**. Samba + LDAP en Ubuntu 16.04**

Vamos a configurar nuestro servidor Ubuntu como Controlador Primario de Dominio en el que se puedan autenticar máquinas con Windows o Linux.

Un servidor LDAP (Lightweight Directory Access Protocol) es un servidor de datos optimizado para la realización rápida de consultas de lectura y orientado al almacenamiento de datos de usuarios a modo de directorio, nosotros emplearemos una implementación gratuita. OpenLDAP. Es algo similar a una base de datos, aunque no exactamente lo mismo. Otra implementación de LDAP es Active Directory de Microsoft.

La idea consiste en disponer de un servidor que facilite la autenticación de los clientes, de modo que éstos recurran al servidor cada vez que un usuario necesite identificarse. De esta forma, la cuenta de usuario no es específica de un equipo cliente, sino que será válida en cualquier equipo de la red que haya sido debidamente configurado.

La principal utilidad de un directorio LDAP es como servidor de autentificación para los distintos servicios de un sistema informático como puedan ser: autentificación para entrar en un PC, para entrar en una aplicación web, para acceder a un servidor ftp, para acceder a servidores de correo entrante POP3 y saliente SMTP, etc...

**¿Qué es un directorio?**

Un directorio es como una base de datos, pero en general contiene información más descriptiva y más basada en atributos.

La información contenida en un directorio normalmente se lee mucho más de lo que se escribe. Como consecuencia los directorios no implementan normalmente los complicados esquemas para transacciones o esquemas de reducción que las bases de datos utilizan para llevar a cabo actualizaciones complejas de grandes volúmenes de datos, Las actualizaciones en un directorio son usualmente cambios sencillos de todo o nada, si es que permiten algo.

Los directorios están para proporcionar una respuesta rápida a operaciones de búsqueda o consulta.

Pueden tener capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y fiabilidad, y a la vez reducir tiempo de respuesta. Cuando se duplica la información de un directorio, pueden aceptarse inconsistencias temporales entre la información que hay en las réplicas, siempre que finalmente exista una sincronización.

Hay muchas formas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de información, establecer requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados. Algunos servicios de directorios son locales, proporcionando servicios a un contexto restringido. Otros servicios son globales, proporcionando servicio en un contexto mucho más amplio.

Si en nuestra red disponemos de un servidor LDAP y configuramos todos los PCs y todos los servicios de la red para que se autentifiquen en él, bastará con crear las cuentas de usuario y grupos de usuarios en nuestro servidor LDAP para que los usuarios puedan hacer uso del sistema y de sus servicios desde cualquier puesto de la red. Es un sistema ideal para centralizar la administración de usuarios en un único lugar.

“Para simplificar la administración de los usuarios del sistema es ideal utilizar una base de datos accesible mediante LDAP. Almacenar las cuentas de usuario de forma centralizada en un único repositorio facilitará la creación, modificación y eliminación de cuentas de usuario y grupos de usuarios. Será necesario configurar los PCs de la red para que utilicen el servidor LDAP como servidor de autentificación.”

**¿Un directorio LDAP es una base de datos?**

El sistema gestor de una base de datos (Database Management System ó DBMS) de Sybase, Oracle, Informix ó Microsoft es usado para procesar peticiones (queries) ó actualizaciones a una base de datos relacional. Estas bases de datos pueden recibir cientos o miles de órdenes de inserción, modificación o borrado por segundo.

Un servidor LDAP es usado para procesar peticiones (queries) a un directorio LDAP. Pero LDAP procesa las órdenes de borrado y actualización de un modo muy lento.

En otras palabras, LDAP es un tipo de base de datos, pero no es una base de datos relacional. No está diseñada para procesar cientos o miles de cambios por minuto como los sistemas relacionales, sino para realizar lecturas de datos de forma muy eficiente.

**Funcionamiento de LDAP**

El servicio de directorio LDAP se basa en un modelo cliente-servidor.

Uno o más servidores LDAP contienen los datos que conforman el árbol de directorio LDAP o base de datos troncal, el cliente LDAP se conecta con el servidor LDAP y le hace una consulta. El servidor contesta con la respuesta correspondiente, o bien con una indicación de donde puede el cliente hallar más información. No importa con que servidor LDAP se conecte el cliente ya que siempre observará la misma vista del directorio; el nombre que se le presenta a un servidor LDAP hace referencia a la misma entrada a la que haría referencia en otro servidor LDAP

**Ventajas en el uso de LDAP**

Un directorio LDAP destaca sobre los demás tipos de bases de datos por las siguientes características:

• es muy rápido en la lectura de registros

• permite replicar el servidor de forma muy sencilla y económica

• muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente

• Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas

• Usa un sistema jerárquico de almacenamiento de información.

• Permite múltiples directorios independientes

• Funciona sobre TCP/IP y SSL

• La mayoría de aplicaciones disponen de soporte para LDAP

• La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.

Ejemplo de jerarquías

Puntos de interés

• El nombre puesto al equipo durante la instalación es: serverLDAP

• El nombre del dominio competo cualificado será: serverLDAP.aula.local

• Después de la configuración, el archivo “/etc/hosts” se modificó para que la línea quedara como: 127.0.1.1 serverLDAP.aula.local serverLDAP para asegurarnos que no hay problemas de resolución de nombres.

• El dominio LDAP es: aula.local

• Esto se traduce a Base DN de: dc=aula, dc=local

LDAP no trabaja sólo: + NSS + PAM

Éste es el método que suele utilizarse en GNU/Linux para obtener una gestión de usuarios globales similar a la que ofrecen los Servidores Windows a través de una estructura de dominios.

**¿Qué es NSS?**

NSS (Name Service Switch) es un servicio que permite la resolución de nombres de usuario y contraseñas (o grupos) mediante el acceso a diferentes orígenes de información. En condiciones normales, esta información se encuentra en los archivos locales del sistema operativo, en concreto en /etc/passwd, /etc/shadow y /etc/group, pero puede proceder de otras fuentes, como DNS (Domain Name System), NIS (Network Information Service), LDAP (Lightweight Directory Access Protocol) o WINS (Windows Internet Name Service).

Como curiosidad, podemos decir que la versión de NSS para GNU/Linux está reescrita desde cero, sin tomar ni una línea de código de la versión de Sun Microsystems.

Los primeros sistemas operativos de tipo Unix accedían directamente a los archivos de configuración o código que dependía de la forma en que se producía la autenticación. Esto hacía que cualquier cambio en el modo de autenticación obligara a cambiar el sistema operativo.

Ultrix fue el primero en ofrecer una funcionalidad muy parecida a NSS, pero fue Sun Microsystems el primero en desarrollar NSS de una forma muy parecida a como lo conocemos en la actualidad. Por lo tanto, el primer sistema operativo que incorporó NSS fue Solaris.

Poco después, se portó a diferentes sistemas operativos, como AIX, NetBSD, FreeBSD o GNU/Linux.

El objetivo de NSS es que los programas o los comandos del sistema operativo puedan manejar información administrativa relacionada con los usuarios, las contraseñas y los grupos (incluidos aspectos como la caducidad de una contraseña o su nivel de complejidad) sin tener que conocer el lugar donde se encuentran almacenados.

**¿Qué es PAM?**

PAM (Pluggable Authentication Modules) establece una interfaz entre los programas de usuario y distintos métodos de autenticación. De esta forma, el método de autenticación se hace transparente para los programas.

Como ocurrió con NSS, PAM surgió en Sun Microsystems, aunque, en este caso, como una propuesta a la Open Software Foundation. Fue Red Hat quien lo desarrolló como una herramienta de Software libre y lo incorporó por primera vez a la versión 3.0.4 de su sistema operativo en 1996.

La idea se basa en la creación de módulos de autenticación reemplazables, de forma que sea transparente para el sistema el uso de distintos métodos de autenticación. Esto hace que, sin realizar modificaciones en el sistema, podamos utilizar métodos que vayan desde el uso típico de un nombre de usuario y una contraseña, hasta dispositivos que faciliten la identificación biométrica de los usuarios (lectores de huellas, de voz, de imagen, etc.). Incluso incorpora opciones para aceptar contraseñas de un solo uso, restringir el acceso a determinados horarios o establecer políticas de autenticación específicas para cada usuario o grupos de usuarios.

Básicamente, PAM complementa en algunos aspectos el funcionamiento de NSS ya que mientras éste se centra en la búsqueda y mapeo de los usuarios, PAM controla la autenticación, el inicio de sesión y su configuración.

En la actualidad, PAM es el método que utilizan la mayoría de las aplicaciones y herramientas de GNU/Linux que necesitan relacionarse, de algún modo, con la autenticación de los usuarios.