punto, sino que se puede realizar más tarde. Aunque el administrador sea la única persona que estará usando este sistema, se recomienda la creación de una cuenta de usuario separada. El uso solamente de la cuenta root puede presentar algunos riesgos de seguridad.

Opciones de cuentas raíz

La cuenta root en Linux también es conocida como cuenta superusuario o administrador. Esta cuenta es obligatoria y durante la instalación se pedirá el ingreso de una password dos veces como protección contra errores de escritura. La mayoría de las distribuciones de Linux tendrán reglas con respecto a la longitud y contenido de la password. Las reglas variarán dependiendo de la distribución pero por lo general la password debe tener al menos cuatro caracteres de largo y no puede tener términos comunes que se encuentren en el diccionario. Algunas distribuciones tendrán otras reglas como que deben tener al menos uno o dos caracteres que no sean letras, como números o signos de puntuación, por ejemplo.

Definición de las cuentas de usuarios durante la instalación

Hay pros y contras en la creación de cuentas de usuarios durante la instalación. El comprender las ventajas y desventajas ayudará a cualquier administrador a determinar qué es lo mejor en base a las implementaciones de seguridad que han sido planeadas.

Se dijo antes que al menos una cuenta de usuario debería ser creada durante la instalación para que la use el administrador del sistema incluso si nadie más usará el sistema o accederá a él. La principal desventaja de crear cuentas de usuario durante la instalación es que muchas de las opciones que de otra forma se tendrían como elegir directorios home no estándares, caducidad de la cuenta y definición de políticas de grupo, no están disponibles.

Opciones de password

Aunque no es en realidad configurable durante el proceso de instalación, es importante hablar sobre las passwords shadow en este momento porque son valiosas en la seguridad del sistema Linux. La mayoría de las distribuciones utilizan los métodos de codificación de password MD5 o DES. Algunas usan MD5 por defecto porque es más nuevo y más seguro que DES. Normalmente, los sistemas Linux y UNIX almacenan información de cuentas y passwords en forma encriptada en un archivo llamado `/etc/passwd`. Este archivo necesita ser accedido por todos los usuarios porque varias herramientas necesitan acceder a este archivo para información que no es de password. Al usar password shadow las passwords son almacenadas en un archivo diferente que no es accesible por los usuarios lo que aumenta mucho la seguridad.

8.6 Configuración de los Datos de Red

Durante la instalación aparecerá la opción de configurar los Datos de Red. Esto puede realizarse después de la instalación pero es mucho más sencillo y recomendable hacerlo durante la instalación.

Cuando se selecciona la opción de configurar los datos de red durante el proceso de instalación, la primera decisión que se necesitará tomar es que el sistema autodetecte el tipo de conexión de red que se usará. Las opciones incluidas para tipos de conexiones de red incluyen una conexión de MODEM normal o una conexión LAN.

Normalmente el sistema detectará la tarjeta de red apropiada que está instalada. Dependiendo de la distribución de Linux que se está instalando los pasos para hacer



esto pueden ser ligeramente diferentes. Sin embargo, en este punto se presentará un prompt para seleccionar si se configurará manualmente o no los datos de red como la dirección IP, la máscara de subred, el nombre de Host, el servidor DNS, y la puerta de enlace predeterminada. La otra opción es seleccionar DHCP si el sistema está conectado a un servidor DHCP que proporcionará toda esta información en forma automática. Algunas distribuciones tendrán otros datos de configuración de red que puede o no ser necesario ingresar en este momento, dependiendo del tipo de red en donde está el sistema. Un ejemplo sería si la red utiliza un servidor proxy, que son servidores que protegen a una red limitando el acceso de entrada y salida a la red. Si la red utiliza un servidor proxy entonces ingrese también la dirección IP de este servidor en este punto.

8.7 Otras Configuraciones y Datos

En este punto la mayor parte del proceso de instalación inicial debería estar completo con la excepción de algunas configuraciones y datos finales. Estas incluyen la configuración de la Zona Horaria, la configuración de la Impresora, la configuración de Servicios, y las Opciones de Inicio.

Configuración de la Zona Horaria

Como en otras ocasiones, las especificaciones sobre cómo configurar la zona horaria variarán dependiendo de la distribución de Linux que se está instalando. Cuando se llega a este punto de la instalación, aparecerá una pantalla que permitirá seleccionar la zona horaria donde está ubicado el sistema.

Algunas distribuciones tienen la opción de fijar el reloj en la Hora de Greenwich (Greenwich Mean Time – GMT), la hora en la ciudad de Greenwich, Inglaterra. En el UNIX tradicional y en los sistemas Linux esto se conoce como Hora Universal Coordinada (Coordinated Universal Time – UTC).

Configuración de Servicios

Los sistemas Linux tendrán una cantidad de servicios diferentes corriendo en ellos. Si el sistema va a ser una estación de trabajo, un servidor Web, o un servidor de correo entonces se necesitarán instalar los servicios apropiados en el sistema. Algunos de estos servicios pueden ser instalados durante la instalación. Cuando esta pantalla aparezca durante el proceso de instalación seleccione las cajas apropiadas. Los servicios que fueron seleccionados ahora serán instalados.

8.8 Opciones de Inicio

La selección y configuración del sistema para que use el cargador de inicio apropiado es otra parte del proceso de instalación del Linux. Linux utiliza uno de los siguientes programas: Linux Loader (LILO) o Grand Unified Bootloader (GRUB). Estos dos programas inician un sistema Linux desde el disco rígido. La mayoría de las distribuciones de Linux usan LILO y algunas de las distribuciones ofrecen GRUB como una alternativa. Después de seleccionar el cargador de inicio a usar, habrá la oportunidad de ajustar algunas de las características. Algunas de estas opciones son las siguientes:

- La mayoría de las distribuciones permitirán elegir entre usar un menú gráfico o basado en texto cuando se seleccione LILO. Si se selecciona GRUB la única opción es el menú gráfico.
- LILO almacena su código de tiempo de inicio en el dispositivo de inicio. Si se está instalando Linux en una unidad EIDE entonces este archivo se ubicará en /dev/hda. Si se está instalando Linux en una unidad SCSI entonces se almacenará en /dev/sda. Esto está bien si Linux es el único sistema operativo



instalado en la unidad. Sin embargo, si este sistema es de inicio dual con otro OS entonces LILO o GRUB necesitarán ser colocados en la partición de inicio de Linux.

- El retraso que utiliza LILO antes de iniciar puede ser ajustado también aquí.
- Hay una opción de inicio compacto que se puede seleccionar que acelera el tiempo de inicio.
- Es posible configurar la tarjeta de video para el cargador de inicio. Si no está configurada, se usará la resolución por defecto, sin embargo es posible cambiar la resolución para el cargador de inicio.
- Linux almacena archivos temporales en el directorio /tmp. Es posible configurar el cargador de inicio para que limpie este directorio cada vez que se inicia Linux.
- En algunas instancias Linux no detectará la cantidad correcta de RAM. Eso significa que Linux sólo podría detectar 64 MB de RAM cuando en realidad hay 128 MB instalados. Una precaución para evitar esto es ingresar en forma manual la cantidad de RAM instalada en esta página de configuración.

Cuando todas las configuraciones han sido ingresadas el programa de instalación procederá con el paso siguiente. Mientras esto sucede, el sistema presentará un resumen de las opciones del cargador de inicio. Estas opciones variarán dependiendo de las configuraciones que fueron ingresadas y de si el sistema está configurado para inicio dual con otro sistema operativo.

9 Administración de Linux

9.1 Interfaz de usuario

Los usuarios pueden ingresar a un sistema operativo Linux usando la Interfase de Línea de Comando (Command-Line Interface – CLI), que es similar a la interfase de Windows 2000. En lugar de mostrar cajas de texto y botones como la GUI de Windows 2000, la CLI de Linux proporciona al usuario una sucesión de prompts de sólo texto para ingresar un nombre de usuario y password. No se necesita información de dominio adicional. A diferencia de Windows 2000, las passwords de Linux son enmascaradas completamente a medida que son escritas, por lo que hay que prestar mucha atención mientras se las ingresa. Los usuarios también deberían tener cuidado de ingresar información de cuenta inválida continuamente, ya que algunos administradores de sistemas implementan funciones de seguridad para bloquear o reiniciar el sistema después de una cantidad de intentos fallidos. Una vez que la información de cuenta ha sido emitida con éxito, el usuario será ingresado al sistema, llevado a su directorio home, y se le dará un prompt de comando.

Cuando el sistema está configurado para iniciarse en la Interface Gráfica de Usuario (Graphical User Interface – GUI), KDE por ejemplo, se necesitará ingresar un nombre de usuario y una password autenticar el usuario en la red.

9.2 Interfase GUI

Las diferencias entre una Interface de Línea de Comando (Command-Line Interface – CLI) y una interfase Gráfica de Usuario (Graphical User Interface – GUI) fueron tratadas anteriormente. Recuerde que Linux utiliza una CLI con comandos basados en texto ingresados en un prompt de comando. Mientras que este formato tiene sus ventajas, también tiene ventajas la GUI usada por Windows. En 1984, un equipo de expertos en software del Massachusetts Institute of Technology (MIT) creó una





interface gráfica llamada "X Window" que le permite al Linux operar en forma similar a los otros GUIs.

Debido al poderoso diseño del sistema operativo Linux, la apariencia y sensación de X Window puede ser fácilmente personalizada y programada de una infinita cantidad de formas. En el OS Windows 2000, los principales elementos de la interfase del usuario que son los iconos, menús, la barra de tareas, etc, son idénticos para todos los usuarios. Los usuarios de Linux pueden personalizar por completo su interfase X Window para satisfacer sus necesidades y deseos específicos instalando diferentes programas llamados "Administradores de Ventanas" y "Entornos de Escritorio".

Similitudes con Windows 2000

Una típica interfase X Window se vería algo familiar para un usuario de Windows 2000. Se utiliza un mouse como dispositivo de señalización. También hay normalmente una barra de tareas, iconos representando los datos, y ventanas mostrando información al usuario. Mientras que los tamaños, formas y colores de estos elementos pueden variar, los principios básicos son muy similares a la GUI de Windows 2000. Este diseño familiar tiene la intención de ayudar a los usuarios a volverse productivos rápidamente con el sistema X Window y normalmente es la aproximación estándar. Pero de nuevo, la flexibilidad de Linux también permite que los programadores creen nuevas e innovadoras interfaces X Window que podrían diferir enormemente de cualquiera vista hasta ahora.

Aprendiendo lo básico

En primer lugar los usuarios de X Window deberían comenzar a conocer los distintos elementos del sistema. Determine si los iconos son activados con un solo clic o con doble clic. Haga clic sobre la barra de tareas para investigar las distintas herramientas que contiene. Practique cómo cambiar de tamaño, minimizar y cerrar la ventana. Una vez que los usuarios se sienten cómodos navegando la interfase X Window, están listos para comenzar a aprender sus funciones básicas.

No importa los colores, estilos y funcionalidad que un entorno X Window pueda tener, hay un elemento importante que siempre será constante. La consola de línea de comando permanece constante. Recuerde que Linux es un CLI, y X Window es en realidad una representación gráfica de este CLI. Por lo tanto tiene sentido que un usuario de X Window probablemente quiera interactuar con una consola de comandos Linux en algún momento. Esto puede hacerse normalmente de dos formas: ventana de terminal y consola principal.

Ventana de terminal

Una ventana de terminal muestra un prompt de comando Linux estándar en una pequeña ventana en la pantalla. El programa estándar de terminal de X Windows se llama "xterm". Al ejecutar xterm muestra una ventana de terminal de Linux para que el usuario ingrese comandos. Busque a xterm o a cualquier otro programa de terminal en el menú de la barra de tareas de X Window.

Consola principal

Además de ejecutar un CLI de Linux en ventana dentro del X Window, los usuarios también pueden pasar sus vistas a la consola principal de pantalla completa. Recuerde que cuando inicia la computadora, Linux es cargado primero seguido del X Window. Como Linux mismo está siempre corriendo en el trasfondo, es posible pasar el sistema desde el X Window al CLI del Linux usando las teclas [CTRL + ALT + (F1 - F6)]. La consola principal y las ventanas de terminal funcionan en forma idéntica; el usar una en lugar de la otra es normalmente una cuestión de preferencia personal. Es posible también ejecutar dos sesiones X al mismo tiempo y usar Terminales Virtuales. X corre





en Terminal Virtual 7 y como se dijo antes puede ser pasado a cualquiera de las Terminales Virtuales CLI usando el comando [CTRL + ALT + (F1 - F6)].

Mientras que muchas tareas comunes de Linux se pueden ejecutar usando las aplicaciones gráficas de X Window, hay muchas más que sólo están disponibles para los usuarios con el prompt de comando. Por esta razón es importante saber cómo acceder a un prompt de comando de Linux desde dentro de X Window.

La última habilidad básica con el X Window que debe saber es salir del sistema. Dependiendo del entorno de escritorio que esté ejecutando actualmente, esto se hace normalmente en forma muy similar a Windows 2000. Simplemente localice el menú de barra de tareas y una de las primeras opciones del menú será Salir. Al seleccionar esta opción se le permite al usuario apagar o reiniciar Linux.

9.3 Interface CLI

La Interfase de Línea de Comando (Command-Line Interface – CLI) de Linux permite al usuario interactuar con el sistema de la misma forma que el intérprete de comandos del Windows 2000. Después de ingresar al Linux, el sistema navega hacia el directorio home del usuario y presenta el prompt de comando. Los usuarios ahora pueden escribir comandos, presionar la tecla ENTER, y ver la salida en la pantalla. Aunque el funcionamiento de Linux sigue el mismo flujo básico que el intérprete de comandos del Windows 2000, la sintaxis de los comandos por lo general es bastante diferente entre los dos.

La mayoría de los sistemas operativos CLI suponen que los usuarios saben lo que están haciendo y no verifican la intención de sus comandos. Por lo tanto los usuarios siempre deberían ser precisos y estar alertas cuando emiten comandos del sistema para evitar resultados no deseados.

Páginas Man

Los usuarios pueden aprender más sobre cualquier comando usando las "páginas man". Abreviatura de "páginas de manual". Estos archivos de ayuda muestran información detallada sobre cualquier comando de Linux disponible para el usuario usando la ayuda de línea de comando conocida como páginas man.

Las páginas man describen lo que usted necesita saber sobre los comandos en línea del sistema, llamadas al sistema, formatos de archivo, y mantenimiento del sistema. Las páginas man en línea son parte del OS Linux y son instaladas por defecto. Las páginas man tienen el formato de pantallas simples basadas en caracteres y no son gráficas.

Para acceder a las páginas man, necesita estar en el prompt de comando. Puede ingresar a la línea de comando o abrir una ventana de Terminar en la interface KDE y comenzar con un prompt de comando. Las páginas man son útiles cuando desea usar un comando o utilitario y ha olvidado la sintaxis o necesita sólo algo de información sobre cómo usarlo. Las páginas man proporcionan información sobre cómo ingresar el comando, una descripción de su propósito, y las opciones o argumentos que están disponibles.

El comando man

El comando man muestra páginas man en línea para cualquiera de los cientos de comandos Linux que están disponibles. Usted puede obtener un listado de todos los comandos Linux con una breve descripción de lo que hacen ingresando man intro en



la línea de comando. Incluso puede mostrar una página man sobre el comando man mismo escribiendo man man.

Usted puede usar el comando man de varias formas. La básica es man nombre, donde nombre es el nombre del comando para el que desea información. Hay varias opciones prácticas para que el comando man ejecute búsquedas por palabra clave y muestre secciones específicas del Manual del Programador.

Los shells del Linux

Los shells del Linux trabajan como un intérprete de comandos. Los shells del Linux funcionan casi de la misma forma que el programa command.com funciona para el MS-DOS. Los shells del Linux toman la entrada que el administrador escribe y usa esa entrada para lanzar comandos y controlar el sistema operativo. Sin embargo, las funciones similares de los shells del Linux y del intérprete de comandos del MS-DOS terminan allí. Por ejemplo, en Linux el shell es cargado en el sistema sólo cuando el usuario lo pide o si el usuario ingresa directamente en el shell. En MS-DOS, el intérprete de comandos está integrado al kernel y siempre está corriendo. En Linux, el shell corre como cualquier otro programa y no está integrado al kernel del sistema operativo. Otra diferencia principal de los shells del Linux es que el usuario puede elegir entre shells muy diferentes. Con Linux, se puede elegir un shell que satisfaga las preferencias o que encaje en el entorno.

El Shell Bourne

Este es conocido como el shell original del UNIX. El nombre del programa es (sh) y se conoce como el shell bash en los sistemas Linux. Este shell proporciona todas las funciones de (sh) además de programación de shell usando archivos script de shell.

El Shell C

Este shell no es muy usado porque es uno de los shells más complicados para trabajar. Utiliza una sintaxis mucho más compleja para la programación del shell que la de los otros shells. Por esta razón el shell C no es recomendado para la programación de shell o para crear programas de shell.

El Shell Korn

Este es un shell que fue escrito por David Korn. Combina las características interactivas que hacen popular al shell C con la sintaxis de programación fácil de usar del shell Bourne.

Shell Otra Vez Bourne (Bourne Again Shell)

Este shell fue creado como una extensión mejorada del Shell Bourne. Este shell es llamado bash shell y se utiliza en muchos sistemas "similares a UNIX", como el Linux.

9.4 Cuentas de usuario y grupos

Antes de entrar en la administración real de las cuentas de usuario y de grupo, es una buena idea aprender el concepto y los detalles de la implementación de las cuentas de usuario en un sistema multiusuario. El comprender estos conceptos puede ayudar a cualquier administrador a planificar en forma efectiva la seguridad de las cuentas de usuario y de grupo.

Cuentas de usuario en un entorno multiusuario

Las cuentas de usuario en un sistema Linux permiten que varias personas ingresen al sistema al mismo tiempo o en diferentes momentos sin interferir entre ellas. Un usuario puede incluso tener múltiples ingresos activos al mismo tiempo. Antes de realizar las



tareas administrativas con las cuentas de usuario o grupo es importante comprender lo que las cuentas de usuarios permiten hacer a un multiusuario en el sistema Linux, y cómo se identifican a diferentes usuarios y grupos.

Hay varios términos importantes que se necesitan saber para comprender el lenguaje que trata de la administración de cuentas de usuario. Primero, el término usuario y cuenta son a veces usados en forma intercambiable. Por ejemplo se pueden oír los términos "eliminar una cuenta" o "borrar el usuario". Para este propósito ellos significan lo mismo, eliminar la cuenta o acceso del usuario al sistema.

Nombre de usuario

Este es un nombre único que se da a cada persona que tiene permitido ingresar en el sistema. Es una buena idea tener reglas sobre los nombres de usuario para que sea más fácil identificar a un usuario por su nombre de usuario. Los nombres de usuario comunes son la primera letra del nombre del usuario y el apellido completo. Por ejemplo el usuario Juan Pérez sería jperez.

Privilegios de ingreso

Después de que se ha dado un nombre de usuario y una password a un usuario y de que se les permite ingresar al sistema, los usuarios sólo podrán tener acceso a ciertos directorios. Los usuarios también están limitados a lo que se les permite hacer en el sistema. Los privilegios de ingreso indican el tipo de derecho que un usuario obtendrá una vez que accede al sistema.

Protección de password

Junto con un nombre de usuario los usuarios deben suministrar una password para ingresar a un sistema Linux. La password está oculta a diferencia del nombre de usuario, que es públicamente conocido. Muchos sistemas Linux tienen reglas con respecto a las passwords como la longitud o los tipos de caracteres usados.

Permisos

El sistema de archivos controla quién tiene permiso para acceder a los archivos y ejecutar programas.

Directorio home

En un sistema Linux todas las cuentas de usuario tienen un directorio home asociado a ellas. Este es un directorio en el cual el usuario tiene completo acceso. El usuario puede agregar o eliminar archivos en este directorio o puede usarlo sólo para almacenar archivos.

Ids de usuario y de grupo

Estos son números que el sistema operativo Linux utiliza para identificar a un usuario o un grupo. Linux no usa nombres. El sistema operativo utiliza números por lo que usa la ID de usuario (UID) para identificar a los usuarios y una ID de grupo (GID) para identificar a los grupos de usuarios.

Shell por defecto

Cuando los usuarios ingresan a un sistema Linux y emiten comandos en la línea de comando, lo están haciendo desde el prompt del shell. Esto es lo que se usa para interpretar a estos comandos para el kernel del Linux. Hay varios shells de donde elegir. EL shell por defecto es el shell presentado al usuario cuando ingresa. Toda esta información de las cuentas de usuarios es almacenada en dos archivos de configuración en un sistema Linux: los archivos `/etc/passwd` y `/etc/shadow`.



Cuentas de usuarios en un sistema multitarea

El sistema operativo Linux es un sistema multiusuario y multitarea. La naturaleza de las cuentas de usuario de Linux es tal que múltiples usuarios pueden ingresar en un sistema Linux al mismo tiempo. Los usuarios pueden ingresar en forma local o remota a través de una red. Por esta razón un sistema multitarea que está siendo usado por usuarios simultáneos necesitará conectividad de red. Estos usuarios pueden estar usando más de un programa al mismo tiempo y estos usuarios pueden incluso usar el mismo programa al mismo tiempo. Por ejemplo, un usuario puede haber ingresado y estar usando XEmacs, otro usuario puede haber ingresado para usar el mismo navegador web, y otros dos usuarios pueden haber ingresado para usar un editor de texto al mismo tiempo. Es posible configurar Linux para que sea un OS de usuario múltiple donde múltiples usuarios pueden ingresar usando una única cuenta de usuario, sin embargo esto no es recomendable por varias razones. El que cada usuario tenga su propia cuenta de usuario le da al administrador la capacidad de controlar la seguridad usuario por usuario.

Tenga presente que aunque Linux es un sistema multitarea no puede soportar una cantidad ilimitada de usuarios simultáneos. Si una gran cantidad de usuarios ingresa al sistema y muchos de estos usuarios intentan usar el mismo programa entonces experimentarán una disminución de rendimiento. La cantidad real de usuarios que un único sistema Linux puede soportar depende de varios factores. Depende de cuáles programas están siendo usados en ese momento. Algunos programas toman más recursos del sistema, como RAM, tiempo de CPU o I/O de disco, que otros. Por esta razón otros factores incluyen cuántos de estos recursos tiene el sistema. Un sistema con más RAM, una CPU rápida, una velocidad de disco más rápida y más capacidad de disco puede manejar más usuarios simultáneos.

La cuenta superusuario

La cuenta de usuario más importante en un sistema Linux es la cuenta de Superusuario. Esta también es conocida como la cuenta raíz. Recuerde que esta cuenta es creada por defecto durante el proceso de instalación. Esta es la cuenta que utiliza el administrador del sistema para realizar cualquier tarea administrativa en un sistema Linux. La cuenta de Superusuario puede ser usada de varias formas:

- Ingreso en raíz [root login] — la cuenta raíz puede ser usada para ingresar a la computadora directamente en la consola principal. En realidad, el ingreso como raíz de esta manera sólo puede ser hecho desde la consola principal. Una vez ingresado cualquier acción que se realice sobre el sistema será hecha como raíz. Esto puede presentar problemas de seguridad por lo que se recomienda que esto se haga por períodos breves y luego se salga de la cuenta Superusuario.
- Su — La cuenta su puede ser usada para adquirir en forma temporal los privilegios del superusuario en un sistema Linux para realizar tareas administrativas o para ejecutar un comando que requiere privilegios de superusuario. Escriba el comando y presione ENTER. Habrá un prompt para la password de superusuario y si la ingresa correctamente recibirá privilegios de superusuario. Para volver a la cuenta con los privilegios normales del usuario escriba exit. El comando su también puede ser usado para pasar a otra cuenta de usuario. Por ejemplo, escriba su jperez para tomar el rol de la cuenta jperez. Esto es porque cuando se ingresa como raíz se recibe el acceso a cualquier cuenta de usuario en el sistema.
- Sudo — Este comando permite que un administrador seleccione ciertos comandos que pueden ser ingresados sin tener que ser raíz, ya que de otra forma necesitarían privilegios de superusuario. Esto se hace editando el



- archivo /etc/sudoers y especificando los usuarios y los comandos que estos usuarios pueden ingresar en la línea de comando sin tener que ser raíz.
- Archivos raíz SUID — Es posible seleccionar un archivo para que se ejecute como si fuera ejecutado por raíz, pero que pueda ser ejecutado por cualquier usuario en el sistema.

Es importante ser muy cuidadoso cuando se usa la cuenta superusuario a causa de los problemas de seguridad y daños que pueden ser causados a la computadora. Por esta razón no se recomienda usar la cuenta raíz como una cuenta regular incluso para el administrador del sistema. Un simple error tipográfico cuando se ejecuta un comando puede causar un daño serio y no intencional al sistema. Por ejemplo, suponga que se debe eliminar /home/jperez/tempdir. Se debería ingresar el comando `rm -r /home/jsmith/tempdir`. Sin embargo, suponga que se cometió un error y se ingresó el comando equivocado. En lugar de `rm -r /home/jsmith/tempdir`, por error se colocó un espacio entre / y home. Esto causaría que la computadora borre todos los archivos en el directorio / además de en /home/jsmith/tempdir. Si esto sucediera mientras se está dentro del sistema con una cuenta de usuario normal habría un prompt para cambiar a cuenta de superusuario para realizar esto y el error sería descubierto antes de completar este comando.

Cuentas de grupo

Los grupos en un sistema Linux son usados para los mismos propósitos que en otros sistemas operativos. Los grupos proporcionan un medio para relacionar a usuarios similares para mejorar la productividad y facilitar la administración de las cuentas de usuarios. Las cuentas de grupos son similares a las cuentas de usuario en que están definidas en un único archivo, /etc/groups, similar al archivo /etc/passwd para las cuentas de usuario. Segundo, los grupos tienen nombres también, similares a los nombres de usuario para las cuentas de usuario. Por último, como se dijo antes, los grupos reciben una ID (GID).

Las cuentas de grupo, sin embargo, no son cuentas de usuario. Las cuentas de grupo son un medio para agrupar una colección de usuarios similares con propósitos de seguridad. Por ejemplo, es posible agrupar a los ejecutivos de una compañía que pueden tener ciertos accesos a archivos y agrupar juntos a otros empleados, que pueden no tener acceso a estos archivos. Recuerde que Linux controla el acceso al hardware a través de los archivos. Los grupos también pueden ser usados para limitar el uso del hardware de un sistema a un grupo específico de usuarios.

La primera cuenta de usuario creada durante una instalación de Linux es la cuenta "raíz". Esta cuenta de superusuario es usada por el administrador del sistema para crear todas las otras cuentas de usuario en el sistema. Por defecto y por razones de seguridad, ningún otro usuario tiene el poder de agregar usuarios excepto el usuario raíz. El proceso de crear un usuario de Linux totalmente personalizado puede ser bastante complejo, por lo que sólo se verán aquí los comandos, flags y parámetros básicos necesarios.

El comando useradd

El usuario raíz crea a los otros usuarios de Linux con el comando useradd. Cuando se ingresa este comando en el prompt, Linux ejecuta muchas tareas simultáneas para crear la cuenta del usuario, como crear un directorio home y asignarle permisos por defecto. La sintaxis básica del comando es la siguiente:

```
useradd nombre usuario -c "nombre real"
```

Por ejemplo: `useradd jperez -c "Juan Perez"`





Esta cadena completa es escrita en el prompt de comandos de Linux antes de presionar la tecla ENTER. El parámetro <nombre usuario> será el nombre de ingreso para el nuevo usuario cuando ingrese al sistema. Es sensible a las mayúsculas y siempre debería ser escrito en caracteres todos en minúscula. El flag -c se utiliza para ingresar el campo comentario, que en la mayoría de los sistemas se usa para almacenar el nombre real del usuario. Existen otros flags y parámetros para el comando useradd y pueden ser encontrados viendo su página man. Los administradores de sistemas normalmente usarán muchas más de estas opciones de comando para personalizar completamente a sus nuevos usuarios.

El comando passwd

Una vez que una nueva cuenta de usuario ha sido creada, se le debe dar una password antes de que el usuario pueda ingresar al sistema. Esto se hace en Linux con el comando passwd. Los usuarios pueden ejecutar este comando para cambiar sus propias passwords, pero el usuario raíz también puede usarlo para modificar las passwords de todos los usuarios. Por lo tanto, después de que se crea una nueva cuenta, el siguiente comando es ingresado por el usuario raíz para crear la nueva password de cuenta:

```
passwd nombre usuario
```

Por ejemplo: passwd jperez

Se le pedirá al usuario raíz que ingrese una nueva password y que la confirme repitiéndola. Una vez que este proceso está terminado, el nuevo usuario estará listo para ingresar al sistema con el nombre de usuario y la password recién creados. Después de ingresar por primera vez, se debería volver a cambiar la password con el comando passwd. Haga esto sin el parámetro nombre usuario, para colocar una que sea más privada y desconocida por el administrador del sistema.

Administración de Cuentas de Usuarios

Con el CLI del Linux, la administración de usuarios es realizada de nuevo por medio de distintos comandos, flags, y parámetros. En particular, el cambio del nombre de usuario, el cambio de la password o la eliminación de una cuenta se puede realizar con comandos mínimos. Sin embargo, el proceso de desactivar una cuenta requiere un poco más de esfuerzo. El administrador del sistema debe editar el archivo que almacena la información de todos los usuarios del sistema y desactivar manualmente la password del usuario.

Este procedimiento no es tan difícil como puede parecer. En la mayoría de los sistemas Linux, las passwords de los usuarios están almacenadas en un archivo central conocido como el archivo "sombra (shadow)", que está ubicado en el directorio /etc. Este archivo puede ser editado con un editor de texto como el Editor vi. El comando para editar el archivo sombra sería el siguiente:

```
vi /etc/shadow
```

Pico, otro editor de texto, permite el uso de las teclas de cursos del teclado para navegar la lista de cuentas de usuario hasta que se localiza la cuenta que se debe desactivar. La información del usuario está listada en forma continua en una única línea con los campos separados por dos puntos (:). El primer campo es el nombre del usuario, y el segundo es la password encriptada del usuario. Para desactivar la cuenta, el administrador del sistema puede simplemente colocar un asterisco (*) en el comienzo de la password encriptada. Esto hará que sea imposible escribir la password en forma correcta cuando quiera ingresar, desactivando así la cuenta hasta que el administrador del sistema elimine manualmente el asterisco otra vez. Para grabar el



archivo sombra, presione CTRL-X para salir de pico y presione la tecla Y para grabar los cambios.

Creación de Grupos y Agregado de Usuarios a los Grupos

Todos los grupos de un sistema Linux pueden tener desde ningún miembro hasta tantos miembros como cuentas de usuario haya en el sistema. Recuerde que la membresía en un grupo es controlada por el archivo `/etc/group`. Este es el archivo que contiene una lista de todos los grupos y miembros de esos grupos en un sistema Linux.

Cada usuario, cuando ingresa a un sistema Linux, ingresa a su grupo primario. Este es el grupo que especifica la membresía al grupo por defecto y está configurado en el archivo de configuración del usuario. Cuando un usuario ingresa a su grupo primario puede acceder a los archivos y ejecutar los programas que están asociados con ese grupo en particular al cual pertenece. Si un usuario desea acceder a archivos o programas que no están en su grupo primario, puede pasar al grupo al que está asociado ese archivo o programa en particular. Sin embargo, el usuario debe ser un miembro de ese grupo para poder pasar a él. Este es un medio excelente para controlar la seguridad en un sistema Linux. Para pasar a un grupo diferente después de haber ingresado al sistema use el comando `newgrp`. La sintaxis para este comando es la siguiente:

```
newgrp <nombre grupo>
```

Por ejemplo: `newgrp ingenieria`

En un sistema Linux, sólo la cuenta raíz, superusuario, tiene el poder de crear y administrar grupos. Estas tareas son realizadas usando comandos simples para crear, renombrar o eliminar grupos del sistema. La mayoría de los usuarios de Linux son asignados a un grupo durante el proceso de creación de las cuentas. La siguiente sintaxis se utiliza para crear un grupo en un sistema Linux:

```
groupadd nombre grupo
```

Por ejemplo: `groupadd ingenieria`

Este comando crea el grupo ingeniería. Después de que el grupo ha sido creado, se pueden agregar los usuarios al grupo. Esto se puede hacer con los siguientes comandos:

Una forma de agregar un usuario a un grupo es hacerlo cuando se crea la cuenta del usuario. La siguiente sintaxis se utiliza para expandir el comando `useradd` :

```
useradd -g grupo nombre_usuario -c "nombre real"
```

Por ejemplo: `useradd -g ejecutivos jperez -c "Juan Perez"`

9.5 Permisos

En comparación con Windows 2000, el sistema de permisos del Linux es mucho más intrincado. Los administradores de sistema ejercen más control con el uso de tres categorías distintas de permisos: leer, escribir y ejecutar. En Windows 2000, el permiso de leer controla la capacidad de un usuario para ingresar y ver un directorio. En Linux esta funcionalidad se divide en dos permisos separados. De esta forma el permiso de ejecución controla la capacidad de un usuario para ingresar a un directorio, mientras que el permiso de lectura controla su capacidad para leer. Esto permite un control más detallado de los permisos del sistema. También la necesidad de seguridad





es más importante cuando usuarios inexpertos pueden no tener conocimiento de los orificios en la seguridad que han creado sin saberlo.

El comando chown

Los permisos de archivo y directorio en Linux son controlados a través del uso de dos comandos muy importantes: chown y chmod. El comando chown es ejecutado para todos los usuarios para especificar la pertenencia de usuario y de grupo de un archivo o directorio y sigue este formato:

```
chown nombre_usuario.grupo nombre_archivo
```

Por ejemplo: `chown jperez.executivos reporte_01`

En este ejemplo, el usuario "jperez" y el grupo "ejecutivos" ahora son propietarios del archivo llamado "reporte_01".

El comando chmod

La propiedad de archivos y directorios es otro concepto importante en Linux porque los permisos son declarados tanto para los usuarios como para los grupos en base a esta propiedad. Por ejemplo, si el archivo "reporte_01" permite un acceso completo a los usuarios y deniega el acceso a todos los grupos, entonces jperez podrá acceder al archivo, pero los miembros del grupo ejecutivos serán bloqueados. Estos permisos son declarados usando el comando chmod:

```
chmod modo nombre_archivo
```

Por ejemplo: `chmod 700 reporte_01`

El ejemplo de comando de arriba ha dado al usuario todos los permisos (lectura, escritura y ejecución), mientras que no da permiso a su grupo ni a todos los demás usuarios. Esto está especificado en el "modo" del comando - en este caso: 700. Cada dígito del número representa los tres tipos diferentes de usuarios en el sistema. Comenzando desde la izquierda, el primer dígito representa al usuario (o poseedor), el dígito del medio representa al grupo, y el dígito de la derecha representa a todos los otros usuarios en el sistema (usuario no del grupo). Los tres tipos de permisos (lectura, escritura y ejecución) reciben valores numéricos como sigue:

Lectura = 4

Escritura = 2

Ejecución = 1

Para dar a un usuario en particular permisos específicos, se suman los números apropiados y luego se listan en el orden correcto. Por ejemplo, para dar al propietario permisos de lectura y ejecución, al grupo permiso de ejecución, y a todos los otros usuarios permiso de escritura, el número apropiado sería: 512. Y por supuesto, para no dar permiso se coloca un cero en la categoría de usuario. La asignación de permisos en Linux es en cierta forma más tediosa que la interfase conducida por menús del Windows 2000. Sin embargo, la flexibilidad del Linux tiende a proporcionar un mayor control al administrador de sistemas experimentado.

9.6 Gestión del sistema de archivos

Los dos comandos que utiliza Linux para montar y desmontar sistemas de archivos y particiones son mount y unmount. La sintaxis del comando mount es la siguiente:

```
mount [-alrsvw] [-t tiposa] [-o opciones]
```





Un administrador usará muy a menudo sólo el argumento por defecto con el comando mount. La sintaxis sería la siguiente:

```
mount /dev/hda4 /mnt/Curso
```

Este comando montaría el contenido de /dev/hda4 en el directorio /mnt/Curso, autodetectando el tipo de sistema de archivo y usando las opciones por defecto.

Uso de unmount

El uso del comando unmount es más simple que el de mount. La sintaxis para usar el comando unmount es la siguiente:

```
umount [-anrv] [-t tiposa] [dispositivo | punto_montura]
```

Los parámetros que se usan con el comando unmount son muy similares a los usados con el comando mount.

Las mismas reglas para mount se aplican a unmount teniendo con respecto a quién tiene permitido ejecutar estos comandos. Sólo el usuario raíz puede usar el comando unmount. Esto es a menos que un usuario específico o propietario listado en el archivo /etc/fstab/ tenga permiso para usar el comando unmount para desmontar una partición, sistema de archivo, o dispositivo.

Uso del comando df

El comando df es un comando útil usado para ayudar a administrar sistemas de archivos en máquinas Linux. El comando df dará información sobre un disco rígido o partición que incluye espacio total, usado y disponible. También hay muchos parámetros que pueden ser usados con este comando.

Se puede mostrar información de un dispositivo o partición específica agregando el dispositivo donde reside la partición o cualquier archivo o directorio en el sistema de archivos, lo que limitará la salida a una partición específica.

Uso del comando du

El comando du es un comando muy útil que puede ser usado para mostrar información sobre sistemas de archivos y particiones que están montados en un sistema Linux. Sin embargo, a veces es necesario encontrar información sobre directorios y archivos individuales que están ubicados en una de estas particiones. Por ejemplo, si se necesita liberar espacio en un disco rígido, utilice el comando du para mostrar información sobre el directorio home de un usuario específico para tomar una decisión sobre cuáles archivos mover o eliminar para hacer espacio. Usando el comando du se puede obtener información sobre la partición o unidad completa pero no sobre un directorio específico.

El comando du puede ser usado solo o en conjunto con estos parámetros para mostrar información sobre cualquier archivo o directorio que está montado en un sistema Linux.

Archivos de Configuración del Sistema de Archivos

Hay dos tipos de archivos de configuración para el sistema de archivos de Linux. Son los archivos de Usuario (User) y de Sistema (System). Los archivos de configuración de usuario almacenan información que es específica a un usuario individual como la ubicación de los iconos del escritorio, las preferencias del administrador de ventanas, y scripts que son creados para ejecutarse automáticamente. Los archivos de configuración de usuario son componentes esenciales que forman un sistema multiusuario. Estos archivos almacenan información para cada usuario por lo que





cuando ingresan al sistema, todas sus configuraciones permanecen intactas. Los archivos de configuración del sistema controlan la configuración del sistema en general. Estos son archivos que controlan servicios que son puestos a correr para cada usuario que ingresa al sistema. El saber dónde localizar estos archivos y editar estos archivos ayudará a cualquier administrador a resolver una variedad de problemas asociados con el sistema operativo Linux.

Archivos de configuración del usuario

Como estos archivos controlan la configuración para cada usuario individual, los archivos que almacenan esta configuración son ubicados en el directorio home de cada usuario. Los archivos de configuración del usuario son almacenados como archivos punto (.). Por ejemplo, las configuraciones del usuario para la interface KDE son almacenadas en los archivos `.kde` y `.kderc`. Estos archivos punto están ocultos y son ignorados por la mayoría de las herramientas de Linux. Si se utiliza el comando `ls` para listar el contenido del directorio home de un usuario estos archivos no se verán. Pueden ser listados agregando el parámetro `-a` al comando `ls`. El OS Linux oculta a estos archivos para que no llamen la atención y parezcan que corren en trasfondo.

Archivos de configuración del sistema

Los archivos de configuración del sistema controlan los aspectos del sistema operativo que están relacionados con el sistema en general en oposición a algún usuario específico. Estos archivos se encuentran normalmente en su subdirectorio correspondiente ubicado en el directorio `/etc`. Por ejemplo, los archivos de configuración para Samba se pueden encontrar en el directorio `/etc/Samba`. Hay unas pocas categorías diferentes de archivos de configuración del sistema. Algunos corren cuando el sistema se inicia, otros controlan al sistema después de que se ha iniciado, y otros controlan a servidores específicos en un sistema Linux.

Archivos de configuración del inicio

El programa principal que se utiliza para correr los archivos de configuración del inicio es el `init`. Este programa usa el archivo de configuración `/etc/inittab` para almacenar los datos sobre cómo debería iniciarse el sistema. Red Hat Linux utiliza el script de inicialización `/etc/rc.d/rc.sysinit`, que está especificado en el archivo de configuración `/etc/inittab` para ejecutar una serie de scripts de inicio que indican cómo se supone que se debe iniciar el sistema. Específicamente, estos scripts son ejecutados de acuerdo al nivel de corrida del sistema. Si el sistema está configurado para que se inicie en el nivel de corrida 5, entonces todos los scripts que están configurados para correr en el script de inicialización `/etc/rc.d/rc.sysinit` comienzan cuando el sistema se inicia en el nivel de corrida 5. Todos los servidores y utilitarios del sistema que están configurados para correr en un nivel de corrida en particular son almacenados en archivos de acuerdo al nivel de corrida particular en el que se inician. En Red Hat Linux el nombre de este archivo es `/etc/rc.d/rc#.d`, donde `#` es el número de nivel de corrida. Los scripts que son almacenados en estos archivos son configurados para que inicien o maten a un servidor o utilitario de sistemas en particular cuando el sistema es iniciado en ese nivel de corrida en particular.

El resultado de estos archivos de configuración de inicio es que un administrador puede configurar a un sistema para que controle los servidores y utilitarios de sistemas que son iniciados en cualquier nivel de corrida dado en forma automática mientras el sistema se inicia.



9.7 Demonios

Puede no ser totalmente correcto llamar a estos procesos de Red /NOS "servicios". Quizás un término más genérico e independiente del sistema operativo podría ser más correcto. Esto es porque si los usuarios se refieren a estas funciones como "servicios", están usando el término que Microsoft utiliza para nombrar a estos procesos de Red. Si los usuarios están usando Linux se referirán a estos servicios como Daemons. Los demonios permiten que el sistema operativo proporcione funciones como Internet, compartir archivos, intercambio de correo, servicios de directorio, administración remota, y servicios de impresión. Sin embargo, funcionan un poco diferentes en Windows que en Linux.

Ejemplos de Daemons de Linux son FTPD y HTTPD. Los Daemons no están integrados al sistema operativo como lo están los servicios en el Windows. Los Daemons corren como procesos de trasfondo. Corren en forma continua sin producir ninguna salida visible. Por ejemplo, el Daemon FTP (FTPD) correrá en el trasfondo. A medida que procesa las solicitudes entrantes, envía los archivos necesarios, pero no mostrará nada en la pantalla. Las actividades de los Daemons son registradas en un archivo de registro. Muchos Daemons pueden correr en un sistema Linux en un momento dado. Hay varios Daemons comunes en el Linux:

- HTTPD – Este Daemon es responsable de las solicitudes del navegador de web.
- Inetd – Este Daemon esperará que aparezca una solicitud entrante y luego enviará esa solicitud al Daemon apropiado.
- Crond – Este Daemon ejecutará scripts en un momento determinado.
- Syslogd – Este Daemon registrará información sobre los programas que están corriendo actualmente en el archivo de registro del sistema.

Inicio, Detención y Reinicio de Daemons

Antes de entrar en las descripciones y ejemplos de Daemons específicos de Linux y cómo configurarlos es necesario primero aprender a iniciar o detener estos servicios.

Cuando un sistema Linux está corriendo e incluso cuando no hay nada en la pantalla salvo un prompt de ingreso aun hay varios programas y servicios que están continuamente corriendo. Algunos de estos son programas simples que manipulan cosas como prompts de ingreso basados en texto. Hay otros servicios más complejos que están corriendo que hacen que el sistema esté disponible para otros sistemas externos. Estos daemons necesitan ser iniciados de alguna forma y en ciertas ocasiones incluso necesitan ser detenidos o reiniciados. Linux proporciona varias formas diferentes de configurar un sistema para que inicie daemons y programas.

Uso de scripts Sys V para iniciar y detener servicios y daemons de Linux

Los scripts Sys V pueden ser usados para iniciar, detener o reiniciar los daemons de Linux. Los scripts están ubicados en directorios particulares, por lo común en el directorio `/etc/rc.d/init.d` o `/etc/init.d`. Para ejecutar estos scripts necesitan ser seguidos por opciones como `start`, `stop` o `restart`. La opción `status` también puede ser usada en algunos scripts para obtener información sobre el estado actual en el que está el daemon. Por ejemplo, el siguiente comando reiniciará el daemon del servidor Web Apache en un sistema Red Hat:

```
# /etc/rc.d/init.d/httpd restart
```

Si por alguna razón este script es ejecutado y devuelve un mensaje `FAILED`, éste indica que hay algo mal en la configuración.





Hay algunas cosas que es importante saber cuando se inicia o detiene manualmente un daemon de esta forma.

Primero, dependiendo de la distribución de Linux que se está usando, el nombre exacto del script puede ser ligeramente distinto. Por ejemplo en algunas distribuciones el servidor Samba usa el script smb y en otros usa el script samba para iniciar, detener o reiniciar manualmente el daemon Samba. Otras ocasiones en las que el nombre del script de inicio podría no ser estándar es cuando hay scripts de operaciones complejas que inician varios otros programas junto con el programa o daemon que se quiere iniciar con el script. El script Network o Networking es un ejemplo que está incluido en algunas distribuciones que se usa para iniciar muchas funciones de red.

Segundo, los scripts de inicio Sys V están diseñados para correr en distribuciones particulares de Linux. Un script de inicio Sys V de Red Hat no funcionará en otras distribuciones de Linux.

Tercero, se mencionó antes lo que indica un mensaje FAILED cuando se ejecuta un script. Sin embargo, un script se ejecutará y parecerá estar funcionando bien aunque no esté funcionando correctamente. Si el daemon no está funcionando bien revise el archivo de registro, normalmente ubicado en el archivo /var/log/messages. Este registro puede proporcionar alguna indicación de los errores que se han generado.

Cuarto, siempre es una buena idea leer la documentación específica del daemon para conocer las diferentes opciones que reconoce el script. Esto es porque algunos scripts soportan diferentes opciones que otros. Por ejemplo, algunos daemons necesitan ser reiniciados cuando se hace un cambio de configuración. Para hacer esto, simplemente ejecute el script con la opción restart. Algunos scripts no necesitan ser reiniciados sino que necesitan ser completamente detenidos y luego iniciados de nuevo. Algunos daemons tienen comandos que sólo releen la configuración sin tener que reiniciarse. Inicio o detención permanente de un daemon o servicio con scripts Sys V.

