TEMA

64

Explotación y administración de sistemas en red.

elaborado por
EL EQUIPO DE PROFESORES
DEL CENTRO DOCUMENTACIÓN

1. EXPLOTACION DE UN SISTEMA EN RED

La explotación de un sistema informático se ocupa de producir resultados informáticos de todo tipo: listados impresos, ficheros soportados magnéticamente para otros informáticos, ordenes automatizadas para lanzar o modificar procesos industriales, etc.

La explotación de un sistema se puede considerar como una fabrica con ciertas peculiaridades que la distinguen de las reales.

Para realizar la explotación de un sistema se dispone de una materia prima, los Datos, que es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio del Proceso informático, el cual está gobernado por un software destinado al efecto. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente o al usuario al usuario.

La explotación se divide en:

Control de Entrada de Datos:

Se analizará la captura de la información en soporte compatible con los sistemas, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes.

Se verificará que los controles de integridad y calidad de datos se realizan de acuerdo a las normas establecidas.

Centro de Control y Seguimiento de Trabajos:

Se analizará cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación de un sistema informático ejecuta procesos por cadenas o lotes sucesivos (Batch), o en tiempo real (Tiempo Real).

Mientras que las aplicaciones de teleproceso están permanentemente activas y la función de explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe una buena parte de los efectivos de explotación.

En muchos sistemas informáticos, éste órgano recibe el nombre de Centro de Control de Batch. Y en muchas ocasiones determina el éxito de la explotación, en cuanto que es uno de los factores más importantes en el mantenimiento de la producción.

Batch y Tiempo Real:

Las aplicaciones que son Batch son aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que lo que hace es relacionar toda la información, calcular cosas y obtener como salida, por ejemplo, informes.

O sea, recolecta información durante el día, pero todavía no procesa nada. Es solamente un tema de "Data Entry" que recolecta información, corre el proceso Batch (por lotes), y calcula todo lo necesario para arrancar al día siguiente. Un ejemplo muy claro son los sistemas informático de la banca.

Las aplicaciones que son Tiempo Real u Online, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son sistemas que tienen que responder en Tiempo Real.

Centro de Control de Red y Centro de Diagnosis:

El centro de Control de Red suele ubicarse en el área de producción de explotación. Sus funciones se refieren exclusivamente al ámbito de las comunicaciones, estando muy relacionado con la organización de software de comunicaciones de técnicas de sistemas.

Debe analizarse la fluidez de esa relación y el grado de coordinación entre ambos. Se verificará la existencia de un punto focal único, desde el cual sean perceptibles todos las líneas asociadas al sistema.

El Centro de Diagnosis es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de software como de hardware.

El Centro de Diagnosis está especialmente indicado para sistemas informáticos grandes y con usuarios dispersos en un amplio territorio. Es uno de los elementos que más contribuyen a configurar la imagen de la empresa.

Los procedimientos de explotación de forma general se pueden resumir en, el conjunto de acciones que se realizan en un sistema cuando este funciona de manera normal o anormal.

En la actualidad el software y el hardware de los sistemas informáticos es altamente sofisticado, y manejan información critica en la mayoría de las ocasiones por lo que se hacer imprescindible el establecer una serie de normas de uso sobre el sistema de manera que produzca un correcto funcionamiento del mismo.

Para ello son necesarias un serie de medidas:

- Se debe restringir al acceso al sistema de personal no autorizado.
- Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.
- Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.
- No debe permitirse la entrada a la red a personas no autorizadas, ni a usar los terminales.
- Se deben realizar periódicamente una verificación física del uso de terminales y de los informes obtenidos.
- Se deben monitorizar periódicamente el uso de la información que se está mostrando en los terminales.
- Se deben hacer auditorías periódicas sobre el área de operación y la utilización de los terminales.
- El operador es el responsable de los datos, por lo que debe asegurarse que los datos obtenidos de otros sistemas sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.
- Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.
- Debe controlarse la distribución de las salidas (informes, cintas, etc.).

- Se debe guardar copias de los archivos y programas en lugares ajenos al edificio donde se encuentra ubicado el sistema informático.
- Se debe tener un estricto control sobre el acceso físico a los archivos.
- En el caso de módulos del sistema, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.
- Se debe tener establecida una política de backups de los datos con los que se trabaja en el sistema, haciendo copia totales, incrementales o diferenciales en cada caso.

Todas estas normas de uso estarán referidas a:

- Entradas.
- Salidas.
- Procesos.
- Especificaciones de datos.
- Especificaciones de proceso.
- Métodos de acceso.
- Operaciones.
- Manipulación de datos.
- Frecuencia y volúmenes de operación.
- Sistemas de seguridad.
- Sistemas de control.

Y por último todas los procedimientos de uso quedarán reflejados en:

- Manual del usuario de todos los módulos del sistema.
- Descripción de flujo de información y/o procesos.
- Descripción y distribución de información.
- Manual de formas.
- Manual de informes.
- Lista de archivos y especificaciones.

Todo esto nos lleva a saber;

- Qué se hace en el sistema informático.
- Quién lo hace.
- Cuándo lo hace.

- Cómo lo hace.
- Sobre qué lo hace.
- Y dónde lo hace.

Aplicaciones de Acceso Remoto

La tecnología de acceso remoto esta optimizada para varias aplicaciones remotas:

Nodo y control remotos: estas aplicaciones son aquellas en las que un usuario remoto desde un PC o estación de trabajo llama para entrar en una red y puede funcionar como punto de la misma (nodo remoto) o para permitirle tomar control de un nodo local (control remoto).

LAN-a-LAN: se soporta una red remota completa por medio de una conexión telefónica; los servidores de acceso remoto en cada extremo actúan como routers para generar una conexión automáticamente cuando se piden recursos remotos; la conexión se mantiene según parámetros establecidos por el administrador de la red para las interrupciones, protocolos permitidos y duración de la conexión.

Acceso a Internet: estas aplicaciones involucran el uso de un servidor de acceso remoto como un router para proteger la red local de los problemas de seguridad presentes en Internet; los filtros son configurados por el administrador de la red para asegurar que sólo se permita al tráfico autorizado pasar entre la red local e Internet.

Compartición de Módems: la habilidad del servidor de acceso remoto de proporcionar acceso a los usuarios de la red a un banco de módems tanto para aplicaciones de entrada como de salida de datos; un software ejecutándose en los servidores de red (normalmente denominado un "redirector") permiten a los usuarios conectarse a los módems conectados a su vez a un servidor de acceso remoto.

La clave para controlar los costes es la habilidad del servidor de acceso remoto para encaminar los protocolos deseados y llevar a cabo decisiones basado en políticas de cómo se manejan las conexiones de marcado entre los diversos sitios.

Estos parámetros incluyen: cantidad de tiempo que el enlace permanecerá conectado si no se está transmitiendo ningún dato; si el enlace permanecerá conectado si sólo ciertos tipos de tráfico están presentes (es decir desconexión en caso de que sólo se están transmitiendo mensajes de control, broadcast, etc.); si se ha de permitir o no a un protocolo en

particular o tipo de paquete viajar a través del enlace entre las dos redes. Algunas características adicionales son la rellamada automática en caso de un módem o línea ocupada, una desconexión no planificada, y limitaciones de entrada/salida de llamadas en función de la hora del día.

2. ADMINISTRACIÓN DE SISTEMAS EN RED

2.1. EL ADMINISTRADOR DE LA RED

El administrador (ó equipo de administración) de un sistema de red es la persona encargada de las tareas de administración, gestión y seguridad de los equipos conectados a la red y de la red en su conjunto, tomada como una unidad global.

Esta unidad global abarca, los servidores de red, las estaciones de trabajo, el hardware de red, el software de red, los servicios de red, las cuentas de usuarios,...

Entre las funciones básicas que debe de realizar un administrador, cabe destacar:

- Instalación y mantenimiento de la red. Esta es la función primaria del administrador. No basta con instalar el sistema operativo de red, sino que hay que garantizar el funcionamiento de los equipos con el paso del tiempo. Ello exige tener las herramientas adecuadas y los conocimientos necesarios para realizar esta función. En la actualidad el trabajo propio de mantenimiento puede ser realizado por miembros de la propia empresa o bien contratar estos servicios en terceras empresas (outsourcing).
- Determinar las necesidades y el grado de utilización de los distintos servicios de red, así como los accesos de los usuarios.
- Diagnosticar problemas y evaluar las posibles mejoras.
- Documentar el sistema de red.
- Informar a los usuarios de la red de los nuevos servicios así de sus accesos.

2.2. CONTROL DE LA CONGESTIÓN DE UNA RED

Una de las tareas más habituales con las que se encuentra un administrador de red es el número de usuarios concurrentes sobre la tecnología del sistema de red empleado. Este es uno de los problemas que nos hacen ver que determinadas tecnologías, características, parametros,... se han quedado limitados. En la actualidad esto sucede sobre todo con LAN con tecnología Ethernet en las que según se van agregando usuarios o según las aplicaciones requieren más datos, las prestaciones se deterioran. Esto es debido a que todos los usuarios en una LAN entran en competencia por el bus Ethernet. Una red Ethernet de 10 Mbps. mode-

radamente cargada puede sostener una utilización del 35% y prestaciones en el entorno de 2.5 Mbps. después de considerar la carga del protocolo, tramos entre paquetes, y colisiones. Una red Fast Ethernet moderadamente cargada comparte 25 Mbps. de datos reales, en las mismas circunstancias.

Los Factores que Afectan a la Eficacia de la Red son, y que serán a tener muy en cuenta por parte del equipo gestor-administrador de la red:

- Cantidad de tráfico.
- Número de nodos.
- Tamaño de los paquetes.
- Diámetro de la red.

Y estos factores serán medidos a través de:

- Promedio de picos de desvío de carga.
- Tasa de colisión.
- Tasa de utilización.

La tasa de utilización es otra estadística ampliamente usada para indicar la salud de una red. Esta estadística está disponible en el monitor de la Consola de Novell y en el monitor de prestaciones de WindowsNT, así como a través de otros paquetes opcionales de software de análisis de LAN. Una tasa de utilización por encima del 35% indicado anteriormente, pronostica problemas potenciales. La utilización del 35% es casi óptima, pero algunas redes experimentan tasas de utilización más altas o más bajas debido a factores como el tamaño del paquete y la desviación de los picos de carga.

Los tiempos de respuesta de la red (las prestaciones de la red visibles desde el punto de vista del usuario) sufren según se incrementa la carga de trabajo de la red, y bajo cargas pesadas los pequeños aumentos en tráfico del usuario a menudo tienen como consecuencia disminuciones significantes en las prestaciones.

Mediante el uso de utilidades de red existentes en la mayoría de los sistemas operativos de servidores que se conectan a una red. el administrador puede determinar las tasas de utilización y colisión. Deben considerarse promedios y picos.

2.3. PROTECCIÓN DEL SISTEMA

La protección de la red comienza, después de la instalación de la red. Un sistema de red que cubra muchas necesidades y brinde muchos servicios debe ser muy seguro, por lo que hay que implantar mecanismos de seguridad contra los distintos riesgos que puedan suceder en el sistema.

2.3.1. Protección eléctrica

Todos los dispositivos de una red necesitan corriente eléctrica para su funcionamiento.

Debido a esta necesidad, y a las perturbaciones que sufre la corriente eléctrica, hay que proteger el sistema sobre estos riesgos. Además de estas perturbaciones, se añade otro problema, las caídas de tensión, que hacen perder información no almacenada en el mejor de los casos, pudiendo llegar incluso a dañar discos o dispositivos de red en el peor de los casos. Para la solución de este problema se utilizan unos dispositivos llamados SAI (sistemas de Alimentación Ininterrumpida) o UPS.

Normalmente los SAI corrigen las deficiencias de la corriente eléctrica, como subidas de tensión, además de asegurar el flujo de corriente continuo en caso de cortes de tensión.

El SAI tiene en su interior una serie de acumuladores que se cargan cuando el sistema de red funciona en régimen normal, y que en caso de corte eléctrico, produce energía eléctrica de forma que los equipos puedan seguir trabajando.

Existen fundamentalmente dos tipos de SAI:

- SAI de modo directo, en el que la corriente eléctrica alimenta al SAI y este proporciona energía constante a las máquinas y dispositivos de la red.
- SAI en modo reserva, en el que la corriente se suministra a las máquinas y dispositivos de la red, actuando el SAI solo en caso de ausencia de corriente.

2.3.2. Protección de datos

La parte de la información más crítica para proteger son los datos de los usuarios, ya que las aplicaciones comerciales en el pero de los casos se pueden volver a instalar.

La forma más segura de proteger la información es duplicándola, pero el cómo hacer esta duplicación es una tarea que debe ajustar muy bien el administrador del sistema.

Las copias de los datos, se realizan en lo que se llaman copias de seguridad o backups. Estas copias se suelen realizar mediante utilidades incorporadas en las herramientas de gestión de la red. Normalmente esta tarea se automatiza dé forma que se realice unos días determinados a unas horas determinadas, haciendo el volcado de la información normalmente a cintas magnéticas, las cuales tienen gran capacidad de almacenamiento, además de utilizar los controladores buenos algoritmos de compresión de datos.

Otra posibilidad que ha caído en desuso, es hacer las copia en discos removibles.

El administrador debe establecer una política de copias de seguridad:

- Copia normal: en la que es el administrador el que selecciona que directorios, ficheros, cuentas de usuarios,... se van a copiar.
- Copia progresiva: en la que la copia se realiza sobre los objetos de red seleccionados en la copia normal pero que hayan sido modificados desde la última copia progresiva.

2.3.3. Sistemas tolerantes a fallos

Otro de los temas a tratar en la protección de la información, es que mecanismos se establecen para que los usuarios de la red puedan seguir trabajando aunque se presenten ciertos problemas sobre ciertos dispositivos de red. Bien pues un sistema tolerante a fallos, es esto, es decir un sistema que aún con ciertos problemas de red permite a los usuarios seguir trabajando. Dichos problemas pueden estar relacionados con fallos en los servicios de red, fallos en el sistema operativo, fallos en el software de la red, fallos de corriente eléctrica,...

Los sistemas de red en este sentido, lo que suelen hacer es duplicar los elementos del sistema. En muchas ocasiones esto es teoría porque, el coste económico es muy importante, por lo que lo que se suele hacer es duplicar solo los elementos más críticos del sistema, y en primera posición tenemos los discos.

En los discos, el caso mas utilizado es tener los discos en espejo (mirror). Es decir se duplican los discos de modo que cualquier operación de escritura llevada a cabo en un disco también se realiza en el otro.

La tecnología mas extendida en la duplicación de discos es la RAID (serie redundante de discos económicos) que ofrecen una serie de niveles de seguridad, que van desde RAID de nivel 0 en el que los datos se reparten entre varios discos, no ofreciendo redundancia de datos, pero incrementando el rendimiento de accesos a disco, hasta RADI de nivel 5 donde los

datos se dividen en bloques repartiendose la información de paridad de modo rotativo entre todos los discos.

2.3.4. Sistema de acceso a la red

El primer aspecto en el que nos debemos fijar una vez instalado el software de red, es establecer un sistema de acceso a la red para todos y cada uno de los usuarios.

El orden y la confidencialidad de cada uno de los puestos de trabajo requieren un sistema que garantice que cada usuario tenga sus datos y aplicaciones en perfecto estado, evitando que cualquier otro usuario pueda ser perjudicado por el uso indebido del sistema.

Uno de los modos mas extendidos y efectivos de hacer distinciones entre cada uno de los usuarios es a través de cuentas de acceso personalizadas.

2.3.4.1. Cuentas de usuario

Las cuentas de usuario son el modo normal de personalizar el acceso a un sistema en red. Así, toda persona, que utilice la red con regularidad deberá tener una cuenta de acceso.

Para que este control sea efectivo, las cuentas deben ser personales para cada uno de los usuarios, contando cada una de ellas con un conjunto de características propias de cada usuario.

Este conjunto de características de cada una de las cuentas suelen ser:

Nombre de usuario: Nombre único que pertenece a cada usuario y que este se utiliza para identificarle en el acceso a la red. Se suele llamar login, y suele ser una cadena de caracteres con una longitud mínima y una máxima.

Dependiendo la política de acceso de los administradores de la red, esta cadena de caracteres deberá contener, símbolos, caracteres alfanuméricos y caracteres numéricos y normalmente se obliga a cambiarla periódicamente para dotar al sistema de mas seguridad.

Contraseña: cadena de caracteres encriptada, que se utiliza para autentificarse y entrar al sistema de red.

Nombre Completo de usuario: cadena de caracteres con el nombre completo de los usuarios. Este campo permite un mayor número de caracteres que en el login. Y este campo

es útil cuando se produce auditorias en una empresa, donde se captura el tráfico de la red local, con los nombres completos de cada uno de los usuarios, para que el equipo que audita que hace que en cada momento.

Horario permitido de acceso a la red: este campo describe las horas, y los días a los que el usuario tiene acceso a la red. Fuera de estos periodos de tiempo se denegará de forma automática el acceso al usuario. Este campo por defecto los sistemas operativos de red lo mantienen en blanco dejando el acceso a todas las horas al usuario.

Estaciones de inicio de sesión: Describe el nombre de los equipos desde donde una usuario puede conectarse a la red.

Caducidad: describe la fecha en la que la cuenta del usuario expirará. Es útil para cuentas de usuarios que solo requieren accesos por periodos de tiempo concretos. Al desactivarse la cuenta, se impide que intrusos se apropien indebidamente de ella. Por tanto este parámetro protege y descarga al servidor de intrusos y accesos indebidos.

Directorio particular: es el lugar físico dentro del sistema de ficheros de la red en el que el usuario puede guardar sus datos. Al presentarse en la red, el sistema operativo de esta, le posiciona en este directorio.

Archivos de inicio de sesión o Profiles: son archivos pertenecientes a cada uno de los usuarios donde existe un conjunto de comandos que se ejecutan cuando el usuario entra con su cuenta en el sistema. Este conjunto de comandos preparan o adaptan el entorno de trabajo del usuario.

Perfil de usuario: cuando un usuario es dado de alta por el administrador se le deberá asignar un perfil, como operador, desarrollador, administrador de bases de datos,... de forma que el administrador pueda crea roles de usuarios y asignarselos a cada uno de los perfiles creados.

Cuota de disco: normalmente a cada uno de los usuarios de un sistema en red se les asigna una cantidad de espacio de disco, para que puedan trabajar. Esto es una de los parámetros importantes que debe ajustar un administrador ya que influirá en el rendimiento de la red.

Éstos son los parámetros básicos acerca de las cuentas de los usuarios de los que una buena gestión de red por parte de un administrador de esta, deberá tener siempre asignados y ajustados a cada uno de los usuarios.

2.3.4.2. Derechos de acceso

Una vez que se ha identificado un usuario con acceso a la red, se deberían arbitrar cuales son sus derechos de acceso. Corresponde al administrador de la red el uso de cada uno de los recursos de la red o las operaciones que cada uno de los usuarios puede realizar.

Cada servicio, recurso o utilidad tiene una información asociada que le indica quien puede utilizarlos y de que forma, de esta forma se denegará el acceso a los usuarios que no dispongan de dicho privilegio.

En este punto es necesario hacer una distinción entre permiso y derecho:

- Un derecho autoriza a un usuario o a un grupo de usuarios a realizar determinadas operaciones sobre un servidor o estación de trabajo.
- Un permiso o privilegio es una marca asociada a cada recurso de red: ficheros, directorios, impresoras,... que regula que usuario tiene acceso y de que manera.

De esta forma los derechos se refieren a operaciones propias del sistema operativo, mientras que los permisos se refieren al acceso de los distintos objetos de la red. Una cosa que debe tener muy clara el equipo de gestión de un sistema de red local es que los derechos prevalecen sobre los permisos.

Esto suele ser uno de los grandes agujeros de los sistemas de red, ya que por defecto se les asigna a los usuarios derechos y permisos en exceso para realizar sus trabajos, haciendo operaciones indebidas con alguno de los privilegios, lo que hace a los piratas informáticos encontrar puertas de entrada.

La asignación de permisos para los usuarios de una red se realiza en dos fases:

1. Se determina el permiso de acceso sobre el servicio de red, por ejemplo asignar el permiso de conexión sobre un disco de la red remoto.
2. Deben configurarse los permisos de los ficheros y directorios que contiene ese servicio de red.

En las redes en las que coexisten varios sistemas operativos de red de distintos fabricantes deben determinar los permisos para cada uno de ellos. A veces los permisos en un tipo de sistema operativo son fácilmente transladables a los otros sistemas operativos, pero en otros casos esto no sucede así.

2.3.4.3. Cuentas de grupo

Para facilitar las tareas de administración de un sistema de red, el uso de los servicios o recursos se organizan en función del acceso de los usuarios, creando entidades de administración llamadas cuentas de grupo.

Una cuenta de grupo no es mas que la colección de un conjunto de cuentas de usuario. Al conceder a un usuario la pertenencia a un grupo se le asignan todas las propiedades, derechos, permisos de ese grupo. De esta forma se centraliza la configuración de acceso y uso sobre determinados recursos de red de manera sencilla para los administradores.

En un sistema de red suelen ser cuentas de grupo comunes, administradores, operadores de copia, operadores de consola, usuarios avanzados y usuarios finales.

2.3.4.4. Perfiles de usuario

En ciertas ocasiones, los administradores deben hacer posible que un usuario no solo accedan a la red desde una estación de trabajo, sino que lo pueda hacer desde diferentes máquinas localizadas en diferentes lugares físicos, para solucionar esto aparecen los perfiles de usuario.

De esta forma a cada uno de las cuentas de usuario se les asigna un perfil de forma que la conexión se realice independientemente del lugar de conexión haciendo transparente el trabajo desde una u otra estación.

Además los perfiles de usuario, permiten al administrador de la red restringir el uso de determinados programas a ciertos grupos de usuarios.

Estas operaciones, son realizadas desde herramientas que ofrecen los sistemas operativos de red.

2.3.4.5. Sistemas globales de acceso

El crecimiento de las redes, en cuento al número de nodos se refiere, y su organización en grupos de trabajo, subredes, dominios,... así como la integración de varios sistemas operativos de red de distintos fabricantes ha llevado a diseñar un sistema de presentación de los usuarios que sé más global.

Estos sistemas de acceso global lo que permiten a los usuarios es presentarse en un sistema, y luego acceder de forma transparente a todos los recursos y servicios de red a los que tengan acceso estén localizados dentro de su subred o en otro dominio. Con estos sistemas de acceso se elimina el trabajo al usuario de tener que identificarse en todos los sistemas a los que acceda.

En la actualidad la mayoría de los sistemas operativos de red como por ejemplo Windows NT, implementan lo que se llaman relaciones de confianza, entre los distintos grupos de la red. Una relación de confianza es un vínculo entre grupos o dominios para facilitar la utilización de recursos de ambos grupos o dominios, dando lugar a una única unidad administrativa de gestión de red.

Simplificando, podemos establecer dos tipos de relaciones de confianza:

- Unidireccional: en la que un dominio confía en los usuarios de otro dominio. Los recursos de red son servidos por el dominio que confía, pero sin embargo los accesos son posibles desde cualquiera de los dominios sin necesidad de que los usuarios de dominos remotos tengan cuenta en el propio dominio del recurso.

- Bidireccional: en este caso cada uno de los dominios puede albergar tantas cuentas como recursos. Por tanto una relación bidireccional entre dominios se compone de dos relaciones unidireccionales de sentido inverso.

Con el fin de optimizar la organización de la red, es conveniente establecer un dominio maestro centralizador de todas las cuentas de la organización y crear una serie de dominios poseedores de recursos de red, sobre los que se establezcan las relaciones de confianza necesarias para su utilización.

2.3.4.6. **Autentificación de usuarios**

Hacer negocios en las redes puede ser arriesgado: los usuarios, mensajes, documentos, software, servidores y otros componentes del mundo online no siempre son lo que parecen. A medida que más usuarios, ya sean empleados, clientes o suministradores, acceden a las redes internas de las empresas aumenta la necesidad de disponer de potentes y eficaces herramientas de autentificación.

La protección que proporcionan las claves o palabras de acceso (password) no es suficiente para asegurar los accesos a la red. Los "piratas informáticos" son capaces de adivinar o interceptar claves de texto pleno y utilizarlas como si fuesen usuarios autorizados. Los

ficheros y mensajes electrónicos pueden ser modificados por terceros no autorizados antes de que lleguen a sus verdaderos destinatarios.

Para obtener un mayor nivel de seguridad es preciso emplear productos de autentificación, que permiten proteger las redes mediante técnicas de encriptación capaces de verificar la integridad e identidad de origen de usuarios, peticiones de recursos, ficheros, mensajes, paquetes, módulos de software y nodos de red. Aunque estos productos difieren entre sí en cuanto a su arquitectura, todos ellos se basan en un procedimiento de entrada al sistema que incluye al menos dos factores de autentificación: una clave de acceso y algún elemento del tipo de "testigo o pase" (token) seguro, diálogo pregunta/respuesta, lector y tarjeta inteligentes, bioidentificación, firma digital o criptografía de clave privada o pública.

Existen dos grandes categorías de soluciones: la oferta de autentificación de usuario, que suministra accesos SSO (single sign-on) a los recursos de red, y productos de autentificación de objetos, que validan tanto la autenticidad e integridad de los mensajes y ficheros como la de los usuarios que los han originado. Como, por lo general, los fabricantes proporcionan herramientas de programación, es posible integrar sus soluciones en la red. Así, aunque algunos productos se implementan, por ejemplo, como servidores de autentificación autónomos, proporcionan herramientas para añadir el código necesario a las estaciones de trabajo a las que dará servicio. Otros, por el contrario, ofrecen el código requerido para incorporar servicios de autentificación a los servidores y clientes de la organización.

- Autentificación de usuario

Los productos de Autentificación de usuario utilizan "testigos" o "pases" basados en hardware o software para responder a las peticiones de comprobación criptográficas procedentes de los servidores de Autentificación. Cuando se inicia un acceso a la de red con identificación de usuario y clave de acceso, se recibe una cadena numérica. Si se trata de un dispositivo de testigo de mano, el usuario ha de escribir en esa cadena su número de identificación personal (PIN). El token utiliza una clave y algoritmo secretos para producir una clave de acceso irrepetible y sólo para esa ocasión, mostrándola en una pantalla LCD. Entonces, el usuario ha de introducir dicha clave de acceso en el ordenador y, si coincide con la que espera el servidor de autentificación, consigue un acceso garantizado.

Con todo, los tokens de mano no siempre son un método idóneo, puesto que obliga a contar con dos dispositivos de entrada (el teclado del ordenador y el teclado numérico del dispositivo de testigo) y dos dispositivos de display (el monitor del ordenador y el LCD del testigo).

En ocasiones es preferible utilizar tokens de software, ya que hace innecesario introducir otra cosa que no sea una clave de acceso o PIN, puesto que se encargan de responder a los mensajes del servidor de autentificación.

Pero por mucha alta tecnología en que se basen, los tokens serán tan seguros como las claves de acceso o PIN que los usuarios deben introducir en ellos. Ahora bien, cuando se implementan y utilizan correctamente, proporcionan un gran nivel de seguridad matemática respecto a la identidad de usuarios, información y recursos de red.

Para conseguir una seguridad prácticamente total, es casi imprescindible emplear elementos biométricos, tales como reconocimiento fisonómico, vocal o de la huella digital. Pero, en la práctica, tal nivel de autentificación sólo será necesario para acceder a información y recursos muy restringidos.

Si para una organización el primer requerimiento consiste en autentificar accesos de usuario a gateways de comunicaciones externas, puertos de mantenimiento y administración de sistemas, routers de marcación y "cortafuegos" (firewall), debería optar por soluciones en las que los servidores de autentificación garantizan o deniegan las peticiones del software cliente de autentificación instalado en el punto de entrada de la red o en el gateway gracias a una base de datos de datos de ID de usuarios, claves de acceso, PINs y claves privadas.

• Autentificación de objetos

Para la autentificación de mensajes, ficheros y otros objetos transmitidos y almacenados en la red, se han de considerar productos que usen tecnologías de firma digital basadas en Public Key Cryptography Standards (PKCS), de RSA Data Security. Una firma digital consiste en una cadena alfanumérica que autentifica al creador de un objeto y da fe de que dicho objeto no ha sido alterado.

Para producir una firma digital, el objeto original se procesa con programas de "resumen" (hashing) del tipo de Secure Hash Algorithm, Message Digest 2, y MD 5, que modifican la cadena de bits del objeto de un modo determinístico. El resultado sé encripta con la clave privada del creador, produciendo la cadena de la firma digital, que será unida y/o transmitida con el objeto original junto con una clave publica para su validación.

El receptor puede verificar la firma digital decodificándola con la clave pública del emisor para recuperar el "resumen" transmitido y entonces correr el programa hashing

de nuevo. Si la cadena de bit resultante es idéntica a la transmitida, existe un elevadísimo grado de certidumbre de que el objeto ha sido originado por el emisor apropiado y no ha sido modificado.

• Herramientas de desarrollo

Como una vez seleccionado un producto de autentificación, el siguiente paso es integrarlo con las redes y aplicaciones corporativas, la evaluación de interfaces de programación de aplicaciones (API) y herramientas de desarrollo suministradas por los fabricantes se convierte en un punto crítico.

Las API permiten que las características y servicios de autentificación sean accesibles desde las aplicaciones de la empresa o transformar los equipos existentes en clientes de los servidores de autentificación. Algunos fabricantes van mas allá y proporcionan kits de desarrollo de software criptográfico sofisticado (SDK) y Dynamic Link Libraries (DLL). El kit de herramientas debe garantizar la construcción de funciones de autentificación de gran rendimiento que sean integradas con los entornos de servidor y de sobremesa corporativos.

• Integración creciente

Es de esperar que, a medida que crezca el mercado de comercio electrónico, flujo de trabajo y otras aplicaciones de internetworking, la demanda de autentificación irá en progresivo aumento, haciendo que el trabajo de los administradores de la red más crítico aún si cabe. En el futuro próximo, las capacidades de autentificación sofisticadas, como firma digital y tokens de software, serán incorporadas directamente a la mayoría de los entornos operativos, aplicaciones, productos de acceso remoto, sistemas de mensajería y "cortafuegos".

2.4. DOCUMENTACIÓN DEL SISTEMA EN RED

Ante la posibilidad de cualquier mejora, cambio o problema que pueda surgir en la red, es evidente que tener un sistema bien documentado con la información del sistema de red, lo mas actualizado posible, puede llegar a ser mucho menos complejo de hacer el trabajo.

En cualquier sistema de red, la documentación que deberá mantener un administrador de red debe estar referida a:

• **Mapa de red:** que es una representación gráfica de la topología de la red.

- **Mapa de nodos:** que es una descripción tanto software como hardware de cada una de las máquinas que componen el sistema de red. Además en esta información también se debe almacenar la configuración de cada uno de los modelos y sus características.
- **Mapa de protocolos:** es una descripción de la organización lógica de la red, así como los protocolos que se utilizan de forma global.
- **Mapa de grupos y usuarios:** descripción de los grupos y usuarios de red, perfiles, accesos y permisos.
- **Mapa de recursos y servicios:** recursos disponibles y servicios que se prestan en toda la red. Para cada uno de los servicios se describirá su localización física y lógica.
- **Calendario de averías:** registro de averías de la red, indicando el motivo y la solución.
- **Informe de costes:** estudio económico del mantenimiento y estudios sobre las nuevas inversiones a realizar.

2.5. CONFIGURACIÓN DE UN SISTEMA EN RED

Una vez que sabemos cual es el sistema operativo elegido, de acuerdo a sus características y necesidades a cubrir, lo único que nos queda es realizar la configuración del sistema operativo además de los servicios y dispositivos que componen la red. Debido a que como hemos visto en el apartado anterior las facilidades, los parámetros, elecciones,... son muy variados y diferentes, a continuación se describen los parámetros o las pautas más normales cuando se realiza la implantación de un sistema de red.

- La dirección (IP, IPX,...) del sistema, con el que se reconocerá a cada uno de los equipos de la red.
- Máscara de red, con este parámetro se especificarán cuales son los nodos que pertenecerán a la red y cuales no.
- Dirección de la pasarela o gateway, cuya función es resolver el destino de los paquetes que lleguen a la red de área local con una dirección desconocida.
- Protocolos que se desean instalar,(TCP/IP, AppleTalk, IPX,...), pero además también deberemos configurar e instalar el protocolo SMTP si queremos tener correo electrónico, SNMP si queremos hacer una gestión remota de la red, NFS si queremos enlazar discos externos de la red,...
- Elección del nombre del servidor de la red.
- Elección del sistema de ficheros que soportará el servidor.
- Elección del controlador de discos, IDE, SCSI,...
- Parámetros de configuración de la tarjeta controladora de discos (IRQ, DMA, Puerto de E/S,...).

- Elección del adaptador de red.
- Elección de los protocolos de red.
- Copia de ficheros de red al servidor.
- Configuración del NDS (Sistema de nombre de dominio).
- Creación de los ficheros de configuración de la red.
- Configuración de permisos y perfiles de usuarios.
- Los servicios de los que dispondrán los usuarios. Estas configuraciones dependerán de las características de los dispositivos suministradas por los fabricantes. Los servicios básicos de una red de área local son: correo electrónico, servicio de impresión, servicios de acceso a disco, servicios de acceso a máquinas remotas y acceso exterior a Internet.

RESUMEN

El administrador (o equipo de administración) de un sistema de red es la persona encargada de las tareas de administración, gestión y seguridad de los equipos conectados a la red y de la red en su conjunto, tomada como una unidad global.

Esta unidad global abarca, los servidores de red, las estaciones de trabajo, el hardware de red, el software de red, los servicios de red, las cuentas de usuarios,...

Entre las funciones básicas que debe de realizar un administrador, cabe destacar:

Las arquitecturas de gestión conforman el marco necesario para una gestión integrada de redes y sistemas basada en estándares e independiente de fabricantes.

Los submodelos debe implementar una arquitectura de gestión con vocación de integración de entornos heterogéneos. Estos submodelos abarcan aspectos tales como:

– Descripción de los objetos gestionados (modelo de información).
– Manejo y soporte de los aspectos organizacionales (modelo organizacional).
– Descripción de los procedimientos de comunicación para propósito de gestión (modelo de comunicación).
– Estructuración de las tareas de gestión (modelo funcional).