Administración de dominios.

Caso práctico

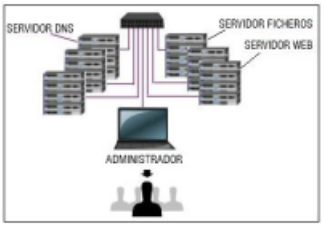
Una de las características de los sistemas operativos configurados en los equipos, que forman parte de la infraestructura de red de "GESTISA", es que permiten compartir recursos (aplicaciones, impresoras, carpetas, ficheros), entre los equipos y usuarios de la red, bajo la supervisión de permisos y niveles de acceso de los diferentes empleados. Las posibles estructuras para trabajar en red dentro de la empresa son: **cliente/servidor** basada en servidores independientes o servidores controladores de **dominio** y**grupo de trabajo**.

La elección depende de las necesidades a la hora de utilizar los sistemas informáticos. Algunas de estas**necesidades** son:

- **Trabajar con aplicaciones compartidas**. (Por ejemplo: "Una aplicación que gestiona la asesoría laboral multiempresa para atender a varios clientes, a dicha aplicación accederán todos los empleados abogados laborales de la empresa GESTISA").
- **Centralizar la seguridad de la red** en un solo ordenador. (Por ejemplo:" Ordenador controlador de dominio que guarda las copias de seguridad de las bases de datos de las aplicaciones y que controla el acceso remoto a los datos de los clientes").
- **Posibilidad de ampliación de equipos y usuarios** sin limitaciones. (por ejemplo: "Instalación de nuevas impresoras por conexión en red compartidas para todos los usuarios").
- **Servicio de aplicaciones y dispositivos**. (Por ejemplo: "Aportar a los usuarios el servicio de correo electrónico propio de la empresa, y el almacenamiento y transferencia remota de información a través de la red").

Las diferentes posibilidades que Carlos, como administrador, tiene para gestionar las instalaciones de los S.O. (sistemas operativos), dependen del modo de trabajo dentro de la infraestructura de la red es decir, tiene instalados sistemas operativos de tipo cliente o servidor tanto en distribuciones Windows como en Linux.

Carlos gestiona y trabaja con los denominados dominios, con el fin de poder centralizar el compartir recursos y aplicaciones entre los usuarios de la red de un modo seguro. Trabaja con equipos formando grupos de trabajo y con ordenadores Linux que actúan de servidores (como por ejemplo para "dar servicio de alojamiento Web, emitir a sus empleados informes y noticias internas de la empresa, etc.").



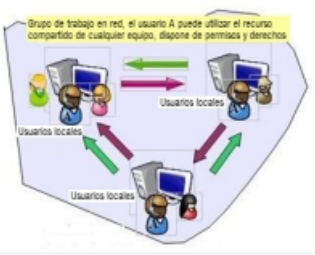
Estructura de trabajo en grupo.

Caso práctico

En muchos entornos de red los ordenadores facilitan la gestión de los **recursos compartidos**, configurando sus equipos en modo **grupo de trabajo**.

"GESTISA" dispone de una subred donde tiene configurado un conjunto de tres equipos formando un grupo de trabajo, utilizados principalmente por los empleados para realizar consultas por Internet, donde tratan asuntos de investigación y proyectos comunes entre grupos de usuarios, (por ejemplo "el estudio de asesoramiento de ciertos casos de clientes por varios abogados), y donde necesitarán compartir documentos y una impresora.

Los usuarios pueden **acceder localmente al sistema operativo de un ordenador, que actúa como terminal de una red en la que existen equipos servidores, todo dependerá del modo en que el usuario se identifique**, o realice el login a la hora de entrar en el sistema. Los ordenadores mediante los **sistemas operativos en red permiten el acceso a sus recursos compartidos mediante dos métodos**:



- **Como miembro de un Grupo de Trabajo.**
- **Como miembro de un Dominio.**

Un grupo de trabajo se define como un conjunto de ordenadores en red que comparten recursos de software y hardware. En el modelo de grupo de trabajo no existe un servidor central y ordenadores clientes, sino que son redes de igual a igual o punto a punto (peer to peer). Para acceder al recurso basta con estar en la red, conocer la ubicación del recurso y su contraseña. Dentro de una misma subred pueden existir diferentes grupos de trabajo.

En un grupo de trabajo cada equipo conserva una lista de los usuarios autorizados y los recursos disponibles. Como son listas descentralizadas hay que dar de alta a cada nuevo usuario en cada ordenador.

Windows, de forma predeterminada, tiene configurada la compartición de recursos en una estructura de grupo de trabajo, (llamado WORKGROUP).

Entre ordenadores con sistema operativo Linux, podemos compartir recursos mediante el servicio NFS que permite el acceso a recursos desde ordenadores clientes a otros que actúan de servidor, siempre que existan los permisos adecuados. Para compartir recursos entre redes mixtas, es decir, que dispongan de ordenadores con S.O. Windows y Linux será necesario utilizar el protocolo SMB.

Para integrar el equipo en un grupo de trabajo en red, debemos tener configurada la tarjeta red de forma correcta dando valores a los protocolos TCP/IP,DNS, puerta de enlace, etc., estudiado ya en unidades anteriores.

Las últimas distribuciones de Windows disponen de la función denominada **Mapa de red**, que permite usar el protocolo LLTD que detecta la topología de red con el fin de mostrarnos un gráfico para ayudarnos a buscar otros equipos y dispositivos que en ese instante están conectados en nuestra red local. Para mostrar el mapa, damos a *Inicio-Panel de control-Red e Internet-Centro de redes y recursos compartidos*, en la parte superior derecha de la ventana, pulsamos en *Ver el mapa completo*. (Con configuración de red como *pública* no funcionará).

Recordemos que las versiones de Windows 7 disponen de un grupo de trabajo especial denominado **Grupo Hogar**, que permite la creación automática, por parte del sistema, del grupo con el fin de facilitar al usuario la compartición de recursos dentro de una red, el único inconveniente es que solamente permite esta configuración a equipos que disponen del sistema operativo Windows 7 o Vista.

Debes conocer

En el siguiente podrás documentarte sobre la configuración del Grupo Hogar en una red domestica en Windows 7.

Configuración Grupo Hogar Windows 7.

Autoevaluación

¿Un equipo Windows Server 2008 puede pertenecer a un Grupo Hogar?

- Verdadero.
- Falso.

Configurar un grupo de trabajo por red en un terminal Windows.

Caso práctico

Carlos tiene **configurado** dentro de la estructura de subred **un grupo de trabajo llamado "Consultas"** del que son miembros dos equipos con sistema operativo Windows 7. En uno de los terminales ha gestionado una carpeta compartida, a la que pueden acceder todos los usuarios del sistema que están realizando trabajos de investigación sobre ciertos casos de clientes.

Un ordenador al iniciar el arranque dentro de un entorno de red puede que se incorpore a un grupo de trabajo. **En Windows para añadir un equipo a un grupo de trabajo debemos seguir los siguientes pasos**: *Inicio-Equipo*, hacer clic al botón derecho del ratón y seleccionamos la opción de *Propiedades*, de la ventana pulsamos en*Configuración avanzada del sistema*, seleccionamos la pestaña **Nombre del equipo** en ella damos clic en el botón*Cambiar* aparece la ventana donde tenemos los campos que identificarán al ordenador dentro de un grupo de trabajo (de forma predeterminada será **WORKGROUP**), desde este lugar podemos cambiar el nombre del mismo para que se incorpore al grupo de trabajo que deseemos.

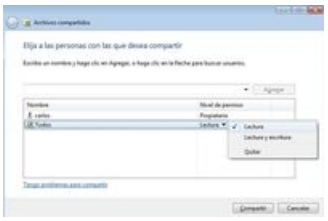
El login de inicio de sesión en Windows, para un usuario en un equipo que pertenece a un grupo de trabajo, presenta la forma de petición de acceso de nombre de usuario local y clave. Cuando se inicia sesión localmente o remotamente, solamente se tiene acceso a los recursos del equipo que la cuenta o grupo permitan. **Para que un usuario pueda acceder localmente a los recursos de un ordenador de un grupo de trabajo, tendrá que estar dado de alta y haber iniciado la sesión en el propio ordenador.**

Si deseamos acceder a un **recurso compartido** por otro ordenador miembro del grupo de trabajo, el usuario deberá estar dado de alta en el ordenador que sirve el recurso, para que cuando le solicite el login de acceso pueda identificarse (si accede con la misma cuenta que el equipo con el que ha iniciado sesión no le solicitará identificación).

Hay que recordar que existe una **cuenta predeterminada** común en todos, con la que se podría acceder si tenemos permisos adecuados al recurso que es la de *Invitado*, pero por seguridad en el sistema se encuentra desactivada, podemos comprobarlo desde*Inicio-Panel de control-Herramientas administrativas-Administración de equipos- Usuarios y grupos locales-Usuarios*, seleccionar la cuenta de *Invitado* y pulsar con el botón derecho del ratón y hacer clic en *Propiedades*, veremos una ventana con los valores de la cuenta de *Invitado*.

En Windows para **comprobar los equipos y los grupos de trabajo pertenecientes a una misma red** se siguen los siguientes pasos: desde **Inicio-Panel de control**, activamos *Ver por Categoría*, pulsamos en el icono *Redes e Internet* y hacemos clic en *Ver los equipos y dispositivos de red*, vemos una ventana con los grupos de ordenadores y los equipos conectados en la red. También podemos acceder desde *Inicio-Equipo*, pulsando en el icono de *Red* del panel izquierdo.

Si deseamos compartir un recurso para los ordenadores del grupo debemos acceder al recurso con el explorador, seleccionar con el ratón y pulsar el botón derecho, hacemos clic en la opción del menú *Compartir con* y seguidamente en *Usuarios específicos* para elegir cuales pueden utilizar el recurso y que permisos (en la siguiente unidad estudiaremos otros modos, los permisos y derechos de los recursos compartidos).



Debes conocer

En el siguiente enlace podrás ver un vídeo para aprender a configurar recursos en un grupo de trabajo en Windows Vista y compartir algún recurso (dentro de la página pulsar en el enlace "Ver demostración" para visualizar el vídeo). La diferencia con Windows 7 es la localización de los parámetros de configuración ya que la capeta de acceso *Público* se encuentra dentro de *Documentos* y la configuración de algunos parámetros de configuración se encuentra dentro de *Centro de redes y recursos compartidos* en el enlace de *Cambiar compartición de uso compartido avanzado*.

Compartir recursos en grupo de trabajo con equipos Windows.

Configurar un grupo de trabajo por red en un terminal Linux con Samba.

Caso práctico

Carlos tiene configurado, dentro de la estructura de subred, un **terminal con sistema operativo Linux** que dispone de una carpeta compartida llamada "Copia" en el escritorio del usuario "Carlos". Todos los usuarios de los equipos que son miembros del grupo de trabajo llamado "WORKGROUP" pueden acceder a ella, con el fin de realizar copias de seguridad de los diferentes trabajos de investigación que se están realizando sobre ciertos casos de clientes.

Linux ofrece varios medios para compartir recursos, cuando se trata de compartir información con clientes con sistemas operativos Windows, dispone de una herramienta de integración llamada **Samba que nos permitirá configurar los equipos Linux para que sean miembros de un grupo de trabajo en red**, con el fin de poder acceder a información e impresoras compartidas entre ambos sistemas operativos.

Al implantar el servicio Samba será necesario instalar en el equipo Linux, la parte del servicio cliente que permite acceder a recursos compartidos por terminales Windows y la parte servidor para poder ofrecer recursos a los otros miembros del grupo de trabajo. Podemos configurar samba modificando con un editor de textos su fichero de configuración **smb.conf** o con herramientas gráficas como son las aplicaciones Swat, system-config-samba, webmin, etc. que nos facilitarán esta tarea. **Samba** también ofrece la posibilidad de **convertir un servidor Linux en un controlador de dominio principal** de un entorno de red con terminales Windows, permitiendo centralizar el acceso de usuarios y equipos del dominio. Hay que destacar que no dispondrá de un verdadero Directorio Activo, como el que tienen los controladores de dominio de servidores con sistemas Windows Server, hasta que no se integre un servicio LDAP como puede ser el OpenLDAP, (el próximo servidor Samba 4, será similar al servidor de archivos e impresión de Directorio Activo de Microsoft).

Debes conocer

Para facilitar la configuración en la compartición de recursos en Linux, se aportan aplicaciones que se ejecutan en entornos gráficos, entre ellas están Swat (que veremos más adelante) y system-config-samba. En los siguientes ficheros encontrarás la información necesaria para agregar un terminal Linux a un grupo de trabajo y **compartir recursos en ese grupo de trabajo** desde herramientas del entorno gráfico.

Grupo de trabajo por red en Linux mediante Samba. (0.35 MB)

En el siguiente enlace veremos cómo realizar la tarea de compartir recursos desde línea de comando modificando el fichero de configuración de SAMBA smb.conf.

Compartir archivos entre Linux y Windows configurando el fichero smb.conf. (0.17 MB)

Para saber más

En el siguiente enlace puedes ver un vídeo para aprender a gestionar recursos compartidos con system-config-samba.

Tutorial sobre la aplicación system-config-samba.

Autoevaluación

¿Cómo se llama el nombre del Grupo de Trabajo que tiene configurado los sistemas Windows, por defecto, después del proceso de instalación?

- Peer to peer.
- SAMBA.
- WORKGROUP.
- NFS.

Acceso a recursos compartidos grupo trabajo desde Windows y Linux.

Para localizar un recurso compartido desde cualquier Windows seguimos los siguientes pasos:

- Desde **Panel de control** seleccionamos la opción *Centro de redes y recursos compartidos*, y pulsamos en la opción *Ver equipos y dispositivos*. Otro camino es pulsar en *Inicio-Equipo-Red*, y seleccionamos el equipo. Si el usuario que accede no es el mismo que el usuario que tiene derechos sobre el recurso compartido, puede que nos pregunte *Nombre de usuario* del recurso compartido y *contraseña* (si el usuario que ha iniciado sesión en Windows es el mismo que el usuario samba de Linux no pedirá usuario y clave al acceder al recurso compartido), seguidamente aparecerán los recursos compartidos por el equipo.

Otra forma de **acceder es escribiendo en la barra de direcciones** del explorador de archivos, la dirección IP del equipo al que deseamos acceder o su nombre NetBIOS, con formato:

\\ip_equipo\ ó \\ip_equipo\recurso_compartido.

Recordemos que siendo un usuario Administrador, desde *Inicio-Panel de control- Redes e Internet*, podemos gestionar todos los aspectos referido a la **configuración de la red**, como pueden ser:

  - **Cambiar la configuración de la tarjeta de red.**
  - **Cambiar las opciones de uso compartido** para distintos perfiles de la red, activando y desactivando opciones como Detección de redes, Permitir el uso compartido de la impresora.
  - **Compartir recursos y acceder a los recursos** compartidos por otros equipos.
  - **Ver el estado** actual de la red.
  - **Conectarse a una unidad de red**, es decir, visualizar en el entorno de trabajo un recurso compartido por otro equipo como si fuera una unidad o dispositivo conectado en el propio equipo, de manera que facilita su acceso en todas las sesiones con un simple clic como si fuera una unidad de disco. Para su realización seleccionamos *Inicio-Equipo*, damos en el icono de *Red* del panel izquierdo y del menú pulsamos en*Conectar a una unidad de red*, seguimos el asistente que nos pedirá un nombre de unidad para el recurso compartido que posteriormente debemos buscar en el entorno de red dando en el botón *Examinar*.

Es importante considerar que **las conexiones múltiples para un servidor o recurso compartido compatible por el mismo usuario, usando más de un nombre de usuario, no están permitidas**. Para poder acceder a otro recurso debemos cerrar todas las conexiones al servidor o recurso compartido y volver a intentar conectar en una nueva sesión.

Vamos a suponer que tenemos un recurso compartido desde un **servidor Samba** en Linux o en un equipo Windows. **Para acceder al recurso compartido desde el entorno gráfico de un terminal Linux**, previamente en el ordenador Linux debemos haber instalado el paquete cliente samba o más concretamente el samba-client (por ejemplo desde la herramienta del Synaptic), y después seguir los siguientes pasos:

- Desde el menú *Lugares-Conectar con el servidor*, en el campo de *Tipo de servicio* seleccionar *Compartido por Windows* y rellenamos los campos especificados en la ventana. El campo más identificativo es indicar la dirección *IP* o el nombre del ordenador que actúa de servidor del recurso compartido, también debemos indicar en el campo *General* el nombre del recurso compartido. Al pulsar clic en el botón de *Conectar* el sistema montará el recurso en el escritorio del usuario.

- Existen distribuciones que al tener instalado samba, permitirán desde el propio explorador visualizar los recursos compartidos desde ordenadores Linux y Windows, para ello debemos ir al menú *Lugares-Red* donde aparecen los equipos Linux y Windows de la red del mismo grupo de trabajo.

Autoevaluación

¿Podemos acceder a un recurso compartido de otro ordenador mediante la herramienta de Conectarse a una Unidad de Red?

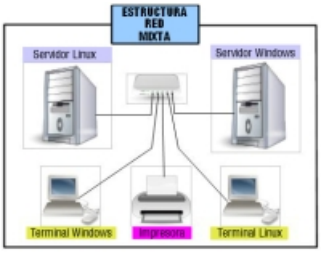
- Verdadero.
- Falso.

Estructura Cliente-Servidor: OpenSSH.

Caso práctico

El **servidor de Linux** de la red de "Gestisa", permite acceder a varios usuarios simultáneamente a su sistema desde cualquier terminal de la red. Carlos, como usuario **root**, administra el acceso seguro de los usuarios mediante el protocolo SSH.

Los empleados utilizan el servidor de Linux para ejecutar aplicaciones de licencia libre, como es el paquete ofimático **OpenOffice**, necesario para realizar tareas administrativas como escribir cartas y estudios estadísticos con la hoja de cálculo, etc.



En una **estructura de red cliente-servidor** los recursos se sirven y administran desde un ordenador central llamado servidor al que se accede desde estaciones de trabajo o terminales cliente que generalmente disponen de pocas prestaciones. Los usuarios en los ordenadores con un S.O. monopuesto se validarán para conectarse en un ordenador principal con el fin de utilizar sus servicios y recursos. El servidor dispone de un S.O. **multitarea y multiusuario** que permitirá, de forma coordinada, la gestión optimizada de los usuarios, recursos y equipos de la red controlando de forma segura el acceso a los datos y servicios. Se puede considerar que un servidor es dedicado cuando solamente realiza funciones de de servidor y no se utiliza como estación de trabajo.

En Windows, el servidor o server dispone de un S.O. que trabaja sobre el concepto de dominio, que permitirá coordinar y compartir de forma segura los recursos, gestionando una base de datos denominada **Active Directory**(AD) o **Directorio Activo**.

Linux dispone, de forma predeterminada, de la función de **multiusuario** necesaria para ser un S.O. servidor independiente, para que todos sus usuarios puedan acceder simultáneamente de forma remota desde un ordenador cliente mediante el protocolo ssh o telnet (ya en desuso por problemas de seguridad). También, puede adquirir la función de **controlador de dominio**, mediante el protocolo SMB (Samba), que permitirá compartir recursos entre sistemas mixtos de Linux y Windows. Además puede disponer de una base de datos que organice y coordine todos los recursos de la red de forma centralizada como hace el Active Directory de Windows, para ello será necesario instalar el **servicio LDAP**.

Cuando se gestiona una infraestructura en red cliente-servidor debemos considerar aspectos importantes como:

- La **cantidad de recursos a compartir** y el nivel de acceso (concesión permisos y derechos a los usuarios).
- Posibilidades de **control de administración de la red**, la potencia en aplicaciones y herramientas que faciliten y permitan una correcta administración de los recursos del servidor.
- Las necesidades de **seguridad** de los datos, usuarios, equipos que son gestionados por el servidor de la red.
- La **cantidad de objetos** (usuarios, equipos, dispositivos, recursos, etc.) de la red a **controlar**.
- La **facilidad de operatividad** entre los sistemas cliente y servidor.

Las funciones y características de los servidores de una red dependerán de **los servicios que ofrezcan a los usuarios** y podemos considerar como importantes los siguientes:

- **Servidor de ficheros**: permite a los usuarios utilizar archivos, carpetas de forma centralizada y segura.
- **Servidor de aplicaciones**: permite a los usuarios del sistema acceder a la aplicación instalada en el servidor.
- **Servidor web**: permite el acceso a ficheros HTML desde los navegadores Web.
- **Servidor de base de datos**.
- **Servidor de correo electrónico o mensajería**.
- **Servidor de transferencia de ficheros o FTP.**
- **Servidor de impresión:** permite utilizar por los ordenadores clientes las impresoras conectadas en la red.
- **Servidor DNS.**

Debes conocer

En el siguiente documento aprendemos a configurar un ordenador cliente o estación de trabajo para acceder a un servidor independiente de Linux.

Acceso al servidor independiente Linux desde estaciones de trabajo por ssh. (0.03 MB)

Para saber más

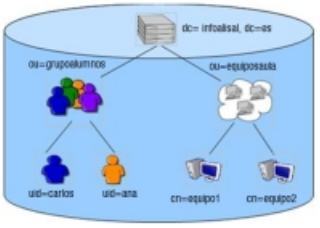
En el siguiente enlace aparece un vídeo para aprender a configurar el servicio de acceso seguro al servidor Linux por ssh.

Configuración ssh.

Protocolo LDAP.

Caso práctico

En los entornos donde existen **ordenadores que controlan y organizan los objetos y recursos** de la red, se utiliza un servicio denominado "**de directorio**". Estos ordenadores disponen de un protocolo especial denominado **LDAP**. Carlos ha analizado y estudiado este modo de organización debido a su gran importancia en las estructuras en red, con el fin de sustituir el servidor de Active Directory cuyo propietario es Windows (necesita licencia de uso) por el directorio LDAP gestionado por la herramienta gratuita OpenLDAP que se puede instalar y administrar en el servidor Linux.



Mediante la activación del llamado servicio de directorio de red se consigue disponer de información ordenada jerárquicamente de los objetos como son los usuarios, equipos, recursos, impresoras, etc. El **protocolo LDAP** es el que se encarga de gestionar el acceso al servicio para permitir a los usuarios almacenar datos, realizar consultas, operaciones de administración, etc., dentro del directorio de red. La propia función Active Directory (AD) o directorio activo de Windows utiliza una tecnología parecida a LDAP junto con el servicio DNS para gestionar y coordinar los recursos de la red de una forma centralizada.

En Linux no existe el concepto de directorio activo pero se puede habilitar la misma función instalando el **servicio LDAP** (Protocolo Ligero de Acceso a Directorios) combinando las aplicaciones Samba con la aplicación***OpenLDAP*** permitiendo gestionar un servicio de directorio mediante una base de datos, que mantendrá la información relacionada de las cuentas de usuarios y objetos existentes en la red. En el siguiente enlace puedes consultar el significado de las diferentes implantaciones de Acceso a Directorios.

El servicio **LDAP permite el acceso a dicha información mediante un esquema de directorio** que contiene las definiciones de los objetos que pueden darse de alta en el directorio. El directorio está **basado en una estructura jerárquica de árbol** de objetos, en la que cada objeto está identificado por propiedades denominadas atributos. Cada atributo se identifica mediante un nombre distinguido o *dn*, tipo o clase de objeto (ObjectClass) y valores asociados. La cantidad de atributos dependerán del objeto, pueden tener atributos como *cn* (describe el nombre común), *sn* (para el apellido).

Cada entrada del directorio es una cadena de caracteres formada por pares **"tipo_atributo"="valor"** separados por comas, que representa la ruta invertida que lleva desde la posición lógica de la entrada en el árbol hasta la raíz del mismo. El nombre raíz del directorio LDAP utiliza la identificación de objetos de la misma forma que los dominios DNS. Por ejemplo, la raíz o base del "IES Alisal" sería: "*dc=alisal, dc=es*".

A partir de esa base, el árbol se subdivide en los nodos o ramas, subnodos y objetos u hojas del árbol. Siguiendo con el ejemplo del dibujo, a continuación se muestra un subconjunto de los atributos del usuario "carlos":

***dn: uid**=carlos, **ou**=grupoalumnos,* **dc**=*infoalisal, **dc**=com*
***objectClass**: person*
***cn**: carlos soto*
***sn**: soto*
***description**: alumno clase*
***mail**: calos@infoalisal.es*

Para saber más

En el siguiente enlace podrás documentarte sobre el proceso de instalación del servicio de directorio OpenLDAP en Linux y ampliar conocimientos sobre el protocolo LDAP. En 2º curso del ciclo se estudiará con más detalle **LDAP** (Lightweight Directory Access Protocol ó Protocolo Ligero de Acceso a Directorios).

Instalación de LDAP en Linux. (1.05 MB)

Autoevaluación

Es cierta la afirmación que dice que OpenLDAP es un servidor LDAP de código abierto, que se ha posicionado como una solución de LDAP para Linux así como también una alternativa al conocido Active Directory de Windows.

- Verdadero.
- Falso.

Los dominios.

Caso práctico

En muchos **entornos de red** llega un momento que es necesario ofrecer a los usuarios una **estructura segura y bien organizada**, para ello se valen de las aplicaciones que dispone el sistema operativo **Windows Server**para gestionar **dominios**.

La red informática de "Gestisa" dispone de un dominio que agrupa un conjunto de estaciones de trabajo y usuarios de la red. Existe un servidor Windows Server 2008 que actúa de controlador de dominio principal, encargado de gestionar el acceso a recursos compartidos como son las impresoras y las aplicaciones. Carlos es el responsable del Dominio.

Windows utiliza el concepto de dominio como una agrupación de ordenadores en un entorno de red, (servidores y estaciones de trabajo), controlados por **un ordenador que actúa de servidor principal**, el cual guarda la lista de usuarios y nivel de acceso de cada uno, así como la gestión centralizada de recursos, equipos, servicios, etc. Estos servidores son **Controladores de Dominio** (Windows Server 2008 y Linux) y ayudan a la administración de la seguridad del grupo. Los ordenadores integrados en el dominio no necesitan físicamente estar en la misma red, además, a diferencia de los grupos de trabajo presentan mayor seguridad y organización.

El AD de Windows es una implementación de LDAP ya que trata los recursos de la red como objetos que tienen propiedades y atributos. Por ejemplo, cada objeto se identifica por un atributo de nombre relativo o nombre común (CN), además también tienen un atributo llamado nombre distintivo (DN) que describe la ubicación del objeto en el directorio.

Cuando un ordenador está configurado para pertenecer a un dominio, se utilizan cuentas usuario de dominio creadas en el servidor para iniciar sesión desde un ordenador cliente. **Cualquier usuario con una cuenta de dominio, puede iniciar sesión desde cualquier equipo que esté incluido en el dominio**, siempre que no esté restringido su acceso desde la configuración del Active Directory del servidor en el caso de Windows, o servicio de directorio en Linux.

Cuando en una red se genera un controlador de dominio, podemos decir que en ese momento se ha creado un dominio. En el caso de Windows Server, se realizará en el momento de instalar los Servicios de dominio de Active Directory. Si **varios dominios forman parte de un sistema de comunicación, se podrán establecer relaciones de confianza entre ellos para compartir los recursos**. Mediante la organización de las redes en dominios, podemos dividir redes grandes en más pequeñas, permitiendo crear dominios principales con sus correspondientes **subdominios** y estructuras jerárquicas independientes.

La estructura jerárquica de un dominio en una red Windows, tiene forma de **árbol** compuesta por un dominio principal o raíz que será el padre de todos los dominios hijos o subdominios del árbol. Un conjunto jerárquico de árboles formarán un **bosque** de dominios. Los árboles de dominio y los dominios de un árbol, se podrán comunicar estableciendo **relaciones de confianza**, que permiten al usuario iniciar sesión en un dominio, y utilizar los recursos gestionados por otro dominio de esta forma podemos compartir recursos entre los dominios.

En una red que tenga una infraestructura grande se necesitará más de un controlador de dominio, todos dispondrán de una copia del Directorio Activo, así el usuario se podrá validar en el que esté más disponible mejorando la actividad de validación de usuarios. Los controladores disponen del llamado **catálogo global**, que tiene la función de mantener una información esquematizada y actualizada de los usuarios, grupos, equipos y recursos de todos los dominios de un bosque.

Para saber más

En el siguiente enlace puedes obtener más documentación referente a la estructura de dominios y su aplicación en Windows Server.

Estructura de dominios y Active Directory.

Autoevaluación

¿Cuál es la afirmación falsa?

- Mediante las relaciones de confianza los controladores de dominio pueden compartir los recursos.
- Un equipo puede pertenecer a un Grupo de Trabajo y a un dominio simultáneamente.
- Dentro de un dominio pueden existir más de un controlador de dominio.
- Un dominio con equipos Windows puede estar controlado por un servidor Linux.

Planificación y requisitos necesarios para montar una estructura de dominio.

Para evitar posibles problemas en el futuro, **antes de comenzar la instalación de los servicios de dominio en un directorio activo**, debemos pensar en una serie de consideraciones relacionadas con ampliaciones de las estructuras de los sistemas y sus configuraciones, como son:

- **Saber cuántos servidores con funciones de controlador de dominio se necesitan**. Debemos tener en cuenta que un sólo dominio puede dar servicio de sus recursos, a gran cantidad de usuarios. En Windows Server 2008 los servidores pueden ser:
  - **Controladores de dominio de sólo lectura (RDOC)**, no garantizan seguridad y por tanto se configuran para disponer de una copia del Active Directory que no se puede modificar.
  - **Controladores de dominio de escritura**, que permiten la validación de usuarios y dispositivos permitiendo la actividad de mantenimiento de altas, bajas y modificaciones de los objetos del Active Directory.
  - **Servidores de archivos que almacenan recursos de la red**, no funcionan como controladores de dominio y por tanto no disponen de copia del AD. Pueden realizar otras funciones de servidor dependiendo del sistema y servicio instalado.
  - **Servidores configurados fuera del dominio**, llamados independientes, que entran a formar parte de una estructura de red en grupo de trabajo cómo estaciones de trabajo a la hora de compartir recursos.
- Conocer que **funciones deben gestionar los dominios y subdominios**. Pensando siempre que las relaciones de confianza que se generen, puedan permitir que los administradores otorguen permisos para que los recursos de cualquiera de los dominios de un bosque o árbol estén disponibles para todos los usuarios de los dominios.
- Pensar cuantas **unidades organizativas** se necesitan y quien gestionara su administración.
- Definir las **directivas de grupo y de seguridad local**.
- Planificar cuántas **cuentas de usuarios, grupos y equipos** gestionará cada dominio.
- Definir un **plan de seguridad** basado en la replicación de los servicios de directorios.
- Mejorar las **necesidades de hardware** para los controladores de dominio, como en los componentes de:
  - **Procesador** rápido o la posibilidad de multiprocesadores. Se mejorarán los procesos de replicación sin que afecte a otros procesos del servidor.
  - Ampliar la **memoria RAM**, como mínimo deberá ser de 2GB.
  - Disponer de suficiente **disco**, para almacenar la información de la base de datos del directorio activo.
  - Disponer de un **sistema de seguridad**, que gestione la tolerancia a fallos, basado en **RAID- 1 o RAID-5**.
- Tener acceso a un servidor que suministre **servicios de nombres de dominio (DNS)**, que puede estar instalado en el propio servidor de dominio siempre que su dirección IP de red sea estática.
- Tener instalado un servidor que actúe de **controlador de dominio principal**, (Windows Server o Linux Server).
- Haber configurado el **protocolo de red TCP/IP**.
- Tener **espacio suficiente en el disco** para montar el servicio de directorio, en el caso de Windows formateada a NTFS.
- Diseñar un **diagrama o esquema**, que identifique la cantidad de servidores y clientes, así como la función y los recursos que prestará cada uno de los servidores.
- Evaluar la posibilidad de **instalar servidores virtuales**. Podemos pensar en el concepto de servidor virtual, que presta las mismas funciones que un servidor real, de manera que en un servidor físico podemos instalar varios servidores virtuales, permitiéndonos un gran ahorro económico en equipos.

Autoevaluación

¿Se considera conveniente disponer de un hardware específico para la instalación de un controlador de dominio?

- Verdadero.
- Falso.

Servicio de directorio: Active Directory (AD) en Windows.

Caso práctico

El **AD es una implementación propietaria**, (creada por **Microsoft**) de los Servicios de Directorio, que permite compartir información y usar recursos dentro de una red de ordenadores de forma segura. **Carlos tiene creado un controlador de dominio maestro** en el servidor de Windows 2008, para controlar los servicios y usuarios del dominio de su red, y poder compartir carpetas, aplicaciones, impresoras siguiendo unos criterios de derechos y permisos de acceso.

En Windows, cuando se instala el AD el equipo se convierte en servidor de dominio o controlador de dominio dentro de la red, proporcionando una fuente centralizada de información, con el fin de facilitar la búsqueda y utilización de los objetos del directorio por parte de usuarios y dispositivos de la red. Recordemos que un directorio activo, dispone de la siguiente **estructura lógica en forma de árbol jerárquico**:

- Raíz del directorio o **dominio raíz**.
- **Clases de objetos** que serán cada uno de los elementos que controla el servicio de Directorio Activo. Serán usuarios, equipos, agrupaciones de usuarios, agrupaciones de equipos, unidades organizativas de los propios objetos. Cada elemento controlado por el servicio de AD se denomina objeto y dispone de unas propiedades dependiendo de la clase de objeto a la que pertenece.
- **Los Subdominios** son dominio hijos que se añaden al dominio principal o raíz, formando el árbol de dominios. Todos los dominios están relacionados por las llamadas **relaciones de confianza**, compartiendo el mismo catálogo global o repositorio de todos los objetos del árbol de dominios, permitiendo de esta manera el acceso a todos los recursos del árbol. **El catálogo global** contiene información resumida de los recursos (usuarios, grupos, equipos, etc.) de todos los dominios. Los subdominios comparten el mismo espacio de nombre que el dominio raíz, formado por su propio nombre más el nombre del dominio raíz.

Un **conjunto de árboles de dominio agrupados y relacionados lógicamente forman un bosque de dominios**. Cada árbol del bosque se gestiona por su propio espacio de nombres, pero comparten el mismo catálogo global permitiendo localizar y acceder a los recursos de todo el bosque de dominios, desde cualquier equipo del propio bosque, agilizando la búsqueda de los recursos.

En dominios Windows, los servidores que pertenecen a un árbol de dominio, pueden ser controladores de dominio secundarios, encargados de tener una copia de la información del directorio activo, o servidores miembros encargados de almacenar los archivos y recursos de la red. La base de datos que se mantiene en el controlador de dominio, se copia o duplica mediante el **proceso de replicación** en todos los controladores de dominio de la red, de manera que cuando se produzca cualquier modificación en el Directorio Activo, se replicará a todos los controladores de dominio.

El AD necesita el servicio DNS, que organiza grupos de equipos en una jerarquía de dominios usada en Internet y basada en diferentes niveles que identifican equipos, dominios de nivel superior asignando nombres de servidor a direcciones TCP/IP. Será necesario configurar el servicio DNS para instalar el AD de Windows. Los archivos que gestionan la información de la base de datos del Active Directory son:

Ficheros de la base de datos del Active Directory.

Fichero de AD	Funcionalidad
Ntds.dit	Contiene el almacén de datos formado por tres tablas indexadas: tabla de datos, de enlace y de seguridad.
Edb.chk	Mantiene la confirmación de las transacciones realizadas en la base de datos y en los archivos log.
Tmp.edb	Utilizado como soporte temporal para la realización de las transacciones.
Edb.log	Contiene registro de las operaciones que no han sido realizadas en la base de datos.
Edbxxx.log	Contiene registro de las operaciones realizadas en la base de datos del Active Directory.

Debes conocer

En el siguiente enlace aprenderás a instalar y desinstalar Active Directory de Windows 2008 Server.

Instalación y desinstalación de Active Directory. (0.69 MB)

Para saber más

En el siguiente enlace podrás ver un vídeo para aprender a instalar Active Directory en Windows Server 2008.

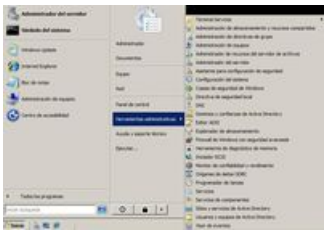
Instalación de un controlador de dominio Windows Server 2008.

El entorno de trabajo de administración de Active Directory.

El usuario administrador del servidor deberá realizar tareas como crear y modificar cuentas de usuario, añadir terminales al dominio, organizar y agrupar objetos, etc. **El sistema operativo Windows Server, dispone de herramientas en el entorno gráfico y en línea de comandos para facilitar la administración de Active Directory (AD).**

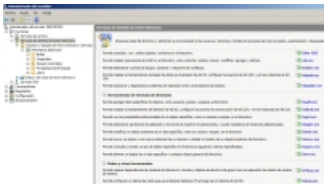
Podemos acceder a las aplicaciones de administración de Active Directory desde el menú *Inicio-Herramientas administrativas*, donde podemos seleccionar opciones que abrirán consolas de administración MMC para la realización de tareas como:

- **Servicios de dominio de Active Directory**, para gestionar los servicios.
- **Usuarios y equipos de Active Directory**, donde podemos realizar tares relacionadas con usuarios, grupos, equipos y unidades organizativas.
- **Dominios y confianzas de Active Directory**, permite trabajar con los objetos de dominio, árboles y bosques creando relaciones de confianza.
- **Administración de directivas de grupo**, podemos realizar las tareas relacionadas con la seguridad de objetos del Active Directory mediante la configuración de las directivas de grupo.
- **Editor ADSI**, realiza diagnósticos del AD para poder resolver problemas creando atributos y propiedades personalizadas para los usuarios y grupos.



Para acceder a algunas herramientas de administración del AD, desde *Inicio-Administración del servidor*, y pulsamos en el enlace descrito como *Servicios de dominio de Active Directory*. Desde este lugar podemos comprobar el estado de los servicios, editar el registro de eventos, administrar funciones, etc., y facilitar la operatividad con los objetos que hay dentro una consola de administración del AD como usuarios, equipos, etc. Windows ofrece las siguientes posibilidades:

- Podemos seleccionar varios objetos a la vez con las teclas de *CTRL* (uno a uno intercaladamente), o *SHIFT*(situados consecutivamente) con el fin de poder realizar una misma operación de forma conjunta.
- Al seleccionar un objeto u objetos y seguidamente pulsar el botón derecho del ratón visualizamos el menú de las diferentes tareas que podemos realizar con el objeto.
- Se pueden mover o cambiar objetos de sitio solamente con seleccionar y arrastrar al lugar deseado.



También podemos ver y ejecutar las diferentes aplicaciones que existen para trabajar en modo de consola de línea de comandos, y consultar la descripción de ayuda de la función que realiza cada una de las aplicaciones. Por ejemplo si deseamos saber como utilizar la orden *DSQUERY*, que permite buscar objetos dentro del AD, desde *Inicio-Símbolo del sistema* en la línea de entrada de comandos escribir lo siguiente: *DSQUERY /?*.

Debes conocer

En el siguiente enlace podemos ver una las herramientas que se utilizan desde la línea de comandos para administrar el AD.

Administrar Active Directory desde la línea de comandos.

Para saber más

En el siguiente enlace podemos ver un documento con ejemplos para aprender a utilizar comandos de Active Directory en Windows Server 2008. Comandos DSMod, DSadd, DSQuery, DSRM, etc.

Ejemplo de administración de Active Directory desde la línea de comandos. (65.2 KB)

Autoevaluación

¿Cuál es el camino a seguir para acceder a comprobar los últimos sucesos o eventos ocurridos en el Active Directory?

- Inicio-Panel de control-Sistema-Administrador de Active Directory.
- Inicio-Herramientas Administrativas-Administración de directivas de grupo.
- Inicio-Administrador del servidor-Servicios de dominio de Active Directory.
- Inicio-Herramientas administrativas- Visor de sucesos.

Administración de unidades organizativas de Active Directory de Windows.

Caso práctico

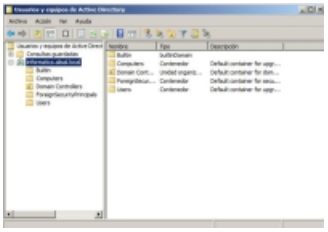
El usuario administrador Carlos tiene **creadas** cuatro unidades organizativas, relacionadas con los grupos de usuarios: el **grupo "asesoria_laboral"** para los usuarios que llevan los casos laborales, el **grupo "asesoria_financiera"** para usuarios relacionados con casos financieros, **"asesoria_contable"** y el grupo**"gestisa_empresa"** relacionados con los usuarios que llevan la contabilidad, nóminas y facturación de la empresa.

Las unidades organizativas (UO) son objetos del directorio que nos permiten agrupar de forma organizada los objetos, (usuarios, grupos,

equipos, recursos compartidos e incluso unidades organizativas), del dominio en el que se definen. Algunas de sus funciones y características son:

- **Facilitan la seguridad** del dominio, aplicando directivas de seguridad a las propias unidades organizativas.
- Permiten **repartir la administración** del AD, entre distintos administradores del dominio con el fin de gestionar los recursos de manera más eficaz y segura.
- **No se pueden crear UO dentro de los contenedores predeterminados del Directorio Activo**, menos en el contenedor **Domain Controllers**.
- Las unidades organizativas **no pueden contener objetos de otros dominios**.
- En la estructura jerárquica del dominio **se sitúa en un nivel inferior al dominio**.
- Se pueden utilizar las unidades organizativas **para crear una estructura funcional de la organización interna departamental**, (almacén, ventas, contabilidad, etc.) de una empresa, en el uso de los recursos y servicios informáticos, ofrecidos por el servidor de dominio, agrupando en conjuntos significativos los usuarios, grupos y recursos según sus necesidades.
- En conclusión, podemos considerar a las UO, como carpetas especiales o contenedores del directorio activo, con directivas de seguridad que servirán para **almacenar o agrupar los usuarios, grupos, equipos, recursos compartidos**, con el fin de tener ordenados los objetos del dominio.

Además de las unidades organizativas, en cualquier dominio el sistema genera de forma predeterminada una serie de carpetas para gestionar los objetos del dominio, y se encuentran en la consola MMC de *Usuarios y equipos de Active Directory*, teniendo activada la propiedad de *Características avanzadas* del menú *Ver* y algunas son:



- **Builtin**: Visualiza las cuentas de usuarios.
- **Computers**: Lista las cuentas de equipo.
- **Domain Controllers**: Es la única unidad organizativa creada de forma predeterminada por el sistema y contiene los controladores de dominio.
- **ForeignSecurityPrincipals**: Describe los objetos de un dominio externo en el que haya una relación de confianza con el dominio actual.
- **NTDS Quotas**: Tiene los datos de cuota de Active Directory.
- **Program Data**: Contiene información de las aplicaciones del Directorio.
- **System**: Visualiza la información de la configuración del sistema.
- **Users**: Lista los usuarios.

Debes conocer

En el siguiente fichero aprendemos a utilizar unidades organizativas realizando operaciones como creación, modificación, traslado y eliminación de las mismas.

Administración de unidades organizativas. (0.60 MB)

Autoevaluación

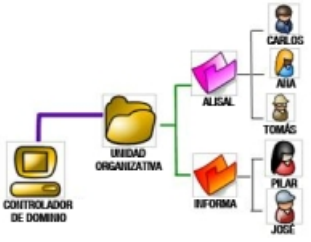
Podemos crear una unidad organizativa dentro del contenedor Users aportado por el Active Directory.

- Verdadero.
- Falso.

Administración de cuentas de usuario de dominio de Windows.

Las cuentas de usuario de dominio, también llamadas globales, permiten acceder a los recursos de todo el dominio de la red desde cualquier terminal que se encuentre asociado al servidor de dominio, y se deben administrar en los servicios del AD donde se podrán conceder permisos y derechos de los recursos del dominio.

Las cuentas de usuario tienen las siguientes características:



- Están definidas por un **nombre y una contraseña** que no se puede repetir, es decir no puede haber dos cuentas de usuarios iguales.
- Los **nombres de la cuenta** están representados por no más de 20 caracteres en mayúsculas, minúsculas, números y caracteres especiales menos: /, |, :, ;, =, <, > y *.
- Las **contraseñas** no contienen menos 7 caracteres, y alguno debe ser en minúsculas, mayúsculas y numérico. El servidor, por seguridad, recordará las últimas 24 contraseñas de un usuario, (durante 1 o 42 días, dependiendo de la configuración).
- Los **nombres de cuenta principales de seguridad dentro del servidor**, están representados por el nombre de usuario y el sufijo @ seguido del nombre del dominio o nombre principal, por ejemplo “carlos@informatica.alisal.local”. Según esto podemos referenciar el nombre de un usuario de dos formas: por su nombre (por ejemplo “carlos”) o por su definición DNS (como “carlos@informatica.alisal.local”).
- Windows define **tipos de cuentas** como:
  - **Administrador**: Generada en el proceso de instalación. Tiene el derecho y los permisos necesarios para la configuración total del

dominio, por eso es miembro de varios grupos relacionados con la administración del sistema. La cuenta Administrador no se puede eliminar ni quitar del grupo Administradores a la que pertenece, pero se puede cambiar el nombre o deshabilitarla. No se puede borrar pero se puede deshabilitar. Por seguridad es conveniente tener más de una cuenta de administrador.
  - **Invitado**: Generada en el proceso de instalación. Es la que utilizan los usuarios que no disponen de cuenta en el dominio para poder acceder a sus recursos. Por seguridad de forma predeterminada está deshabilitada y se puede borrar. Es miembro del grupo de Invitados.
  - **Usuarios**: En el momento que se crea el controlador de dominio en el servidor los usuarios locales pasan a ser usuarios del dominio.
  - **De contacto**: Son cuentas de correo electrónico.

- Las cuentas de usuario se gestionan dentro de la carpeta ***Users*** o de un contenedor creado como unidad organizativa de la ventana de gestión del domino del Directorio Activo.

- Cada cuenta de usuario dispone de identificador de seguridad **SID**, que se crea en el momento de dar de alta al usuario, este número representa al usuario dentro de los procesos del sistema.

Para saber más

En el siguiente fichero están descritas las diferentes tareas de Administración de cuentas de usuarios dentro del AD.

Tareas de administración de usuarios del Active Directory. (0.72 MB)

Autoevaluación

¿En qué campo de la pestaña Perfil en la ventana de Propiedades de la cuenta de un usuario podemos indicar un script de inicio de sesión que pueda contener, por ejemplo la orden para conectar con una unidad de red de un recurso?

- ○ Script de inicio de sesión.
- ○ Fichero bat de arranque.
- ○ Ruta de acceso al perfil.
- ○ Net use.

Administración de grupos de usuarios en Active Directory de Windows.

Caso práctico

El usuario administrador Carlos ha **creado** cuatro grupos de usuarios: el **grupo "asesoria_laboral"** para los usuarios que llevan los casos laborales, el grupo **"asesoria_financiera"** para usuarios relacionados con casos financieros, "**asesoria_contable**" y el grupo "**gestisa_empresa**" relacionados con los usuarios que llevan la contabilidad, nóminas y facturación de la empresa.

Las **cuentas de grupo** las utilizamos para **gestionar la administración** de los recursos de varios usuarios a la vez dentro del directorio activo. Con los grupos podemos formar conjuntos de usuarios que van a tener una administración común, en permisos y recursos compartidos con el fin de facilitar la administración de usuarios, y así evitar hacerlo de forma individual (usuario por usuario).

Los **grupos de usuarios** pueden contener a **otros grupos** produciendo una estructura **jerárquica** de anidamiento de grupos dentro del directorio. Cuando creamos un grupo en el AD debemos definirle dos características:

Características de los Grupos de usuarios de Active Directory.

Tipo de grupo	De seguridad	Se utilizan para asignar usuarios con permisos y derechos sobre los recursos.
	De distribución	Son usuarios sin seguridad con los que se tiene comunicación por correo electrónico.
Ámbito del grupo	Universal	Usuarios, grupos Globales y Universales que incluso pueden pertenecer a otros dominios. Se almacenan en el catálogo global y se replican por toda la red.
	Global	Los usuarios podrán acceder a cualquiera de los dominios del árbol, sus usuarios y grupos Globales deben pertenecer al mismo dominio. No se replica fuera del dominio.
	Local de dominio	Sus miembros acceden a los recursos locales del dominio. Son miembros usuarios, grupos Globales de cualquier dominio, grupos locales del mismo dominio o grupo

		Universal. Los grupos locales no se pueden procesar en otros dominios.

Cuando se crea el AD, el sistema genera grupos predeterminados con permisos y derechos predefinidos. Éstos se encuentran en la consola MMC de **Usuarios y grupos del Active Directory** dentro de la carpeta **Users** (como grupos globales y universales) y de la carpeta **Builtin** (como grupos de dominio local).

Desde *Inicio-Herramientas administrativas-Usuarios y equipos de Active Directory*, al seleccionar la carpeta **Users**o **Builtin** tenemos en el panel derecho la lista de usuarios y grupos predefinidos, en la columna de **Descripción** podemos ver su funcionalidad y en la de**Tipo** vemos las cualidades ámbito y tipo de grupo.

Para saber más

En el siguiente fichero se encuentran descritas las diferentes tareas de Administración que se pueden realizar con los grupos de usuarios dentro del Active Directory.

Administración de grupos del Active Directory de Windows. (0.26 MB)

Autoevaluación

Cuando se elimina una cuenta de grupo se borran del sistema sus miembros.

- Verdadero.
- Falso.

Administración de cuentas de equipos de Active Directory de Windows.

Caso práctico

Todas las **estaciones de trabajo de la red de "Gestisa"** que no forman parte del grupo de trabajo, están dadas de alta como **cuentas de equipo** en la unidad organizativa de equipos, en el **Active Directory** del servidor del dominio Windows server 2008.

Se pueden gestionar **cuentas de los equipos de la red** que pertenecen al dominio, con el fin de controlar el acceso y los recursos de la red. Pueden estar almacenadas en cualquier unidad organizativa como puede ser**Computers**, (creada por el sistema de forma predeterminada) donde se almacenan todas las cuentas de los equipos, menos las de los equipos que son controladores de dominio, que se guardan en el contenedor **Domain Controllers**.

Cuando una cuenta de un equipo esta creada en el Directorio Activo, desde el propio servidor que actúa de controlador de dominio, podemos administrar remotamente el equipo. El controlador de dominio almacena el nombre del equipo y un identificador único dentro del sistema.

Es recomendable intentar que la mayoría de los **equipos clientes dispongan de un sistema operativo y de hardware homogéneo**, para facilitar la administración de los mismos, por ejemplo mediante la creación de imágenes del sistema.

Es importante recordar, que para realizar cualquier operación de administración el usuario debe disponer de los permisos y derechos necesarios, es decir, debe pertenecer a algún grupo de administradores.

Debes conocer

En el siguiente fichero encontramos descritas las diferentes tareas de Administración que se pueden realizar con las cuentas de equipos de la red que pertenecen al dominio dentro del Active Directory.

Administración de equipos del Active Directory de Windows. (0.27 MB)

Para saber más

Con el siguiente enlace aprendemos a unir una cuenta de equipo con S.O. Linux Desktop (Debian) a un controlador de dominio con S.O. Windows Server.

Unir Linux Debian a un dominio de Active Directory.

Autoevaluación

Desde que lugar de la configuración del AD podemos eliminar una cuenta de equipo que no haya iniciado sesión en el dominio.

- Desde Inicio-Herramientas administrativas-Usuarios y equipos de Active Directory-Computer- Seleccionamos la cuenta de quipo y pulsamos el botón derecho del ratón- del menú pulsar en Eliminar
- Desde Inicio-Herramientas administrativas-Usuarios y equipos de Active Directory-Computer- En el campo Nombre escribimos el nombre del equipo y seguidamente pulsamos el botón Eliminar.
- Desde Inicio-Herramientas administrativas-Usuarios y equipos de Active Directory-Escribimos el nombre de equipo y pulsamos el botón Eliminar.
- Desde Inicio-Herramientas administrativas-Usuarios y equipos de Active Directory-Computes- Seleccionamos la cuenta de quipo y pulsamos el botón derecho del ratón- del menú hacemos clic en Borrar.

Administración de replicación a sitios entre controladores de Active Directory.

Caso práctico

Debido al **volumen de actividad empresarial "Gestisa"**, ubicada en Madrid, ve la posibilidad de ampliar su empresa creando una sucursal en Barcelona donde también tendrá que crear una subred y un dominio. Para poder controlar la comunicación entre ambos dominios tiene que identificar a cada red por un sitio del Active Directory. En un principio creará el sitio del dominio "Madrid".

Para controlar el tráfico de comunicación con el AD se pueden crear **sitios que pueden representar al conjunto de equipos de una red** LAN **o** WAN, p or lo tanto, un sitio será un objeto del Directorio Activo con el cual podemos administrar un conjunto de equipos ubicados físicamente en un mismo lugar.

Lógicamente una subred está identificada por un sitio, pero un sitio puede representar a muchas subredes. Además los sitios pueden agrupar parte de los equipos de un dominio.

Cada dominio estará representado por un objeto sitio que estará gestionado por un controlador de dominio permitiendo poder realizar la replicación entre diferentes sitios y dominios.

El proceso de replicación permite la transmisión de las modificaciones realizadas en los Directorios Activos, entre los controladores de dominio. Mediante la gestión de sitios, se controla la sincronización del tráfico de datos en el bosque de dominio, mejorando los tiempos de respuesta.

Al realizar la instalación del Active Directory se crea un sito por defecto, con el nombre **Default-First-Site-Name** y un enlace o vínculo a él con el nombre**DEFAULTIPSITELINK**.

Para gestionar un sitio debemos de realizar las siguientes operaciones:

a. Crear el sitio.
b. Crear las subredes y asociarlas al sitio.
c. Asociar un controlador de dominio al sitio.
d. Realizar enlaces a otros sitos.

Debes conocer

En el siguiente fichero tenemos la información para controlar el tráfico de replicación de la red cuando disponemos de una estructura de árbol con un dominio raíz y varios dominios hijos.

Administración de sitios en el Active Directory. (0.19 MB)

Autoevaluación

La replicación sirve para que el servicio de directorio Active Directory mantenga réplicas de los datos de directorio en múltiples controladores de dominio.

- Verdadero.
- Falso.

Relaciones de confianza entre controladores de dominio.

Caso práctico

En el momento que **Carlos**, cree el **dominio en la segunda subred**. Se creará una **relación de confianza**entre los controladores de dominio de la sucursal de **Madrid y de Barcelona**.

Las relaciones de confianza permiten a los usuarios el poder conectarse y utilizar los recursos de varios dominios. El Active Directory crea relaciones de confianza entre los dominios del un mismo árbol e incluso de un bosque. Para los dominios externos de diferentes bosques o de controladores no Windows (dominio Kerberos) la confiabilidad la tendrá que crear el propio usuario.

Existen cuatro maneras de establecer relaciones de confianza que son las siguientes:

Diferentes opciones de establecer relaciones de confianza ente dominios.

Tipo de relación de confianza	Descripción
Unidireccional	Establecida entre dos dominios solamente se establece la confianza en una dirección, los usuarios del primer dominio pueden acceder al segundo, pero los del segundo no pueden acceder al primero. Se establecen cuando son dominios externos.
Bidireccional	Establecida entre dos dominios en ambas direcciones, los usuarios del primer dominio pueden acceder a los recursos del segundo y los del segundo al primero.
Transitiva	Establecida entre tres dominios, los usuarios de todos ellos pueden acceder a los tres dominios. De forma predeterminada entre los dominios de un mismo bosque, se establece este tipo de confianza.
Compuesta	Pueden existir combinaciones de relaciones, por ejemplo transitivas y entre algunos de sus miembros unidireccionales.

Una relación de confianza, no da derecho a los usuarios a tener otorgados automáticamente permisos, será tarea de los administradores que le otorgarán los privilegios entre los dominios. Se pueden administrar dominios entre los que se ha establecido una relación de confianza siempre que se delegue el control del dominio.

Debes conocer

En el siguiente fichero tenemos descrito el modo de establecer una relación de confianza con dominios externos y la gestión de administración remota de otro controlador de dominio.

Administración de relaciones de confianza del Active Directory. (0.25 MB)

Autoevaluación

¿Desde dónde se configuran las relaciones de confianza dentro del Active Directory?

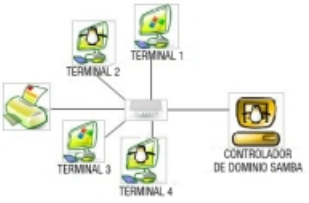
- Inicio-Panel de control-Sistema-Administrador de Confianzas.
- Inicio-Herramientas administrativas-Seleccionar el dominio y botón derecho de ratón- Seleccionar Relaciones de confianza.
- Inicio-Herramientas administrativas-Dominios y confianzas de Active Directory.
- Inicio-Herramientas administrativas-Confianzas de Active Directory.

Administración de un controlador de dominio en Linux.

Caso práctico

En Linux los servidores pueden actuar como **controladores de un dominio** en una red o como **servidores independientes**. En contenidos anteriores, hemos aprendido a operar con Linux como servidor independiente y a compartir recursos en redes mixtas bajo la estructura de grupo de trabajo en red mediante la implementación en el sistema del protocolo **SMB** con la instalación de **Samba**. La última versión de Samba puede operar con el**Active Directory** de Windows. Con Samba podemos hacer que un servidor de Linux pase a ser un controlador de dominio Windows para que los usuarios de equipos clientes en Windows se validen en un controlador de dominio Linux.
Carlos como usuario administrador de "Gestisa" ve la posibilidad de instalar el ordenador **servidor de Linux como controlador de dominio de la red**, como alternativa **gratuita** frente a Windows cuyo uso del software es mediante compra de licencias.

Si gestionamos un controlador de dominio en Linux, debemos de tener en cuenta las siguientes consideraciones:



- Los servicios de **Samba no generan una estructura de árbol y bosque** como en Windows, simplemente actúan como controladores de dominio permitiendo centralizar la gestión de los usuarios que acceden desde cualquier equipo cliente a los recursos o servicios compartidos que ofrece el propio servidor controlador de dominio.
- **Samba combina LDAP con funciones de autentificación** permitiendo sustituir a los controladores de dominio de Windows.
- Los servicios de Samba se administran mediante el demonio **smdb** que gestiona el acceso remoto y el recurso de compartir archivos e impresoras, el demonio **nmbd** que soluciona la resolución de nombres NetBIOS de Windows (buscando a través de servidores WINS) para que Linux se integre como un ordenador más en el sistema Windows y el demonio **winbind** que da servicio para resolver información de usuarios y grupos de servidores Windows NT.
- Dentro de un **controlador de dominio Linux** existirán **dos tipos de usuario** los del servidor independiente, (pueden acceder localmente y remotamente por **ssh**), y los usuarios de Samba o controlador de dominio, (pueden acceder desde un equipo cliente o terminal integrado en el controlador de dominio).
- Instalado Samba se instalará todo el servicio formado por la aplicación servidor Samba-server y la aplicación cliente Samba-client. **El fichero de configuración de samba es /etc/samba/smb.conf.**
- Para facilitar la configuración se puede utilizar la aplicación **SWAT**, que se ejecuta bajo un interfaz gráfico Web que nos facilitará la configuración del fichero **smb.conf.** Para su implantación dentro del sistema será necesarios instalar:

Aplicaciones que se necesitan para implantar un controlador de dominio en Linux.

DNS	apt-get install bind9 bind9-doc	Servidor de nombres de dominio.
Samba	apt-get install samba samba-doc smbfs winbind	Servidor de archivos e impresoras.
Apache	apt-get install etapache2 apache2-doc	Servidor web HTTP de código abierto.
Php	apt-get install php5 libapache2-mod-php5	Lenguaje de programación para entornos Web.
Mysql	apt-get install mysql-server mysql-client	Sistema de gestión de base de datos relacional.
SWAT	apt-get install swat, netkit-inetd	Aplicación de administración samba vía Web.
Cups	apt-get install gnome-cups-manager	Sistema de impresión modular para Linux.

Para ejecutar **SWAT** debemos modificar el supervisor de servicios de internet **inetd**, siguiendo los siguientes pasos:

1. Salimos a un terminal de línea de comandos desde el menú *Aplicaciones-Accesorios-Terminal* y editamos el fichero /etc/inetd.conf con la orden: sudo gedit /etc/inetd.conf.
2. Dejamos la línea sin comentario quitando el # de la línea swat stream tcp nowait.400 root /usr/sbin/tcps /usr/sbin/swat.
3. Arrancamos el inetd con la orden: sudo /etc/init.d/inetd start.

Autoevaluación

¿El demonio nmdb dentro del servicio Samba soluciona la resolución de nombres NetBIOS de Windows?

- Verdadero.

Falso.

Instalar en Linux un controlador de dominio con Samba.

Caso práctico

Para **compartir recursos en el grupo de trabajo** entre máquinas Linux y Windows de la red de "Gestisa",**Carlos tuvo que instalar el servicio Samba** y realizar su configuración. Ahora ha modificado el servicio, para que el servidor Linux actúe de controlador de dominio de los equipos y usuarios de la red. Para ello ha utilizado la aplicación Swat como herramienta que se ejecuta en el entorno gráfico y que facilita la administración de Samba.

Para configurar Linux como controlador de dominios será necesario modificar el fichero de configuración de SAMBA **smb.conf.** Para facilitar la tarea utilizamos **SWAT**:

1. Por seguridad realizamos una copia del fichero original de configuración Samba desde el menú*Aplicaciones-Accesorios-Terminal* y desde la línea de comandos escribimos la siguiente orden: carlos@carlos-laptop:~$ sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.copia
2. Como usuario **root** ejecutamos **Swat** entrando al navegador desde *Aplicaciones-Internet-Navegador web Firefox*, en el campo de Url o barra de direcciones escribimos http://localhost:901. Nos solicita el nombre de usuario y clave, será el usuario **root** con su clave.
3. Seguidamente pulsamos en el botón identificado como **GLOBALS**. Pulsamos en Advanced para configurar todos los parámetros necesarios. Debemos modificar los siguientes campos que puedes consultar accediendo al siguiente enlace sobre significado de los diferentes parámetros de configuración del fichero /etc/smb.conf. (0.04 MB)
4. Después de dar valor a los campos pulsamos en el botón *Commit Changes* para guardar los cambios. Para poder ver el fichero de configuración**smb.conf** podemos pulsar el botón **VIEW**. Para que el servidor tenga en cuenta los cambios es necesario reiniciar el servicio Samba pulsando al botón **STATUS** y en Restart All.

Debes conocer

En el siguiente enlace podemos aprender a instalar samba como controlador de dominio.

Instalación controlador de dominio con SAMBA.

Para saber más

Con este enlace podemos visualizar un vídeo que muestra como operar con la aplicación Swat para gestionar un controlador de dominio.

Controlador de dominio Samba.

Autoevaluación

Después de realizar cambios en el fichero smb.conf. ¿Qué orden ejecutamos desde la línea de comandos para que tenga efecto en el servicio Samba?

- sudo Commit Changes.
- sudo Restar All.

- sudo /etc/init.d/samba restart.
- Al guardar los cambios.

Administración de usuarios de un controlador de dominio Linux con Samba.

Caso práctico

En el **controlador de dominio del servidor Linux** de la red de "Gestisa", están dados de alta los usuarios del dominio para que se puedan **identificar desde cualquier terminal y acceder al sistema**.

En Linux primero debemos crear los usuarios locales que pueden acceder al servidor, seguidamente habilitamos a dichos usuarios para que sean también miembros usuarios del **servicio Samba**.

Habrá que tener en cuenta que los derechos y privilegios estarán separados, unos para el acceso a los recursos del servidor como servidor independiente y otros para los recursos Samba, y que las contraseñas se almacenan en ficheros diferentes: Los **usuarios locales** al servidor se almacenan en /etc/shadow y las **contraseñas** de Samba, dependerá de la configuración realizada en el fichero /etc/samba/smb.conf, que de forma predeterminada las guarda en /var/lib/samba/passdb.tdb.

Para la creación de usuarios Samba podemos utilizar la aplicación Swat siguiendo los siguientes pasos como usuario **root**:

1. Debemos dar de alta a los usuarios como usuarios locales, desde el menú *Sistema-Administración-Usuarios y grupos*, pulsamos en el botón *Añadir usuario*, y como ya hemos estudiado en unidades anteriores (recordamos que también se puede dar de alta a los usuarios mediante el comando **adduser**), rellenamos los campos de la ventana de edición.
2. Ejecutamos Swat entrando al navegador desde *Aplicaciones-Internet-Navegador web Firefox*, en el campo de Url o barra de direcciones escribimos:
   http://localhost:901

   Nos solicita el nombre de usuario y clave, será **root** con su clave. Pulsamos en el botón **PASSWORD**, aparece una pantalla donde introducimos el mismo nombre del usuario local creado anteriormente en el servidor y la contraseña, seguidamente hacer clic en el botón *Add New User*.
3. Siempre que realizamos un cambio en el fichero smb.conf podemos comprobar que todo está bien configurado mediante un comando que testea el valor de los parámetros cambiados. Para su ejecución ir a menú *Aplicaciones-Accesorios-Terminal* y desde la línea de comandos escribimos la siguiente orden:
   carlos@carlos-laptop:~$ sudo testparm

Para configurar los perfiles móviles de usuarios dentro del fichero *smb.conf* se encuentra la directiva ***logon path***, que contiene el valor que indica la ruta**donde deseamos guardar los perfiles de los usuarios** que se validan en el equipo, serán **perfiles móviles**, y podemos dejar el valor por defecto:

\\%N\%U\profile, donde %N es el nombre del equipo controlador de dominio, %U es el nombre de usuario con el que se creará el perfil y profile es la carpeta donde se guarda el perfil. Es decir en **/home/nombre_usuario/profile.***

Para saber más

En el siguiente enlace podemos ver un vídeo sobre gestión de usuarios Samba con Swat.

Configurar usuarios del controlador dominio Linux en Samba con Swat.

Autoevaluación

¿Cuál es el comando en Linux que permite probar la integridad del fichero de configuración smb.conf?

- profile.
- testparm.
- passdb.tdb
- shadow.

Administración de cuentas de equipos en un controlador de dominio Linux con Samba.

Caso práctico

En el **controlador de dominio del servidor Linux de "Gestisa"**, están dadas de alta las cuentas de equipo para que los **usuarios del dominio** puedan **identificarse** desde terminales que se han integrado al dominio.

Las cuentas de equipos en Linux, **sirven para crear cuentas de estaciones de trabajo Windows** y así permitir el acceso desde equipos clientes con el sistema operativo Windows. Se gestionan como cuentas de usuarios con una configuración especial. Para crear cuentas de equipos debemos seguir los siguientes pasos:

1. Debemos crear un grupo de usuarios en el servidor que obligatoriamente **tendrá el mismo nombre que el dominio**. Como usuario root desde el menú *Sistema-Administración-Usuarios y grupos–Gestionar grupos-Añadir grupo*, escribimos el nombre en el campo **Nombre grupo** y pulsamos en *Aceptar*.
   También se puede realizar la misma operación desde la línea de comandos, desde el menú *Aplicaciones-Accesorios-Terminal* escribiendo la orden:

   carlos@carlos-laptop:~$ sudo groupadd nombre_del_dominio

   Recordamos que en unidades anteriores ya hemos aprendido a administrar grupos de usuarios en un servidor Linux.

2. Seguidamente pasamos a **crear la cuenta de usuario especial que representará la cuenta de equipo**. Para ello debemos obtener o saber el nombre NetBIOS del quipo Windows que deseamos dar de alta y pasamos a su creación en modo terminal, ya que requiere tener el signo "$" al final del nombre, y habrá que incluir un parámetro en la orden (–force-badname) para permitir escribir mal un nombre. Desde el menú *Aplicaciones-Accesorios-Terminal* y escribimos la orden:
   carlos@carlos-laptop:~$ sudo adduser –force-badname nombre_del_equipo$

3. Posteriormente pasamos a **agregar el usuario creado al grupo** gestionado en el primer paso. Desde el menú *Sistema-Administración-Usuarios y grupos–Gestionar grupos*, seleccionamos el nombre del grupo y pulsamos en el botón de *Propiedades*, en la lista de *Miembros del grupo* seleccionamos la cuenta especial de usuario que representa al equipo y pulsamos en *Aceptar*. En modo comando sería:
   carlos@carlos-laptop:~$ sudo adduser nombre_del_equipo$ nombre_dominio

4. Ahora debemos **añadir la cuenta especial o cuenta de equipo como cuenta de usuarios samba**.
   Podemos realizarlo desde la aplicación Swat ya estudiada en contenidos anteriores o desde la línea de comando (sin el signo "$") con la orden:
   carlos@carlos-laptop:~$ sudo smbpasswd -a -m nombre_del_equipo

5. **Reiniciamos todos los servicios Samba** desde *Aplicaciones-Internet-Navegador web Firefox*, en el campo de Url o barra de direcciones escribimos http://localhost:901. Nos solicita el nombre de usuario y clave, será *root* con su clave. Pulsamos en el botón *STATUS*, seguidamente hacemos clic en el botón *Restar All*. En modo comando sería:
   carlos@carlos-laptop:~$ sudo /etc/init.d/samba restart

Para saber más

En el siguiente enlace aprenderás a realizar la configuración de equipos Windows para que se integren en un servidor Linux que actúa de Controlador de dominio.

Integración de equipos clientes Windows en un controlador de dominio Linux server.

Autoevaluación

En un equipo Windows configurado como inicio de sesión en un dominio Linux también podemos iniciar sesión en modo local con

un usuario dado de alta en el equipo.

- Verdadero.
- Falso.

Administración de cuotas de disco en Windows y Linux.

Caso práctico

Dentro de la empresa **Gestisa**, será necesario permitir el **acceso a los servicios del controlador de dominio a varios trabajadores de la empresa**. El administrador deberá controlar el espacio de almacenamiento reservado para cada uno de ellos, con el fin de no agotar el recurso de capacidad del disco o discos de almacenamiento en el propio servidor. Para ello gestiona las cuotas de disco de cada usuario en el servidor de Windows y en el de Linux, (espacio particular de cada empleado para el almacenamiento de información).

La administración de cuotas, consiste en limitar el espacio de almacenamiento en el disco del servidor a los usuarios con derechos y permisos de acceso al servicio de archivo, con el objetivo de evitar que el servidor nunca se quede sin espacio de disco libre y así no ocasionar anomalías en el funcionamiento del mismo.

Generalmente cada usuario dispone de una carpeta en el servidor, que le permitirá compartir y almacenar información. Mediante la gestión de cuotas el controlador de dominio enviará notificación, (por ejemplo, por correo electrónico) a los usuarios antes de sobrepasar el límite de espacio de disco asignado, además podrá generar informes y registrar los eventos producidos, para poder realizar un seguimiento y analizar el aprovechamiento del espacio de los volúmenes de disco.

La cuotas se pueden configurar para **no permitir sobrepasar el límite asignado o permitir pero con advertencias de uso**.

Debes conocer

En el siguiente fichero podemos ver la forma de Administrar cuotas de disco en los sistemas Windows Server 2008 y Linux Ubuntu.

Administración de cuotas de disco. (0.56 MB)

Para saber más

Enlace a un vídeo que nos ayudará a gestionar cuotas de disco en Linux Ubuntu.

Gestión de cuotas en Linux Ubuntu.

Autoevaluación

El establecimiento de cuotas en un servidor de Linux por el número de archivos que el usuario puede almacenar dentro del sistema se identifica por el nombre de:

- La cuota por almacenamiento.
- La cuota por bloques.

- La cuota por inodo.
- La cuota por disco.