¿Es OPENLDAP una buena solución libre para la centralización de usuarios?

Tatiana Marcela Gómez Sarmiento[1], María Alejandra Morera González[2], Aura María Muñoz Moreno[3] and Claudia Patricia Santiago Cely[4]

[1]*Estudiante de Ingeniería de sistemas de la Escuela Colombiana de Ingeniería Julio Garavito, Colombia, tatiana.gomez-s@mail.escuelaing.edu.co*

[2]*Estudiante de Ingeniería de sistemas de la Escuela Colombiana de Ingeniería Julio Garavito, Colombia, maria.morera@mail.escuelaing.edu.co*

[3]*Estudiante de Ingeniería de sistemas de la Escuela Colombiana de Ingeniería Julio Garavito, Colombia, aura.munoz@mail.escuelaing.edu.co*

[4]*Ingeniera, profesora de la Escuela Colombiana de Ingeniería Julio Garavito, Colombia, claudia.santiago@escuelaing.edu.co*

Abstract– This article establishes the state of the art about existing solutions in the market, free or licensed that allow the centralization of users, independent to the operating system they use (OS X, Windows, Linux); all of the above in a context of authorization and user authentication (AAA). There is an analysis of the use of the OpenLDAP platform as a mechanism for centralizing users, their advantages and limitations, the presentation of a design, and recommendations based on the implementation of the system in a heterogeneous infrastructure with more than three hundred (300) members.

Keywords-- Operating Systems, AAA, centralizing users, OpenLDAP, centralization, free software.

Resumen– En este artículo se propone el estado del arte acerca de las soluciones existentes en el mercado, tanto libres como licenciadas que permiten la centralización de usuarios en una organización independiente del sistema operativo que utilicen (OS X, Windows, Linux); todo esto en el marco de la autorización y autenticación de usuarios (AAA) . Se analiza la utilización de la plataforma OpenLDAP como mecanismo de centralización de usuarios, sus ventajas y limitaciones, se presenta un diseño y recomendaciones de uso basado en la implantación del sistema en una infraestructura heterogénea con más de trecientos (300) usuarios.

Palabras claves-- Sistemas Operativos, AAA, centralización de usuarios, OpenLDAP, centralización, software libre.

I. INTRODUCCIÓN

En el entorno tecnológico en el que hoy nos encontramos inmersos, el uso de diferentes sistemas operativos es una actividad muy común en empresas y entidades académicas como universidades y colegios; ahora esto puede generar un mayor trabajo en la administración de los usuarios, lo que incluirá la creación, mantenimiento, modificación e inclusive en algunos casos la eliminación de las cuentas en cada sistema. Tener un sistema centralizado de administración de usuarios que involucre varios sistemas operativos es la solución más utilizada y muchos proveedores han puesto a disponibilidad de las empresas sus ofertas con software que implementa la centralización de usuarios.

Estas situaciones, en la mayoría de los casos, tienen un costo importante asignado al licenciamiento; sin embargo este proyecto tiene como objetivo evaluar una solución de software libre que permita dar respuesta a la problemática de autenticación y autorización de usuarios, incluyendo sus ventajas y limitaciones.

En principio se presenta brevemente la metodología de investigación empleada a lo largo del desarrollo del proyecto. Luego se presenta un marco teórico con el fin de entrar en contexto frente a los diferentes términos que se utilizarán en el artículo, seguido de la presentación del entorno de aplicación, en el cual se evidencia la problemática y propuesta de solución planteada; finalmente con toda la información obtenida se concluye y presentan recomendaciones para tratar el tema de la centralización de la autenticación y autorización de usuarios.

II. MARCO TEÓRICO

Al hablar de administración de usuarios es importante tener en cuenta que esto implica como mínimo la autenticación y la autorización de los mismos[1]. El proceso de autenticación servirá para verificar la identidad de los usuarios mediante diferentes técnicas que generalmente están relacionada con lo que el usuario sabe, lo que el usuario tiene y lo que el usuario es. Por otra parte la autorización hace referencia a la gestión del proceso encargado de conceder los privilegios con los que cuenta cada usuario de acuerdo a un perfil definido, y por lo general especificados por el administrador del sistema. Esta administración se puede

[1] *Dentro de la administración usualmente también se incluye el registro o contabilización de las actividades de los usuarios, con lo cual se completa la triada AAA (Authentication, autorization and Accounting) sigla muy utilizada en este tema. Lo referente a registro, no fue objeto de revisión de éste proyecto.*

hacer de manera distribuida o de manera centralizada, la primera implicará realizar los procesos de autenticación y autorización en cada sistema de forma independiente; en la centralizada, estos procesos se realizarán en un sitio central lo cual traerá; ventajas tanto para el usuario del proceso de autenticación como para el administrador del mismo.

Ahora, el problema de la administración de usuario ha sido estudiado por varios años y existen estándares internacionales que han sido definidos sobre este tema. Es tal el caso del conjunto de recomendaciones X.500 | ISO 9594- Information technology - Open Systems Interconnection - The Directory, es un estándar para solucionar el problema de directorios; contiene partes enfocadas a la definición los modelos de cómo debe estar organizada la información, el modelo de información de usuario, el modelo de información administrativa y el servicio de directorio, que define como debe estar distribuida la información entre varios sistemas, también contiene el estándar de autentificación y seguridad usado para SSL, indicaciones de cómo debe ser la replicación entre sistemas [1]. El estándar X.500 es un servicio de directorio que contiene información de forma jerárquica y categorizada, que puede incluir nombres, directorios y números telefónicos; una de la ventajas más importantes que del X.500 es consolidar en un repositorio central toda la información de la organización. Posterior a estas recomendaciones, aparece LDAP (Lightweight Directory Access Protocol / Protocolo de acceso a directorios ligero) es un protocolo pensado para actualización y búsquedas de directorios orientados a Internet (TCP/IP) [2]. Por esta razón, a veces se habla de LDAP como "X.500 Lite."

Basado en dicho estándar, varios proveedores de tecnologías han presentado sus implementación, entre las cuales se encuentra Directorio Activo (DA) de Microsoft, el cual brinda una infraestructura organizada de almacenamiento de datos de usuarios y también, de ordenadores, impresoras y otros periféricos, que se administran de forma centralizada; dicha estructura permite al usuario disponer de espacio de almacenamiento externo a su equipo, así como acceder a los dispositivos periféricos incluidos en el DA. Por otro lado, en el mundo del software libre se han creado propuestas para el manejo centralizado de usuarios como FreeIPA y 389 Directory Server de Red Hat bajo una licencia GPL(General Public License / Licencia Pública General) . Este tipo de software ofrece a los usuarios independencia como lo es ejecutar el programa para cualquier propósito, libertad de estudiar la manera en la que el programa funciona, libertad de mejorar el programa y distribuir mejoras al público, finalmente da la libertad de redistribuir copias del programa [3]; sin embargo es válido aclarar que decir software libre no es decir “gratis”, pues requiere de profesionales especializados para su desarrollo, configuración y mantenimiento. Aquel software que requiere un pago por licenciamiento es llamado software pago, para mencionar alguno de ellos, hablaremos del DA de Microsoft que es una reconocida implementación del protocolo LDAP. Un ejemplo de software libre para administración centralizada de usuarios es OpenLDAP, es una implementación de Linux y del cual se hablará más adelante.

III. METODOLOGÍA DE INVESTIGACIÓN

A. Evaluación de implementaciones LDAP.

Se recolectó información acerca de las diferente implementación del protocolo LDAP, a dicha información se le aplicaron los siguientes criterios: desarrollador, versión, fecha de la última versión, si es o no código abierto, plataformas que los soportan, nivel de seguridad y rendimiento, con el fin de elegir la opción más destacada.

B. Lectura de artículos.

Se revisó en la diferentes bases de datos a las cuales tenemos acceso por pertenecer a la Universidad y en otras que son de libre acceso , artículos relacionados con temas como la centralización de usuarios , implementaciones LDAPs, sistemas de autorización y autenticación en los sistemas operativos OS X, Linux y Windows .

C. Indagar en otras Universidades en Bogotá.

Se contactó a la Universidad de los Andes y a la Universidad Minuto de Dios para saber cómo se llevaba a cabo en cada universidad el proceso de autorización y autenticación de usuarios sin importar el sistema operativo en el que se encuentre el usuario; dicha información fue de gran ayuda para el desarrollo de la solución planteada.

D. Lectura de otros proyectos relacionados.

El problema que se plantea en este artículo no es un problema nuevo , que muy seguramente tiempo atrás se ha tratado de solucionar, es por eso que recolectamos información acerca de los proyectos relacionados y con base en estos se tomaron algunas decisiones y se llegaron a algunas conclusiones de las que hablaremos en detalle más adelante .

E. Implementación

Inicialmente se implementó OpenLDAP en Linux sobre la distribución Ubuntu 14.04 LTS, pero la solución definitiva se implementará en la distribución Slackware 14.1, acompañada de una serie de pruebas en Linux, Windows y OS X.

IV. ENTORNO DE APLICACIÓN

El entorno de aplicación definido por el proyecto consiste en un centro de cómputo, en el cual los usuarios realizan procesos de autenticación bajo tres sistemas operativos Windows, Linux y OS X, utilizando el mecanismo de usuario / clave.

En este centro de cómputo se quiere centralizar el proceso de autenticación de usuarios y su respectiva autorización de servicios a todos los servidores que desde allí se administran. Tanto los equipos clientes como los servidores podrán tener instalados diferentes sistemas operativos (Windows, Linux o OS X). Y el servidor de autenticación estará operando desde una máquina Linux con distribución Slackware.

Es válido aclarar que la problemática y propuesta de solución proyectadas más adelante no se limita para los centros de cómputo, ésta podría extrapolarse para otros ambientes con problemáticas similares de centralización de la gestión de usuarios.

A. Problemática

En muchas entidades la administración de los usuarios está implementada mediante sistemas de autenticación independientes por cada sistema operativo que allí se maneje, dicha independencia va generando progresivamente a través del tiempo dificultades en el manejo por parte de los usuarios del sistema y el administrador de los mismos, desde la perspectiva del usuario, se tiene claves y usuarios distintos, y desde la perspectiva del administrador, la creación de un nuevo usuario depende del número de servidores con los que se cuenten.

Actualmente existen soluciones comerciales que resuelven en una gran medida el problema, pero ¿Qué pasa con las organizaciones que no cuentan con el dinero suficiente para comprar el licenciamiento? o ¿Qué pasa con la plataforma tecnológica que tienen configurada, las soluciones comerciales son una opción?

Lo planteado anteriormente postula un ideal del querer implantar un sistema centralizado de autenticación en donde todos los usuarios y sistemas se direccionen a un sistema central y sea éste quien autorice el ingreso a la infraestructura de la organización según un perfil definido.

B. Propuesta de solución

Después de realizar una revisión de diferentes alternativas de software libre en las que se incluyeron soluciones como FreeIPA y 389 Directory Server de Red Hat la opción destacada de implementaciones LDAP, fue la de OpenLDAP, esta alternativa tiene las siguientes ventajas: es código abierto, las plataformas que lo soportan son las más usadas en el mercado (Linux, Windows BSD, HP-UX, Solaris, Mac, AIX, Solaris, Microsoft Windows), el nivel de seguridad junto con el de rendimiento es bueno y ofrece la opción de mejorarlo.

Para evidenciar de forma más detallada la propuesta de solución, lo dividiremos en los siguientes seis ítems.

1) Montaje

En el montaje se hace referencia a la infraestructura física y de software con las características propias de los dispositivos involucrados, y para lo cual se deben tener en cuenta estos aspectos:

- Definir las características del equipo para realizar el montaje del servidor y del cliente.
- Definir que distribución de Linux se va usar como sistema operativo.
- Escoger bajo que versión de OpenLDAP se va trabajar, sin embargo se sugiere utilizar la última versión.
- Diseñar la estructura de directorio que a lo largo del artículo la llamaremos árbol, en donde se deben diferenciar los perfiles de usuario; cada perfil de usuario se distingue por los permisos y sistemas a los que tiene acceso.

Una vez analizados los aspectos anteriores, procedemos a plantear nuestro montaje; el cual se detalla así:

- Se utilizaron computadores con sistemas operativos Windows 8.1 y Linux Ubuntu.
- Distribución Linux: Ubuntu; versión: 14.04 LTS, en la cual se realizó la configuración del LDAP elegido.
- OpenLDAP versión 2.4.40 que frente a las demás versiones tiene la ventaja de poder borrar y modificar los elementos del árbol, con el servicio funcionando.
- SAMBA versión 4.2 que permite validar usuarios Windows haciendo de Controlador Principal de Dominio (PDC).
- En la imagen 1, presentamos un bosquejo del árbol general diseñado y utilizado en la configuración.

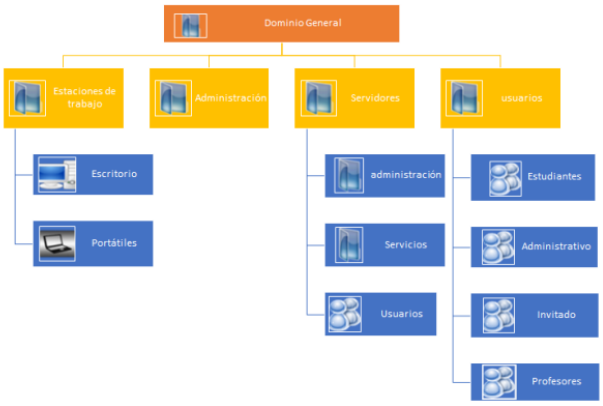

Imagen 1. Árbol de autorizaciones.

1.1. Montaje servidor:

1.1.1. Proceso de instalación de OpenLDAP

- Instalar el paquete *slapd ldap-utils* para la administración de LDAP.

1.1.2. Configuración básica de OpenLDAP

- Se define el dominio, nombre de la organización, contraseña del servido LDAP, motor de base de datos HDB ya que permite renombrar subárboles en caso que se requiera.
- Establecer autenticación de clientes Linux: configuración del PAM (Pluggable Authentication Modules) que proporciona soporte de autenticación dinámica a servicios y aplicaciones Linux y el NSS(Name Service Switch) que provee una interfaz que permite configurar y acceder a diferentes bases de datos de cuentas de usuarios y claves.
- Crear la estructura del directorio: se crea la estructura jerárquica del árbol en un archivo con extensión ***.ldif***.
- Añadir un usuario y un grupo a través del comando *sudo ldapadd -x -D cn=nombre de usuario, dc=Dominio -W -f archivo extensión .ldif.*
- Probar las configuraciones anteriores a través del comando *ldapsearch* que permite hacer una búsqueda en el directorio.
- Instalar *PhpLdapAdmin* para administrar LDAP con una interfaz web: definir datos de autenticación.

1.1.3. Proceso de instalación de SAMBA

Samba, es una implementación libre del protocolo SMB, que permite compartir archivos entre Windows y Linux.

- Instalar los siguientes paquetes samba, samba-doc, smbldap-tools para integrar SAMBA con LDAP.

1.1.4. Configuración básica de SAMBA

- Copiar y descomprimir el archivo samba.schema.gz en el directorio /etc/ldap/schema.
- Crear un directorio de salida agregando el archivo descomprimido anteriormente.
- Crear el archivo *samba.ldif* que permitirá reconocer el dominio para lograr la conexión con LDAP.
- Configurar el archivo *smb.conf* para el uso de LDAP.
- Editar el archivo de configuración *smbldap_bind.conf* para especificar las operaciones de administración y grupos del servidor LDAP.
- En el archivo *smbldap.conf* se editarán los parámetros para el dominio samba y para la especificación del servidor LDAP.

1.2. Montaje cliente

1.2.1. Linux y OS X:

- Realizar la configuración como cliente: se define contraseñas e IP del servidor OpenLDAP, se modifica el archivo *ldap.conf* del cliente.
- Actualizar NSS y configurar PAM para que utilicen LDAP.
- Comprobar que funciona iniciando sesión con un usuario creado en servidor LDAP.

1.2.2. Windows:

- Configurar el dominio de la máquina agregándola al dominio LDAP.
- Reiniciar máquina.
- Iniciar sesión con un usuario del servidor LDAP.

2) Problemas

- Instalación de los paquetes relacionados con Open LDAP tales como slapd ldap-utils y slapd-config varias veces porque no funciona.
- Configuración del servidor LDAP varias veces por errores de definición de las variables y parámetros de los archivos de configuración LDAP y Samba.
- La búsqueda de los archivos de configuración es bastante tediosa, pues la documentación encontrada por lo general no está alineada con la última actualización del archivo, dejándolo en una ruta o con argumentos de configuración muy distintos.

3) Aspectos críticos

- Integración de SAMBA con el servidor LDAP, pues se debe alinear el proceso de autenticación que se lleva en el servidor SAMBA y unirlo al de Open Ldap, y así tener archivos de configuración integrados.
- Configuración de los mismos permisos para los clientes Linux, Windows y OS X.
- Configuración para que un cliente Windows se pueda autorizar mediante un servidor Linux.
- Lograr la configuración equivalente hecha en la Ubuntu para Slackware.

4) Diseño

Es necesario tener claro el mapa de autorizaciones que se va a configurar en el directorio, en donde se plantean perfiles y permisos de los usuarios del sistema. Además, es importante que dicho mapa sea escalable.

5) Pruebas.

El sistema centralizado propuesto e implantado debe autenticar y autorizar a los usuarios que se conectan a través de cualquier sistema operativo sin discriminación alguna, para la realización de pruebas se tuvieron en cuenta las políticas de cada sistema operativo.

V. CONCLUSIONES

El propósito de la investigación fue evaluar una solución de software libre que permitiera solucionar la problemática de la autenticación y autorización de usuarios, para lo cual se realizaron diferentes pruebas lo que permite concluir los siguientes resultados:

1. La implementación del servicio no tiene limitaciones para el tipo de empresa, puede ser implantado en cualquier área de la organización siempre y cuando le sea útil.
2. Aunque la solución se propone mediante un software libre, esto no implica que no exista ninguna inversión, ya que el mantenimiento del software es un costo.
3. Es importante hacer la instalación y configuración del dominio SAMBA para poder realizar la comunicación entre el servidor LDAP y un cliente Windows.
4. La organización al momento de ubicar los archivos de configuración y posterior sincronización de datos es vital para detectar errores de configuración y realizar ajustes de requerimientos.
5. El dominio OpenLDAP y el dominio SAMBA pueden ser nombrados de manera diferente, sin embargo para efectos de unificación se nombran de la misma manera.
6. LDAP es un modelo cliente-servidor, jerárquico con directorios y flexible, que permite administrar y gestionar toda la información de una máquina, permitiendo políticas de administración usando un directorio OpenLDAP para almacenar información de servidores y clientes.
7. Se ha presentado el diseño, la configuración de un servicio y dificultades que permiten centralizar la información como alternativa de control de acceso en usuarios en Linux usando LDAP.

REFERENCIAS

[1] ITU, «ITU INTERNATIONAL TELECOMMUCATION UNION,» 14 MAYO 2014. [En línea]. Available: http://www.itu.int/rec/T-REC-X.501/e. [Último acceso: 14 FEBRERO 2015].

[2] E. B. Alejandro, «Administración de Sistemas con GOsa,» 28 MARZO 2005. [En línea]. Available: http://warping.sourceforge.net/gosa/manual_gosa_es/node9.html. [Último acceso: 14 FEBRERO 2015].

[3] «BLOG AZLEK,» 08 ENERO 2013. [En línea]. Available: http://aztlek.org/2013/01/08/una-propuesta-para-afrontar-la-crisis-de-la-carrera-de-ingenieria-de-sistemas/. [Último acceso: 02 FEBRERO 2015].

[4] FUNDACIÓN WIKIPEDIA, INC, «WIKIPEDIA,» 23 ENERO 2015. [En línea]. Available: http://es.wikipedia.org/wiki/Autenticaci%C3%B3n. [Último acceso: 28 ENERO 2015].

[5] FUNDATION WIKIPEDIA, «WIKIPEDIA,» 08 DICIEMBRE 2014. [En línea]. Available: http://es.wikipedia.org/wiki/Autorizaci%C3%B3n. [Último acceso: 28 ENERO 2015].

[6] FUNDATION WIKIPEDIA, INC, «WIKIPEDIA,» 20 DICIEMBRE 2014. [En línea]. Available: http://es.wikipedia.org/wiki/Protocolo_AAA. [Último acceso: 01 FEBRERO 2015].

[7] TECNET MAGAZINE, 2015. [En línea]. Available: https://technet.microsoft.com/es-es/magazine/2008.12.linux.aspx. [Último acceso: 30 ENERO 2015].

[8] UNIVERSIDAD AUTONOMA DE MADRID, 2008. [En línea]. Available: http://www.uam.es/ss/Satellite/es/1234886352083/1242648930754/servicioti/ServicioTI/Directorio_Activo_(DA).htm. [Último acceso: 30 ENRO 2015].

[9] FUNDATION WIKIPEDIA, INC, «WIKIPEDIA,» 03 FEBRERO 2015. [En línea]. Available: http://es.wikipedia.org/wiki/Sistema_operativo. [Último acceso: 30 ENERO 2015].

[10] «DEFINICION.DE,» 2008 - 2015. [En línea]. Available: http://definicion.de/centralizacion/. [Último acceso: 02 FEBRERO 2015].

[11] «THE FREE DICTIONARY,» 2007. [En línea]. Available: http://es.thefreedictionary.com/centralizar. [Último acceso: 02 FEBRERO 2015].

[12] «WIKIPEDIA,» 29 ENERO 2015. [En línea]. Available: http://es.wikipedia.org/wiki/Software_libre. [Último acceso: 02 FEBRERO 2015].

[13] Ubuntu.com, «Ubuntu Documentation,» Ubuntu.com, 2012. [En línea]. Available: https://help.ubuntu.com/14.04/serverguide/samba-ldap.html#samba-ldap-samba-configuration. [Último acceso: 04 03 2015].

[14] M. J. Armando, «Configurar un servidor Controlador de Dominio con Samba y OpenLDAP en Ubuntu,» 2011. [En línea]. Available: http://tuxjm.net/docs/Configurar_Servidor_Controlador_de_Dominio_con_Samba_y_OpenLDAP/Ubuntu/html-multiples/caracteristicas-de-la-implementacion.html. [Último acceso: 02 03 2015].

[15] J. Palka y I. Motyl, «USE OF ACTIVE DIRECTORY IN SECURING THE CLIENT APPLICATIONS.,» de *Annals of DAAAM & Proceedings . 2010, p407-408. 2p. 1 Diagram.*, 2010.