Tema 5

INTEGRACIÓN DE WINDOWS SERVER Y GNU/LINUX.

CASO PRÁCTICO

El año pasado, la empresa CARMINFO S.L. fue contratada por el ayuntamiento de Villapedrusco para organizar sus recursos informáticos de forma eficiente.

En aquél momento, la propietaria de la empresa, Carmen, indicó al alcalde y a los concejales que una de las mejores formas de mantener organizados lo recursos y controlar el acceso a los mismos era instalar y configurar Active Directory.

Y así lo hicieron. Para ello, se compraron equipos para realizar la función de controladores de dominio. Y no sólo hubo que conseguir el hardware, las licencias de Windows Server 2008 R2 también fueron legalmente adquiridas. Por otro lado, todos los equipos miembros del dominio fueron debidamente actualizados y el sistema operativo que ahora utilizan es Windows 7, con el consiguiente coste en el pago de licencias para el ayuntamiento.

Por desgracia, los últimos presupuestos municipales obligan a reducir más gastos de lo que sería deseable y el alcalde está intentando reducir gastos administrativos, por lo que se le ocurre ponerse en contacto con CARMINFO S. L. y consultarle una idea:
-Hola, Carmen. Soy Francisco Pacheco, el alcalde de Villapedrusco. ¿Me recuerda?
-Claro, Francisco. ¿Qué desea? -contesta Carmen.
-Necesito hacerte una consulta.

Francisco le explica a Carmen la precaria situación económica del ayuntamiento.
-...y por eso me preguntaba si sería posible utilizar sistemas operativos libres -termina diciendo el alcalde.
-Sería posible, sí. Pero su red ya está completamente configurada con la tecnología Active Directory. Para utilizar una alternativa completamente libre y, por lo tanto, prescindir de los controladores de dominio, que utilizan Windows Server, tendríamos que crear la estructura de usuarios, grupos, etc., desde cero. Serían muchas horas de trabajo que, lógicamente, habría que facturar.
-No sé si la he entendido muy bien, pero de momento, no quiero poner el sistema patas arriba. Se me ocurre algo, Carmen. ¿Sería posible, como primer paso, que los ordenadores de trabajo, los que se usan principalmente para labores ofimáticas, utilizasen Linux?
-Sí, por supuesto. Podrían utilizar la suite de OpenOffice o de LibreOffice, que seguramente cubriría sus necesidades. Y sí, podemos hacer que esos equipos sean miembros del dominio ya existente, con lo que funcionarían con los mismos usuarios de siempre -responde Carmen.
-Estupendo -se alegró el alcalde.

1.- Descripción de escenarios heterogéneos.

Tras recibir el encargo por parte del alcalde, Carmen conversa con Laura, su empleada de mayor confianza, para enfocar el objetivo que persiguen.

-Quisiera enumerar punto por punto qué es lo que el alcalde nos está pidiendo -dice Laura-. Para que no se nos escape nada.
-Recordemos -responde Carmen-. Hace un tiempo fuimos al ayuntamiento y les montamos un dominio, *villapedrusco.com*, con Active Directory. También creamos cuentas de usuario para los concejales, el alcalde y el personal del ayuntamiento. Por supuesto, con los grupos necesarios.

-Muy bien. ¿Cuántos controladores de dominio? -pregunta Laura.
-Uno, con Microsoft Windows Server 2008 R2 -responde Carmen.- También había un servidor de ficheros, igualmente con Windows Server.
-Y los equipos miembros del dominio, ¿qué sistemas operativos utilizan? -sigue preguntando Laura.
-Windows XP y Windows 7 -contesta Carmen.
Laura reflexiona y continúa con el resumen:
-Vale. Y la idea sería sustituir Windows por GNU/Linux en todos los equipos clientes que sea posible. Define eso de "ser posible", Carmen.
-Tenemos que analizar qué aplicaciones se utilizan en cada equipo -dice Carmen- y, en el caso en el que dichas aplicaciones se puedan utilizar en GNU/Linux o tengan sustitutos aceptables sobre dicho sistema, el equipo será candidato para pasar a GNU/Linux.
-¿Y tienes alguna idea de si eso va a ser posible en muchos equipos? -pregunta Laura.
-Por lo poco que he visto, creo que la mayoría, porque lo que más utilizan son aplicaciones de oficina, de correo electrónico e Internet -responde Carmen.
Laura asiente y hace una última pregunta:
-Comprendido. ¿Y no habéis hablado de sustituir también el sistema operativo del controlador de dominio?
Carmen contesta:
-Sí, pero aún no daremos ese paso, porque primero quieren adaptarse a los nuevos cambios.

Como ya sabes, los objetivos de un servicio de directorio son almacenar y organizar la información sobre los usuarios y usuarias de una red de ordenadores, organizar los recursos de red y permitir a los administradores y administradoras gestionar el acceso de los usuarios a los recursos sobre dicha red. Los recursos de la red son impresoras, carpetas y archivos (que ya has gestionado en la unidad anterior) y también los propios equipos que forman parte de la red.

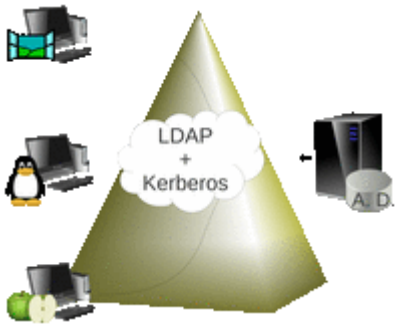
1.1.- Convivencia de distintas plataformas en el mismo servicio de directorio.

Hasta ahora, has aprendido a utilizar Active Directory, que es la implementación de Microsoft de un servicio de directorio. La tendencia inicial es utilizar, por lo tanto, sistemas operativos de Microsoft para trabajar en entornos de Active Directory. Sin embargo, hoy en día cada vez es más común trabajar en **entornos heterogéneos**, entendiendo como tales aquellos que **mezclan diferentes** tecnologías, empezando por los sistemas operativos instalados en los equipos. En otras palabras, hoy es común que en una misma red te encuentres equipos con sistemas operativos diversos, como Microsoft Windows Server, Windows XP/Vista/7, distribuciones diversas de GNU/Linux y Mac OS en sus diferentes versiones.

También has aprendido a configurar Active Directory de modo que, entre otras ventajas que ofrece, la acreditación de usuarios se realice en el controlador de dominio. Además, la gestión de recursos compartidos implica configurar permisos de acceso basados en esas cuentas de usuario que residen en Active Directory. El problema que se plantea al introducir sistemas operativos "no Microsoft" en entornos de Active Directory es el siguiente: ¿pueden esos sistemas operativos realizar una **autenticación** de cuentas de usuario que residan en Active Directory?

La respuesta es sí. Por ejemplo, puedes configurar un equipo en el que hayas instalado una distribución de GNU/Linux para que trabaje con la base de datos de Active Directory. Esto permite que los usuarios y usuarias de la red puedan utilizar la misma cuenta tanto en GNU/Linux como en Windows, facilitando la integración de estos sistemas.

¿En qué casos concretos puede esto resultar interesante? Se puede pensar en infinidad de ellos. Por ejemplo, en un entorno de trabajo en el que se utilicen aplicaciones que corren sobre Windows, como puede ser el Microsoft Office, y servidores con GNU/Linux que ejecutan servicios Web como Apache, servidores de comunicaciones como Asterisk, etc. Otra situación es la del caso práctico: utilizar puestos de oficina sobre GNU/Linux, pero acreditando las cuentas de usuario en Active Directory. La **acreditación** de usuarios contra Active Directory desde sistemas operativos no Microsoft, es posible gracias a que para esta autenticación se utilizan protocolos conocidos, en concreto **LDAP** y **Kerberos.**



LDAP son las siglas de ***L**ightweight **D**irectory **A**ccess **P**rotocol* (en español *Protocolo Ligero de Acceso a Directorios*) que hacen referencia a un protocolo de nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos a la que pueden realizarse consultas. De hecho, Active Directory es un esquema LDAP versión 3, lo cual permite integrar otros sistemas que soporten el protocolo. En este LDAP se almacena información de usuarios, recursos de la red, políticas de seguridad, configuración, asignación de permisos, etc.

En cuanto a **Kerberos**, es un protocolo de autenticación de redes de ordenadores que permite a dos computadores en una red insegura demostrar su identidad mutuamente de manera segura. Todos los sistemas Windows Server, así como Windows XP/Vista/7, usan una variante de Kerberos como su método de autenticación por defecto.

Por lo tanto, para autenticarse con usuarios de Active Directory, el sistema operativo de la máquina cliente tiene que saber "hablar" en estos dos protocolos. Afortunadamente, hoy en día los sistemas operativos más comunes así lo hacen. Ten en cuenta, no obstante, que cuando desees integrar un sistema operativo como GNU/Linux en un entorno de Active Directory, las versiones de protocolo soportadas por el cliente y el nivel funcional del dominio deben ser compatibles.

PARA SABER MÁS

En este enlace puedes encontrar más información sobre el protocolo LDAP.

Texto enlace: Protocolo LDAP.

URL: http://es.wikipedia.org/wiki/LDAP

2.- Integrar GNU/Linux en Active Directory.

CASO PRÁCTICO

Carmen y Laura debaten sobre el método adecuado de abordar la tarea que se les ha encomendado.

-Nunca hemos hecho esto antes, Carmen -dice Laura-. Opino que antes de empezar a hacer cambios en los equipos de Villapedrusco, deberíamos hacer unas pruebas en nuestros equipos.
-Sí, ya lo había pensado. Haremos lo siguiente: montaremos un dominio de Active Directory aquí en la oficina y realizaremos el proceso de integración de GNU/Linux en él. Es muy importante documentarlo bien.
-Habrá que asegurarse de que cubrimos las necesidades del ayuntamiento -apunta Laura.
-Por supuesto -contesta Carmen-. Y después de haberlo comprobado todo, iremos a Villapedrusco y utilizaremos las mismas versiones de software.
-Me parece bien -confirmó Laura.
-Haz tú las pruebas. Cuando lo tengas todo listo enseña a Alberto y Marisa cómo lo has hecho, porque después serán ellos los que vayan al Ayuntamiento a realizar el trabajo.

Cuando Laura comienza a trabajar, se encuentra con una pequeña incomodidad: como está integrando GNU/Linux en Active Directory tiene que hacer configuraciones en ambos sistemas, lo que le obliga a "moverse" entre dos equipos diferentes. Cuando expresa sus quejas en voz alta, Alberto le dice:
-¿Por qué no accedes desde GNU/Linux al escritorio de Windows Server?

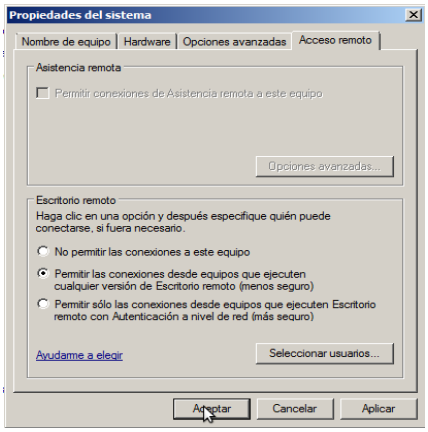
En este capítulo vas a aprender dos formas de conseguir que un equipo con GNU/Linux realice la autenticación de usuarios en Active Directory. Para ello, en los ejemplos, se parte de un dominio en Active Directory ya instalado, llamado villapedrusco.com, con nivel funcional Windows Server 2003. Como máquina cliente se utiliza Ubuntu Desktop 11.04 para 32 bits. También aprenderás cómo acceder a un equipo Windows desde un programa instalado en máquinas GNU/Linux. Esto es muy útil para gestionar servidores Windows remotamente (como controladores de dominio).

Acceso remoto a máquinas Windows mediante el cliente de Terminal Server.

Muchas veces necesitarás realizar tareas de administración en un servidor que no se encuentra físicamente cerca de ti pero sí está accesible a través de la red. Por ejemplo, puedes estar uniendo un equipo con GNU/Linux al dominio y necesitar crear un usuario en Active Directory para comprobar que puedes iniciar sesión.

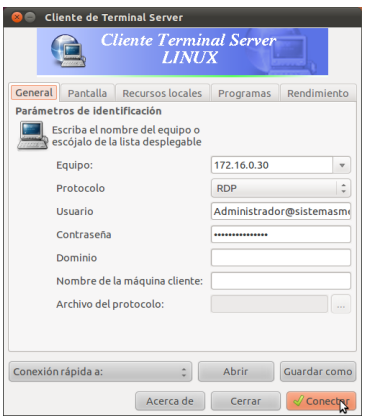
En lugar de desplazarte hasta el lugar en el que se encuentre el servidor para iniciar sesión, puedes realizar un acceso mediante Terminal Services (Servicios de Terminal). Se trata de un componente de Microsoft Windows que permite a los usuarios y usuarias acceder a datos y aplicaciones presentes en un equipo remoto a través de la red, utilizando el Protocolo de Escritorio Remoto (RDP – Remote Desktop Protocol). Ten en cuenta que a partir de la publicación de Windows Server 2008 R2, estos servicios pasaron a llamarse Remote Desktop Services (Servicios de Escritorio Remoto).

Veamos un ejemplo práctico. Tienes un controlador de dominio, cuya dirección IP es la 172.16.0.3. Deseas poder iniciar sesión en ese equipo COMO SI ESTUVIERAS DELANTE DE SU TECLADO Y SU MONITOR, pero a través de la red, utilizando otro equipo.



En primer lugar, debes configurar el equipo para que acepte las conexiones de escritorio remoto. Para ello, ve a Inicio → Sistema y seguridad → Sistema y en el panel de la izquierda accede a "Configuración de Acceso remoto". Se abre una ventana en la que deberás elegir la segunda o la tercera opción, dependiendo del nivel de seguridad que exijas en tu red. Para usos normales, puedes elegir la segunda opción.

a) Si el equipo en el que estás ejecuta Windows, puedes usar el comando: mstsc. Tendrás que especificar la IP a la que deseas conectarte. Te solicitará nombre de usuario y contraseña del equipo remoto.



b) Si el equipo en el que estás ejecuta GNU/Linux, tienes que instalar el Cliente de Terminal Server, llamado rdesktop. Hacer esto es una operación realmente sencilla. Simplemente, en un terminal, ejecuta el comando:
sudo apt-get install rdesktop

Después, puedes comprobar que en el menú Aplicaciones → Internet ha aparecido un icono nuevo llamado "Cliente de Terminal Server". Ábrelo y sólo tendrás que introducir la IP del equipo al que te vas a conectar, el nombre de usuario con el que deseas iniciar sesión y la contraseña. Pulsa Conectar y tendrás un escritorio de Windows idéntico al que tendrías si hubieras iniciado sesión localmente en el equipo remoto.

2.1.- Integrar GNU/Linux en Active Directory mediante Winbind y Samba.

Probablemente ya hayas oído hablar del paquete Samba. Es muy útil para acceder a recursos compartidos en Windows desde clientes GNU/Linux. Como verás en este apartado, Samba también te servirá para incorporar una máquina GNU/Linux a Active Directory.

Optar por este método (en lugar del que te mostramos en la sección siguiente) significa invertir mucho más tiempo en la configuración de los clientes GNU/Linux de la red. Sin embargo, lo puedes preferir si te interesa controlar a fondo todas las opciones que intervienen en el proceso. También es interesante desde el punto de vista didáctico, ya que requiere mucha más interacción con el sistema.

Para realizar esta configuración necesitarás, por lo menos, dos equipos (físicos o virtuales):

En uno de ellos, que tendrá Windows Server 2008 R2 instalado, configurarás un dominio en Active Directory. Puedes llamarlo como quieras. En nuestro ejemplo, hemos utilizado villapedrusco.com. Como nivel funcional del dominio, elige Windows Server 2003 o superior.
En el otro equipo (repetimos, puede ser físico o virtual) instalarás una distribución moderna de Ubuntu Desktop. En el ejemplo hemos utilizado Ubuntu Desktop 11.04 para 32 bits.

Ambos equipos (o máquinas virtuales) deben estar conectados en red. Si utilizas máquinas virtuales, nuestra recomendación es que las tarjetas de red de las máquinas estén en modo "puente". De este forma tendrás las máquinas virtuales como si fueran equipos adicionales de tu red local, lo que permitirá:

1. Que se vean entre ellas.
2. Que la máquina con Ubuntu Desktop tenga acceso a Internet (imprescindible para instalar algunos paquetes).

PARA SABER MÁS

En el siguiente enlace encontrarás más información sobre cómo configurar las interfaces de red en VirtualBox.

Texto enlace: Configuración de las interfaces de red en VirtualBox.
URL: http://www.adictosaltrabajo.com/tutoriales/tutoriales.php?pagina=VirtualBox

En el proceso que te presentamos a continuación es muy importante no cometer errores ortográficos o de capitalización. Te recomendamos que utilices máquinas virtuales y que vayas realizando el proceso a medida que lo lees. También es importante que, al menos la primera vez, uses las mismas versiones de software que en la presentación. Ten paciencia si algo no te sale: seguramente será un error tonto que descubrirás si lees con atención lo que hayas escrito en los ficheros de configuración.

DEBES CONOCER

Sólo te queda ponerte manos a la obra. El proceso completo lo puedes encontrar en la siguiente presentación.

Texto enlace: Cómo unir Ubuntu con Active Directory utilizando Winbind y Samba.
URL: SOR05_CONT_R07_WinbindSamba.odp

2.2.- Una solución más sencilla: Likewise Open.

Probablemente, el proceso anterior te haya parecido tedioso y complicado. Sobre todo, cuesta imaginarse el tener que hacerlo en muchas máquinas. Evidentemente, podrías buscar alguna forma de agilizar el proceso, como copiar los archivos implicados directamente en los nuevos equipos que se unan al dominio.

Sin embargo, existe un método muchísimo más ágil de unir un equipo GNU/Linux a un dominio de Active Directory. Es tan simple como instalar un programa y realizar una mínima configuración. El inconveniente, si es que se puede considerar así, es que tienes que **utilizar software de terceros.**

Existen varios productos para realizar este trabajo, pero nos hemos decantado por el más popular: **Likewise Open.** Recientemente, este producto ha cambiado de nombre, y ahora se le conoce como P**owerBroker Identity Services Open Edition.**

Se trata de una aplicación libre y de código abierto, que utiliza los **PAM** (Pluggable Authentication Modules – Módulos de Autenticación Conectada) y **NSS** (Name Service Switch – Conmutador de Servicio de Nombres). ¿Te suenan estas siglas? Se corresponden con algunos de los servicios que has configurado en el apartado anterior. Dicho de otra forma, la aplicación Likewise Open hace las modificaciones necesarias en estos servicios (parte de lo que tú hiciste "a mano" en el apartado anterior) de forma automática.

El proceso para unir un equipo que ejecuta GNU/Linux o Mac OS X a Active Directory es realmente sencillo. En la siguiente presentación tienes todos los pasos para el caso de un equipo con Ubuntu 11.04. Como en el apartado anterior, te recomendamos que vayas realizando el proceso a medida que lo lees. Respeta, si puedes, las versiones del software que hay en la presentación. De esa forma, puedes evitar problemas de incompatibilidad.

DEBES CONOCER

¡A por ello! Sigue los pasos y verás lo sencillo que resulta. Ten en cuenta algo muy importante: el cliente GNU/Linux debe tener como servidor DNS principal la dirección IP del servidor DNS del dominio. En la presentación del apartado anterior te mostrábamos cómo se realiza esa configuración.

Texto enlace: Cómo unir Ubuntu con Active Directory con Likewise Open.
URL: SOR05_CONT_R09_LikewiseOpen.odp

3.- Acceder a recursos compartidos.

CASO PRÁCTICO

Alberto y Marisa acaban de integrar el primer equipo con GNU/Linux en Active Directory y siguen trabajando con el resto de los equipos. Sin embargo, ha surgido un problema que no habían previsto: Don José, el administrativo que utiliza dicho equipo, al acceder al nuevo sistema, les plantea una pregunta:

-¡Chicos! Perdonad, pero es que... no encuentro mis datos.
-No se preocupe -le responde Alberto-. Hemos hecho copias de seguridad de todo su disco antes de instalar GNU/Linux, de modo que no se ha perdido nada.
-De todos modos -continuó diciendo-, ¿no recuerda que hablamos con usted sobre qué datos quería conservar y que se los habiamos puesto en una carpeta, con un acceso directo en el escritorio? Se llama "datos_windows".
-No me refiero a eso, sino al "disco Z:" -aclara Don José.
-¿El disco Z:? Usted se refiere a la unidad de red que se conecta con su carpeta personal en el servidor de archivos -matiza Alberto.
-¿El qué? No sé, yo digo el disco Z: que aparecía cuando entraba en "Equipo" -contesta Don José-. Siempre nos dicen que guardemos ahí las cosas importantes.
-No se preocupe, ahora se lo arreglamos -le tranquiliza Alberto.

Alberto se dirige a Marisa:
-Marisa, se nos está olvidando ponerles un acceso a su carpeta compartida en el servidor de ficheros.
-Es verdad. ¡Qué fallo! Menos mal que nos hemos dado cuenta.

En unidades anteriores de este módulo has aprendido que una de las motivaciones para configurar un servicio de directorio en tu red es facilitar la gestión de los recursos compartidos. Con recursos compartidos nos referimos, principalmente:

- Carpetas.
- Archivos.
- Impresoras.

Si te has esforzado por unir equipos con GNU/Linux a un dominio de Active Directory, es lógico pensar que también te interesará acceder desde esos equipos a los recursos compartidos existentes en la red.

Cuando se desea utilizar recursos compartidos de Windows en sistemas GNU/Linux, se utiliza el servicio Samba. **Samba** es una implementación libre para sistemas de tipo UNIX del protocolo de archivos compartidos de Microsoft Windows, antiguamente llamado **SMB,** renombrado recientemente a **CIFS** (Common Internet File System – Sistema de Archivos Común de Internet). De esta forma, es posible que ordenadores con GNU/Linux, Mac OS X o UNIX, en general, se vean como servidores o actúen como clientes de recursos compartidos en redes de Windows.

En el siguiente apartado vas a aprender a configurar una máquina GNU/Linux como cliente para acceder a carpetas compartidas en un servidor Windows.

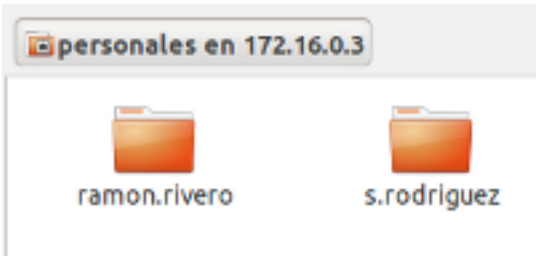
3.1.- Acceder a carpetas compartidas con el cliente Samba.

En el ejemplo que desarrollamos a continuación, existe una carpeta compartida llamada PERSONALES que se encuentra en el equipo con dirección IP 172.16.0.3, cuyo sistema operativo es Windows Server 2008 R2. A partir de ahí, vas a trabajar en una máquina GNU/Linux. Nosotros hemos utilizado, como en apartados anteriores, un equipo con Ubuntu Desktop 11.04 para 32 bits.

Los pasos que has de realizar para poder acceder a dicha carpeta compartida son:

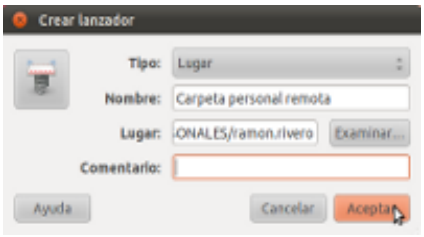
1. Abre el **navegador** de archivos (Nautilus). Puedes hacerlo en el menú Lugares → Carpeta personal.
2. Pulsa **Ctrl+L** para que la barra de navegación pase a modo **texto.**
3. En la barra de navegación, escribe: *smb://172.16.0.3/PERSONALES*.

4. Se te solicitará un nombre de usuario y una contraseña. Introduce unas credenciales que tengan permiso suficiente para acceder a la carpeta compartida. Ten en cuenta que los permisos que se aplican al acceder a una carpeta compartida desde el cliente Samba son los mismos que si se accede desde un equipo con Windows.



En capítulos anteriores, aprendiste que es posible conseguir que un usuario que inicia sesión en un dominio desde una máquina Windows tenga una unidad de red asociada a su carpeta **personal remota.** Esta unidad de red aparece automáticamente en "Mi Pc" o en "Equipo". ¿Se puede hacer lo mismo cuando el cliente es un equipo con GNU/Linux? Se puede hacer algo parecido. En concreto, te vamos a mostrar cómo el usuario *ramon.rivero* puede tener, en su escritorio, un acceso directo a su carpeta en el servidor de archivos.

1. Inicia sesión con el usuario de Active Directory (en nuestro caso, *ramon.rivero*).
2. Haz clic con el botón secundario sobre el escritorio y elige "Crear lanzador".
3. En el tipo de lanzador selecciona "Lugar". En "Nombre" y "Comentario" puedes escribir lo que quieras. En "Lugar" tienes que escribir la ruta al recurso compartido:
smb://172.16.0.3/PERSONALES/ramon.rivero.

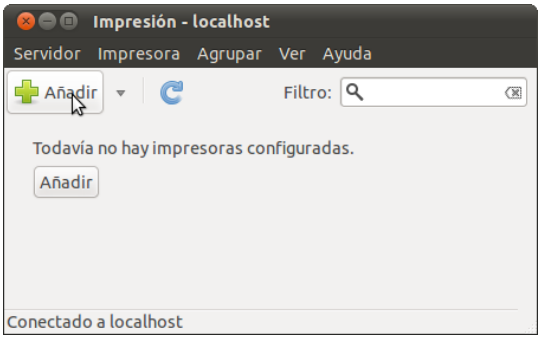


3.2.- Acceder a impresoras compartidas con el cliente Samba.

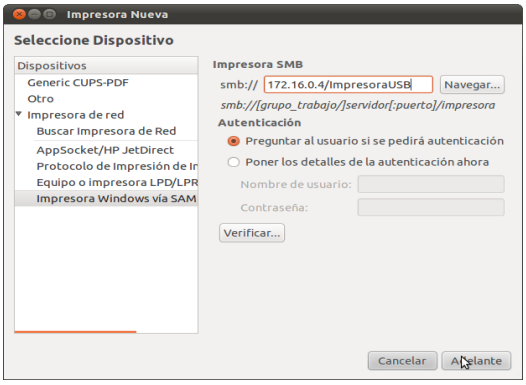
Otro uso muy común del cliente Samba es el acceso a impresoras compartidas en Windows. Ya sabes compartir una impresora en Windows; incluso sabes cómo asignarle permisos. Pues bien, debes saber que desde GNU/Linux también podrás utilizar las impresoras que hayas compartido en Windows.

Tenemos el siguiente escenario: un equipo con Windows 7, cuya dirección IP es la 172.16.0.4. Existe una impresora conectada mediante un cable USB a dicho equipo y esta impresora se ha compartido en red. Ahora, veamos cómo se puede utilizar esta impresora desde un equipo GNU/Linux, en concreto, una distribución Ubuntu Desktop 11.04.

En el equipo GNU/Linux, debes acceder a Sistema → Administración → Impresión. En esta herramienta, pulsa el botón "Añadir".



Se abre un asistente. Como estamos accediendo a una impresora que está en otro equipo, debes elegir **"Impresora de red"** y en ese menú puedes encontrar la opción **"Impresora Windows vía Samba"**. Y aquí llega el aspecto **importante: el nombre de la impresora.** Sabes la dirección IP del equipo en el que está (también puedes usar el nombre del equipo en la red). En nuestro ejemplo, utilizaremos la IP, que es 172.16.0.3. También sabes el nombre con el que compartiste la impresora. En nuestro caso es "ImpresoraUSB". Pues bien, el nombre "Samba" será: smb://172.16.0.4/ImpresoraUSB. En el cuadro de texto correspondiente, debes introducir los datos para formar este nombre, como puedes ver en la imagen.



Tras esto, tendrás que **elegir un controlador** para la impresora. Afortunadamente, las distribuciones actuales de GNU/Linux incluyen controladores para gran cantidad de modelos de impresoras. Como puedes ver, se trata de un proceso muy sencillo. Eso sí, no debes olvidar que, para que puedas imprimir, la cuenta de usuario que utilices debe tener permisos efectivos sobre la impresora.

4.- Configurar recursos compartidos en GNU/Linux.

CASO PRÁCTICO

En el ayuntamiento de Villapedrusco ya han empezado a cambiar el sistema operativo de algunos de los ordenadores que se emplean para labores ofimáticas.

El personal se está acostumbrando al nuevo sistema. Algunos han protestado por el cambio, pero en general se están adaptando bastante bien al nuevo entorno. En algunos equipos se mantienen los sistemas operativos Windows, debido a que es necesario ejecutar aplicaciones que no funcionan en otros sistemas. En los controladores de dominio se mantiene Windows Server.

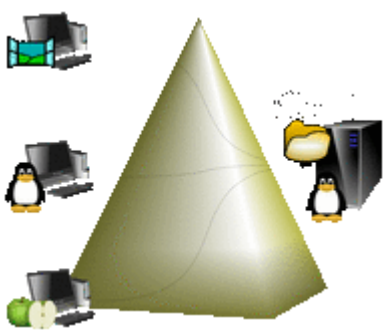
El alcalde está bastante satisfecho, ya que en el próximo año van a ahorrar bastante dinero con las licencias de software. Sin embargo, desea ir un poco más allá y le pide a Carmen que analice si sería posible cambiar el sistema operativo de alguno de los servidores que están utilizando sin alterar la estructura de usuarios, grupos, etc.

-Verá Francisco. De entre los equipos que existen en el ayuntamiento hay uno que actualmente se utiliza como servidor de ficheros y de impresoras, pero no como controlador de dominio. Eso significa que podemos emplear GNU/Linux para que realice sus funciones, en lugar de Windows Server, que es el sistema que hay actualmente instalado -explica Carmen.
-¿Seguiría todo funcionando igual? -pregunta Francisco.
-Los trabajadores y trabajadoras no notarían la diferencia al acceder a los recursos compartidos -le tranquiliza Carmen.
-Entonces adelante -confirma Francisco.

Tras esta conversación, Carmen habla con sus empleados:
-Vamos a configurar un equipo en GNU/Linux como servidor de ficheros y de impresoras -les anuncia Carmen.
Marisa reflexiona unos segundos y apunta:
-Vale... Como los clientes van a ser equipos tanto de Windows como de GNU/Linux, lo mejor es usar Samba, ¿no?
-Mmmm... no sé -interviene Alberto-. Yo creo que para compartir impresoras, hoy por hoy, es mejor usar CUPS.
-Estudiadlo bien y me lo decís -dice Carmen.

4.1.- Configuración de carpetas compartidas mediante Samba.

Una de las **ventajas** que puedes encontrar a la hora de utilizar GNU/Linux en tus equipos frente a otras alternativas como Windows es el **coste** del sistema operativo. Como ya sabes, numerosas distribuciones de GNU/Linux son libres y gratuitas. Por otro lado, GNU/Linux es un sistema que incorpora muchos paquetes, también gratuitos, que te permiten configurar completos servidores: de páginas web, de bases de datos, de archivos...



Es en este último punto en el que nos vamos a centrar ahora: imagina que tienes un **escenario** como el de los apartados anteriores: un dominio configurado con Active Directory. En él, has introducido un equipo con sistema operativo **GNU/Linux** y deseas que ese equipo funcione como **servidor de ficheros**. Es decir, en dicho servidor residirán carpetas compartidas de la red. Los usuarios y usuarias van a acceder a las carpetas compartidas residentes en el servidor GNU/Linux desde equipos con Windows y con GNU/Linux.

Este escenario se resuelve utilizando **Samba** para la **compartición** de archivos. A continuación te mostramos el proceso para compartir una carpeta llamada PRESUPUESTOS en el servidor de ficheros.

- **Instala** el paquete de servidor de Samba: *sudo apt-get install samba*.
- Si aún no lo has hecho, **crea la carpeta** que vas a compartir. En nuestro ejemplo, situamos la carpeta en /VILLAPEDRUSCO/SHARES, por lo que el comando será:
sudo mkdir -p /VILLAPEDRUSCO/SHARES/PRESUPUESTOS
- **Edita** el fichero *smb.conf*. (*sudo gedit /etc/samba/smb.conf*). **Añade** al final las siguientes líneas:
  [PRESUPUESTOS]
  path=/VILLAPEDRUSCO/SHARES/PRESUPUESTOS
  guest ok=yes
  read only=no
- **Reinicia** el servicio Samba: *sudo /etc/init.d/smbd restart*. En este punto, si desde una máquina con Windows abres el navegador y escribes como ruta: \\LINUX02\PRESUPUESTOS (para lo cual estarías suponiendo que el *hostname* (nombre del equipo) de tu servidor de ficheros GNU/Linux es LINUX02) se abrirá una ventana que mostrará el contenido de la carpeta compartida.

El nombre entre corchetes **([])** será el nombre del **recurso compartido,** y lo que pongas tras la variable **"path"** (path en inglés significa "camino" o "ruta") es la **ruta** en el sistema de archivos a la carpeta que deseas compartir. El parámetro "**guest ok=yes**" indica que se puede acceder a la carpeta como **invitado,** es decir, sin necesidad de introducir un nombre de usuario o contraseña. El parámetro "**read only=yes**" indica que la carpeta es de **lectura solamente**, por lo que no se podrán realizar cambios en ella.

El **problema** que se plantea entonces es el de los **permisos**. ¿Qué permisos se estarán aplicando? Al igual que en el caso de carpetas compartidas en Windows, se aplica la combinación más restrictiva entre los permisos locales y los permisos de compartición. En nuestro ejemplo, los permisos de compartición que has seleccionado son los **más permisivos posibles,** ya que permites a todos los usuarios tanto leer como escribir

- "**guest ok**=yes".
- "**read only**=no".

Por lo tanto, en este caso, se aplicarían directamente los permisos locales establecidos para la carpeta.

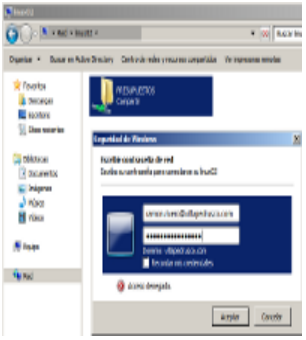
DEBES CONOCER

Para saber manejar los permisos locales en sistemas GNU/Linux, sigue el siguiente enlace:

Texto enlace: Configuración de los permisos locales en GNU/Linux.
URL: http://linuxcomandos.blogspot.com/2008/02/chmod-permisos-en-linux.html

4.2.- Configuración de los permisos para compartir carpetas en Samba.

En esta sección, vas a continuar configurando el servidor de ficheros Samba de forma que controles los permisos con los que accederán los usuarios a la carpeta PRESUPUESTOS. En lugar de dejar que se apliquen los permisos locales, como en el apartado anterior, vas a hacer que cuando se a**cceda a través de la red** a la citada carpeta, el grupo ***DL_LecturaPresupuestos*** tenga permisos de **lectura** y el grupo ***DL_EscrituraPresupuestos*** tenga permisos de **escritura.**



Ambos grupos los tienes que crear en Active Directory y serán grupos locales de dominio. También crearás dos grupos globales, llamados *G_Concejalías* y *G_Personal*. Lo que se persigue es que los miembros del grupo *G_Concejalías* tengan permisos para leer y escribir en la carpeta PRESUPUESTOS, mientras que los miembros del grupo *G_Personal* sólo puedan leer. Para ello, el grupo *G_Concejalías* será miembro de *DL_EscrituraPresupuestos* y el grupo *G_Personal* será miembro de DL_*LecturaPresupuestos*. Para que puedas hacer las pruebas, crea al menos dos usuarios: *ramon.rivero*, que será miembro de *G_Concejalías* y *s.rodriguez*, que será miembro de *G_Personal*.

En resumen:

- El usuario **ramon.rivero** podrá **escribir** en la carpeta PRESUPUESTOS.
- El usuario **s.rodriguez** sólo podrá **leer.**
- Procurarás que cualquier **otro usuario** que no pertenezca a los grupos indicados **no pueda acceder** a la carpeta.

Una vez que hayas creado esta estructura de usuarios y grupos, pasarás a la **configuración** del servidor Samba, para lo cual debes iniciar sesión con un usuario que pueda ejecutar *sudo*.

1. **Edita** el fichero de **configuración** de samba: *sudo gedit /etc/samba/smb.conf*
2. Deja la s**ección de la carpeta PRESUPUESTOS** de la siguiente forma:

```
[PRESUPUESTOS]
path=/VILLAPEDRUSCO/SHARES/PRESUPUESTOS
read only=no
writeable=yes
read list=@DL_LecturaPresupuestos
write list=@DL_EscrituraPresupuestos
```

Con esto, permites que se escriba en la carpeta ("read only=no" y "writeable=yes") y dices que los que pueden leer son los miembros del grupo *DL_LecturaPresupuestos* y que los que pueden escribir son los miembros del grupo *DL_EscrituraPresupuestos*. Como son **grupos,** tienes que poner una **"@" delante.**

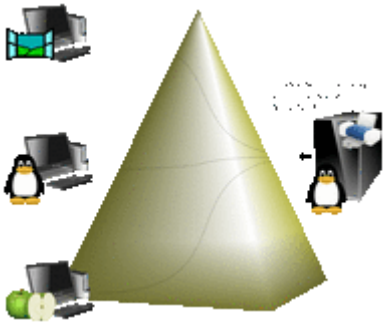
3. **Ajusta los permisos locales:** cuando accedas a través de la red, los permisos locales que se aplican son los de "otros", por lo que debes asegurarte de que éstos tienen los tres permisos: rwx. Para ello, ejecuta: *sudo chmod o+r,o+w,o+x /VILLAPEDRUSCO/SHARES/PRESUPUESTOS*
4. Por último (y este es un inconveniente de utilizar Samba para compartir carpetas) tienes que **ejecutar el comando *smbpasswd*** PARA **CADA USUARIO** CON EL QUE QUIERAS ACCEDER. Cuando te soliciten una contraseña, introduce una. En este ejemplo, tendrías que ejecutar:

```
sudo smbpasswd -a ramon.rivero@villapedrusco.com
sudo smbpasswd -a s.rodriguez@villapedrusco.com
```

Tras esta configuración, ya puedes acceder a la carpeta desde otro equipo. Cuando tengas que introducir las credenciales, utiliza el nombre de usuario con el mismo formato que utilizaste en el comando *smbpasswd* (con el nombre del dominio tras una "@") y la contraseña que introdujiste al ejecutar dicho comando.

4.3.- Configuración de un servidor de impresión mediante CUPS.

Cuando has configurado el servicio Samba, habrás podido observar que en el archivo de configuración existe una sección que tiene que ver con las **impresoras** (la sección encabezada con **[printers]).** Utilizar Samba para **compartir** impresoras con sistemas Windows ha sido algo muy común y aún hoy se sigue utilizando. Sin embargo, la configuración del servicio y, en definitiva, conseguir que funcione, es un **proceso laborioso**. Ese es uno de los motivos por los que hoy por hoy es común utilizar el sistema **CUPS** para configurar un servidor de impresión basado en GNU/Linux.



CUPS son las siglas de Common UNIX Printing System (Sistema de Impresión Común de UNIX). Está desarrollado para sistemas operativos de tipo UNIX que permite que un computador actúe como servidor de impresión. Un servidor de impresión es un equipo que puede **aceptar tareas de impresión desde otros equipos clientes**, los procesa y los envía a la impresora apropiada. CUPS permite configurar un servidor de impresión sofisticado, que maneje varias impresoras a la vez, creando **grupos** de impresoras (llamados **clases),** gestionando permisos, etc. Es una alternativa mucho más potente que Samba para la compartición de impresoras.

Llegar a imprimir trabajos en una impresora que se comparte a través de la red mediante CUPS requiere que realices dos configuraciones: la del servidor CUPS y la del cliente. En esta sección te mostramos ambos procesos. El servidor CUPS será un equipo GNU/Linux, por lo que puedes utilizar alguno de los que hayas empleado para los ejemplos de secciones anteriores. Como equipo cliente para acceder a la impresora emplearás un equipo con algún sistema Windows. Nosotros te mostraremos el proceso desde Windows 7.

DEBES CONOCER

En esta presentación encontrarás el procedimiento para configurar un servidor CUPS y compartir una impresora conectada al mismo.

Texto enlace: Cómo configurar un servidor de impresión CUPS y compartir una impresora.
URL: SOR05_CONT_R21_ConfServidorCUPS.odp

DEBES CONOCER

Y en este vídeo podrás ver el procedimiento para utilizar la impresora compartida mediante CUPS en la presentación anterior. NOTA: la dirección IP que aparece en el vídeo es la del servidor CUPS.

Texto enlace: Cómo acceder a una impresora compartida mediante CUPS.
URL: SOR05_CONT_R22_AccesoImpresoraCUPS.flv

5.- Utilizar GNU/Linux como controlador de un dominio NT.

CASO PRÁCTICO

Ha pasado un año desde que Alberto y Marisa integraron equipos con GNU/Linux en el dominio del ayuntamiento de Villapedrusco.

En ese tiempo, las cosas han funcionado razonablemente bien en las oficinas de la casa consistorial. Además, pudieron disminuir el gasto en licencias informáticas. Sin embargo, el alcalde está preparando más ajustes presupuestarios, por lo que, de nuevo, se pone en contacto con CARMINFO S. L. para consultar la viabilidad de su idea.

Tras los saludos iniciales, Francisco, el alcalde, va directamente al grano:
-Mire, Carmen, estamos bastante satisfechos con el funcionamiento de los ordenadores. Por desgracia, es necesario ahorrar aún más y he tenido una idea.
-Cuénteme su idea, Francisco -responde Carmen.
-El año pasado me dijo que era complicado sustituir los equipos con Windows Server por sistemas Linux, pero que se podía hacer -le recordó Francisco.
-Si no recuerdo mal, tenían ustedes un controlador de dominio con Windows Server. El problema es que, para sustituirlo por otro sistema, hay que volver a crear los usuarios y los grupos, y eso puede llevar tiempo -dijo Carmen.
-Lo entiendo, pero creo que nos merece la pena la inversión -sopesó el alcalde-. Me gustaría hacer unos cálculos. ¿Podrías pasarnos un presupuesto?

Tras esta conversación, Carmen se sentó a estudiar el problema y plantear un presupuesto. Finalmente, la empresa CARMINFO S.L. fue designada para realizar la tarea.

En este capítulo, vas a aprender a sustituir el controlador de dominio, que actualmente funciona con Windows Server, por un equipo con GNU/Linux. ¿Cómo es esto posible? La respuesta es: gracias a Samba, al que ya conoces por la compartición de recursos que has estudiado en secciones anteriores.

Esta solución es **aceptable** para **entornos pequeños**, sin grandes necesidades en lo referente a gestión de grupos y usuarios. Y por supuesto, no es aplicable en dominios que formen estructuras de árbol o de bosque. Es equivalente a los dominios que se creaban con Windows NT, antes del surgimiento de Active Directory. Para utilizar un servicio de directorio **más sofisticado** con software libre, tendrás que recurrir a **OpenLDAP**.

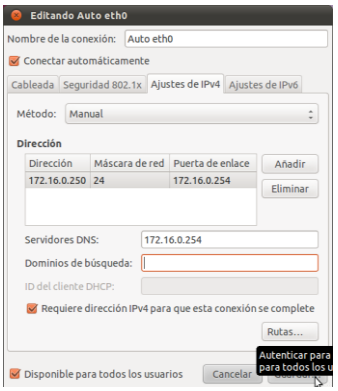
Para seguir los procedimientos que encontrarás a continuación, necesitarás un equipo (físico o virtual) con GNU/Linux para convertirlo en controlador de dominio y otro equipo (físico o virtual) con Windows, que funcionará como un equipo miembro del dominio. En estos ejemplos hemos usado, como en el resto de la unidad, Ubuntu Desktop 11.04 y Windows 7.

5.1.- Pasos preliminares.

Antes de hacer que un equipo con GNU/Linux funcione como controlador de dominio, tienes que asegurarte de que se cumplen ciertos **requisitos.** Es importante que realices estos pasos en un equipo "limpio", es decir, un equipo en el que no hayas realizado operaciones relacionadas con el servicio Samba anteriormente.

1. El equipo debe t**ener instalado el servicio Samba.** Si no es así, lo puedes instalar con el comando:

sudo apt-get install samba



2. Debes **establecer un nombre** para el equipo menor de quince caracteres. Tendrás que editar el fichero */etc/hosts* y el fichero */etc/hostname*, tal y como te indicamos en apartados anteriores. En nuestro ejemplo, el equipo se llama *pdcubuntu*.
3. Siempre se recomienda que los controladores de dominio tengan una **IP fija**. Por lo tanto, debes asignar una al equipo. Gráficamente, puedes hacerlo en Sistema → Preferencias → Conexiones de red.
4. Es muy conveniente que, antes de lanzarte a la configuración de Samba para que el equipo actúe como controlador de dominio, **compruebes** que el **servidor Samba funciona adecuadamente**. Para ello, crea una carpeta en el equipo, que compartirás en red. En nuestro ejemplo, la carpeta se llama *datosvillapedrusco* y la hemos ubicado en el directorio */var*, por lo que el comando para crearla es:

sudo mkdir /var/datosvillapedrusco.

Haremos que se pueda escribir en la carpeta, por lo que hay que **cambiar los permisos** locales de la misma:

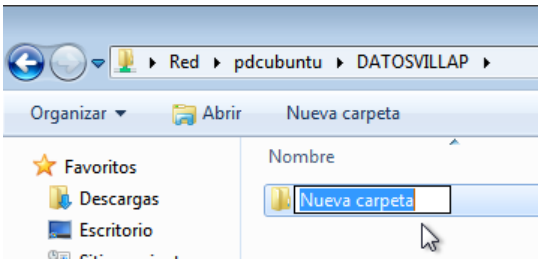
sudo chmod o+w /var/datosvillapedrusco

5. Como viste en el apartado correspondiente, para compartir la carpeta, debes introducir el siguiente texto en el fichero ***/etc/samba/smb.conf*.** Como puedes observar, estamos permitiendo el acceso a los invitados, pero esto es sólo porque estamos comprobando que el servidor funciona. Más tarde, cámbialo.

```
[DATOSVILLAP]
path=/var/datosvillapedrusco
read only=no
writeable=yes
guest only=yes
```

1. ¡No olvides **reiniciar el servicio!** Utiliza el comando:

sudo /etc/init.d/smbd restart

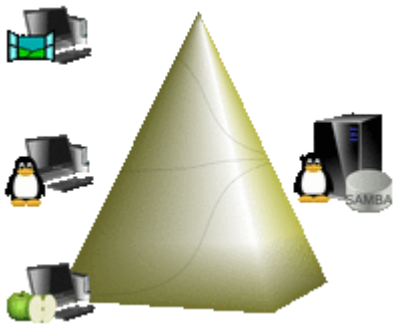


2. Para completar la prueba, accede desde un equipo Windows conectado a la misma red, utilizando la ruta: *\\172.16.0.250\DATOSVILLAP*. Lógicamente, la **dirección IP** que aparece es la **del equipo con GNU/Linux.**

5.2.- Configuración de los parámetros Samba.

Ahora que ya tienes el equipo preparado, ha llegado el momento de convertirlo en controlador de dominio. Vas a realizar ciertos cambios en el archivo de configuración de Samba. Pero a**ntes de realizar cambios**, asegúrate de hacer **una copia de seguridad del mismo**: *sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.bak*.

Ahora, edita el fichero. Como en apartados anteriores, puedes utilizar el editor gedit. Ejecuta, por tanto, el comando *sudo gedit /etc/samba/smb.conf*. Vas a cambiar ciertas líneas, de forma que queden como te indicamos. Si alguna directiva no aparece, escríbela en una nueva línea. ¡Muy importante! Las líneas pueden empezar por el carácter **(#) o (;).** Esos símbolos **hacen que la línea no sea interpretada por el servicio Samba**, pues se considera un **comentario.** Por lo tanto, para las directivas que te indicamos a continuación, debes asegurarte de que la línea no tiene (#) ni (;) como primer carácter.



- *workgroup=VILLAPEDRUSCO*

Es decir, ponemos el nombre NetBIOS del dominio. Ten en cuenta que este nombre debe ser inferior a 15 caracteres.

- *netbios name=PDCUBUNTU*

En esta línea estás estableciendo el **nombre NetBIOS** del equipo controlador de dominio y NO debe coincidir con el nombre NetBIOS del dominio.

- *security = user*
- *encrypt passwords = yes*
- *os level = 64*
- *preferred master = yes*

Con esta opción, estás indicando que éste será el **controlador** de dominio **principal,** frente a otros controladores de dominio GNU/Linux.

- *domain master = yes*
- *local master = yes*

Estas dos últimas opciones tienen que ver con la **visibilidad** en la red de los **controladores** de dominio.

- *wins support = yes*

Aquí le estás indicando a Samba que utilice el servicio **WINS.**

- *dns proxy = yes*

Con esta opción, estás indicando a Samba que haga peticiones para nombres de máquinas usando DNS cuando no ha sido posible identificar a la máquina usando WINS.

Ya casi lo tienes. Sólo quedan unos pocos **ajustes** relacionados con la identificación de los **usuarios.**

- *domain logons = yes*
- *logon path = \\%L\profiles\%U*

En esta opción estás indicando dónde quieres que se **almacenen los perfiles de usuario** de las cuentas de usuario que se autentiquen contra el equipo. Es muy similar a la ruta que especificabas cuando creabas usuarios de Active Directory. Simplemente, **%L** representa es el **nombre NetBIOS del equipo** (que tendrá una carpeta compartida en Samba llamada *profiles*) y **%U** es el **nombre del usuario** (la variable %username% de Windows Server). Lógicamente, deberás asegurarte de que creas un recurso compartido para almacenar los perfiles. Pero ya te ocuparás de ello más adelante.

- *logon drive = H:*

Esta es la unidad de red que se creará cuando un usuario de Active Directory se conecte al dominio y que apuntará a su carpeta personal en red.

- *logon home = \\%L\%U*

Este parámetro especifica la **ubicación del directorio personal** al que se conecta la unidad de red anterior.

- *time server = yes*

Con este parámetro, estás indicando que los **clientes deben sincronizar su reloj** con el del controlador del dominio.

Ya casi has terminado. En la siguiente sección puedes ver cómo tienes que crear las c**arpetas de datos** y de **perfiles,** y cómo crear los usuarios para poder conectarse al dominio.

Si algo falla, no te desesperes. Restaura la copia de seguridad del fichero que hiciste al principio

sudo cp /etc/samba/smb.conf.bak /etc/samba/smb.conf

5.3.- Creación de los recursos compartidos.

En el apartado anterior asignaste unas rutas de red para los perfiles de los usuarios y para sus carpetas personales. Nos estamos refiriendo a las directivas “logon path” y “logon home”. Sin embargo, no basta con indicar las rutas en dichas directivas. Debes asegurarte de que estas carpetas compartidas estén disponibles. Para ello, introduce las siguientes líneas en el fichero ***/etc/samba/smb.conf*.**

```
[homes]
comment=Home Directories
browseable = no; esta opción establece que el recurso esté oculto en el entorno de red.
writable = yes ; el usuario tendrá permisos de escritura.

; Recurso Profiles, donde se almacenara la información de los perfiles móviles de cada usuario.
[profiles]
comment = User profiles share
path = /var/lib/samba/profiles
browseable = no
read only = no
create mask = 0600 ; Define los permisos locales que tendrán los archivos creados.
directory mask = 0700 ; Define los permisos locales que tendrán los directorios creados.
```

Es muy posible que ambos recursos ya te aparezcan en el fichero de configuración, pues se suelen incorporar por defecto. Asegúrate de configurarlos como te indicamos aquí y de que las directivas no estén comentadas.

Analiza los datos que has introducido: en primer lugar, fíjate en [homes]. Como ya sabrás, en GNU/Linux, las carpetas personales de los usuarios se suelen almacenar en el directorio */home*, con lo que si un usuario se llama, por ejemplo, *pepito*, su directorio personal será */home/pepito*. Al configurar en Samba el recurso [homes] estás consiguiendo que todos los usuarios del sistema puedan acceder mediante la red a su propia carpeta compartida, utilizando como ruta de red *\\Nombre_del_servidor\Nombre_del_usuario.* Si te fijas bien, podrás ver que en el apartado anterior hemos utilizado este formato en la directiva *logon_home*. En resumen, combinando las configuraciones de este apartado y del anterior, cuando un usuario inicie sesión en un equipo cliente, le aparecerá en “Equipo” una unidad de red que apuntará a su directorio personal en el controlador de dominio.

En segundo lugar, has configurado un recurso llamado [profiles]. En este caso, se trata de la carpeta que debe almacenar los perfiles de los usuarios. El objetivo es que los usuarios puedan trabajar con perfiles móviles. No olvides comprobar que la carpeta de perfiles existe y que tiene los permisos adecuados. Si no es así, créala y concede permisos de escritura a los “otros”:

sudo mkdir -p /var/lib/samba/profile
sudo chmod o+w /var/lib/samba/profiles

De esta forma, cuando un usuario **inicie sesión** en el dominio, **tomará los datos de perfil de dicha carpeta** y, cuando los modifique, almacenará los cambios en la misma. Por esto último es por lo que debe poderse escribir en la carpeta, motivo por el cual has asignado la directiva “read only = no” en la configuración del recurso en Samba y por el que has asignado permiso de escritura (w) a “otros” (o).

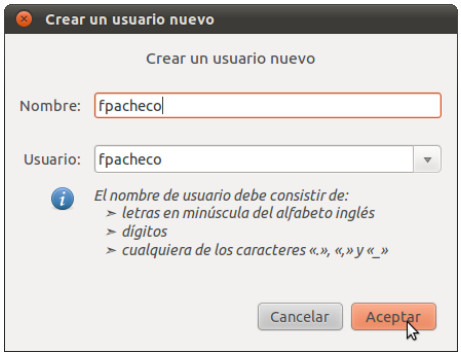
La configuración de Samba ha terminado. Guarda los **cambios** en el fichero de configuración y **reinicia** el servicio con:

sudo /etc/init.d/smbd restart.

5.4.- Creación de los usuarios y de los grupos.

Ahora, ha llegado el momento de crear los usuarios que se vayan a utilizar en el dominio. Para crear usuarios "de dominio" en un controlador de dominio GNU/Linux, debes:

1. **Crear una cuenta de usuario local** en GNU/Linux. Puedes hacer esto en el entorno gráfico en Sistema → Administración → Usuarios y grupos. También puedes usar el comando: *sudo adduser fpacheco*.



2. Hacer que dicha cuenta de **usuario lo sea también de Samba**. Para ello, ejecuta el comando:
sudo smbpasswd -a fpacheco
y asigna una contraseña. Lógicamente, en el ejemplo, el nombre de la cuenta es *fpacheco*.

Tendrás que realizar este **proceso con cada usuario** del dominio que quieras crear. Si el número de usuarios es elevado, puede ser interesante la utilización de *scripts* que automaticen el proceso.

En cuanto a los grupos que puedes configurar, se trata de **grupos locales** del controlador de dominio. Para crear un grupo, por ejemplo el grupo *concejales*, tendrás que ejecutar el comando:

sudo addgroup concejales

Y para añadir usuarios a dicho grupo:

sudo addgroup fpacheco concejales

El comando anterior hace que el usuario *fpacheco* sea miembro del grupo *concejales*.

Si deseas **utilizar grupos para asignar permisos** en los recursos compartidos de Samba, no olvides poner delante del nombre del grupo el símbolo "@". Por ejemplo: *write list = @concejales*.

PARA SABER MÁS

Existe una herramienta para configurar los parámetros de Samba de forma gráfica. Se llama **"Swat"** y puedes encontrar información sobre ella en el siguiente enlace:

Texto enlace: Herramienta swat.
URL: http://www.taringa.net/posts/linux/7454394/Configurar-Samba-via-web-con-SWAT.html

5.5.- Creación de las cuentas de equipo.

Finalmente, sólo te queda incorporar los equipos al dominio. Para ello, es necesario que crees **un usuario Samba para cada equipo**. Puede que esto te sorprenda, porque cuando unías equipos a Active Directory no tenías que crear cuentas para ellos. El motivo es que en Active Directory esta acción se realiza automáticamente cuando un equipo cliente se une al dominio. Sin embargo, en este caso tienes que realizar esta acción manualmente. Este es otro motivo por el que sólo es aconsejable utilizar Samba como controlador de dominio si se trabaja con entornos pequeños.

En primer lugar, crea un grupo llamado "machines":

sudo addgroup machines

A continuación, crea un usuario que tenga por nombre el nombre NetBIOS del equipo que deseas añadir, pero añadiendo un símbolo de dólar **($) al final**. Lo más cómodo es que utilices el comando:

sudo useradd -g machines -d /dev/null -s /bin/false EQUIPO01$

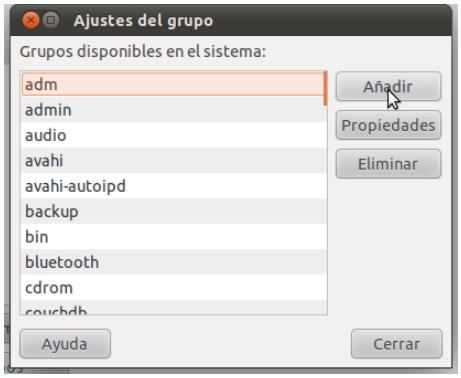
Veamos que significa cada opción:

- ***-g machines*:** indica que el **usuario debe pertenecer al grupo "machines".**
- ***-d /dev/null*:** le **asigna** a dicho usuario el **directorio** personal */dev/null.* Éste es un directorio nulo, lo que tiene lógica, porque esta cuenta de usuario es sólo para poder unir la máquina al dominio y no se va a utilizar para generar datos.
- ***-s /bin/false*:** esta opción hace que esta cuenta de usuario **no se pueda utilizar para iniciar sesión** en ninguna máquina.
- **EQUIPO01$:** es el nombre de la cuenta de usuario que estás creando. EQUIPO01 es, en este caso, el nombre NetBIOS del **equipo que deseas incorporar al dominio.**

Aún habiendo especificado la opción "-s /bin/false", debes asegurarte de **deshabilitar** esta cuenta para ejecutar **comandos.** Esto lo puedes conseguir con:

sudo passwd -l EQUIPO01$

No olvides que toda la configuración anterior también la puedes realizar con la herramienta gráfica "Usuarios y grupos" en Ubuntu.



Con esto, has creado una cuenta de usuario local para el equipo. Ahora, simplemente tienes que **crear una cuenta Samba**:

sudo smbpasswd -a -m EQUIPO01$

Observa el parámetro "-m". Indica que el tipo de cuenta samba es de "máquina".

CITA PARA PENSAR

"Los ordenadores son buenos siguiendo instrucciones, no leyendo tu mente."

Atribuida a Donald Knuth, profesor de la Universidad de Stanford.

5.6.- Unir los equipos al dominio.

Para poder unir las máquinas al dominio, es necesario que controles la cuenta *root* del controlador de dominio. En Ubuntu, esta cuenta está deshabilitada por defecto. Para habilitarla, simplemente le asignamos una contraseña:

sudo passwd root

Y para poder utilizarla con Samba, ejecutamos el comando:

sudo smbpasswd -a root

Con esto, has terminado de configurar todo lo necesario en el controlador de dominio. A partir de ahora, el resto del trabajo lo realizarás en el equipo cliente que deseas unir al dominio.

Inicia sesión con una cuenta que tenga **privilegios de administración** en dicho equipo, como por ejemplo, Administrador.

Si el equipo que estás uniendo al dominio usa Windows 7, tienes que **modificar** el registro de Windows (programa *regedit* en Windows) para añadir las siguientes claves, ubicadas en:

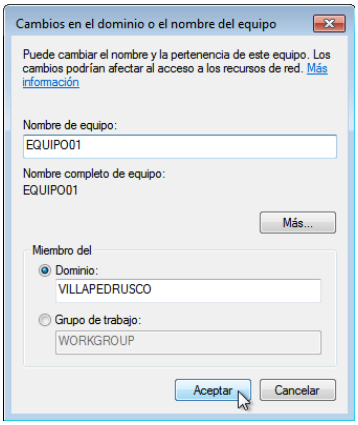
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\LanmanWorkstation\Parameters]:
"DomainCompatibilityMode"=dword:00000001
"DNSNameResolutionRequired"=dword:00000000

Y alterar las que se muestran debajo, ubicadas en:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Netlogon\Parameters]:
"RequireSignOnSeal"=dword:00000000
"RequireStrongKey"=dword:00000001

No olvides reiniciar Windows tras alterar estas claves.

Como ya has hecho cuando uniste equipos a dominios de Active Directory, debes acudir a la ventana en la que se te permite cambiar el nombre del equipo. La única particularidad es que en el nombre del dominio especificarás únicamente su nombre NetBIOS, como puedes ver en la imagen.



Al pulsar "Aceptar", el sistema te pide el nombre de un usuario con credenciales para unirse al dominio, introduce como nombre de usuario **"root"** y como contraseña la que hayas establecido en el comando ***smbpasswd*.**

Tras reiniciar, podrás iniciar sesión con los usuarios que definiste en el controlador de dominio.

6.- Servicios de directorio en escenarios heterogéneos.

CASO PRÁCTICO

Tras finalizar el encargo del alcalde de Villapedrusco, Carmen se reúne con sus empleados y empleadas para analizar las tareas desarrolladas.

-Estoy muy contenta. Habéis hecho un buen trabajo en Villapedrusco. Hace un año configurasteis los equipos "de escritorio" de forma que utilicen GNU/Linux con los usuarios de Active Directory. También el servidor de archivos e impresoras en GNU/Linux. Y finalmente, en este último encargo, habéis conseguido que la función del controlador de dominio la realice un equipo también con GNU/Linux.
-Sí, y parece que el personal del ayuntamiento ya se ha acostumbrado al nuevo sistema. -dice Marisa.
-Evidentemente, les llevó algo de tiempo -replica Carmen-. En cualquier caso, hemos realizado con eficacia el encargo que nos hicieron. ¿Os ha resultado difícil?
-No especialmente, Carmen. Al principio pensábamos que nos iba a costar más -responde Alberto.
Marisa interviene:
-Pero tengo una sensación agridulce: la configuración final del dominio no es tan funcional como un dominio con Active Directory. Por ejemplo, no se puede añadir subdominios al árbol. ¿No existe una alternativa libre a Active Directory que sea lo suficientemente sofisticada?

En esta unidad has aprendido a integrar sistemas GNU/Linux en una estructura de Active Directory. La convivencia entre **diferentes sistemas operativos** dentro de una misma red es una realidad que tiende cada vez más hacia la **integración** de los mismos. El motivo de esta heterogeneidad en los sistemas utilizados es, principalmente, la diversidad de las aplicaciones que se usan. Es muy normal utilizar aplicaciones desarrolladas para Microsoft Windows junto con otras que se adaptan mejor a GNU/Linux. Por otro lado, en ciertos ámbitos profesionales, lo normal es utilizar equipos y sistemas operativos de Apple.

6.1.- Algunas alternativas a Active Directory.

En esta unidad nos hemos centrado en un modelo basado en el servicio de directorio de Microsoft, Active Directory, pero con clientes de diferentes sistemas operativos, en especial GNU/Linux. También hemos sustituido el controlador de dominio por una máquina GNU/Linux, pero a costa de perder posibles funcionalidades frente a Active Directory.

No obstante, existen alternativas a este modelo. Dicho de otra forma, **existen servicios de directorio alternativos** a Active Directory y, aunque sería imposible abordarlos en este módulo, debes conocer su existencia. Algunos de ellos son:

- **Novell Directory Services** (Servicios de directorio de Novell): También conocido como eDirectory, es la implementación de **Novell** utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. La ventaja de esta implementación es que corre en **diversas plataformas**, por lo que puede adaptarse fácilmente a entornos que utilicen más de un sistema operativo.

- **OpenLDAP**: Se trata de una **implementación libre del protocolo LDAP** que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP. Es independiente de la plataforma, por lo que se puede utilizar sobre diferentes sistemas operativos, como GNU/Linux, Mac OS X, Solaris, Windows 2000/XP...

- **Red Hat Directory Server (Servicio de Directorio Red Hat):** Asociado a la distribución Red Hat Linux. Es un servidor basado en LDAP que **centraliza** configuración de aplicaciones, perfiles de usuarios, información de grupos, políticas así como información de control de acceso dentro de un sistema operativo independiente de la plataforma.

PARA SABER MÁS

Si quieres hacer alguna prueba con un servicio de directorio alternativo a Active Directory, puedes utilizar OpenLDAP de forma fácil y gratuita. En este enlace tienes amplia información sobre ello.

Texto enlace: Servicio de directorio OpenLDAP.
URL: http://www.ite.educacion.es/formacion/materiales/85/cd/REDES_LINUX/frames/frameset_10.html