Tema 3

Administración de redes de área local. Gestión de usuarios. Gestión de dispositivos. Monitorización y control de tráfico.

Guion-resumen

1. Introducción

Una de las definiciones de red podría ser la que la muestra como un número de equipos independientes que se conectan con el objetivo de compartir datos y otros recursos.

La palabra clave es "compartir", pues es el propósito fundamental a la hora de definir una red. La capacidad de compartir información y dispositivos de forma eficiente es lo que le proporciona a los sistemas informáticos conectados en red su potencia.

Aun así, no pueden olvidarse los aspectos de negocio y económicos. Desde las primeras redes, la respuesta a la pregunta de por qué son necesarias siempre ha sido la misma: las redes aumentan la eficiencia y reducen los costes. Las formas para conseguirlo suelen ser:

— Compartiendo información. Existen numerosos indicadores que muestran que cuando se comparte información se reducen costes, aumenta la productividad y mejora la comunicación.

— Compartiendo hardware y software. Desde el principio fue uno de los grandes objetivos, reducir el gasto en periféricos de coste elevado. La evolución técnica permite compartir sistemas de almacenamiento de grandes prestaciones. De forma adicional, la gestión del software también se mejora gracias al uso de una red, tanto en su despliegue como en su mantenimiento y coste de licencias.

— Centralizando la administración y el soporte de los sistemas informáticos. Administradores y técnicos de soporte se benefician de la existencia de una red, tanto por aspectos de homogeneidad en hardware y software como por la asistencia, que podrá hacerse en remoto, eliminando la obligación de desplazamiento. No es una cuestión menor, sobre todo en organizaciones con un alto grado de dispersión geográfica.

Podría establecerse una analogía entre una red que conecta sistemas informáticos y un equipo, tanto de una disciplina deportiva como de un proyecto empresarial. A través de los esfuerzos de todos los elementos involucrados, se cumplen los objetivos. Compartir y comunicar pueden parecer tareas sencillas pero la realidad es muy diferente. El gran número y complejidad de las tareas que pueden llegar a formar parte de una red, sobre todo en grandes organizaciones, exigen la presencia de profesionales que se encarguen de su administración.

Este conjunto de tareas podría resultar abrumador sin la ayuda de herramientas, de utilidades y plataformas de gestión. Permiten realizar de manera eficiente la gestión de usuarios, de dispositivos –desde discos hasta impresoras–, así como gestionar uno de los aspectos que más incidencias puede ahorrar y que más puede mejorar muchos de los flujos de negocio en una organización: la monitorización y el control del tráfico de red.

2. Administración de redes de área local

La administración de un sistema en red consiste en el conjunto de tareas que garantizan su correcto funcionamiento y documentación. Entre estas tare-

as, puede citarse, por ejemplo, la asignación del direccionamiento, segmentación de la red y definición de redes privadas virtuales (en inglés *Virtual LANs*, VLANs), uso de servidores, administración de usuarios y recursos o el control de los mecanismos de monitorización y gestión de la red. Conviene no olvidar la gestión de la seguridad de la red, de gran relevancia tanto hacia el interior de la organización como hacia el exterior.

Los objetivos de la administración de red persiguen la continuidad de la operatividad, resolución de incidencias, su uso eficiente, reducción de costes, seguridad, control de cambios y gestión de la configuración entre otros.

La gran mayoría de las tareas de administración de una red van a precisar la intervención de un sistema operativo de red. Aspectos como la gestión de memoria, tiempo de CPU, asignación de discos o la gestión de dispositivos periféricos dependen del sistema operativo de red.

La elección del sistema operativo de red no es una decisión sencilla. La dirección de tecnologías de información ha de, en primer lugar, determinar la arquitectura de la red que mejor se adecúe a las necesidades de la organización. Aspectos como la interoperabilidad, el tipo de servicios de red que se requerirán o la seguridad determinarán, sin duda, la elección.

Administrar una red precisa conocer la información referente a su estado y subsistemas, en forma de registros, eventos, etc., de manera que se presente a los administradores de forma legible y manejable. La información debe almacenarse y estar disponible para su análisis o tomar las acciones correctivas necesarias.

Serán necesarios servidores de consulta para lograr una gestión eficiente de los recursos. Servicios como Directorio Activo, Windows Internet Naming Service (WINS) o Network Information System ayudarán al sistema operativo en esta fundamental tarea de administración.

La administración exigirá una definición correcta de cuentas, grupos, dominios y unidades organizativas (OUs), etc. La asignación de permisos para el acceso a los recursos y la definición de grupos, dominios o unidades organizativas es responsabilidad del administrador.

La administración de usuarios debe incluir la información de los procedimientos de uso del sistema y documentarlo con guías.

En cuanto a la administración de periféricos, como las impresoras o sistemas de almacenamiento, suele ser normal implementar un servidor dedicado a esas tareas. Los sistemas operativos incluyen facilidades como la compartición o la definición de prioridades y permisos.

Los servidores de archivos, por su parte, agilizan la administración de ficheros en red, en lo relativo a permisos de acceso, a la coordinación de dicho acceso para gestionar situaciones de accesos simultáneos evitando posibles conflictos y recuperación remota de información.

Otro de los pilares de la administración es la monitorización de red, que facilita en tiempo real información del nivel de operatividad del sistema y su

rendimiento. Una monitorización eficiente puede conseguir adelantarse a la aparición de incidencias; es una administración proactiva, que permitirá al administrador adoptar medidas.

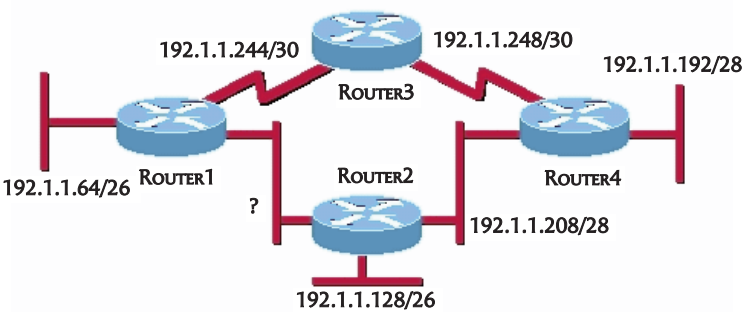
La monitorización debe incluir la redacción de informes periódicos sobre los aspectos de gestión de la red, tales como la configuración, respuesta frente a errores o su seguridad.

Por último, la planificación de la seguridad es un elemento fundamental en el diseño y administración de una red. Siempre será más fácil implementar la seguridad en una red que afrontar su recuperación desde una pérdida. Existen elementos cruciales para la viabilidad de una organización, como que sus datos permanezcan seguros. Habitualmente, los datos residirán en la red por lo que un plan de almacenamiento seguro, de redundancia, de tolerancia a fallos en los sistemas, así como un plan de recuperación ante desastres se antojan innegociables.

2.1. Tareas de administración

Un esquema primario de las tareas de administración de un sistema en red local podría estructurarse en los aspectos de direccionamiento, gestión de usuarios, gestión de recursos, administración de servicios, gestión de la red y gestión de la seguridad.

— **Direccionamiento.** El administrador de red debe proveer el plan de direccionamiento de la red. Existen diversas aproximaciones, desde una asignación manual de direcciones hasta una asignación automática o la utilización de un modelo mixto en función de las necesidades o restricciones de la organización. Si se decide optar por una asignación automática de direcciones, lo más habitual es utilizar un servidor que ejecute el protocolo *Dynamic Host Configuration Protocol* (DHCP), que lógicamente debe ser instalado, configurado y administrado, con especial atención a los aspectos de seguridad, pues es un protocolo que ha sufrido muchos ataques debido a que no exige autentificación, lo que provocaba que un atacante que lograse la concesión de una dirección también conociera todos los demás valores que un servidor DHCP otorga en el momento de la concesión: dirección IP del servidor WINS o del servidor DNS, por ejemplo. Un atacante podría solicitar un gran número de concesiones, lo que podría originar una denegación de servicio del servidor DHCP que también podría extenderse al servidor DNS.



El direccionamiento debe tener en cuenta la segmentación de la red por lo que su administrador ha de ser perfecto conocedor de técnicas que lo posibiliten. Habitualmente, una red puede segmentarse mediante:

- **Subnetting**. Consiste en dividir la red en otras más pequeñas o subredes. Una subred es un rango de direcciones lógicas. Esta técnica consigue dos aspectos fundamentales:
  - Logra una red más manejable a la hora de administrarla.
  - Logra reducir el tamaño de los dominios de difusión amplia (en inglés, *broadcast*). Esta reducción ayuda a que la difusión no colapse las líneas de comunicaciones.
- **Supernetting**. Consiste en combinar dos o más redes o subredes que cuentan con un prefijo de encaminamiento común. Su aplicación soluciona las siguientes situaciones:
  - La ineficiencia en la asignación de rangos de direcciones, que provocaría un agotamiento del direccionamiento en algunos tipos de redes.
  - El aumento del tamaño de las tablas de encaminamiento. La técnica de supernetting permite ahorrar espacio en las tablas, simplifica su encaminamiento y se reducen las rutas entre encaminadores (en inglés, *routers*).

Otros aspectos importantes a considerar en la tarea de direccionamiento es el método para salir a Internet: si se contará con direccionamiento público en todas las máquinas que lo precisen o si se implantará un sistema de traducción de direcciones de red (en inglés *Network Address Translation,* NAT).

NAT es un mecanismo que permite a los encaminadores intercambiar paquetes entre redes que asignan direcciones incompatibles entre ellas. Convierten, en tiempo real, las direcciones que se han utilizado en los paquetes. Existen numerosas posibilidades para realizar NAT, desde configurar con comandos los dispositivos al uso de software (WinGate, PF, IPFilter) o una combinación de software y hardware (por ejemplo un sistema Proxy).

— **Gestión de usuarios.** La creación de usuarios, la decisión de agruparlos o no, y sobre todo la administración de sus permisos y derechos es una de las labores más importantes de la administración de red. Los usuarios, entendidos como personas, no como cuentas, deben ser informados de las normas y cambios en la operativa de trabajo y utilización del sistema, en general confeccionando guías y recomendaciones de utilización de los sistemas y recursos.

Los sistemas operativos ofrecen muchas y variadas herramientas para la administración de usuarios, destacando la gestión de grupos, que agiliza la asignación de permisos, directivas de seguridad, aspectos de distribución, acceso a dominios, visibilidad y características similares.

Algunas de estas herramientas son las políticas de directivas que ofrece Microsoft Windows Server o las listas de control de acceso (en inglés *Access Control List, ACL*) también presentes en entornos tipo Unix/Linux. Además, estas utilidades suelen presentarse en entorno gráfico para una administración más intuitiva.

De especial importancia es la gestión de la cuenta de usuario administrador, superusuario o root, según el sistema operativo en que uno se encuentre. Esto es debido a que al poseer todos los permisos sobre el sistema y sus recursos, su utilización debe ser cuidadosa en extremo, recomendándose únicamente en labores de administración, evitando realizar con ella tareas que pueden realizarse con cuentas de menos privilegios.

— **Gestión de recursos.** En la gestión de recursos en red destacan la administración de archivos y de dispositivos de red.

La administración de archivos en red es un trabajo típico y delicado. Un sistema de archivos permite el almacenamiento y la organización de los datos. A partir de este momento, los datos podrán ser accedidos, manipulados y recuperados.

Es habitual que cada sistema operativo cuente con su propio sistema de archivos. Normalmente están clasificados en las siguientes categorías:

- Sistema de archivos de disco.
- Sistema de archivos de red.
- Sistema de archivos de propósito especial.

Existen numerosos sistemas de archivos, desde los veteranos FAT, VFAT o FAT32 hasta los que se utilizan actualmente como NTFS *(New Technology File System)* en el caso de los sistemas Microsoft Windows Server, *Unix File System (UFS)* para entornos UNIX y el *Extended File System (ext)* en el caso de entornos Linux.

NTFS fue la respuesta de Microsoft a la carencia en materia de seguridad que hasta la fecha de su salida al mercado existía en los sistemas de archivo de sistemas de escritorio y que, prácticamente, los inhabilitaba para su implantación en servidores con orientación empresarial, esto es, con alta disponibilidad, tolerancia a fallos, redundancia, etc.

En el caso de UNIX, es UFS el sistema de archivos más ampliamente utilizado, aunque es común que los distintos fabricantes incluyan versiones propias mejoradas. En UFS se conoce dónde está almacenada la información gracias a unas referencias, denominadas inodos, que señalan la posición o posiciones de los discos por donde está repartido un archivo. Los inodos hacen referencia a estas posiciones pero también contienen información sobre el archivo, por ejemplo su propietario, quién puede acceder al mismo, la hora de creación, de acceso, etc.

En Linux su sistema de archivos se basó, inicialmente, en aspectos del sistema UFS de UNIX y también en el del sistema operativo

Minix pero, debido a su orientación educativa, contaba con ciertas restricciones por lo que la comunidad Linux hubo de desarrollar otros sistemas de archivos con más prestaciones que las que ofrecía MINIX: ext2, ext3 y ext4.

En el caso de los sistemas de archivo de red es común la presencia de los sistemas de archivo distribuido. Permiten compartir objetos como archivos, impresoras y otros recursos de forma persistente. Los más conocidos son *NFS (Network File System)* y *CIFS (Common Internet File System):*

- NFS. Creado por Sun Microsystems, NFS es el sistema de archivos de red utilizado en los entornos UNIX y Linux. Es independiente del equipo, del sistema operativo y del protocolo de transporte.
- CIFS, es la evolución que hizo Microsoft de SMB (*Server Message Block, creación de IBM*). CIFS es un protocolo que permite compartir objetos entre equipos que utilizan el sistema operativo Microsoft Windows Server.

Para garantizar la compatibilidad entre ambos sistemas de archivos se desarrollaron herramientas. La más conocida y utilizada es Samba, evolución del protocolo SMB. Samba permite que sistemas Unix, Linux o Mac OS X puedan ser accedidos como clientes desde redes con sistemas operativos Microsoft Windows Server. Samba configura los directorios existentes en los sistemas de modo que aparezcan como recursos compartidos a través de la red. A los usuarios de la red de Microsoft Windows Server estos recursos les aparecerán como carpetas de red.

Tanto los sistemas Microsoft Windows Server como los de tipo Unix/Linux permiten compartir dispositivos de red que serán accesibles para usuarios o grupos.

Es muy común que los sistemas operativos de red, con la ayuda de utilidades de los fabricantes de dispositivos, cuenten con funcionalidades para gestionar sus propiedades. En el caso de las impresoras, por ejemplo, le permitirían a un administrador gestionar su direccionamiento, las colas de impresión, soporte remoto y tareas de contabilidad y facturación.

— **Gestión de servicios.** Los servicios de red se configuran en redes locales para lograr una utilización y administración más eficiente de los recursos. Es muy habitual que estos servicios se instalen en más de un sistema, siempre buscando una mejor disponibilidad, una tolerancia a fallos y un equilibrio de la carga de trabajo.

La administración de los servidores de red es otro de los aspectos críticos de la administración de sistemas en red, debido a las implicaciones de seguridad y rendimiento que comportan para las organizaciones.

En función del tipo de organización, existirán más o menos servicios de red. Los más comunes son:

- *DHCP,* reduce la complejidad de la configuración del direccionamiento en los sistemas y la carga administrativa en entornos TCP/IP.

- *DNS,* permite la traducción directa e inversa entre nombres y direcciones *IP*.
- Correo electrónico, permite el intercambio de mensajes y archivos a través de un canal electrónico.
- *FTP (File Transfer Protocol)*. El protocolo de transferencia de archivos permite el intercambio de archivos entre sistemas conectados mediante el protocolo *TCP/IP*.
- *SNMP (Simple Network Management Protocol)*. El protocolo simple de gestión de red permite el intercambio de información entre los dispositivos de una red. Gracias a *SNMP* las tareas de supervisión, monitorización y administración son más eficaces y permiten adelantarse a la existencia de problemas en un entorno de red.
- Servicio de archivos de red, permite compartir objetos a los usuarios de una red.
- Servicio de directorio, posibilita la organización de la información de los objetos de una red, por ejemplo usuarios y recursos.
- Servicio de impresión, permite gestionar el sistema de impresión de la organización.

Algunos de los aspectos más complejos de la administración de los servicios de red son su diseño y su configuración. Además, es preciso estar muy atento a su rendimiento mediante una monitorización constante. Conviene no olvidar la seguridad pues alguno de estos servicios representan una parte importante del negocio por lo que, en el caso de estar comprometidos, podrían suponer enormes costes, tanto económicos como de imagen para una organización.

— **Gestión de red.** La administración de la red se referiría a tareas propias de supervisión y mantenimiento del sistema. Incluiría el conjunto de procedimientos, actividades, informes y herramientas que permiten la monitorización y supervisión constante de los equipos y sistemas.

El objetivo de la administración de la red es mantener su disponibilidad, garantizar su correcto funcionando y establecer un principio de proactividad que permita tomar decisiones ante comportamientos anómalos. La configuración previa de una serie de umbrales permitirá monitorizar la infraestructura para, cuando se incumplan, adoptar medidas que impidan una caída en el servicio de red o en cualquiera de sus dispositivos.

Las herramientas que facilitan estas labores utilizan protocolos de gestión de red como el ya comentado SNMP, que permite una gestión de los sistemas dispersos a lo largo de la red.

Las herramientas de gestión de red suelen ofrecer facilidades de gestión de configuración, guardando un inventario del hardware y soft-

ware instalado y operativo en el sistema, recogiendo periódicamente la información del estado de los dispositivos o gestionando su actualización.

También facilitan la gestión de incidencias, siendo fundamentales en la proactividad comentada. Mediante configuración de umbrales como operación típica se puede anticipar la detección, diagnóstico y reparación de averías en la red. A partir de la recepción de mensajes de error o la falta de respuesta de un equipo pueden localizarse los puntos de fallo.

Otra de las utilidades más importantes de estas herramientas es la evaluación del rendimiento de la red. Mediante el análisis estadístico de los factores que se consideren críticos en el desempeño, como los tiempos de respuesta o el tráfico cursado, puede estimarse el grado de eficiencia del sistema, su capacidad máxima, proponer mejoras, ampliaciones o procedimientos de optimización.

— **Gestión de la seguridad**. La administración de la seguridad de la red es uno de los aspectos más amplios, comprometidos y que más preocupa a las organizaciones. La protección del sistema y sobre todo de la información puede ser vital para la continuidad de la organización ante situaciones de crisis o emergencia.

Además, dependiendo de la entidad de la información y de la organización de que se trate, la legislación obliga a establecer algunas de medidas de seguridad que deben incluirse en los sistemas de red.

La implantación de la seguridad representa un impacto económico y organizativo muy importante para las organizaciones. Suele buscarse un equilibrio entre el tipo de empresa, su facturación y las obligaciones y responsabilidad que pueda asumir. En cualquier caso, suele suceder que la no implantación de la seguridad siempre será más caro, en el largo plazo, que la correcta implantación de la misma.

Afortunadamente para los administradores, ha aumentado exponencialmente la conciencia en materia de seguridad por todos los actores que intervienen en materia de redes. Desde los fabricantes de sistemas operativos hasta los de dispositivos de conectividad de red, pasando por la enorme variedad de herramientas existentes para gestión de la seguridad, hacen más sencilla una tarea enorme en todos los sentidos.

3. Gestión de usuarios

Los usuarios, sean personas, sistemas o servicios, toman forma en un sistema con una cuenta de usuario. Esta define los datos relativos a su administración como el propietario, contraseña de acceso o grupos a los que pertenece.

Una cuenta local se define en una máquina. El acceso se realiza contra una base de datos local. La administración es también local, permitiendo establecer políticas de seguridad y se realiza con la cuenta del usuario Administrador en entornos *Microsoft Windows Server* o del usuario *root* en entornos UNIX/Linux.

En entornos Microsoft Windows Server suele implantarse una estructura de dominio para la gestión de usuarios. Un dominio es un grupo lógico de objetos ubicados dentro de un directorio. Los usuarios de un mismo dominio tendrán un inicio de sesión único en un servidor, denominado controlador de dominio para acceder a los recursos de red, así como una cuenta única para acceder a máquinas del dominio, etc.

Otra estructura administrativa para gestión de usuarios es el grupo. Un grupo es un conjunto de usuarios reunidos con algún criterio. La administración de grupos asigna los mismos permisos a todos sus miembros.

La gestión de usuarios incluye aspectos lógicos y burocráticos. No es suficiente con la definición física de un usuario en el sistema sino que debe existir una política de usuarios; disponer de algún tipo de formulario de registro bien definido, donde se incluya la firma del sujeto, aceptando condiciones, responsabilidades y posibilidad de acreditación que supone ser usuario del sistema.

Los procesos de registro y auditoría permiten dejar evidencia del uso de los recursos por parte de usuarios y procesos. La forma de configurar el sistema de registro depende del entorno, de los sistemas operativos existentes y de las políticas de la organización.

La gestión de usuarios y grupos debe prever otros aspectos importantes:

— Asignación de cuotas de disco.

— Monitorización y análisis de los registros de uso de los recursos.

— Estrategia de copias de seguridad.

3.1. Entornos Microsoft Windows Server

En los entornos Microsoft Windows Serv*er* pueden encontrarse dos modelos:

— **Grupo de trabajo.** Cada equipo define sus usuarios y directivas de seguridad.

— **Dominio.** Los equipos de pertenecientes a un dominio comparten el listado de usuarios y directivas de seguridad, el denominado Directorio Activo (en inglés *Active Directory,* AD). El directorio activo es el componente fundamental de la estructura de los sistemas Microsoft Windows Server, no únicamente para la gestión de usuarios y equipos sino para otros servicios existentes en una Organización, por ejemplo el correo electrónico con Microsoft Exchange Server.

  Las cuentas de usuario creadas en un directorio activo representan entidades físicas, esto es, personas pero también representan cuentas de servicio para algunas aplicaciones.

  La terminología de los entornos Microsoft Windows Server también acepta que las cuentas de usuario se puedan denominar entidades de seguridad. Una cuenta de usuario autentifica la identidad de un

usuario y autoriza o deniega el acceso a los recursos del dominio debido a que las cuentas son objetos del directorio activo que reciben automáticamente un identificador de seguridad (*SID*). Es el *SID* quien proporciona esas capacidades.

3.1.1. Cuentas de usuario

Existen tres tipos de cuentas de usuario integradas en un entorno de directorio activo:

— **Administrador**. Es la primera cuenta creada cuando se configura un dominio y se instalan los servicios de directorio activo. Es la cuenta con el mayor número de derechos y permisos en el dominio. Cuenta con el control total en el dominio. También puede asignar derechos de usuario y permisos de acceso a otros usuarios del dominio. Se recomienda que esta cuenta se utilice únicamente cuando sea imprescindible, para las tareas que la requieran, así como configurarla con una contraseña especialmente segura. Esta cuenta no puede eliminarse pero sí renombrarse o deshabilitarse. De hecho, suele ser una buena práctica para reducir riesgos ante posibles ataques que quieran localizar la cuenta para fines malintencionados.

— **Invitado**. Es la cuenta que pueden utilizar aquellos usuarios que no dispongan de cuenta en el dominio. No precisa de contraseña. Es una cuenta deshabilitada de forma predeterminada y se considera una buena práctica mantenerla en ese estado hasta que sea necesario su uso.

— **Asistente de ayuda**. Es la cuenta que se utiliza para permitir sesiones remotas de soporte. Se crea de forma automática cuando se inicia el asistente de ayuda y tiene acceso limitado al equipo. Se elimina si no existen peticiones de ayuda en estado pendiente.

3.1.2. Protección de las cuentas de usuario

El uso apropiado de las cuentas de usuario en una red garantiza la identificación de los usuarios que inicien sesión en dicha red y accedan únicamente a los recursos permitidos.

Prácticamente todo el mundo es conocedor desde hace bastantes versiones del sistema Microsoft Windows Server de la existencia de las cuentas de Administrador e Invitado. Por ello se hace casi obligado recurrir a cambiar su nombre o pasarlas a estado deshabilitado para evita que un usuario o un software malintencionado haga uso de ellas y acceda al dominio. El cambio de nombre de una cuenta no afecta a su identificador de seguridad (SID) por lo que conservaría sus propiedades (pertenencia a grupos, contraseña, perfiles y permisos y derecho asignados).

La combinación del uso de contraseñas seguras y una política de bloqueo de cuentas elimina riesgos ante sucesivos intentos de iniciar sesión en una red.

3.1.3. Grupos

Un grupo es un conjunto de cuentas de usuario, de contactos, de equipos o de otros grupos. Pueden administrarse como una unidad. Los usuarios pertenecientes a un grupo se denominan miembros. En un entorno de directorio activo los grupos son objetos existentes en un dominio y que se almacenan en unidades organizativas. Los grupos son útiles para:

— Simplificar la administración, sobre todo en el momento de asignar permisos.

— Delegar la administración, mediante la utilización de directivas de grupo.

— Crear listas de distribución de correo electrónico.

Habitualmente los grupos se caracterizan:

— **Por su ámbito**. Determina el alcance dentro de un dominio. Existen 3 ámbitos de grupo:

  • **Local de dominio**. A sus miembros únicamente se les puede asignar permisos dentro un dominio.

  • **Global**. A sus miembros se les puede asignar permisos en cualquier dominio del bosque.

  • **Universal**. A sus miembros se les puede asignar permisos en cualquier dominio del bosque o del árbol de dominios.

— **Por su tipo**. Determina si un grupo puede utilizarse para asignar permisos desde un recurso compartido o bien si puede utilizarse únicamente para las listas de distribución de correo electrónico.

  • **Grupos de distribución**. Se usan para crear listas de distribución de correo electrónico. Únicamente pueden utilizarse con aplicaciones de correo electrónico con Microsoft Exchange Server para enviar mensajes a grupos de usuarios.

  • **Grupos de seguridad**. Controlan el acceso a los recursos compartidos en la red. Con estos grupos es posible:

    - Asignar derechos de usuario a los grupos de seguridad.

    - Asignar permisos para recursos de los grupos de seguridad.

En un entorno de directorio activo, los grupos se crean en los dominios. Si se cuenta con los permisos adecuados, se podrán crear grupos en el dominio raíz del bosque, en cualquier dominio del bosque o en una unidad organizativa.

El sistema de archivos utilizado en los entornos Microsoft Windows Server es NTFS. Una de las principales características la incorporación de seguri-

dad avanzada a nivel de archivos y carpetas. Permite definir listas de control de acceso (*Access Control List, ACL*) para establecer de forma independiente los permisos para cada usuario o grupo.

3.2. Entornos Unix/Linux

En entornos Unix un usuario representa una conexión lógica al sistema.

La seguridad de un sistema UNIX/Linux se basa en la asignación de un nombre, un identificador de usuario (UID) y una contraseña exclusivos para cada usuario. Cuando un usuario inicia sesión, se utilizará el UID para validar todas las peticiones de acceso a los archivos.

El usuario principal en un sistema UNIX/Linux es el usuario root. Los permisos de archivo no se aplican a este usuario, por lo que puede leer, modificar y suprimir todos los archivos que desee. Con excepción de algunas operaciones que, obviamente no pueden realizarse (por ejemplo desmontar sistemas de archivos en uso), el usuario root puede hacerlo todo en el sistema. Es más, la inmensa mayoría de las tareas de mantenimiento de sistemas únicamente las puede ejecutar el usuario root.

Junto al usuario root, los sistemas UNIX/Linux cuentan con usuarios predeterminados. Estos no deben utilizarse para iniciar sesión, sino que se usan para facilitar el correcto funcionamiento de determinadas aplicaciones y procesos (demonios, en terminología de estos sistemas). Tampoco pueden utilizarse para realizar tareas de administración: es necesario utilizar el usuario root para ello.

Por último, están las cuentas de usuario. Su finalidad es la proporcionar a sus usuarios el acceso a un sistema UNIX/Linux para que realicen sus tareas.

Los usuarios que necesitan acceder a un conjunto de archivos se ubican en grupos. Un usuario puede pertenecer a varios grupos. Cada grupo cuenta con un identificador exclusivo, el GID. Cada usuario siempre pertenecerá a un grupo como mínimo, el grupo primario. Además, los usuarios pueden pertenecer a otros grupos, los secundarios.

La creación de grupos para organizar y distinguir los usuarios de un sistema o una red forma parte de la administración de un sistema. Las directrices para formar grupos no pueden estar al margen de la política de seguridad. La definición de grupos en organizaciones de gran tamaño puede ser bastante compleja. Resulta muy conveniente realizar una cuidadosa planificación de la estructura de grupos antes de ejecutarla, pues luego es más complicado cambiarla.

Existen dos grupos en un sistema UNIX/Linux:

— **Grupos de usuario**. Deben crearse para quienes precisen compartir archivos en el sistema.

— **Grupos definidos por el sistema**. Se utilizan para controlar otros sistemas o subsistemas.

Al crearse un archivo, el UID asociado al proceso que lo ha creado se asigna al archivo. Únicamente el propietario y el usuario root pueden modificar los permisos de acceso.

Toda la información de usuarios, grupos, características y contraseñas se almacena en los archivos */etc/psswd, /etc/shadow, /etc/gshadow y /etc/group*. El contenido de estos ficheros es:

— **/etc/psswd.** Almacena los usuarios del sistema e información complementaria. Posee permisos de lectura para el propietario (root), grupo y usuarios.

— **/etc/shadow.** Almacena la contraseña cifrada de cada usuario. Solo tiene permisos de lectura para "root". Si existe este fichero, en /etc/psswd no se ve la contraseña. Se aconseja usar este fichero.

— **/etc/group.** Refleja la pertenencia de un usuario a cada grupo. Un usuario puede pertenecer a varios grupos, pero como poco pertenecerá al suyo propio, definido en /etc/psswd.

En entornos Unix/Linux, a cada archivo se asigna un propietario, grupo y permisos. Por ejemplo, un archivo con los permisos drwx-w-r-x, indica que es un directorio (d), cuyo dueño posee todos los permisos (rwx, lectura, escritura y ejecución), el grupo solo permisos de escritura (-w-) y el resto, lectura y ejecución (r-x).

El acceso a servidores Unix/Linux se hace con nombre y contraseña que se almacena cifrada, en general, con los algoritmos de cifrado propios de cada distribución.

Resulta de vital importancia que todas las contraseñas cifradas estén protegidas de los propios usuarios. Los ficheros que almacenan las contraseñas son de lectura-escritura para el usuario root. Los usuarios no pueden acceder a ellos, con excepción de unos pocos programas SUID que forman parte del entorno de los propios ficheros */etc/shadow* o */etc/gshadow*.

Aun usando un fichero */etc/shadow* o */etc/gshadow* y teniendo cifradas las contraseñas, estas pueden romperse con programas que ejecutan ataques a contraseñas. Por tanto, debe establecerse una política de contraseñas que dificulte este tipo de ataque. Estos ficheros también implementan la caducidad de las contraseñas. Este mecanismo obliga a los usuarios a cambiar periódicamente sus contraseñas.

Otro mecanismo de protección es la configuración de los módulos PAM *(Pluggable Authentication Modules).*

Se utilizan para que los administradores establezcan una política de autentificación sin tener que recompilar programas de autentificación del sistema y conectar módulos de autentificación a un determinado programa con ficheros de configuración sencillos. Por tanto, PAM supone un método útil de seguridad. La configuración *PAM* se realiza en el fichero */etc/pam.d*, donde una serie de ficheros representan cada programa al que aplicar los módulos *PAM* especificados.

De modo análogo a los servicios de información de red existentes en los entornos Microsoft Windows Server, los entornos UNIX/Linux también cuen-

tan con uno: NIS *(Network Information Service)*, desarrollado por Sun Microsystem como sustituto del sistema DNS para redes pequeñas que no precisaban de conexión a Internet.

NIS cuenta con capacidades de acceso a bases de datos que pueden utilizarse para distribuir la información contenida en los ficheros /etc/passwd y /etc/group a los nodos de un sistema NIS. Así, la red parecería un sistema individual, con las mismas cuentas en todos los nodos.

NIS también puede utilizarse para distribuir la información de nombres de equipos contenida en los ficheros /etc/hosts.

4. Gestión de dispositivos

Un dispositivo es un elemento que permite realizar operaciones de entrada y salida. Entran en esta categoría los dispositivos de almacenamiento, los de comunicaciones y los de energía. Es fácil suponer la gran cantidad y heterogeneidad de dispositivos que pueden englobarse en estas categorías por lo que resulta complicada una gestión genérica por parte del sistema operativo. Estos dispositivos pueden presentar diferencias en los siguientes aspectos:

— La **unidad de transferencia**. Ratón o teclado utilizan el byte mientras que otros dispositivos (discos, cintas magnéticas, cabinas de almacenamiento) almacenan la información en bloques.

— La **velocidad**. Existe una gran disparidad en este parámetro. Dispositivos de comunicación y discos transfieren millones de caracteres por segundo y a velocidad constante mientras que el teclado transmite unos pocos caracteres por segundo y en períodos concretos.

— Los **protocolos de comunicación**. Los dispositivos utilizarán diferentes protocolos que dependerán tanto del dispositivo como del bus de comunicación.

— Las **operaciones**. Pese a la existencia de dispositivos de entrada, de salida y de entrada salida, algunos dispositivos concretos requieren operaciones específicas. Es el caso del cabezal de lectura y escritura al posicionarse en un disco.

— La **representación de los datos**. Los dispositivos, incluso los mismos, pueden utilizar diferentes codificaciones configurables en el momento de la instalación. Es el caso de los teclados o de los monitores.

— Los **errores**. Varían en función del dispositivo. Pueden tratarse como situaciones específicas (una impresora que se quedó sin tóner) o genéricas (un cabezal que no apoya bien en el disco y provoca lecturas y escrituras erróneas).

Los fabricantes, tanto de sistemas operativos como de dispositivos, idearon los controladores para facilitar un modo más homogéneo de direccionar los dispositivos. De esta forma, el sistema operativo conectará con la interfaz

que representa al dispositivo y no con él directamente. Son operaciones de funciones de bajo nivel que dependen del hardware.

Existen numerosas clasificaciones de dispositivos. Una de ellas atendería a la siguiente división:

— **Dispositivos de carácter**, aquellos que no permiten acceso aleatorio sino que, únicamente puede ser leído y escrito secuencialmente. Algunos ejemplos lo constituirían:

  • La consola, sea el teclado, el monitor o el ratón.

  • Terminales serie conectados al sistema.

  • Impresoras.

  • Tarjetas de sonido.

  • Dispositivos de carácter virtuales.

    - Los **dispositivos null**.

      • /dev/null, utilizado para deshacerse de aquellos datos que no se necesitan.

      • /dev/zero, utilizado para crear infinitos ceros binarios.

    - Los **dispositivos random**. Los números aleatorios son realmente importantes en el campo de la seguridad informática.

      • /dev/random. Los sistemas UNIX/Linux implementan este dispositivo que contiene una gran cantidad de números aleatorios o fuente de entropía.

      • /dev/urandom. Genera números aleatorios mientras la fuente de entropía no se encuentre vacía y pseudo-aleatorios cuando se vacíe.

En entornos Unix/Linux todos los dispositivos de carácter tienen representación en /dev. Si se hiciera un listado de los dispositivos de carácter en /dev todos los dispositivos comenzaría por la letra c, indicando que se trata de un dispositivo de carácter.

Los dispositivos serie suelen utilizarse para la conexión de módems a los sistemas. Pese al evidente desuso de estos dispositivos a nivel de usuario, no debemos olvidar que los proveedores de servicios de Internet (ISP) mantienen operativas enormes granjas de módems a través de tarjetas multipuerto para ofertar sus servicios de conectividad. En entornos UNIX/Linux los dispositivos serie *COM1* y *COM2* se identifican como /dev/ttySo y /dev/ttyS1 respectivamente.

Dispositivos como las tarjetas de sonido son identificados como /dev/dsp.

Los dispositivos que se conectan a los puertos paralelo, por ejemplo las impresoras, se identifican en UNIX/Linux como */dev/lpo y /dev/lp1* para representar a las impresoras *LPT1* y *LPT2* respectivamente.

En entornos *Microsoft Windows Server*, se usan palabras reservadas para referirse a dispositivos: CON, PRN, LPT1, AUX, COM, etc.:

— **Dispositivo CON.** Abreviatura de consola. Se refiere a teclado y monitor. Como el primero es un dispositivo de entrada y el segundo de salida, no existe ambigüedad.

— **Dispositivo PRN.** Abreviatura de "*printer*". Se refiere a la impresora conectada al primer puerto paralelo (*LPT1*). También existen dispositivos específicos para indicar los puertos paralelo (*LPT*).

— **Dispositivos COM. Son los puertos serie.**

— **El dispositivo AUX.** Hace referencia a un puerto auxiliar.

— **Dispositivo NUL.** Abreviatura de *null*. Se refiere a un dispositivo virtual llamado nulo. Se usa para simular transferencias de información. Utilizado como entrada de datos, no hay entrada y usado como salida, no hay salida. Por ejemplo, al enviar mensajes de salida de un programa al dispositivo nulo no se mostrará nada en pantalla aunque el programa lo simulará.

— **Dispositivos de bloque**, aquellos que permiten el acceso aleatorio. Algunos ejemplos son:

  • **Discos duros**. Constituyen la forma más habitual de almacenamiento permanente en un sistema. Los tipos más comunes son IDE, SATA, eSATA, discos USB y discos de estado sólido (SSD).

  • **Dispositivos virtuales de bloques.**

    - *RAID, Redundant Array of Inexpensive Disks*. Es una técnica creada para aumentar el rendimiento de los discos mediante el empaquetado conjunto de un gran número de ellos. Se precisa un software de control adicional para presentarlo al sistema operativo como un dispositivo lógico que resultaba más rápido, más fiable y de mayor tamaño que los discos individuales.

    - *LVM, Logical Volume Manager*. Es una técnica que permite superar las limitaciones del sistema tradicional de particionamiento de discos. Cada disco se asigna a un grupo de volúmenes, que podrá subdividirse en extensiones físicas de tamaño idéntico. Estas se combinan en volúmenes lógicos. Cada volumen lógico será un dispositivo de bloques que podrá ser presentado al sistema operativo. Es posible, incluso, que un volumen lógico contenga su propio sistema de archivos.

En entornos UNIX/Linux, la numeración de los dispositivos IDE está basada en cómo se conecta al dispositivo:

— /dev/hda, es el maestro sobre el primer bus en el primer adaptador.

— /dev/hdb, es el esclavo en el primer bus en el primer adaptador.

— /dev/hdc, es el maestro en el segundo bus sobre el primer adaptador.

Y así sucesivamente. En caso de discos duros, se añade al final el número de la partición (lógica) a la que se hace referencia, siendo el 1 la primera partición del disco: /dev/hda1, etc.

En el caso de los dispositivos SCSI, los nombres de los dispositivos se basan en su identificador. Los drivers detectarán e inicializarán cada uno de los adaptadores y el bus SCSI por turno, en función del identificador más bajo. Todos los dispositivos están asignados a una entrada de dispositivo en el orden en que fueron detectados. El primero suele denominarse */dev/sda*, el segundo */dev/sdb*, etc.

4.1. Gestión de discos

Las pistas de un disco se dividen en sectores, la unidad mínima que se puede leer o escribir. En general son sectores de 512 bytes. La estructura lógica de un disco, distingue:

— **Sector de arranque** *(Master Boot Record)*. El que contiene la tabla de particiones y un pequeño programa de inicialización, ejecutado al arrancar la máquina. Su cometido es leer la tabla de particiones y ceder el control a la partición primaria activa.

— **Espacio particionado.** Con las particiones del disco. Una partición es una división de tamaño fijo de un disco asociada a una unidad lógica (C, D.... en los entornos Microsoft Windows). Una partición ocupa un bloque de cilindros contiguos del disco duro. Cada una puede definir un sistema de archivos distinto.

— **Espacio sin particionar.** Se gestiona teniendo en cuenta que la tabla de particiones del disco duro contiene un máximo de 4 entradas, lo que determina el número máximo de particiones primarias a crear en un disco duro. Para ampliar ese límite de 4 se puede usar una entrada para definir una partición extendida (por tanto, como máximo habrá 3 particiones primarias y 1 extendida). En la partición extendida ya se podrán crear tantas unidades lógicas como se desee. Las particiones primarias se usan, en general, para albergar el sistemas operativos (ya que son arrancables) y las lógicas para almacenamiento, ya que no son directamente arrancables. Para indicar qué partición primaria arranca se marca como partición activa.

Antes de usar un disco duro se deben definir sus particiones. Una vez hecho, se les proporciona un formato, es decir, la estructura del almacenamiento con un determinado sistema de archivos. En un sistema de archivos FAT (propio de sistemas Microsoft Windows), la estructura lógica de una par-

tición está formada por: sector de arranque, copias de la FAT, directorio raíz y área de datos. La FAT (*File Allocation Table*, tabla de asignación de archivos) es el índice del disco. Indica los grupos (clusters o unidades de asignación) que usa cada archivo, grupos libres y defectuosos.

El concepto de grupo usado por los sistemas operativos se refiere al bloque mínimo que el sistema puede leer o escribir en disco. Un grupo estará formado por 1 o varios sectores físicos del disco. Cuanto mayor sea el grupo más espacio se desaprovechará al almacenar archivos pequeños. Un archivo de 1 byte podría llegar a ocupar 32 kB en disco si el grupo fuesen 64 sectores. Es la idea de fragmentación. La estructura de una partición Unix tradicional está formada por: bloque de arranque, superbloque, vector de inodos y bloques de datos.

4.1.1. Tipos de formato

No debe confundirse el formato de las particiones, también conocido como sistema de archivos, con el tipo de partición (primaria, extendida, etc.). Existen numerosos sistemas de archivos, pues habitualmente cada fabricante ha propuesto el suyo:

— **FAT**, desarrollado para el sistema operativo MS-DOS y para las principales versiones de sistemas operativos de Microsoft Windows no destinadas al entorno profesional. Es el sistema habitual en tarjetas de memoria y medios de almacenamiento extraíble (excepto CDs y DVDs), como las memorias USB de hasta 2 GB.

— **FAT32**. Fue la respuesta para superar el límite de tamaño de FAT16. Apareció con Microsoft Windows 95. Actualmente puede utilizarse en Microsoft Windows 7 pero Microsoft recomienda el uso de NTFS. También se utiliza en memorias USB de 4 a 32 GB de capacidad.

— **NTFS**. Es el formato habitual en entornos Microsoft Windows Server desde Windows 2000 Server. También es el recomendado para Microsoft Windows 7, 8 y 10. Permite definir, de forma independiente al tamaño de la partición, el tamaño del cluster a partir de 512 bytes.

— *Unix File System*, **UFS**. Es un sistema de archivos utilizado por varios sistemas operativos UNIX, sobre todo en aquellos que proceden de BSD (Solaris NetBSD, OpenBSD, etcétera). También se ofrece en los sistemas Mac OS X como alternativa al sistema HFS.

— **XFS**. Creado por la empresa Silicon Graphics (hoy SGI) para el sistema operativo de sus estaciones de trabajo IRIX (implementación de UNIX). Es el sistema de archivos para los sistemas UNIX que antes ofreció journaling. Soporta un sistema de archivos de hasta 8 exabytes y de 16 para los volúmenes. En la actualidad, la versión 7 de la plataforma Red Hat Enterprise Linux (RHEL) ha apostado por XFS como su sistema de archivos por defecto.

— **ext2** (second extended filesystem). Fue el principal sistema de ficheros de las distribuciones Linux. Fue escrito basándose en especifica-

ciones del sistema UFS. Sus límites son de 2 terabytes (TB) para el tamaño de los archivos y 4 TB para la partición.

— **ext3** (third extended filesystem). La gran novedad que ext3 proporcionó a los sistemas de archivo fue la capacidad de ser transaccionales (en inglés *journaling*). Esta característica permitió a los sistemas de archivos guardar en ficheros de registro las actividades que se iban a realizar de modo que, ante un fallo del sistema que provocase un apagado no ordenado, en el siguiente arranque el sistema sabría qué hacer consultando el fichero de registro y siguiendo las tareas allí anotadas. Esta técnica consigue evitar problemas de inconsistencia. Ha sido el sistema de archivos más ampliamente utilizado en las distribuciones Linux. El límite del tamaño que puede gestionar, tanto de ficheros como de los volúmenes, es variable en función de los tamaños de los bloques (que oscilan entre 1 kB y 8 kB). El tamaño de los bloques se especifica en el momento de creación del sistema de archivos.

— **ext4** (fourth extended filesystem). Es la evolución del sistema ext3 y presenta mejoras en el soporte de volúmenes, menor utilización del uso de CPU así como mejoras en la velocidad de las operaciones de lectura y escritura. Este sistema de archivos puede trabajar con ficheros de hasta 16 TB y volúmenes de hasta 1 exabyte (EB).

— **HFS**, *Hierarchical File System* (sistema de archivos jerárquico). Es el sistema de archivos desarrollado por la compañía Apple para su utilización en los sistemas Mac OS X. Presenta límites de hasta 2 GB de tamaño de archivo y 2 TB para los volúmenes.

4.1.2. Sistemas RAID

RAID se implementó con la idea de abaratar el coste del almacenamiento, extremadamente caro en aquellos momentos. Inicialmente, las siglas se correspondían con *Redundant Array of Inexpensive Disks*, conjunto o matriz redundante de discos baratos, pero hoy está más aceptada la correspondencia con matriz o conjunto redundante de discos independientes.

Se caracterizan por ser tolerantes a errores y usar un conjunto de discos organizados de forma que si uno falla el ordenador siga trabajando. Esto se consigue con información redundante, que no sería necesaria si no se diese el error.

La gestión de sistemas RAID es transparente al usuario. Puede realizarse por hardware, con tarjetas RAID específicas o por software, como herramienta del sistema operativo. La forma hardware es más eficiente, al liberar a la CPU de esos procesos, y habitualmente más cara.

Los sistemas RAID suelen distinguir varios niveles de organización:

— **RAID 0** *(disk striping,* discos en bandas). La información se distribuye entre los discos del conjunto. Esto acelera la transferencia al acce-

der todos los discos a un mismo archivo. No es tolerante a fallos. Si falla un disco se pierde la información. Se necesitan 2 discos como mínimo para implementar *R*AID 0.

— **RAID 1** (disk mirroring, espejo de discos). Consiste en usar discos adicionales que dupliquen la información. Las escrituras se realizan en todos los discos para mantener la coherencia. Se garantiza que ante el fallo de un disco, el sistema continúe funcionando. Suele implementarse RAID 1 con 2 discos. Lógicamente, el máximo de información a almacenar es la capacidad de un disco, ya que el segundo (espejo) es redundante.

— **RAID 0** puede combinarse con RAID 1 constituyendo el sistema RAID 1+0. La información se distribuye en bandas por varios discos y cada disco se duplica, por lo que se requiere un número par de discos.

— **RAID 2.** Usa un código de redundancia (el de Hamming) para detección y/o corrección de errores. Esta técnica se incluye de forma nativa en los discos, por lo que ha dejado de utilizarse.

— **RAID 3.** Se usa un disco para almacenar la paridad. La información de redundancia se distribuye entre los discos del conjunto. En caso de fallo, se reconstruye la información con un XOR (OR exclusivo) del resto de discos. Por tanto, precisa al menos 3 discos. Como los discos funcionan de forma síncrona, posee un coste en rendimiento, en especial en sistemas transaccionales en que se den muchos accesos de poco volumen.

— **RAID 4.** Es similar a RAID 3, distribuyendo los datos a nivel de bloque y permitiendo el acceso individual a cada disco. Aumenta el rendimiento en pequeñas lecturas que afecten a un solo disco.

— **RAID 5.** La información de paridad se almacena de forma distribuida, eliminando el cuello de botella del disco de paridad de los RAID anteriores. Es más eficiente; ofrece mayor tasa de rendimiento y es más barato por unidad de información. Precisa al menos 3 discos, obteniendo el mejor rendimiento a partir de 7 unidades.

— **RAID 6.** Es una configuración similar a la de RAID 5. Distribuye de igual forma los bloques de información pero genera dos bloques de paridad que se distribuirán entre los discos, de ahí que también se le conozca como distribuida con doble paridad. La configuración podrá admitir hasta dos fallos de disco en el conjunto o, incluso, un fallo mientras se reconstruye un volumen que había fallado. Son necesarios, al menos, cuatro discos.

— **RAID 7.** Es una configuración propia de la empresa Storage Computer Corporation. Se basa en añadir cachés a configuraciones en RAID 3 o RAID 4 con el objetivo de mejorar su rendimiento.

Los sistemas RAID 3, 4 y 5 son conocidos como discos en bandas con paridad (en inglés, *disk striping with parity*). La capacidad máxima se obtiene

como suma de la capacidad de los discos menos la del disco redundante. RAID 0 no incluye tolerancia, por lo que su capacidad es la del conjunto. La capacidad de RAID 1 es la de un disco.

Algunos sistemas soportan intercambio en caliente (en inglés, *hot swap*), que permite reemplazar un disco que ha fallado por otro nuevo, sin apagar el sistema. La técnica de reserva en caliente (en inglés, *hot spare*) se refiere a mantener un disco adicional instalado en el sistema, en reserva, a la espera ante fallos.

4.1.3. Herramientas y utilidades de gestión de discos

Resultan de gran ayuda en las tareas de administración de discos. Pese a que, cada vez con más frecuencia, los fabricantes de sistemas operativos tratan de incluir de serie todo tipo de herramientas -habitualmente también fabricada por ellos- es bastante amplia la oferta de todo tipo de utilidades. Algunas categorías podrían ser:

— **Gestores de particiones.** Existen numerosas herramientas que permiten gestionar las particiones de los discos de un sistema. Uno de los aspectos más importantes a la hora de decantarse por el uso de una o de otra es la capacidad de mover o redimensionar particiones ya existentes. Algunos ejemplos son Gparted en el caso de entornos UNIX/Linux o Diskpart y el Administrador de discos en entornos Microsoft Windows.

— **Desfragmentador.** Es una herramienta para reducir la fragmentación generada al grabar en disco los trozos de cada fichero. Esto optimiza el almacenamiento al acelerar la lectura de datos. Consiste en reorganizar esos trozos de los ficheros de forma compacta. Una organización poco fragmentada evita que los cabezales de lectura y escritura del disco realicen muchos movimientos. En entornos Microsoft Windows se puede usar el comando defrag o la herramienta Desfragmentador de disco. En entornos Unix/Linux no se requieren estas herramientas puesto que su organización evita estos problemas.

— **Comprobación de errores.** Analizan el disco en busca de incoherencias en el sistema de archivos. Por ejemplo, dos archivos apuntando al mismo contenido generarán un error tipo vínculos cruzados. Los errores en la estructura lógica del disco se suelen dar por cortes de luz o cierres del sistema impropios. En estos casos, los sistemas operativos suelen ejecutar utilidades de comprobación al siguiente arranque del sistema.

  Un ejemplo de este tipo de herramientas en entornos Microsoft Windows es ScanDisk, y en entornos Unix/Linux es fsck o alguna de sus variantes, en modo comando, en función de la distribución.

— **Compresión.** Consiste en reducir el tamaño de los datos sin pérdida de información. El espacio ganado tiene un coste temporal, ya que los algoritmos de compresión cargan el proceso. Como la compresión depende de la herramienta usada, podrían darse problemas de incompatibilidades o pérdida de datos en caso de error.

Los sistemas operativos de Microsoft incorporan mecanismos de compresión integrados. En entornos Unix/Linux el comando para comprimir archivos es gzip. Para comprimir un árbol de directorios completo, se usa el comando tar para compactarlo a un único archivo (*.tar*) seguido del comando gzip para comprimirlo (*.gz*).

— **Copia de seguridad**. La copia de seguridad (*backup*) del contenido del disco en otro medio de almacenamiento es fundamental desde el punto de vista del valor de la información.

Se distinguen, tres tipos de copias de seguridad: completas, incrementales (o progresivas) y diferenciales. Las primeras realizan una copia de todo el contenido. Las copias incrementales almacenan los datos nuevos o modificados desde la última copia incremental. Las copias diferenciales almacenan los datos nuevos o modificados desde la última copia completa.

La diferencia entre estas últimas está, por tanto, en que para recuperar los datos de una copia incremental se necesitan la última copia completa y todas las incrementales hasta el punto de restauración, mientras en las copias diferenciales precisan la última copia completa y la última diferencial.

Los sistemas operativos suelen incluir herramientas de copias de seguridad pero ofrecen proporcionar funcionalidades muy básicas. Bien en cierto que, en los últimos tiempos, Microsoft ha tomado gran conciencia con todos los aspectos de seguridad para sus sistemas operativos y ofrece también soluciones de backup con Microsoft Azure. En entornos empresariales resulta de lo más conveniente acudir a soluciones de alta gama, también en función de los requisitos y posibilidades de cada organización. Algunos de los productos más conocidos son EMC Networker, Acronis, Symantec Backup, Commvault, etc.

4.2. Gestión de impresoras

Las impresoras son dispositivos de amplia presencia y utilización en redes locales. Su administración nunca ha sido sencilla, pues exige bastante mantenimiento. Desde la gestión de usuarios que pueden imprimir en según qué impresora, el tipo de impresión que se permite, la facturación o incluso la gestión de alertas ante incidencias (falta de papel, disponibilidad de tóner, etc.) son aspectos que obligan a una correcta de la planificación de las impresoras de una organización para que no se convierte en una tarea inabarcable. La tendencia de los últimos años de integrar en un único dispositivo físico las características de impresión, de fax y de escáner (comúnmente conocida como multifunción) ha complicado aún más su administración.

Es habitual encontrarse con dos tipos de instalación: impresoras locales e impresoras conectadas en red.

— Una **impresora local** se refiere a la que se conecta directamente al equipo en cuestión.

— Una **impresora en red** es aquella a la que se accede a su servicio a través de la conexión de red.

Debido al entorno complejo expresado anteriormente, cada vez es más común contar con un servidor de impresión que facilite las tareas de administración. Suelen ser independiente de las aplicaciones, permiten la generación de códigos de barras o, incluso, replican las copias de carbón típicas de las impresoras matriciales, por lo que permiten su sustitución. Su objetivo final es el de realizar una gestión unificada de las impresiones en una organización. Otros objetivos serían:

— Gestión de la política de impresión de la organización.

  • Control del color.

  • Política de impresión ecológica.

— Gestión inteligente de la documentación.

— Recuperación ante fallos de impresión.

— Gestión centralizada de las colas de impresión.

— Producción de impresión segura.

— Impresión en cualquier parte.

— Gestión del almacenaje.

— Archivado de la copia o del trabajo de impresión.

— Facturación de la impresión.

Una impresora en red requiere la configuración de un servidor de impresión, que ofrezca su servicio al resto de equipos. Pueden conectarse directamente al servidor de impresión, aunque lo más habitual es que todos los dispositivos utilicen la red local para estar comunicados.

La comunicación se hace entonces configurando los parámetros de red de la impresora, que sería gestionada por el servidor de impresión, en particular, para las colas de impresión.

Como en otras circunstancias, los fabricantes de sistema operativos suelen incluir utilidades que permiten conectar impresoras, tanto a equipos como en red. En entornos Microsoft Windows, para la instalación de impresoras se dispone del Asistente para agregar impresoras, que ofrece la posibilidad de instalar una impresora en red o local. Una vez en funcionamiento, se puede consultar la cola de impresión, cambiar prioridades, etc. El administrador del servidor será el que controle la cola. Los usuarios sólo tendrán permisos sobre sus trabajos enviados a imprimir.

En entornos Unix/Linux también se proporcionan utilidades. Aunque existen varias, pues prácticamente cada distribución cuenta con la suya, la más genérica y ampliamente utilizada es CUPS *(Common Unix Printing System).*

CUPS permite que un sistema actúe como servidor de impresión y que acepte trabajos de impresión enviados desde los sistemas clientes. Utiliza el protocolo IPP *(Internet Printing Protocol)* para gestionar tareas y colas de impresión. Además de la cola de impresión, CUPS se compone de un planificador y un sistema de filtros que permite la conversión de datos a imprimir en formatos conocidos. CUPS también es configurable a través de línea de comandos.

Las impresoras se definen en el archivo */etc/printcap*, cuya configuración presenta un aspecto similar al siguiente:

rlaser5|Impresora remota laser:

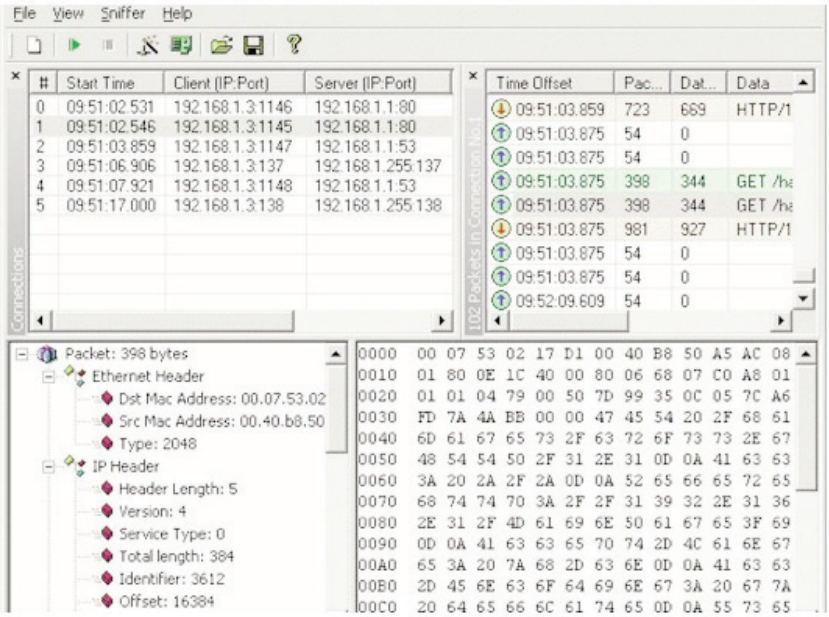
:lp=/dev/null:

:rm=192.168.2.63:

:rp=impresora:

:sd=/var/spool/lpd/remote

La línea "lp" indica el archivo de dispositivo (si la impresora fuese local se usaría /dev/lpo), "rm" la dirección IP de la impresora en red, "rp" el nombre de impresora remota y "sd" indica el directorio de la cola de impresión.



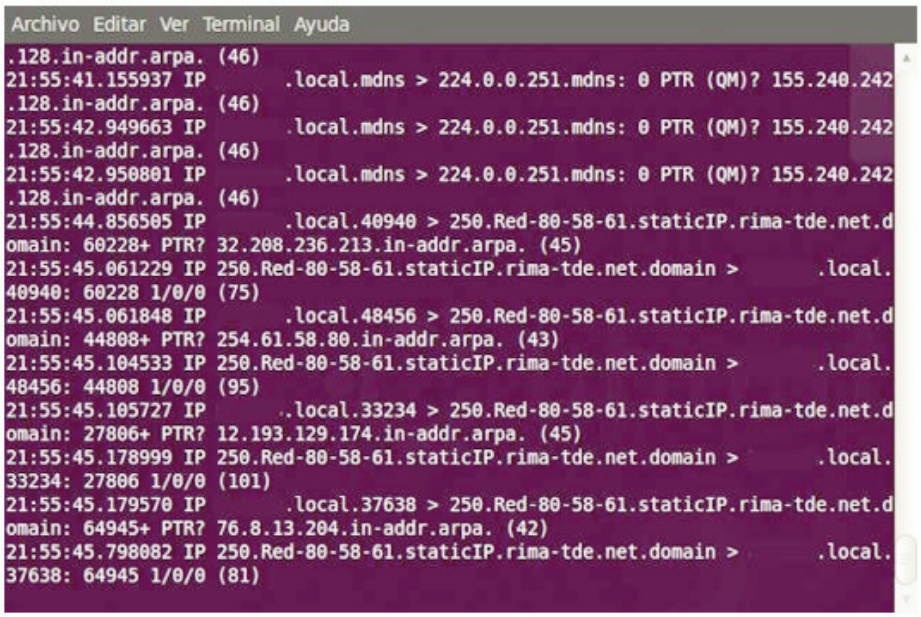
5. Monitorización y control de tráfico

La optimización del tráfico de red es consecuencia de una adecuada planificación, organización y de la realización de tareas preventivas y correctivas que se basan en la monitorización y control de dicho tráfico. De forma similar a cómo las cámaras de videovigilancia, los semáforos y la cartelería luminosa de señalización regulan el tráfico rodado, el sistema de monitorización y control del tráfico de datos permite tomar decisiones, prevenir y corregir estados de saturación o ineficiencia que pueden tener muy diversos desencadenantes.

Por ejemplo, una tarjeta de red defectuosa o un equipo portátil no controlado pueden generar problemas de lentitud y es posible que sea muy difícil diagnosticar la causa de forma ágil. Las herramientas de monitorización serán el principal recurso de diagnóstico mediante la auditoría del tráfico de red.

La mera observación del tráfico mediante el "escaneo" de red nos puede ayudar a identificar los posibles fallos, aunque pueden darse casos complicados de diagnosticar como ocurre con ciertos virus, que enmascaran las direcciones IPs fuentes del tráfico irregular.

Una vez diagnosticado el problema, las acciones correctoras precisas pueden ir desde desconectar ciertos equipos, cambiar reglas de enrutamiento según proceda o habilitar nuevas medidas de descongestión del tráfico.



Las funciones de gestión de red se pueden agrupar en dos categorías:

— **Monitorización**, basada principalmente en la "lectura" del tráfico. Su objetivo es observar y analizar el estado y comportamiento de la configuración de red y sus componentes.

— **Control**, basada principalmente en acciones correctoras. Su objetivo es la configuración de los parámetros de los componentes de red.

La monitorización recogerá información sobre el tráfico de diverso tipo.

— **Estática:** configuración actual de la red y de sus elementos (por ejemplo, el número de puertos de un router). Esta información es generada y almacenada por el propio elemento de red (un router almacena su propia configuración).

— **Dinámica:** información relacionada con eventos en la red (por ejemplo, la transmisión de un paquete por la red). Esta información puede almacenarla el propio elemento u otro encargado de ello; en una LAN cada elemento puede almacenar el número total de paquetes que envía, o un elemento de la LAN puede estar escuchando y recoger esa información (se denomina monitor remoto).

— **Estadística:** información que puede ser derivada de la información dinámica (por ejemplo, el número medio de paquetes transmitidos por unidad de tiempo por un sistema final) de forma que puede enviarse la información dinámica al gestor de red para que realice las estadísticas.

Los cuatro elementos principales que intervienen en la monitorización son:

1. La propia aplicación de monitorización que gestiona la visibilidad de la red para el usuario.
2. El gestor o módulo de la red que recoge la información de los elementos de la red.
3. El agente que recoge y almacena información de uno o varios elementos de la red y los envía al gestor.
4. Los objetos gestionados y la información de gestión que representa los recursos de red y su actividad.

La información de monitorización es recopilada y almacenada por los agentes y enviada a uno o más gestores. Para el envío de dicha información se usan dos técnicas:

— **Sondeo (polling):** el gestor solicita información al agente que responderá a la petición.

— **Informe de eventos (event reporting):** la iniciativa de la comunicación es tomada por el agente teniendo que estar por tanto el gestor a la espera de información de este tipo.

Ambas técnicas se suelen usar conjuntamente en la monitorización de una red.

Tanto la utilización del protocolo *SNMP,* la aplicación de las especificaciones definidas en el modelo OSI como de los sistemas propietarios le dan al usuario bastante flexibilidad para determinar el énfasis con que utiliza cada uno de los métodos. La elección de uno u otro dependerá de factores como:

— La cantidad de tráfico generado por cada método.

— Respuesta ante situaciones críticas.

— Capacidad de procesamiento de los dispositivos gestionados.

— La cantidad de tiempo requerida para que el gestor de la red reciba la información.

— Las aplicaciones de gestión que se utilicen.

Los cuatro elementos principales que intervienen en el control son:

1. La propia aplicación de control que gestiona las funciones de configuración y seguridad.

2. El gestor que es el módulo que envía peticiones de operación al resto de los elementos de la red.

3. El agente que recibe los comandos de control y actúa convenientemente sobre los elementos de la red que depende de él.

4. Los objetos gestionados y la información de gestión que representan los recursos de red y su actividad.

Igualmente la propia estación que ejecuta la aplicación de control es también un elemento de la red y debe gestionarse. El gestor comenzará siempre la comunicación enviando comandos a los agentes y, en función del tipo de comando, puede haber una respuesta del agente o no.

Los comandos son generados por diversos motivos:

— Por iniciativa del administrador de la red.

— Por comandos preprogramados que pueden ser periódicos o como respuesta a eventos o sucesos.

Estableceremos las políticas de gestión de la red en función de la definición de un cuadro de mando de indicadores donde estableceremos:

— **Medidas orientadas a los servicios** como la disponibilidad, el tiempo de respuesta o la fiabilidad.

— **Medidas orientadas a la eficiencia** como las prestaciones (en inglés, *throughput*) o la utilización.

La disponibilidad se define como el porcentaje de tiempo que un elemento de la red o una aplicación está disponible para el usuario, de forma que la disponibilidad de una red está basada en la fiabilidad de sus componentes. La fiabilidad de un componente es la probabilidad de que este realice la función esperada durante un tiempo especificado bajo determinadas condiciones también especificadas. La fiabilidad de un componente suele expresarse por los fabricantes por su MTBF *(Mean Time Between Failures,* promedio de tiempo entre fallos).

Idealmente, los tiempos de respuesta deberían ser tan cortos como sea posible, pero casi siempre un menor tiempo de respuesta significa un mayor coste. Aunque se puede medir directamente el tiempo de respuesta global en un entorno de red, esta medida no es por sí sola suficiente para corregir problemas y planificar el crecimiento de la red.

La fiabilidad de la transmisión de datos entre los equipos de la red es esencial, es útil monitorizar la tasa de errores que se produce a partir, por ejemplo, de patrones de prueba. Esto puede ser indicativo de fallos intermitentes en una línea o de la existencia de una fuente de ruido o interferencias.

Igualmente las prestaciones *(throughput)* deben ser continuamente evaluadas, por ejemplo:

— Las transacciones de un tipo determinado durante un cierto período de tiempo.

— Las sesiones para una aplicación determinada durante un cierto período de tiempo.

— El número de llamadas para un entorno de conmutación de circuitos.

Por otra parte, la utilización real de las diferentes líneas de datos nos puede ayudar a ajustar el tráfico por cada una de ellas, estableciendo rutas alternativas o planificando el aumento o reducción de la capacidad de dichas líneas. Con ajustes de este tipo en la red se puede conseguir una mejor adecuación entre la carga planeada y la real.

La monitorización de la red detectará problemas provocados por un mal funcionamiento de algún elemento y generará alarmas. Ante los posibles fallos caben diversas estrategias y consideraciones de diagnóstico atendiendo a sus posibles causas y a la posibilidad de observación directa (un solo fallo puede afectar a muchos elementos, generando mucha información de fallos que puede enmascarar la causa real).

A veces los procedimientos de recuperación pueden destruir evidencias importantes sobre la naturaleza del fallo, no permitiendo el diagnóstico preciso, en este contexto adquieren cada vez mayor trascendencia las técnicas de informática forense para poder detectar ante cualquier contingencia lo que ha sucedido, por ejemplo a través del examen de ficheros log, bitácoras, análisis de errores con muestras de prueba, etc.

Durante el normal funcionamiento de la red la gestión de la configuración puede llevar a cabo ajustes en respuesta a comandos del usuario o en respuesta a otras funciones de gestión de red (por ejemplo, si la gestión de fallos detecta y aísla un fallo, la gestión de configuración puede reencaminar el tráfico por un camino alternativo).

En las funciones específicas de control de tráfico de red adquiere especial importancia la gestión de configuración de recursos físicos y lógicos que permita establecer la especificación del recurso y de los atributos de ese recurso (por ejemplo: nombre, dirección, número de identificación, estados, características operacionales y versión del software). El gestor de red podrá actuar sobre esta información reparametrizando elementos de la red mediante la modificación de los diferentes atributos de configuración.

Ejemplos de este tipo de operaciones pueden ser permitir al administrador "cortar" una conexión entre dos nodos o designar una dirección alternativa o de backup para utilizar en caso de que el destino primario de una petición de conexión no responda. También la gestión de configuración debe incluir mecanismos que permitan al administrador inicializar o apagar la red o una subred, así como distribuir software como versiones, actualizaciones, ejecutables, tablas y otros datos que controlen, por ejemplo, el comportamiento de un nodo a través de las tablas de encaminamiento.

Los mecanismos de seguridad en la gestión de la red deben garantizar que los recursos deben ser modificables solo por usuarios autorizados.

Existen varios protocolos de gestión que permiten establecer las normas de comunicación entre agentes y estaciones de gestión. Por ejemplo *Common Management Information Protocol* (CMIP) o *Desktop Management Interface* (DMI) pero, con casi total seguridad, el más extendido es el protocolo SNMP.

5.1. El protocolo SNMP

SNMP *(Simple Network Management Protocol,* Protocolo Simple de gestión de red) es el protocolo por excelencia para organización de la información de red. SNMP ofrece mecanismos de descubrimiento de dispositivos, y una base de datos normalizada sobre la red, válida para la mayoría de las plataformas y dispositivos.

SNMP se compone de un conjunto de normas para la gestión de la red, incluyendo una capa de aplicación del protocolo, una base de datos de esquema y un conjunto de objetos de datos. Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Existe la versión 3 (SNMPv3), que incluye novedades y mejoras, fundamentalmente en aspectos de seguridad, pero está teniendo alguna dificultad para su aceptación completa por parte de todos los fabricantes de hardware.

La característica de descubrimiento automático, donde los nuevos dispositivos detectados en la red se sondean automáticamente, representa a veces un riesgo de seguridad por la transmisión en texto plano de dicha información.

SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que normalmente soportan SNMP incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem etc. SNMP facilita a los administradores supervisar el funcionamiento de la red, buscar y resolver problemas, y planificar el crecimiento de la red.

En los usos típicos de SNMP se establecen uno o más equipos administrativos, llamados gerentes, que tienen la tarea de supervisión o la gestión de un grupo de hosts o dispositivos de red. En cada sistema gestionado se ejecuta, en todo momento, un componente de software llamado agente que comunica información de red al gerente.

El protocolo permite realizar tareas de gestión de activos como la modificación de una nueva configuración a través de la modificación remota de variables. Las variables accesibles a través de SNMP están organizadas en jerarquías y almacenadas en la Base de Información de Gestión (en inglés *Management Information Base,* MIB).

Una red administrada a través de SNMP consta de tres componentes clave:

— Los sistemas administradores de red (Network Management Systems, NMS's).

— Los dispositivos administrados.

— Los agentes.

El sistema administrador de red (NMS) ejecuta las aplicaciones que supervisan y controlan a los dispositivos administrados.

Un dispositivo administrado es un dispositivo que contiene un agente SNMP y reside en una red administrada. Estos recogen y almacenan información de administración, la cual es puesta a disposición de los NMS's.

Un agente es un módulo de software de administración de red que reside en un dispositivo administrado.

Las estaciones de gestión acceden a las MIBs correspondientes con operaciones de lectura y escritura. Los agentes pueden enviar alertas (conocidos en inglés como *traps*) a las estaciones de gestión notificando incidencias. SNMP utiliza los puertos 161 y 182 UDP para recibir las alertas.

SNMP funciona con comunidades. Una comunidad es un grupo formado por dispositivos y por las estaciones que los gestionan. Se usa un nombre de comunidad para identificar a cada grupo y asociar las operaciones soportadas por los agentes. Los dispositivos pueden pertenecer a una o varias comunidades, pero no responderán a estaciones de una comunidad a la que no pertenecen. Las comunidades SNMP se representan con cadenas de texto que se utilizan a modo de claves de autentificación. Las comunidades típicamente utilizadas que, además son las predeterminadas, serían:

— **Public**, de lectura.

— **Private**, de escritura.

Un ejemplo de MIB del protocolo SNMPv2 sería el siguiente:

SNMPv2-MIB::sysDescr.0 = STRING: "hardware": x86 Family 6 Model 9 Stepping 5

AT/AT COMPATIBLE - "software": Windows 2008 v 5.1 (Build 2600

Uniprocessor Free)

SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.1

DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (444424) 1:14:04.24

SNMPv2-MIB::sysContact.0 = STRING: idefix

SNMPv2-MIB::sysName.0 = STRING: IDEFIX

[...]

IF-MIB::ifIndex.2 = INTEGER: 2

IF-MIB::ifDescr.1 = STRING: MS TCP Loopback interface

IF-MIB::ifDescr.2 = STRING: Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter

IF-MIB::ifDescr.3 = STRING: NIC Fast Ethernet PCI Familia RTL8139 de Realtek

[...]

IF-MIB::ifPhysAddress.2 = STRING: 0:4:23:66:ee:ad

IF-MIB::ifPhysAddress.3 = STRING: 0:c:6e:8a:f8:39

5.2. Herramientas de monitorización y control de tráfico

Existen una gran variedad de herramientas en ambos ámbitos. Pueden encontrarse herramientas y plataformas de monitorización tanto comerciales como de código libre. Al igual que en otras circunstancias, la elección dependerá de la estructura, de las posibilidades económicas y de disponibilidad de personas que realicen las tareas de administración en una organización. Algunos ejemplos podrían ser:

5.2.1. SolarWinds

Entre las características ofrecidas por este producto se citan:

— Supervisa y analiza estadísticas de rendimiento de red detalladas y en tiempo real para enrutadores, conmutadores, puntos de acceso inalámbrico, servidores y cualquier otro dispositivo con SNMP habilitado.

— Supervisa servidores VMware® y rastrea automáticamente el rendimiento de las máquinas virtuales (VM).

— Supervisa conmutadores virtualizados con la misma facilidad que los servidores físicos.

— Supervisa problemas de rendimiento de canal de fibra y VSAN con alertas e informes en tiempo real.

— Simplifica la administración de los componentes al proporcionar una visión unificada del estado de la red de centro de datos.

— Permite conocer rápidamente el estado de los principales servicios de TI y centros de datos a través de alertas refinadas que agrupan en forma dinámica los sistemas y dispositivos relacionados; genera alertas sobre problemas reales al habilitar dependencias de alertas de red avanzadas para eventos correlacionados, condiciones sostenidas y combinaciones complejas de estados de dispositivos.

— Escanea periódicamente la red para detectar cambios, indica que supervise dispositivos nuevos, proporciona capacidades de actualización para los mapas de red, y muestra automáticamente conexiones entre dispositivos.

— Muestra la red en forma gráfica y permite rastrear visualmente las estadísticas de rendimiento en tiempo real a través de mapas dinámicos de red.

— Admite el análisis dispositivo por dispositivo y la visualización de información detallada de sistema.

5.2.2. Nagios

Nagios es un sistema de monitorización de equipos y de servicios de red, creado para ayudar a los administradores a tener siempre el control de qué está pasando en la red que administran y conocer los problemas que ocurren en la infraestructura antes de que los usuarios de la misma los perciban.

Es un sistema muy completo en cuanto a sus características que además hace uso en algunos casos de diversos sistemas como por ejemplo sistemas gestores de bases de datos, servidores web, etcétera. Es relativamente complejo de instalar y configurar.

Nagios es un software usado en todo el mundo, que monitoriza todo tipo de sistemas y que permite extender su funcionalidad con la utilización/creación de extensiones. Está liberado bajo licencia GPL de la Free Software Foundation.

Los dispositivos que se pueden monitorizar con Nagios pueden ser:

— Servidores.

— Impresoras.

— PCs.

— Encaminadores (*Routers*).

— Conmutadores (*Switches*).

— Cualquier servicio que se ofrezca en la red (*http, https, DNS, Samba, NFS*, etcétera).

Nagios cuenta con la siguiente estructura:

— Un núcleo de la aplicación, que forma la lógica de control de negocio de la aplicación. Contiene el software necesario para realizar la monitorización de los servicios y máquinas de la red para la que está preparado.

— Hace uso de diversos componentes que vienen con la aplicación y puede hacer uso de otros componentes realizados por terceros.

— Aunque permite la captura de paquetes SNMP trap para notificar sucesos, no es un sistema de monitorización y gestión basado en SNMP, sino que realiza su labor basándose en una gran cantidad de pequeños módulos software que realizan chequeos de parte de la red.

— Muestra los resultados de la monitorización y del uso de los diversos componentes en una interfaz web a través de un conjunto de CGI's (Common Gateway Interface) y de un conjunto de páginas HTML que vienen incorporadas de serie y que permiten al administrador una completa visión de qué ocurre, dónde y, en algunos casos, por qué.

— Por último, si se compila para ello, Nagios guardará los históricos en una base de datos para que, al detener y reanudar el servicio de monitorización, todos los datos sigan como iban, sin cambios.

Otros ejemplos de software de monitorización lo constituirían Zabbix, PRTG Network Monitor, HP OpenView, IBM Tivoli, Microsoft System Center, etc.

5.2.3. WireShark

Al igual que en el caso de las herramientas de monitorización de redes, existen numerosas herramientas de control de tráfico. En este caso, con casi total seguridad la más conocida es WireShark, la heredera de la conocidísima Ethereal desde 2006.

Es una herramienta gráfica para identificar y analizar el tráfico. Permite analizar los paquetes de datos en una red activa y desde un archivo de lectura previamente generado, como sería el caso de generar un archivo con tcpdump para luego analizarlo con Wireshark.

WireShark hoy en día está categorizado como uno de los mejores "sniffer" junto a Nessus y Snort.

Algunas de las características de **WireShark** son las siguientes:

— Disponible para UNIX, LINUX, Windows y Mac OS.

— Captura los paquetes directamente desde una interfaz de red.

— Permite obtener detalladamente la información del protocolo utilizado en el paquete capturado.

— Cuenta con la capacidad de importar/exportar los paquetes capturados desde/hacia otros programas.

— Filtra los paquetes que cumplan con un criterio definido previamente.

— Realiza la búsqueda de los paquetes que cumplan con un criterio definido previamente.

— Permite obtener estadísticas.

— Sus funciones gráficas son muy poderosas ya que identifica mediante el uso de colores los paquetes que cumplen con los filtros establecidos.

— Es importante tener presente que WireShark no es un IDS *(Intrusion Detection System*, sistema de detección de intrusión) ya que no es capaz de generar una alerta cuando se presentan casos anómalos en la red.

— Es un programa de software libre y multiplataforma, que podremos instalar tanto en Microsoft Windows como en Mac o Linux.

Otros ejemplos de herramientas de control de tráfico que cuentan con características similares a WireShark son Nessus, Snort, Network Monitor en entornos Microsoft Windows Server, etcétera.