

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 **BK Sistemas informáticos**, 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.



[Jonny Goldstein \(CC BY\)](#)

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 **BK Sistemas informáticos**”).
- ✓ 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”).

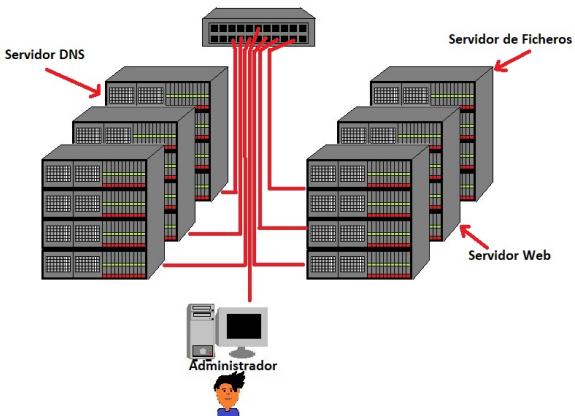
—**Vindio** y a **Laro**, como administradores que somos, tenemos que gestionar las instalaciones de los SO (sistemas operativos), dependen del modo de trabajo dentro de la infraestructura de la red, es decir, tiene instalados sistemas operativos de tipo cliente o servidor tanto en distribuciones Windows como en Linux.

—Pero **Juan**, tendremos que gestionar y trabajar 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. ¿No es así?

Efectivamente **Vindio**, pero además tendremos que trabajar 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.”).

En esta unidad aprenderás a administrar un ordenador servidor con función de controlador de dominio, en redes mixtas con Windows Server 2019 y Linux Ubuntu. Serás el usuario administrador del sistema y vas a realizar las tareas más importantes relacionadas con la configuración y gestión de los objetos pertenecientes a un Directorio Activo. Para ello, tendrás que tener configurado en máquinas virtuales con VirtualBox, los tres sistemas bajo el sistema real o principal del propio ordenador.

Es importante que realices el estudio de estos contenidos a la vez que vas practicando y comprobando su funcionamiento en el propio ordenador. Por ejemplo, a la hora de estudiar el contenido de "instalación y desinstalación del Active Directory" puedes ir creando y configurando dicha herramienta en tu propio ordenador.



Antonio López (Elaboración propia)



[Ministerio de Educación y Formación Profesional](#) (Dominio público)

Materiales formativos de FP Online propiedad del Ministerio de Educación y Formación Profesional.

[Aviso Legal](#)

1.- Estructura de trabajo en grupo.

Caso práctico



[Alain Bachellier \(CC BY-NC-SA\)](#)

Naroba le comenta a **Vindio** que en muchos entornos de red los ordenadores facilitan la gestión de los recursos compartidos, configurando sus equipos en modo **grupo de trabajo**.

—Tienes mucha razón, de hecho, en nuestra empresa disponemos 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.

— **Vindio**, aquí no utilizáis el Grupo Hogar de Windows.

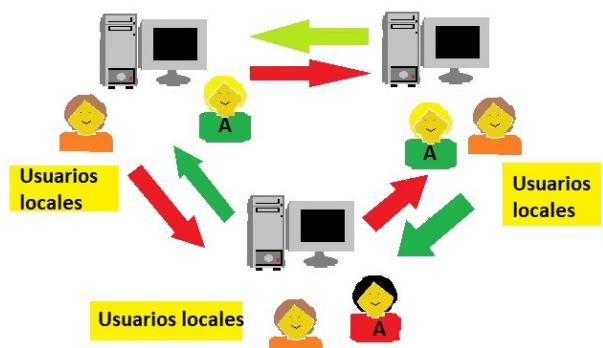
— **Noiba**, el grupo hogar es una característica de Windows que ya no se usa en Windows 10.

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.

Grupo de trabajo en red, el usuario A puede utilizar el recurso compartido de cualquier equipo, dispone de permisos y derechos.



Antonio López (Elaboración propia)

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 SO 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.

En Windows 10 ya no esta disponible el **Grupo Hogar**, que permitía 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.

Tampoco esta disponible en Windows 10 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). Desde Windows 8 esta opción ya no esta disponible.

Debes conocer

Dominios y Grupos de trabajo en Windows: ¿Cuál es más conveniente?

[Grupos de trabajo o dominios](#)

Autoevaluación

¿Un equipo Windows 10 puede pertenecer a un Grupo Hogar?

- Verdadero.
- Falso.

Lee con atención la pregunta.

Muy bien, has respondido correctamente.

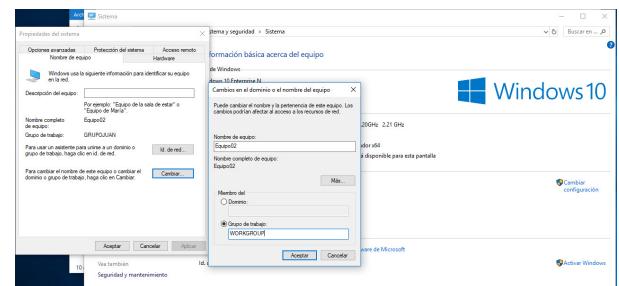
Solución

1. Incorrecto
2. Opción correcta

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

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: En la barra de búsqueda escribimos **Grupo de trabajo**, pinchamos en el resultado **Cambiar grupo de trabajo**. Se abre una ventana donde nos aparece información del nombre del equipo y del grupo de trabajo. Para cambiar el grupo de trabajo, pinchamos en el botón **Cambiar**, aparece la ventana donde tenemos los campos que identificarán al ordenador (nombre de equipo) 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.

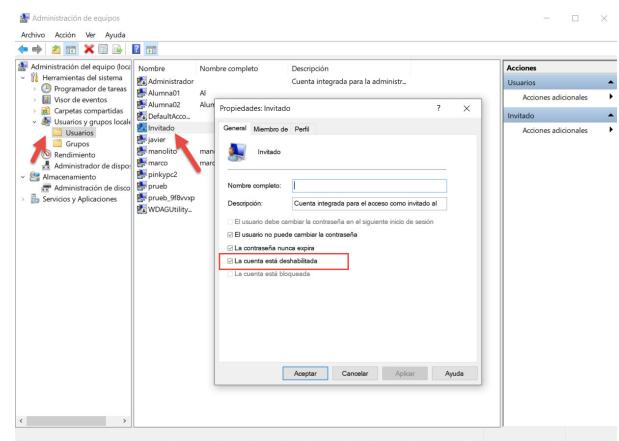


Windows (Elaboración propia)

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.**

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 escribiendo en el panel de búsqueda **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*. 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).



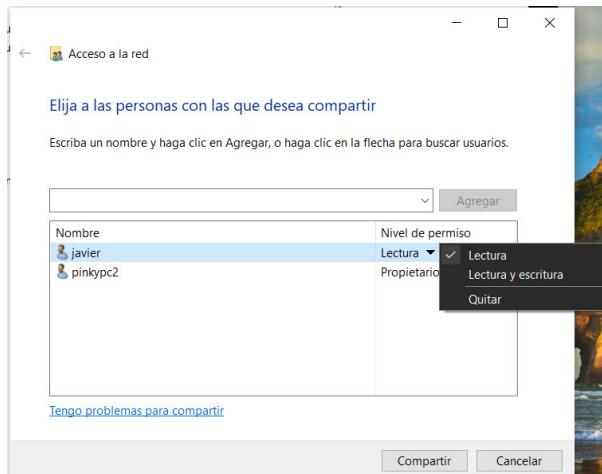
Windows (Elaboración propia)

En Windows para **comprobar los equipos y los grupos de trabajo pertenecientes a una misma red** se siguen los siguientes pasos: en el panel de búsqueda escribimos **Panel de control**, pinchamos en el resultado

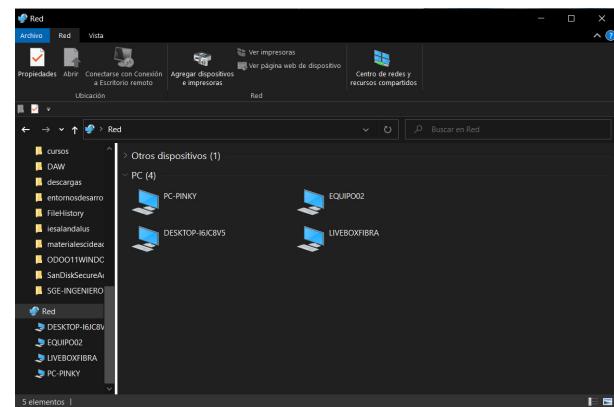
panel de control, hacemos clic en **Redes e internet->Ver los equipos y dispositivos de red**. Nos aparece la ventana de Red, donde se muestran todos los equipos que están en nuestro grupo de trabajo.

También podemos acceder abriendo el explorador de archivos con **Tecla Windows + E**, en el panel de la izquierda, pulsamos en el ícono de **Red**.

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 **Conceder acceso a** 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).



Windows (Elaboración propia)



Windows (Elaboración propia)

Debes conocer

Cambiar el grupo de trabajo en Windows

[Cambiar el grupo de trabajo en Windows](#)

Crear una red local en Windows

[Crear una red local en Windows](#)

Uso compartido de archivos por una red en Windows

[Compartir archivos en red en Windows](#)

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

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, webmin, nautilus-share, 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.

Asignar un grupo de trabajo en Linux

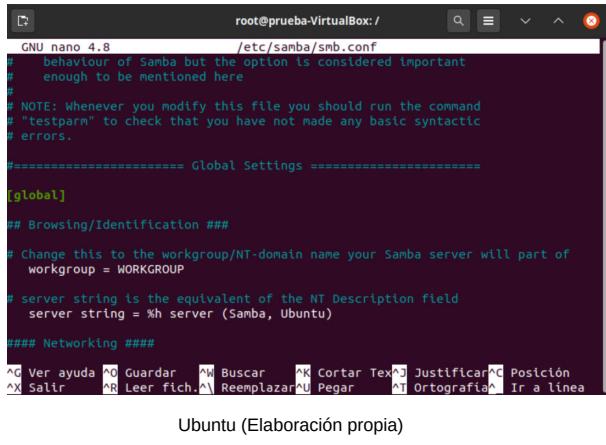
Para poder realizar esto tenemos que instalar el servicio Samba. Instalado samba tenemos que acceder al fichero de configuración de samba:

```
sudo nano /etc/samba/smb.conf
```

Antes de modificar este fichero es conveniente, hacer una copia de seguridad del mismo. Para ello, escribimos el siguiente comando:

```
sudo cp /etc/samba/smb.conf /etc/samba/smbcopia.conf
```

Una vez editado el fichero smb.conf, buscamos y modificamos la línea **workgroup = WORKGROUP**



```
GNU nano 4.8          /etc/samba/smb.conf
# behaviour of Samba but the option is considered important
# enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.

===== Global Settings =====

[global]

## Browsing/Identification ##

# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = WORKGROUP

# server string is the equivalent of the NT Description field
server string = %h server (Samba, Ubuntu)

#### Networking ####

^Q Ver ayuda ^Q Guardar ^W Buscar ^K Cortar Tex^Z Justificar^C Posición
^X Salir ^R Leer fich.^M Reemplazar^U Pegar ^T Ortografía^L Ir a linea
```

Ubuntu (Elaboración propia)

Podemos sustituir el grupo de trabajo WORKGROUP, que es el que aparece por defecto, por el nombre que queramos.

Guardamos los cambios y reiniciamos el servicio de samba, para ello ejecutamos:

```
sudo systemctl restart smbd.service
```

Compartir una carpeta en modo gráfico

Para compartir una carpeta en modo gráfico, en Ubuntu desde hace varias versiones ya no se puede utilizar la herramienta gráfica system-config-samba. Para ver el procedimiento para compartir una carpeta en modo gráfico pincha [aquí](#).

Compartir recursos desde línea de comando modificando el fichero de configuración de SAMBA smb.conf

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. Pincha [aquí](#).

Debes conocer

Compartir recursos entre Linux y Windows en modo gráfico

[Compartir carpetas de Ubuntu y Windows en modo gráfico](#)

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 recursos desde línea de comando usando el fichero de configuración de Samba](#)

Cómo compartir una carpeta desde Windows usando Samba

[Compartir carpetas desde Windows usando Samba](#)

Para saber más

Configuración avanzada de Samba

[Configuración de Samba](#)

Solución del error: "No se puede obtener acceso a esta carpeta compartida"

[No se puede obtener acceso a esta carpeta compartida](#)

¿Qué es OpenLDAP?

[OpenLDAP](#)

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.

No es correcta porque ésta es un tipo de red entre iguales.

Incorrecta, porque samba es un servicio para compartir recursos.

Muy bien, es la respuesta correcta.

Respuesta incorrecta, porque NFS es un servicio Linux.

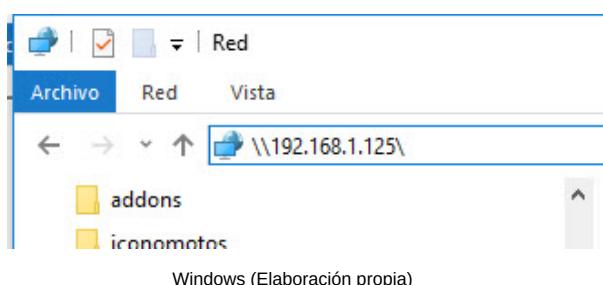
Solución

- 1. Incorrecto
- 2. Incorrecto
- 3. Opción correcta
- 4. Incorrecto

1.3.- Acceso a recursos compartidos grupo trabajo desde Windows y Linux.

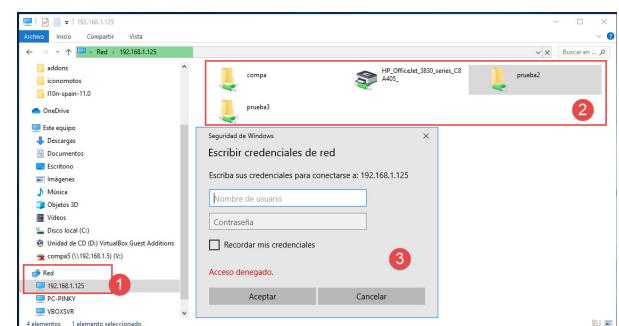
Para localizar un recurso compartido desde cualquier Windows seguimos los siguientes pasos:

Desde **Panel de control** seleccionamos la opción **Redes e Internet ->Centro de redes y recursos compartidos**, y pulsamos en la opción **Ver equipos y dispositivos**. Otro camino es abrir el **Explorador de archivos** desde la barra de tareas y pulsar en **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.



Administrador, desde el panel de búsqueda escribimos **Panel de control** pinchamos sobre **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



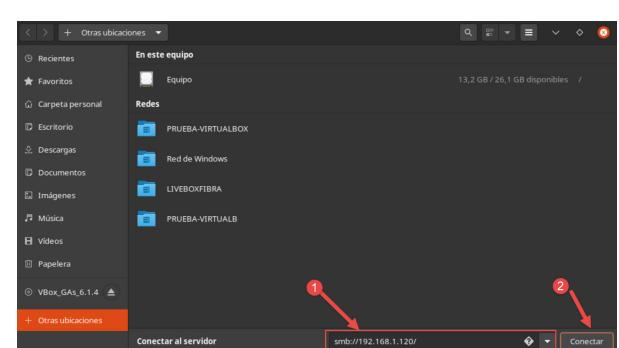
Windows (Elaboración propia)

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
\\ip_equipo\recurso_compartido.

ó

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



Ubuntu (Elaboración propia)

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 *Conectarse 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.

Para localizar un recurso compartido en Linux seguimos los siguientes pasos:

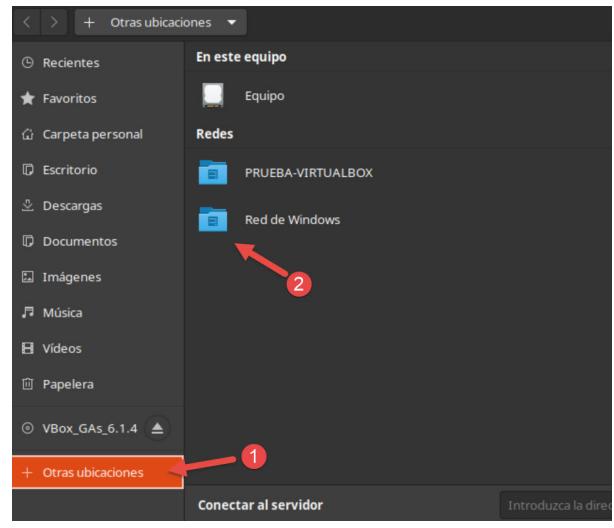
Vamos a suponer que tenemos un recurso compartido desde un **servidor Samba** en Linux o en un equipo Windows. **Para acceder al recurso compartido desde el entorno gráfico de un terminal Linux**, previamente en el ordenador Linux debemos haber instalado el paquete samba (por ejemplo desde la herramienta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

- ✓ Abrir *Nautilus* (explorador de archivos de Linux), pinchamos en *Otras ubicaciones* (esta en el panel izquierdo), nos aparece un rectángulo que está en la parte inferior y escribimos lo siguiente:

```
smb://192.168.1.120/
```

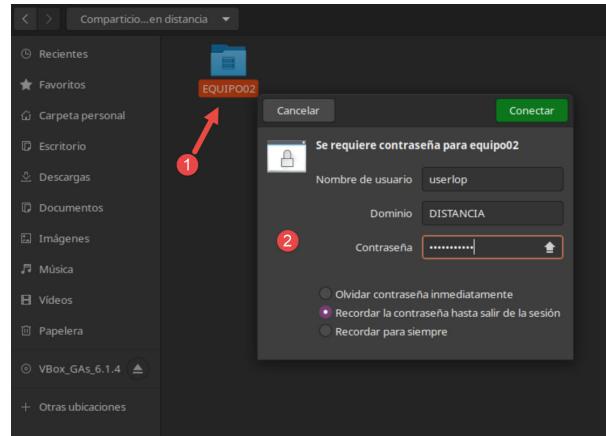
Donde 192.168.1.120 es la dirección IP del equipo al que nos vamos a conectar. Después pulsamos en el botón *Coneectar*.

- ✓ Existen distribuciones que al tener instalado samba, permitirán desde el propio explorador visualizar los recursos compartidos desde ordenadores Linux y Windows, para ello abrimos *Nautilus* (explorador de archivos de Linux), hacemos clic en *Otras ubicaciones->Red de Windows* aquí nos aparecen los grupos de trabajo que comparten los equipos Linux y Windows . Pinchamos encima del grupo de trabajo y dentro de él nos aparecen los equipos que pertenecen a ese grupo de trabajo. Pinchamos sobre el equipo y nos aparecerán los recursos compartidos.



Ubuntu (Elaboración propia)

Ubuntu (Elaboración propia)



Para saber más

Cómo ver las carpetas compartidas en Windows Server

[Ver carpetas compartidas en Windows Server](#)

[Listar recursos compartidos en un archivo txt](#)

Ver recursos compartidos en Ubuntu

[Ver recursos compartidos en Ubuntu](#)

Ver carpetas compartidas en Windows

[Cómo ver carpetas compartidas en Windows](#)

Autoevaluación

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

- Verdadero.
- Falso.

Muy bien, sigue así.

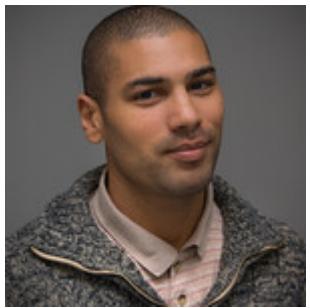
No es correcto: Deberías volver a leer la unidad.

Solución

1. Opción correcta
2. Incorrecto

2.- Estructura Cliente-Servidor: OpenSSH.

Caso práctico



[Alain Bachellier \(CC BY-NC-SA\)](#)

Juan informa a **Vindio** y a **Laro** de que el servidor de Linux de la red de **BK Sistemas Informáticos**, permite acceder a varios usuarios simultáneamente a su sistema desde cualquier terminal de la red.

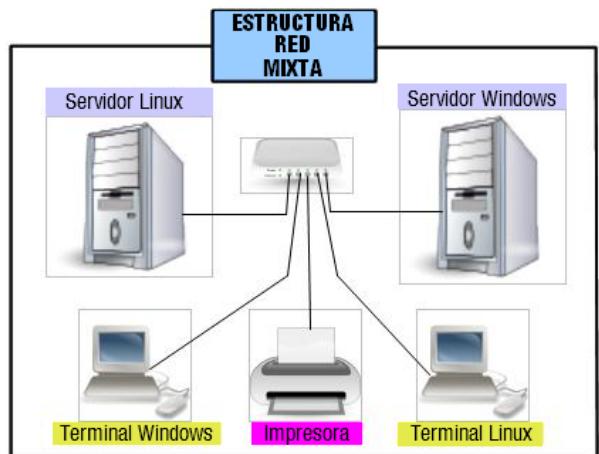
—Juan, ¿usas el protocolo SSH para administrar el acceso seguro de los usuarios?

—Efectivamente **Vindio**, utilizo el protocolo SSH para administrar el acceso seguro de los usuarios.

—¿Para qué utilizan los empleados de la empresa el servidor de Linux?

—Buena pregunta **Laro**, 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 sistema operativo monopuesto se validarán para conectarse en un ordenador principal con el fin de utilizar sus servicios y recursos. El servidor dispone de un sistema operativo **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.



isoalisl (Elaboración propia)

En Windows, el servidor o server dispone de un sistema operativo 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 sistema operativo 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

Configura un servidor SSH en Ubuntu para acceder a tu equipo de forma remota

[Configurar un servidor SSH en Ubuntu](#)

Para saber más

Servidor SSH en Linux: Manual de configuración para máxima seguridad

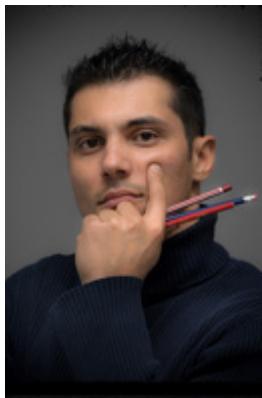
[Configuración para máxima seguridad en SSH](#)

Configuración remota con SSH en Ubuntu

[Configuración remota con SSH en Ubuntu](#)

3.- Protocolo LDAP.

Caso práctico



Alain Bachellier (CC BY-NC-SA)

—Juan, en los entornos donde existen ordenadores que controlan y organizan los objetos y recursos de la red, se utiliza un servicio denominado “de directorio”. ¿Sabes que protocolo usan estos ordenadores?

—Laro, estos ordenadores disponen de un protocolo especial denominado LDAP. El problema es que Windows es de pago (necesita licencia de uso). Sin embargo, en Linux existe la herramienta gratuita OpenLDAP que se puede instalar y administrar en el servidor Linux.

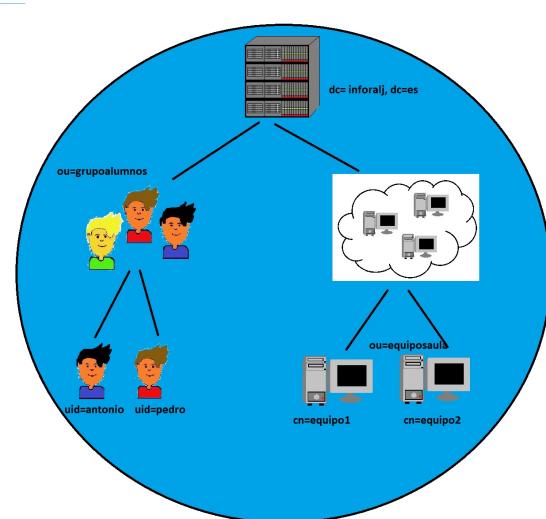
Así es. Lo estoy analizando y estudiando este modo de organización debido a su gran importancia en las estructuras en red, con el fin de sustituir el servidor de

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 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. Pincha [aquí](#).



Antonio López (Elaboración propia)

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 de la empresa *Inforalj S.A* sería: “dc=*inforalj*, 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 “antonio”:

```
dn: uid=antonio, ou=grupoalumnos, dc=inforalj, dc=com
objectClass: person
cn: antonio lopez
sn: lopez
description: alumno clase
mail: antonio@inforalj.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.

[Instalar y configurar OpenLDAP](#)

Diferencias entre LDAP y Active Directory

[LDAP y Active Directory](#)

Debes conocer

LDAP: Qué es y para qué se utiliza este protocolo

[LDAP](#)

¿Qué es OpenLDAP?

[OpenLDAP](#)

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.

Excelente. Veo que vas avanzando.

Incorrecta, repasa un poco más el tema.

Solución

1. Opción correcta
2. Incorrecto

4.- Los dominios.

Caso práctico



[Jonny Goldstein \(CC BY\)](#)

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

—¿Sabéis a qué me refiero?

—Juan, puedes referirte a los dominios. Me imagino que en nuestra empresa tendremos uno.

—Efectivamente Laro, la empresa dispone de un dominio que agrupa un conjunto de estaciones de trabajo y usuarios de la red. Existe un servidor Windows Server 2019 que actúa de controlador de dominio principal, encargado de gestionar el acceso a recursos compartidos como son las impresoras y las aplicaciones. Yo soy el responsable del Dominio, pero vosotros también debéis aprender a realizar tareas de administración sobre el dominio.

—Vamos a investigar todo lo que tiene que ver con la administración de dominios.

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 2019 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.



isoalusal (Elaboración propia)

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.](#)

Dominios, Unidades Organizativas, Arboles y Bosques

[Dominios, Unidades Organizativas, Arboles y Bosques](#)

¿Que es Active Directory?

[¿Que es Active Directory?](#)

Debes conocer

Conceptos básicos en una estructura de Directorio Activo

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.

No has acertado ya que ésta es una de las funciones al confiar entre dominios.

Excelente, esta es la respuesta correcta.

No has acertado ya que es conveniente por seguridad tener más de un controlador.

No has acertado ya que configurando samba, Linux puede ser un controlador de dominio.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

4.1.- 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.
- ✓ **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.



bocian (CC0)

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

- Verdadero.
- Falso.

Correcto.

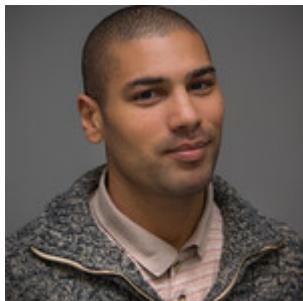
Respuesta incorrecta, repasa un poco más el tema.

Solución

1. Opción correcta
2. Incorrecto

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

Caso práctico



Alain Bachellier (CC BY-NC-SA)

—**Laro**, ¿sabes lo que es el Active Directory?

—Claro que sí, **Vindio**. 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.

Juan, ¿tenemos creado un controlador de dominio en nuestra empresa?

—Efectivamente **Laro**, tenemos **creado un controlador de dominio maestro** en el servidor de Windows Server 2019, 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**:

- ✓ 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. 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



isoalisal (Elaboración propia)

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.

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.
Temp.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.



0:00

Antonio José López Fernández. [Descripción textual alternativa del vídeo "Instalación de Active Directory en Windows Server 2019"](#) (Elaboración propia)

Debes conocer

Cómo crear un controlador de dominio y configurar DNS en Windows Server.

[Instalar un controlador de dominio y configurar el DNS](#)

Cómo degradar un controlador de Dominio en Windows Server

[Degradar un controlador de dominio en Windows Server](#)

Para saber más

Instalación de Active Directory y configuración del DNS en Windows Server

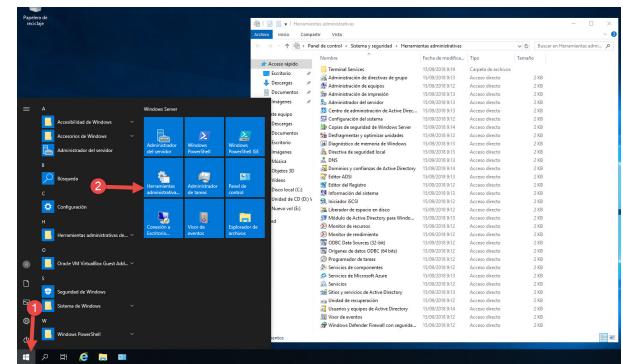
[Instalación de Active Directory y configuración del DNS en Windows Server](#)

5.1.- 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 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 tareas relacionadas con usuarios, grupos, equipos y unidades organizativas.
- ✓ **Sitios y servicios de Active Directory**, para administrar los objetos específicos del sitio que implementan la topología de replicación entre sitios. Estos objetos se almacenan en el contenedor de sitios de los Servicios de dominio de AD.
- ✓ **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 AD 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.



Windows (Elaboración propia)

Para poder administrar el AD, tenemos el *Administrador del Servidor*. El Administrador del servidor es una herramienta donde tenemos el control centralizado de todas las tareas que se ejecutan en el servidor tales como roles y características.

Con el Administrador del servidor podemos:

- ✓ Analizar y gestionar los roles y características instaladas en Windows Server.
- ✓ Ejecutar tareas de administración asociadas a los servicios implementados en el servidor tales como iniciar, parar, detener o eliminar servicios.
- ✓ Analizar el comportamiento de los roles y características de Windows Server.
- ✓ Verificar el estado operativo del servidor en tiempo real.

Para abrir el Administrador del servidor hacemos clic en *Inicio-Administración del servidor*. Para ver como usar en Administrador del servidor, pincha [aquí](#). Desde el podemos acceder a diferentes herramientas que nos permiten administrar el servidor y un dominio. Para acceder a ellas, abrimos el administrador del servidor y pulsamos en el menú *Herramientas* que se encuentra en la parte superior derecha. Algunas de estas herramientas son:

- ✓ **Herramientas de administración del dominio**: nos permiten administrar diferentes aspectos del dominio. Algunas de ellas son:

Dominios y confianzas de Active Directory: permite aumentar el nivel de funcionalidad de nuestro dominio, añadiendo nuevas características al Directorio Activo y crear relaciones de confianza entre dominios.

Usuarios y equipos de Active Directory: nos permite definir el modo en el que se usará nuestra infraestructura de red. Nos permite crear y administrar las cuentas de usuario que podrán usar los recursos de AD y las cuentas para los ordenadores desde los que dichos usuarios podrán conectarse. Además nos facilita su organización en grupos, unidades organizativas, etc.

Sitios y servicios de Active Directory: esta herramienta permite definir la topología de nuestro directorio activo, creando y administrando los sitios que forman la estructura geográfica de la red y creando vínculos entre ellos.

- ✓ **Herramientas de administrador del servidor:** nos permiten administrar diferentes aspectos del servidor. Algunas de ellas son:

Programador de tareas: con ella podemos programar tareas repetitivas para que se realicen automáticamente, sin que el usuario tenga que estar pendientes de ellas.

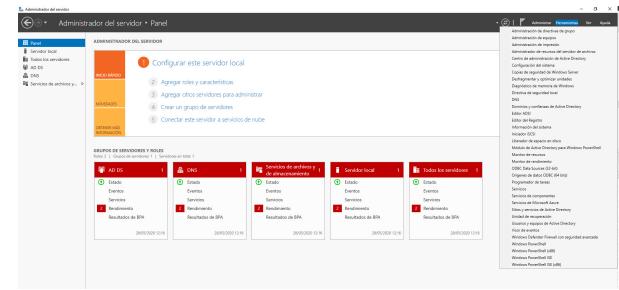
Windows PowerShell: es una herramienta con la que podemos realizar múltiples tareas administrativas.

Monitor de recursos: nos permite monitorizar el tráfico y recursos en nuestro servidor.

Copias de seguridad de Windows Server: nos permite crear una política de copias de seguridad en nuestro servidor.

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 <i>DSQUERY</i>, que permite buscar objetos dentro del AD, desde *Inicio-Símbolo del sistema* en la línea de entrada de comandos escribir lo siguiente:

```
DSQUERY /?
```



Windows (Elaboración propia)

```
C:\> Administrador: Símbolo del sistema
C:\Users\Administrador>dsquery /?
Descripción: el conjunto de comandos de esta herramienta le permite consultar el directorio de acuerdo con los criterios especificados. Cada uno de los siguientes comandos de dsquery busca objetos de un tipo específico, excepto dsquery *, que puede consultar cualquier tipo de objetos.

dsquery computer - busca equipos en el directorio.
dsquery contact - busca contactos en el directorio.
dsquery subnet - busca subredes en el directorio.
dsquery group - busca grupos en el directorio.
dsquery user - busca unidades organizativas en el directorio.
dsquery site - busca sitios en el directorio.
dsquery server - busca instancias de DC/LDS de Active Directory en el directorio.
dsquery user - busca usuarios en el directorio.
dsquery quota - busca especificaciones de cuota en el directorio.
dsquery partition - busca particiones en el directorio.
dsquery * - busca cualquier objeto en el directorio con una consulta genérica en LDAP.

Para obtener ayuda sobre un comando específico, escriba
"dsquery <tipoObjeto>/?", donde <tipoObjeto> es uno de los tipos de objeto comprobables mostrados más arriba. Por ejemplo, dsquery ou /?.

Notas:
Los comandos dsquery te ayudarán a buscar objetos en el directorio que cumplen un criterio específico de búsqueda: la entrada para dsquery es un criterio de búsqueda y la salida es una lista de objetos que coinciden con la búsqueda. Para obtener las propiedades de un objeto específico, use los comandos dsget (dsget /?).

Los resultados de un comando dsquery se pueden canalizar como entrada a otra de las herramientas de la línea de comandos del Servicio de directorio, como
```

Windows (Elaboración propia)

Podemos usar la herramienta PowerShell para realizar tareas de administración sobre nuestro AD. Para abrir PowerShell, hacemos clic en *Inicio-Windows PowerShell ISE*. Se abre una consola donde para trabajar con los objetos del AD, tenemos que escribir el siguiente comando, que nos permite importar el módulo servermanager:

```
Import-Module servermanager
```

Podemos por ejemplo comprobar los miembros del grupo grupolop, para ello ejecutamos el siguiente comando:

```
Get-ADGroupMember grupopolop
```

```
PS C:\Users\Administrador> Import-Module servermanager
PS C:\Users\Administrador> Get-ADGroupMember grupopolop

distinguishedName : CN=Antonio,OU=Distancia,DC=antonio,DC=edu
name : Antonio
objectClass : user
objectGUID : eb3b115f-9703-4bbd-a8df-e261c265cf1d
SamAccountName : user1top
SID : S-1-5-21-2570075631-2836053550-1436456986-1110

distinguishedName : CN=pedro,OU=Distancia,DC=antonio,DC=edu
name : pedro
objectClass : user
objectGUID : c94dbbb1-e567-4756-b538-4e5851ec4e20
SamAccountName : user1top2
SID : S-1-5-21-2570075631-2836053550-1436456986-1112

distinguishedName : CN=EMILIO,OU=Distancia,DC=antonio,DC=edu
name : EMILIO
objectClass : user
objectGUID : 7446ae58-1a47-4e72-bf74-854abc3075a2
SamAccountName : user1top3
SID : S-1-5-21-2570075631-2836053550-1436456986-1113

distinguishedName : CN=jose jm. jimenez,OU=Distancia,DC=antonio,DC=edu
name : jose jm. jimenez
objectClass : user
objectGUID : 76cd747b-5b13-4899-a2bd-bfd04ba6f509
SamAccountName : jose1top
SID : S-1-5-21-2570075631-2836053550-1436456986-1124

PS C:\Users\Administrador>
```

Windows (Elaboración propia)

Debes conocer

Administrar el dominio desde la linea de comandos

[Administrar usuarios en Windows Server](#)

[Administrar unidades organizativas](#)

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

Servicios de dominio de Active Directory

[Servicios de dominio de Active Directory](#)

Administrar un servidor Server Core

[Administrar un servidor Server Core](#)

Administrar Active Directory con PowerShell

[Administrar Active Directory con PowerShell](#)

Desplegar un dominio de Active Directory en PowerShell

[Instalar un dominio con PowerShell](#)

En el siguiente enlace podemos ver un documento con ejemplos para aprender a utilizar comandos de Active Directory en Windows Server

[Comandos en Active Directory](#)

[Crear cuentas de equipo con Dsadd](#)

[Crear grupos con Dsadd](#)

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.

Incorrecta, vuelve a leer la unidad ya que esta opción no es correcta.

No es correcta, lee con atención la pregunta en este lugar no existe esta opción.

Correcto, ese es el camino.

Respuesta incorrecta, repasa un poco más el tema.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

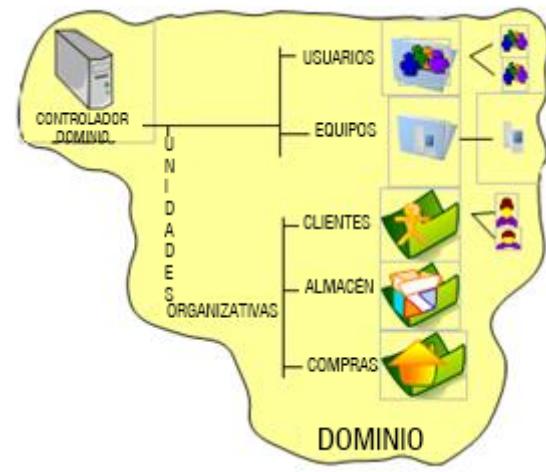
5.2.- Administración de unidades organizativas de Active Directory de Windows.

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 AD*, 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.



isoaisal (Elaboración propia)

Usuarios y equipos de Active Directory			
Nombre	Tipo	Descripción	
Builtin	builtinDomain	Default container for up...	
Computers	Container	Default container for do...	
Domain Controllers	Unitad organi...	Default container for sec...	
ForeignSecurityPrincipals	Container	Default container for sec...	
Managed Service Accounts	Container	Default container for ma...	
Users	Container	Default container for up...	

Windows (Elaboración propia)

- ✓ **NTDS Quotas:** Tiene los datos de cuota de AD.
- ✓ **Program Data:** Contiene información de las aplicaciones del Directorio.
- ✓ **System:** Visualiza la información de la configuración del sistema.
- ✓ **Users:** Lista los usuarios.

Debes conocer

Utilizar las unidades organizativas en Windows Server

[Vídeo tutorial de manejo de unidades organizativas y otros objetos en un dominio](#)

[Crear una unidad organizativa y asignarle contenido](#)

[Administrar unidades organizativas con PowerShell](#)

Autoevaluación

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

Sugerencia

- Verdadero.
- Falso.

Incorrecta, vuelve a leer la unidad.

Excelente, vas por buen camino.

Solución

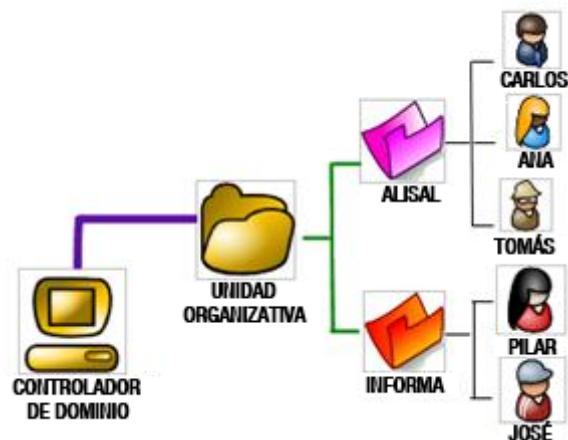
1. Incorrecto
2. Opción correcta

5.3.- 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 “antonio@informatica.alisal.local”. Según esto podemos referenciar el nombre de un usuario de dos formas: por su nombre (por ejemplo “antonio”) o por su definición DNS (como “antonio@informatica.sur.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 dominio del Directorio Activo.



isoalisal (Elaboración propia)

- ✓ 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.

Debes conocer

Administrar usuarios de un dominio en Windows Server

[Crear usuarios y grupos en un dominio](#)

[Crear una plantilla de usuario](#)

Para saber más

Administrar usuarios de un dominio en Windows Server

[Crear usuarios en Active Directory Windows Server](#)

[Crear usuarios con plantillas](#)

[Crear usuarios, grupos y unidades organizativas](#)

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.

Correcto, sigue así.

Incorrecta, lee con atención la pregunta ya que no existe este campo.

Respuesta errónea, repasa un poco más el tema éste campo está inventado.

No es correcta, repasa un poco más el tema éste no es un campo, es un comando.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto
4. Incorrecto

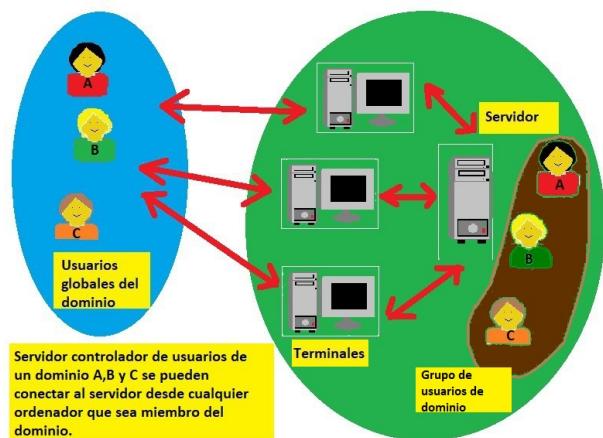
5.4.- Administración de grupos de usuarios en Active Directory de Windows.

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



Antonio López (Elaboración propia)

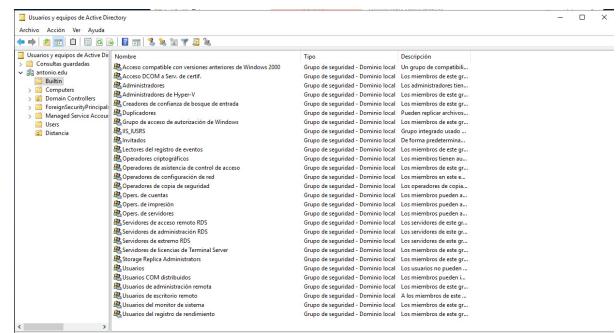
deben pertenecer al mismo dominio. No se replica fuera del dominio.

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.

Desde *Inicio-Herramientas administrativas- Usuarios y equipos de AD*, 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. 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 AD** dentro de la carpeta **Users** (como grupos globales y universales) y de la carpeta **Builtin** (como grupos de dominio local).



Windows (Elaboración propia)

Debes conocer

Cómo crear usuarios y grupos en un dominio en Windows Server

[Usuarios y grupos en un dominio en Windows Server](#)

Gestionar unidades organizativas, usuarios y grupos en Windows Server

[Gestionar unidades organizativas, usuarios y grupos](#)

Para saber más

Grupos e Windows Server

[Grupos en Windows Server](#)

Usuarios y grupos en Windows Server

[Usuarios y grupos en Windows Server](#)

Autoevaluación

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

- Verdadero.
- Falso.

Respuesta incorrecta, vuelve a leer la unidad.

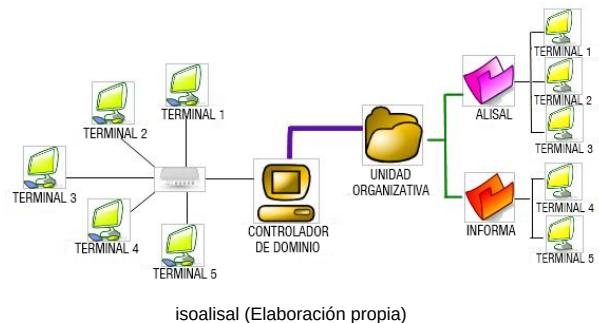
Muy bien, eso es correcto.

Solución

1. Incorrecto
2. Opción correcta

5.5.- Administración de cuentas de equipos de Active Directory de Windows.

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

Administrar cuentas de equipo del dominio en Windows Server

[Administrar cuentas de equipo del dominio en Windows Server](#)

Para saber más

Unir un equipo con Windows 10 a un dominio Windows Server

[Añadir Windows 10 a un dominio Windows Server](#)

[Unir un equipo a un dominio](#)

[Cómo unir Ubuntu a un dominio en Windows Server](#)

[Unir un cliente Ubuntu a un dominio en Windows Server](#)

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 equipo 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 equipo y pulsamos el botón derecho del ratón- del menú hacemos clic en Borrar.

Correcto.

Respuesta incorrecta, lee con atención la respuesta ya que no existe esta opción.

No es correcta, repasa un poco más el tema ya que por este camino no consigues eliminar la cuenta.

Incorrecta, repasa un poco más el tema ya que algunas opciones no existen.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

4. Incorrecto

5.6.- Administración de replicación a sitios entre controladores de Active Directory.

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, por 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 Directarios 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 AD se crea un sitio por defecto, con el nombre **Default-First-Site-Name** y un enlace o vínculo a él con el nombre **DEFAULTIPSITELINK**.

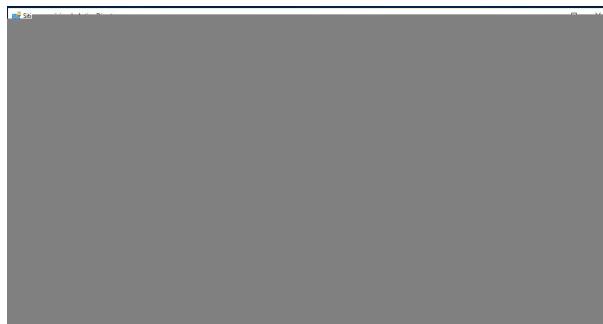
Para gestionar un sitio debemos de realizar las siguientes operaciones:

- 1.- Crear el sitio.
- 2.- Crear las subredes y asociarlas al sitio.
- 3.- Asociar un controlador de dominio al sitio.
- 4.- Realizar enlaces a otros sitios.

Creación de un sitio

- ✓ Desde Inicio-Herramientas administrativas-Sitios y servicios del AD, seleccionamos la carpeta Sites y en el menú contextual elegimos Nuevo-Sitio. En la ventana escribimos el nombre del sitio (no puede contener espacios en blanco ni caracteres especiales) y seleccionamos un objeto de vínculo para que se pueda conectar con otros sitios. Pulsar en Aceptar.

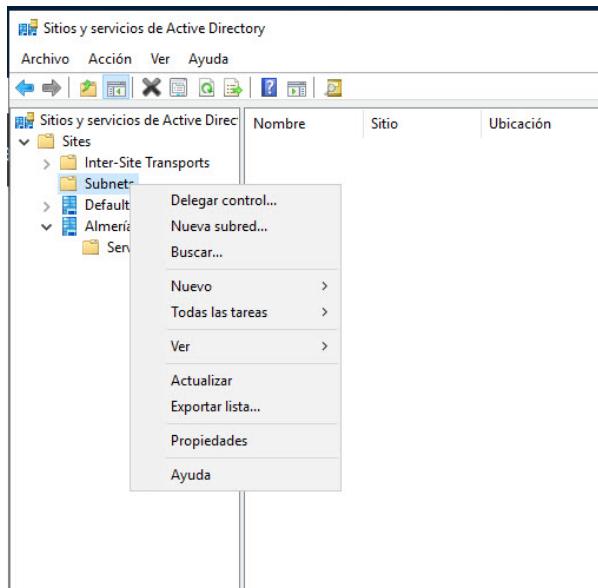




Windows (Elaboración propia)

- ✓ Se visualiza una ventana con una lista de opciones pendientes de realizar y seguidamente comprobamos que el sitio se ha añadido.

Asignación de subredes



Windows (Elaboración propia)

- ✓ Desde Inicio-Herramientas administrativas-Sitios y servicios del AD-Sites, seleccionamos la carpeta Subnets y elegimos Nueva-Subred del menú contextual.
- ✓ En la ventana de edición en el campo Prefijo debemos escribir la identificación de la dirección de la red y con su prefijo o número que identifique la máscara de red. En el campo Seleccionar un sitio de objeto para este prefijo debemos elegir un sitio que asocia con la subred. Pulsamos en Aceptar y vemos que aparece la subred.

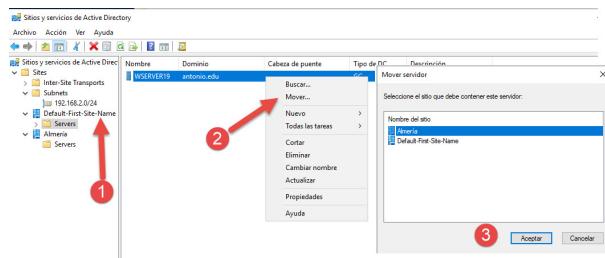
Asociar un controlador de dominio a un sitio

- ✓ Automáticamente cada vez que se añada un controlador de dominio a la dirección de red o subred del sitio se asociará dicho controlador con el sitio.

Windows (Elaboración propia)

Para los controladores creados con anterioridad al sitio es necesario asociarlos mediante los siguientes pasos:

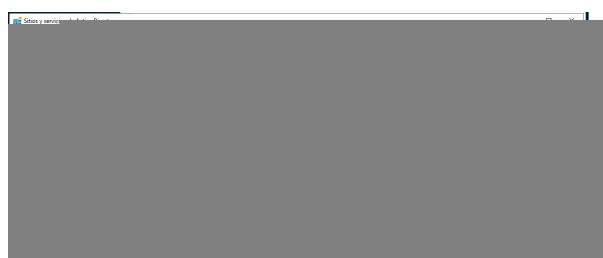
Buscar el controlador de dominio, posiblemente por defecto se encontrará dentro del sitio por defecto en *Default-First-Site-Name*, seleccionamos el nombre del controlador y elegimos del menú contextual, la opción Mover y seleccionamos el sitio donde deseamos asociar el controlador y Aceptar.



Windows (Elaboración propia)

Enlaces con otros sitios

- ✓ Desde *Inicio-Herramientas administrativas-Sitios y servicios del Active Directory-Sites*, seleccionamos la carpeta *Inter-Site Transport*, podemos crear un enlace a otro sitio por la dirección IP seleccionamos dicha carpeta y pulsamos el botón derecho del ratón para elegir *Nuevo vínculo a sitios*.
- ✓ En la ventana de edición se escribe un nombre para el vínculo y se selecciona el sitio que aún no esté relacionado con el vínculo, seguidamente pulsamos en el botón *Agregar* y finalizamos aceptando.



Debes conocer

Organización de Sitios y Servicios de Active Directory en Windows Server

[Organización de Sitios y Servicios de Active Directory](#)

Para saber más

Conceptos de replicación de Active Directory

[Replicación Active Directory](#)

[Administración de la replicación y la topología de AD con PowerShell](#)

[Sitios y servicios de Active Directory](#)

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.

Es correcto, muy bien.

Respuesta incorrecta, repasa los contenidos del tema.

Solución

1. Opción correcta

2. Incorrecto

5.7.- Relaciones de confianza entre controladores de dominio.

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.



isoaisal (Elaboración propia)

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

Diferentes opciones de establecer relaciones de confianza entre 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.

Para saber más

Relaciones de confianza

[Relaciones de confianza](#)

[Relaciones entre dominios](#)

Debes conocer

Crear una relación de confianza entre dominios de Windows Server

[Crear una relación de confianza](#)

[Relaciones de confianza con dominios de otros bosques](#)

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 confanzas de Active Directory.
- Inicio-Herramientas administrativas-Confanzas de Active Directory.

Incorrecta, vuelve a leer la unidad este lugar no existe.

No es correcta, lee con atención la pregunta ya que con estos pasos no llegas a ningún sitio.

Muy bien, eso es lo correcto.

Respuesta errónea, repasa un poco más el tema este lugar no existe.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

6.- Administración de un controlador de dominio en Linux.

Caso práctico



[Jonny Goldstein \(CC BY\)](#)

—Juan, ¿es posible que un Servidor Linux pase a ser un controlador de dominio en Windows?

—Laro, en Linux los servidores pueden actuar como controladores de un dominio en una red o como servidores independientes. Los servidores Linux pueden trabajar como un 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**. Pero también utilizando Samba pueden pasar a ser un controlador de dominio Windows para que los usuarios de equipos clientes en Windows se validen en un controlador de dominio Linux.

—Y, ¿tenemos en la empresa un servidor de Linux como controlador de dominio de la red?

—Precisamente estoy viendo 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 autenticación** 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

isoalislal (Elaboración propia)

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 de samba antes se podía utilizar la aplicación **SWAT**, que se ejecuta bajo un interfaz gráfico Web que nos facilitará la configuración del fichero **smb.conf**. Pero desde hace unos años esta obsoleto y su uso está desaconsejado. Por ello para compartir carpetas de usuario (modo gráfico) en Linux se utiliza la opción de compartir del cuadro de diálogo de la carpeta en el explorador de archivos y con comandos podemos configurar el fichero **smb.conf**. Pulsa [aquí](#) si quieres ver información la instalación y configuración de samba.
- ✓ Para crear y administrar un dominio con Samba + OpenLDAP + Kerberos podemos utilizar Zentyal que es una distribución basada en Ubuntu Server que está especializada en montar servidores para PYMEs como alternativa a Windows Server y que tienes su propia interfaz web de administración remota.



Zentyal (Elaboración propia)

Debes conocer

Instalar y configurar Samba en Ubuntu

[Instalar y configurar Samba](#)

[Instalar Samba y compartir con Windows](#)

Para saber más

Instalación y configuración de Samba

[Instalación y configuración de Samba](#)

Documentación oficial de Zentyal

[Documentación oficial de Zentyal](#)

Descargar Zentyal

[Descargar Zentyal](#)

Autoevaluación

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

- Verdadero.
- Falso.

Excelente.

Incorrecta, repasa los contenidos anteriores del tema.

Solución

1. Opción correcta
2. Incorrecto

6.1.- Instalar en Linux un controlador de dominio con Samba.

Para facilitar la configuración de samba antes se podía utilizar la aplicación **SWAT**, que se ejecuta bajo un interfaz gráfico Web que nos facilitará la configuración del fichero **smb.conf**. Pero desde hace unos años SWAT esta obsoleto y su uso esta desaconsejado.

Para crear y administrar un dominio con Samba + OpenLDAP + Kerberos podemos utilizar Zentyal que es una distribución basada en Ubuntu Server que está especializada en montar servidores para PYMEs como alternativa a Windows Server y que tiene su propia interfaz web de administración remota.

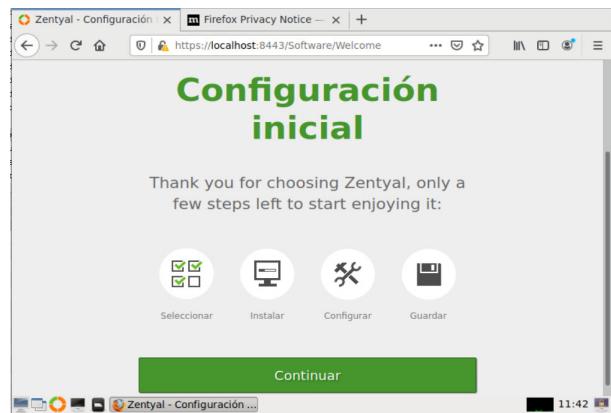
Para instalar Zentyal nos podemos descargar de su página oficial. Descargar [aquí](#). Para instalarla sus requisitos hardware serían los siguientes:

- ✓ 2 GB de RAM.
- ✓ 10 GB almacenamiento de disco duro.
- ✓ 2 tarjetas de red.
- ✓ Hardware estándar de arquitectura x86_64 (64-bit)

El proceso de instalación es sencillo, es parecido a la instalación de un sistema operativo Ubuntu. Pulsar [aquí](#) para ver como se instala Zentyal.

Al arrancar Zentyal por primera vez aparecerá un pantalla de presentación mostrando los pasos a realizar. Pulsamos en el botón *Continuar*. Comienza un asistente en la interfaz web, donde tenemos que seleccionar los paquetes a instalar, entre ellos se encuentra *Domain Controller and File Sharing*, lo seleccionamos y pulsamos al botón *Instalar*. El sistema nos informará que su instalación hay una serie de dependencias y se instalarán los siguientes paquetes: DNS Server, Firewall, Network Configuration, NTP Service, Domain Controller and File Sharing, Mail y Web Mail. Pulsamos en el botón continuar y empieza el proceso de instalación. Terminada la instalación se realizan una serie de configuraciones:

- ✓ Configuración de la red, se elige que interfaz es externo y cual interno.
- ✓ Asignación de tipo de IP, asignada por DHCP o estática, IP asociada, etc.
- ✓ Seleccionar el tipo de servidor y el nombre de dominio.
 - Stand Alone, elegimos esta opción.
 - Controlador de dominio adicional.



Zentyal (Elaboración propia)



Zentyal (Elaboración propia)

- ✓ Seleccionamos el dominio virtual de correo. Por defecto, se usa el nombre de dominio escogido en el paso anterior.

Se configuran todos los módulos instalados. Terminado este proceso, ya podemos acceder a Dashboard y a la configuración específica de cada uno de los componentes.

Ya tendríamos nuestro controlador de dominio instalado y podemos hacer todos las tareas de configuración y administración sobre el. Para ver otras tareas a realizar sobre el dominio en Zentyal pincha [aquí](#).

Zentyal (Elaboración propia)

Debes conocer

Instalar y configurar Zentyal

[Instalar y configuración inicial de Zentyal](#)

Instalar en Zentyal un controlador de dominio

[Instalar en Zentyal un controlador de dominio](#)

Para saber más

Documentación oficial de Zentyal

[Documentación oficial de Zentyal](#)

Descargar Zentyal

[Descargar Zentyal](#)

Autoevaluación

El fichero de configuración de Samba es:

- /etc/conf/smb.conf
- /etc/samba/samba.conf
- /etc/samba/smb.conf
- /etc/smb/smb.conf

No es correcto ya que esta es una opción de la aplicación Swat, no un comando.

Incorrecto, lee con atención la pregunta, éste es el nombre de un botón en la aplicación Swat.

Respuesta correcta. Veo que vas avanzando.

Respuesta errónea, ya que al guardar cambios con un editor no reinicias el servicio.

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta
4. Incorrecto

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

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 el terminal y escribimos lo siguiente:

```
$sudo smbpasswd -a userlop
```

Nueva contraseña de SMB:

Vuelva a escribir la nueva contraseña de SMB:

Usuario agregado usuariosamba

De esta manera hemos convertido el usuario local *userlop* en un usuario Samba.

Desde Zentyal podemos crear usuarios del dominio pulsando en el panel lateral en la opción *Usuarios y equipos -> Gestionar*. Aquí se muestran todos los usuarios y equipos de dominio. Como ejemplo vamos a crear el usuario *dominioadmin* que va a ser el usuario administrador de nuestro dominio. Para crear el usuario realizamos los siguientes pasos:

- ✓ En el panel de la izquierda pulsamos en la opción *Usuarios y equipos -> Gestionar*.
- ✓ Pulsamos en el botón en forma de cruz verde.
- ✓ Se nos abre un formulario donde podemos crear un usuario, un grupo o un contacto. En este caso, estamos creando un usuario. Rellenamos los datos: nombre de usuario, nombre, apellido, descripción (opcional), contraseña. Tenemos la opción de asignarle un grupo, pinchando en el desplegable grupo. Rellenados los datos pulsamos en el botón *Añadir*.

Zentyal (Elaboración propia)

Zentyal (Elaboración propia)

- ✓ Para que el usuario se administrador del dominio debe pertenecer al grupo *Domain Admins*. En el paso anterior hemos dicho que podíamos hacer miembro del grupo *Domain Admins* a nuestro usuario pinchando en la lista desplegable grupo y seleccionando el grupo *Domain Admins*.
- ✓ Otra forma de hacerlo, una vez creado el usuario, es pinchando en *Users*, se despliega a la derecha la lista de usuarios del dominio y hacemos clic en el usuario *dominioadmin* en el icono en forma de lápiz, esto nos permite editar las propiedades del usuario.

Zentyal (Elaboración propia)

- ✓ Se abre un formulario, donde podemos modificar las propiedades del usuario, una de ellas es la lista desplegable *Grupos del usuario*. Hacemos clic en ella y seleccionamos el grupo *Domain Admins*, de esta forma nuestro usuario será administrador del dominio.

Zentyal (Elaboración propia)

Perfiles móviles con Zentyal

Zentyal nos ofrece la posibilidad de habilitar la función “perfiles móviles” (roaming profiles) para nuestros clientes Windows.

Zentyal (Elaboración propia)

Cuando habilitamos los perfiles móviles copiamos los datos y configuraciones de cada usuario en el servidor, además de localmente. Cuando el usuario se autentica en cualquier máquina del dominio el perfil almacenado en el servidor se carga localmente y cuando cierra su sesión el perfil remoto se sincroniza con el local.

La necesidad de sincronizar el perfil local y el perfil remoto al iniciar y cerrar sesión supone un aumento significativo del tiempo preciso para realizar ambas operaciones. Este problema puede paliarse mediante la “redirección de carpetas” que permite al cliente montar localmente el recurso remoto.

El proceso para configurar la redirección de carpetas está detalladamente descrito en la documentación de **Samba** en su sección *Using a Group Policy Preference*. Pincha [aquí](#) para ver el procedimiento para hacerlo.

Perfiles móviles con Samba usando el fichero smb.conf

Para configurar los perfiles móviles de usuario 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 del equipo controlador de dominio, %U es el nombre del usuario con el que se creará el perfil y profile es la carpeta donde se guarde el perfil. Es decir en /home/nombre_usuario/profile.

Ubuntu (Elaboración propia)

Debes conocer

Crear usuarios del dominio en Zentyal

[Crear usuarios del dominio en Zentyal](#)

Autoevaluación

¿Cuál es el comando en Linux que permite convertir un usuario del sistema en un usuario Samba?

- useradd.
- smbpasswd.
- passwd
- adduser.

No es correcta, lee con atención la pregunta ya que esto no es un comando.

Excelente, vas por buen camino.

Incorrecta, repasa un poco más el tema ya que éste es un fichero de claves de usuarios samba.

Respuesta errónea, vuelve a leer la unidad ya que shadow puede que sea un fichero de contraseña de usuarios.

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto
4. Incorrecto

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

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:

- ✓ Debemos crear un grupo de usuarios en el servidor que obligatoriamente **tendrá el mismo nombre que el dominio**. Como usuario root, pinchamos en *mostrar aplicaciones* y en el cuadro de búsqueda escribimos *Usuarios y grupos*, pinchamos en el resultado que aparece. Hacemos clic en *Gestionar grupos-Añadir grupo*, escribimos el nombre en el campo **Nombre grupo** y pulsamos en *Aceptar*.

Ubuntu (Elaboración propia)

También se puede realizar la misma operación desde la línea de comandos, abrimos el terminal con *CTRL+ALT+T* y escribimos la orden:

```
prueba@prueba-ord:~$ sudo groupadd nombre_delDominio
```

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

- ✓ 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 equipo 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 *Terminal* escribimos la orden:

```
prueba@prueba-ord:~$ sudo adduser --force-badname nombreDelEquipo$
```

- ✓ Posteriormente pasamos a **agregar el usuario creado al grupo** gestionado en el primer paso. Pinchamos en *mostrar aplicaciones* y en el cuadro de búsqueda escribimos *Usuarios y grupos*, pinchamos en el resultado que aparece. Hacemos clic en *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:

```
prueba@prueba-ord:~$ sudo adduser nombreDelEquipo$ nombreDominio
```

- ✓ Ahora debemos **añadir la cuenta especial o cuenta de equipo como cuenta de usuarios samba**. Lo realizamos desde la línea de comando (sin el signo "\$") con la orden:

```
prueba@prueba-ord:~$ sudo smbpasswd -a -m nombre_del_equipo
```

Ubuntu (Elaboración propia)

- ✓ **Reiniciamos todos los servicios Samba** para ello escribimos el comando:

```
prueba@prueba-ord:~$ sudo systemctl restart smbd
```

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 en una distribución Zentyal.

[Integración de equipos clientes Windows en un controlador de dominio en Zentyal](#)

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.

Excelente, vas por buen camino.

No es correcta, lee con atención la pregunta.

Solución

1. Opción correcta
2. Incorrecto

7.- Administración de cuotas de disco en Windows y Linux.

Caso práctico

—Juan, dentro de la empresa **BK Sistemas informáticos**, hay algunos trabajadores que tiene que tener permiso para acceder a los servicios del controlador de dominio de la empresa.

—Félix, entonces tendré que 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, hay que gestionar 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).

[Let Ideas Compete \(CC BY-NC-ND\)](#)

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.

isoalisal (Elaboración propia)

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.

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

Debes conocer

Administrar cuotas con File Server Manager en Windows Server

[Administrar cuotas con File Server Manager en Windows Server](#)

[Administración de cuotas de disco \(2^a forma\)](#)

Administrar cuotas de disco en Linux

[Cuotas de disco en Linux](#)

Para saber más

Administración de cuotas en Windows Server

[Administración de cuotas](#)

[Habilitar cuota de disco para equipos del dominio por GPO](#)

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.

Incorrecta, vuelve a leer la unidad no existe esta definición.

No es correcta, lee con atención la pregunta y repasa los contenidos anteriores.

Excelente, es la respuesta correcta.

Respuesta errónea, deberías volver a leer los contenidos anteriores.

Solución

1. Incorrecto

- 2. Incorrecto
 - 3. Opción correcta
 - 4. Incorrecto
-

Condiciones y términos de uso de los materiales

Materiales desarrollados inicialmente por el Ministerio de Educación, Cultura y Deporte y actualizados por el profesorado de la Junta de Andalucía bajo licencia Creative Commons BY-NC-SA.

Antes de cualquier uso leer detenidamente el siguiente [Aviso legal](#)

Historial de actualizaciones

Versión: 01.00.00

Fecha de actualización: 23/07/20

Versión inicial de los materiales.

