FACULTAD DE CIENCIAS DEL HOMBRE Y LA NATURALEZA

Tema:

“Sistema centralizado de contraseñas con OpenLDAP”

Asignatura:

Sistema Operativo de Redes.

Docente:

Lic. Irwin Guardado

No.	ESTUDIANTE	CARNET	PARTICIPACIÓN
1	Arturo Angel Miguel Mena	MM01134391	100%
2	Javier Edgardo Hernández Salinas	HS01134092	100%
3	Karla Maricela Rodríguez Orellana	RO01134088	100%

San Salvador, 06 de junio de 2019.

Indice

Resumen (Abstract) 3
PALABRAS CLAVES 4
INTRODUCCIÓN 5
OBJETIVOS 6
1. MARCO TEÓRICO 7
LISTA DE ACTIVIDADES LLEVADAS A CABO PARA LA REALIZACIÓN DEL PROYECTO 15
DIAGRAMA DE GANTT 16
COMPARATIVA DE OPENLDAP CON NOVELL DIRECTORY SERVICE 18
Factibilidad Económica 19
RESULTADOS 20
CONCLUSIÓN 21
RECOMENDACIONES 22
BIBLIOGRAFÍA 23
ANEXO 24

Índice de ilustraciones

Ilustración 1: Esquema de consulta 11
Ilustración 2: Proceso de autenficacion 13
Ilustración 3: Diagrama de actividades para Implementacion de proyecto sistema centralizado de contraseñas con OpenLDAP 18

Resumen (Abstract).

Este documento constituye una guía para el diseño e implantación de un sistema de autenticación centralizada basado en OpenLDAP en entornos de red típicos de sistemas informáticos de universidades o grandes empresas. Estos entornos se caracterizan por tener un gran número de usuarios a los que debe dar una serie de servicios de red (moodle, correo electrónico, FTP. . .), así como posibilitar el acceso identificado a cuentas de usuario tradicionales. En concreto, El propósito de este artículo es sugerir una posible solución al inconveniente que, en el mundo actual, pero en especial las organizaciones actuales, los usuarios deben dar pruebas de quiénes son para así verificar si pueden acceder a cierto tipo de información de la compañía, universidades, colegios etc. Hay archivos, datos, documentos, gráficos y otros "secretos" que sólo ciertas personas privilegiadas pueden conocer. El problema radica en que, en la mayoría de los casos, los usuarios deben usar tantos mecanismos de autenticación como sistemas de información, lo cual es bueno para mantener fuera a los invasores, pero bastante incómodo y laborioso para los autorizados. Y con esto se pretende minimizar la cantidad de claves que se deben utilizar sin minimizar la seguridad que se les brinda a los sistemas de información.

PALABRAS CLAVES.

- uid (user id): Identificación única de la entrada en el árbol.
- objectClass: Indica el tipo de objeto al que pertenece la entrada.
- cn (common name): Nombre de la persona representada en el objeto.
- givenname: Nombre de pila.
- sn (surname): Apellido de la persona.
- o (organization): Entidad a la que pertenece la persona.
- u (organizational unit): El departamento en el que trabaja la persona.
- mail: dirección de correo electrónico de la persona.
- Seguridad: proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente.
- control de acceso: consiste en la autenticación, autorización de acceso y auditoría. Una definición más estrecha de control de acceso abarcaría únicamente la aprobación de acceso, por lo que el sistema adopta la decisión de conceder o rechazar una solicitud de acceso de un sujeto ya autenticado, sobre la base a lo que el sujeto está autorizado a acceder.
- Autenticación es el proceso que debe seguir un usuario para tener acceso a los recursos de un sistema o de una red de computadores. Este proceso implica identificación (decirle al sistema quién es) y autenticación (demostrar que el usuario es quien dice ser). La autenticación por sí sola no verifica derechos de acceso del usuario; estos se confirman en el proceso de autorización.
- Hosts: El término host o anfitrión se usa en informática para referirse a las computadoras u otros dispositivos conectados a una red que proveen y utilizan servicios de ella. Los usuarios deben utilizar anfitriones para tener acceso a la red.
- Protocolo: Un protocolo de red designa el conjunto de reglas que rigen el intercambio de información a través de una red de computadoras.
- Servidor: Un servidor es una computadora que maneja peticiones de data, email, servicios de redes y transferencia de archivos de otras computadoras (clientes).

INTRODUCCIÓN

En la actualidad la seguridad se h vuelto indispensable debido a la cantidad de información que se maneja en línea y es por eso que todas las aplicaciones toman sus medidas para garantizar que su servicio no sea violentado y darle mal uso a esa información y por tal razón las aplicaciones exigen que el usuario que necesita acceder a ellos demuestre su identidad, normalmente mediante la introducción de un nombre de usuario y una clave secreta. Puede tratarse de servicios restringidos a determinados colectivos o del acceso a información privada del propio usuario (como ficheros o mensajes de correo electrónico). La información que almacena el sistema sobre los usuarios y las claves permitidas puede estar en el ordenador al que se accede para obtener el servicio, o residir en un sistema distribuido en el cual todos los sistemas comparten copias de esa misma información; puede existir un repositorio central al que los sistemas consulten la validez de la información de autenticación aportada por el usuario, etc. Con la tendencia actual de que no exista un gran ordenador central que proporcione todos los servicios, sino que estos sean aportados por una serie de ordenadores especializados (por razones de coste, fiabilidad al poder replicar los servicios, etc.), así como la variedad de servicios que actualmente se proporcionan (cuentas interactivas en los ordenadores, correo electrónico, acceso a páginas web restringidas, etc.), es especialmente importante implantar un modelo de información sobre datos de identidad de los usuarios que pueda ser accesible desde todos ellos. Este modelo de información deberá tener una gran fiabilidad y estabilidad y deberá ser fácil de gestionar. El uso de los servidores de directorio apoyados en la tecnología LDAP para cumplir estos objetivos es cada vez más generalizado.

En nuestro proyecto se demuestra como es su funcionamiento ya que lo hemos instalado en un hosting virtual, donde se ha instalado OpenLdap que es la versión gratuita de Ldap y para conocer su configuración lo hemos enlazado con Moodle; plataforma educativa, y como aporte ofrecemos un video tutorial como manuales de programador y usuario.

OBJETIVOS

Objetivo General.

- Implementar un servidor de autenticación configurado en un sistema operativo LINUX utilizando la herramienta Open LDAP.

Objetivos Específicos.

- Definir qué es un directorio activo LDAP.
- Nombrar los diferentes tipos de directorios activos.
- Explicar el funcionamiento de un servidor LDAP.
- Señalar las características de operación de la herramienta Open LDAP.
- Configurar un servidor con Open LDAP.

1. MARCO TEÓRICO

La presencia de servidores centralizados en el entorno de las empresas se ha convertido en algo natural desde años atrás y se trata de un factor que toda gran firma debe tener en cuenta por una serie de buenos motivos. De forma derivada, contar con estos servidores implica disponer en plantilla de un especialista en administración de sistemas que se ocupe de su correcta supervisión.

Estos servidores cubren necesidades de todo tipo de empresas relacionadas con la informática y la tecnología. Uno de los aspectos que se encargan de potenciar es la seguridad en el entorno informático de la empresa. El administrador de sistemas tiene la posibilidad de gestionar registro de usuarios y contraseñas de forma absolutamente personalizada para que siempre exista el mayor nivel de seguridad.

Un servidor centralizado se ocupa de conectar a todos los usuarios de la red de la empresa a través de su sistema. Esto también implica que los usuarios dependen de estos servidores centralizados y que se apoyan en ellos a nivel técnico. Para la empresa supone tener más controlados a los usuarios y minimizar al máximo la cantidad de registros y de accesos distintos que se realizan en su entorno. Al mismo tiempo, el control desde los servidores centralizados también se aplica a los propios ordenadores. Para una empresa es muy útil a la hora de crear una imagen más corporativa, dado que se puede influir, por ejemplo, en el contenido con el que se encuentran los usuarios de la red al encender sus equipos.

Además de ser seguro, el sistema que proporciona un servidor centralizado aumenta la comodidad. Esto se debe a que se crea una red absolutamente segura y privada a la cual solo tienen acceso los usuarios de la red y, por lo tanto, los de la empresa. Este acceso es configurable y da opción a compartir archivos y documentos, creando un fondo de almacenamiento al que pueden acceder todos los usuarios a fin de compartir elementos sin depender de procesos de envío más lentos como el correo electrónico.

QUE ES AUTENTICACION

Autenticación se refiere al proceso por medio del cual un usuario de una red adquiere el derecho a usar una identidad dentro de la dicha red. Hay maneras de autenticar un usuario, como el uso de claves, Biométricos, smart cards, certificados digitales. La ventaja es que la identidad del usuario en la red no necesariamente tiene que ser igual al nombre de la persona. Una misma persona puede tener muchas identidades virtuales y vise versa.

Existen tres tipos de autenticación:

a. Autenticación por conocimiento específico: El nombre de mi mamá, la clave del cajero, una palabra clave, etc.

b. Autenticación por posesión: Una tarjeta inteligente.

c. Autenticación por identidad: La huella digital, la retina, la voz, u otras características físicas.

EL RETO

En la actualidad cada sistema operativo tiene su propia forma de autenticar. Lo mismo ocurre con las aplicaciones y sistemas de información que tienen las organizaciones. Esto hace que el usuario final se vea obligado a usar varias formas diferentes de autenticación, con nombres de usuarios y claves o llaves distintas, lo cual hace difícil, confuso e inseguro el acceso a estos sistemas, debido a que en muchos casos las personas tienden a usar claves fáciles o lo que es peor, anotar las claves y dejarlas encima del computador, en la billetera o en otro lugar donde no sólo lo puede encontrar el dueño, sino cualquiera.

El reto es lograr que el usuario tenga una única clave, la cual le sirva para ingresar a todos los servicios logrando una mayor seguridad en los sistemas y aplicaciones; para lograr esto es necesario acudir a una arquitectura de autenticación centralizada.

QUE ES AUTENTICACION CENTRALIZADA

Existen dos modelos de autenticación uno descentralizado y otro centralizado. En el modelo descentralizado, cada servicio de la red maneja sus claves de forma independiente, por ejemplo los usuarios de Oracle, los usuarios de un firewall, los administradores de un sitio Web; cada uno de estas aplicaciones maneja por separado sus claves y las mimas no son compartidas.

En la autenticación centralizada los usuarios y sus claves se ubican en un repositorio central, las diferentes aplicaciones se configuran para identificar este lugar y hacer la autenticación contra el repositorio. Para nuestro caso las claves estarán ubicadas dentro de un servidor de directorio LDAP, pero en general podrían estar almacenadas en un archivo de texto plano o en una base de datos relacional entre otros métodos de almacenamiento de información.

Lightweight Directory Access Protocol (LDAP)

Es un protocolo cliente servidor hecho para acceder a un servicio de directorio en el modelo TCP/IP. Está basado en el protocolo X.500 un protocolo estándar para los servicios de directorio en el modelo OSI.

Un directorio LDAP es similar a una base de datos, pero tiende a contener información más descriptiva. La información en un directorio es consultada muchas más veces de lo que es modificada; como consecuencia, los directorios no tienen esquemas de "roll-back" que las bases de datos usan por el alto-volumen de actualizaciones. Las actualizaciones del directorio son típicamente simples cambia todo o nada.

Los directorios pueden ser afinados para dar una contestación rápida a las búsquedas de grandes volúmenes de datos. Ellos pueden tener la habilidad de replicar la información en varios sitios para aumentar la disponibilidad y la confiabilidad, mientras se mantiene un tiempo mínimo en la contestación.

COMO TRABAJA LDAP

El servicio de directorio LDAP se basa en una arquitectura cliente servidor, uno o más servidores de LDAP contienen los datos que forman el árbol de directorio. Como se observa en la figura 1, un cliente se conecta con un servidor LDAP y le hace una pregunta, el servidor responde con la información o con un apuntador indicando donde el cliente puede conseguir más información (típicamente, otro servidor de LDAP). No importa la forma en que un cliente se conecte a un servidor LDAP, siempre la información se ve de la misma forma. Éste es un rasgo importante de un servicio de directorio global como LDAP.

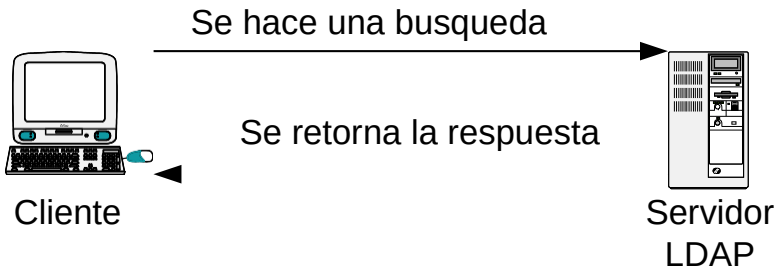

Ilustración 1: Esquema de consulta

CARACTERISTICAS DE LOS DIRECTORIOS LDAP

A continuación se enumeraran algunas de las características principales de los directorios LDAP.

A) Dinámicos

Los directorios con los que estamos familiarizados son relativamente estáticos, esto se debe a que no cambian muy frecuentemente, por ejemplo el directorio telefónico cambia una vez al año, la guía de

Televisión todas las semanas, los catálogos de las tiendas varias veces al año, entre otros ejemplos; pero se observa que todos ellos cambian la información día a día con lo cual los datos se vuelven obsoletos.

En contraste observamos que los directorios en línea tienen la capacidad de estar mucho más actualizados, usualmente es una capacidad que no siempre se usa, algunas veces los administradores utilizan procedimientos automáticos para mantener al día los datos.

Usando esta capacidad de mantenerse actualizados podemos ver como un servicio de autenticación puede ser usado, para autorizar el acceso a las aplicaciones de una compañía, ya que si tiene la información de los empleados al día podrá saber cuando un empleado se retiro y por lo tanto no dejarlo acceder a la aplicación, todo esto simplemente manteniéndolo sincronizado con la aplicación de la oficina de Recursos Humanos.

B) Flexibles

Otra importante característica de los directorios es la gran flexibilidad que permiten, esta flexibilidad se ve en dos aspectos, primero pueden almacenar varios tipos de información y segundo la forma en que puede ser almacenada y buscada la información.

Los directorios "on-line" pueden almacenar diferentes tipos de información ya que a diferencia de los estáticos pueden ser fácilmente extendidos generalmente sin recurrir en costos adiciones, por ejemplo la reimpresión; el costo de añadir información es, simplemente el del tiempo en que demore en introducirse los datos al sistema y del almacenamiento de los mismos.

Los directorios "on-line" son flexibles pues se puede buscar la misma información de diferentes maneras, por ejemplo en el directorio telefónico solo se puede buscar la información por nombres mientras que en los directorios electrónicos se puede hacer también por dirección, numero telefónico e inclusive por partes del mismo nombre.

C) Seguros

Los directorios tradicionales no ofrecen ninguna seguridad, ya que una vez son adquiridos se puede

acceder a toda la información que está contenida en ellos, mientras en un directorio "on-line" el administrador puede decidir hasta que punto un usuario puede consultar cierta información.

D) Personalizados

Otra diferencia entre los directorios tradiciones y los "on-line" es en que en los segundos puedo colocar o no información relevante y no relevante para la organización y el aspecto o diseño con el cual se desea mostrar la información.

IMPLEMENTACIONES DE SERVICIOS DE DIRECTORIOS LDAP

Existen varias implementaciones de directorios LDAP algunas implementaciones se ajustan más al estándar mientras otras buscando más flexibilidad se alejan un poco del este, pero siempre buscando el mejor desempeño para las funcionalidades que se implementaran sobre los directorios.

Algunas de las implementaciones más conocidas son: Novell Directory Service, Openldap, Iplanet Directory Service y Microsoft Active Directory.

SERVICIOS DE AUTENTICACION

Los servicios de autenticación son herramientas que me permite verificar la identidad de un usuario o servicio, esto lo hacen intercambiando de manera segura la información entre un cliente y un servidor, el cual a su vez se convierte en un cliente del servidor LDAP donde están almacenadas las claves tal como se muestra en la figura 2.

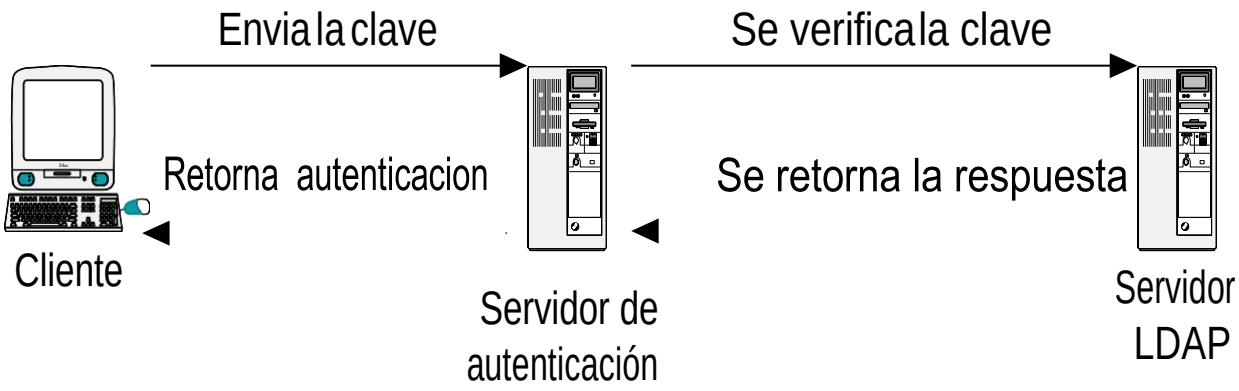

Ilustración 2: Proceso de autenficacion

Existen muchos servicios de autenticación entre los más conocidos y utilizados encontramos Kerberos y Radius.

La diferencia entre los dos radica en que Kerberos está orientado hacia la autenticación tanto de la estación de trabajo como del usuario usando un Intermediario llamado Key Distribution Center el cual es el encargado de validar las cubicaciones entre el origen y el destino, mientras que radius lo que busca es validar un usuario el cual generalmente se encuentra remotamente directamente con el servidor.

2. IMPLEMENTACION de un SERVIDOR LDAP CON OpenLDAP

Este capítulo menciona la manera de cómo se configura un Servidor OpenLDAP para controlar el acceso a la información de una Organización y muestra de manera sencilla la forma de cómo obtener el Software de instalación.

Se requiere configurar, debido a que es necesario personalizar la aplicación, aunque se sabe que el Software es libre y se puede obtener desde una dirección electrónica, se tiene la necesidad de adaptarlo a las necesidades de la empresa. En este caso se usa para autenticar a usuarios dentro de una red y por otro lado autorizar a los usuarios para usar los servicios previamente acordados, en esta ocasión los servicios son archivos.

2.1 Obtención de Software.

Open LDAP es un software libre, por lo tanto es posible poder descargar la aplicación OpenLDAP de la siguiente dirección electrónica: http://www.openldap.org/software/download/ , este software es de uso libre, por lo cual no es necesario pagar por el costo de una licencia, una ventaja más del uso de este software. OpenLDAP es un servidor que se distribuye bajo licencia GNU (Open Source), que permite que el software se pueda usar de forma gratuita, tanto de forma educativa como profesional. Además se dispone del código fuente para poder realizar modificaciones.

Existen varias versiones de OpenLDAP:
- OpenLDAP Release. (se recomienda verificar la última versión a instalar)
-OpenLDAP Stable Release. (La versión más fiable)
-OpenLDAP Test Releases. (Normalmente es una versión de
prueba) Los paquetes que incluyen las distribuciones de OpenLDAP
son:
- Servidor LDAP (ldapd)
- Servidor de replicación LDAP (slurpd)
- Software Development Kit (ldap)

El software OpenLDAP funciona en los siguientes sistemas operativos:
- Apple Mac OS X
- Linux: Debian, Red Hat,Suse, Fedora, Mandrake
- Free BSD
- IBM AIX
- Microsoft Windows 2000/NT
- Net BSD
- Solaris

3. Materiales y Métodos (Metodología)

1. Materiales

-Computadora (debian-SOR-ULS)
- Hosting de 2 GB memory / 50 GB Disk / Debian strech 9.7, 64bits
- Internet
- Memoria USB

2. Metodología

- 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, configuración, si es o no de código abierto, plataformas que los soportan, nivel de seguridad y rendimiento, con el fin de elegir la opción más destacada.

LISTA DE ACTIVIDADES LLEVADAS A CABO PARA LA REALIZACIÓN DEL PROYECTO.

1. Formación del Equipo de Trabajo.
2. Elección del Proyecto
3. Investigación de Tecnologias a Utilizar
4. Elaboración del Perfil de Proyecto
5. Recopilación de Información
6. Investigar sobre los Protocologos OpenLDAP
7. Elaboración del primer avance
8. Investigación y practica
9. Elaboración del segundo Avance
10. Verificación de del Funcionamiento del Proyecto
11. Elaboración de Correcciones al Proyecto
12. Realización de Pruebas Finales
13. Entrega del Proyecto Funcionando
14. Elaboración de Proyecto Final

DIAGRAMA DE GANTT

	ACTIVIDAD	INICIO	FINAL	CALENDARIO																							
				ENERO				FEBRERO				MARZO				ABRIL				MAYO				JUNIO			
				SEM1	SEM2	SEM3	SEM4	SEM1	SEM2	SEM3	SEM4	SEM1	SEM2	SEM3	SEM4	SEM1	SEM2	SEM3	SEM4	SEM1	SEM2	SEM3	SEM4	SEM1	SEM2	SEM3	SEM4
1	Formación de equipo de trabajo.	21/01/2019	31/01/2019																								
2	Elección del Proyecto	01/02/2019	20/02/2019																								
3	Investigación de tecnología a utilizar	29/02/2019	19/03/2019																								
4	Elaboración del Perfil de proyecto	20/03/2019	31/03/2019																								
5	Recopilar Información	25/03/2019	07/04/2019																								
6	Investigar sobre los Protocolos openLDAP	01/04/2019	21/04/2019																								
7	Elaboración del Primer Avance	22/04/2019	07/05/2019																								
8	Investigacion y prectica	01/05/2019	15/05/2019																								
9	Elaboración Segundo Avance.	07/05/2019	21/05/2019																								
10	Verificación del Funcionamiento del Proyecto	07/05/2019	21/05/2019																								
11	Elaboración de Correcciones al Proyecto.	16/05/2019	31/05/2019																								
12	Realización de Pruebas Finales.	28/05/2019	07/06/2019																								
13	Entrega del Proyecto Funcionando	08/06/2019	15/06/2019																								
14	Elaboracion de reporte final	08/06/2019	15/06/2019																								

Ilustración 3: Diagrama de actividades para Implementacion de proyecto sistema centralizado de contraseñas con OpenLDAP

Factibilidad del proyecto

Seleccionamos el proyecto a desarrollar durante el ciclo l - 2019, es pertinente realizar un estudio de factibilidad, los cuales permitirán determinar los aspectos importantes que se tomarán en cuenta para el desarrollo del proyecto, que es “Sistema centralizado de contraseñas con openLDAP”.

Factibilidad Técnica.

Para la Implementación del Sistema Centralizado de Contraseñas con OpenLDAP, se requiere tanto de protocolos, como de diversos paquetes que tienen los requerimientos técnicos para el desarrollo y puesta en marcha del proyecto.

Se llevó a cabo la evaluación necesaria tanto de Hardware y Software que se utilizará para el desarrollo del proyecto.

Hardware:

-Hosting (maquina virtual) de 2 GB memory / 50 GB Disk / Debian strech 9.7, 64bits

-Internet

-Modem USB

Software:

-Sistema Operativo: Debian Strech.

-Paquetes OpenLDAP, Phpidapadmin.

De acuerdo al software y hardware, determinamos el proyecto es factible en la parte operativa del proyecto.

COMPARATIVA DE OPENLDAP CON NOVELL DIRECTORY SERVICE

Aspectos	OpenLDAP	Novell Directory Service
Autor/Desarrollador	OpenLDAP Foundation/ Proyecto OpenLDAP	NetIQ Lanzamiento estable 9.1.3
Sistemas Operativos	Multiplataforma	Multiplataforma
Licencia de software	Es una implementación libre y de código abierto del protocolo Lightweight Directory Access Protocol (LDAP) desarrollada por el proyecto OpenLDAP.	Licencias del software de NetIQ eDirectory es una implementación libre y de código abierto.
Descripción General	Esta es una implementación libre del protocolo OpenLDAP. Tiene su propia licencia y es compatible con otros servidores que utilicen el mismo protocolo. Es utilizado por distintas distribuciones Linux y BSD	Este es el servidor de directorio propio de Novell para gestionar el acceso a un almacén de recursos en uno o varios servidores conectados en red. Se compone de una estructura de base de datos jerárquica orientada a objetos en la que se almacenan todos los objetivos típicos de los directorios
	Se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP. Tiene su propia licencia, la OpenLDAP Public License. Al ser un protocolo independiente de la plataforma, varias distribuciones GNU/ Linux y BSD lo incluyen, al igual que AIX, HP-UX, Mac OS X, Solaris, Windows (2000/XP) y z/OS	También conocido como eDirectory es la implementación de Novell utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. Entre los cuales se crean permisos para el control de acceso, por medio de herencia. 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.

Factibilidad Económica.

A continuación, se presenta los costos de los recursos, que se determinaron se utilizarán para el desarrollo del proyecto.

DETALLE CANTIDAD COSTO.

DESCRIPCION	CANTIDAD	PRECIO
Paquetes de Internet	5	$ 25.00
Impresiones	2	$ 10.00
Viaticos Alimentación	Varios	$ 50.00
Viaticos Transporte	Varios	$ 30.00
TOTAL		$ 115.00

Es muy importante destacar que el Sistema Centralizado de Contraseñas con OpenLDAP no ocasiona ningún costo de Licencia y es beneficioso ya que no incrementa el costo del desarrollo del proyecto.

Factibilidad Operativa.

Nuestro objetico como grupo, es lograr la implementación del Servidor Centralizado de Contraseñas con OpenLDAP. Dentro de la factibilidad económica se describe uno de los beneficios que permitirá en gran medida realizar el proyecto; también los paquetes de OpenLDAP que al descargarlos no tienen ningún costo el uso de su tecnología.

Nuestra finalidad como grupo es buscar el funcionamiento del servidor Centralizado de Contraseñas con el directorio OpenLDAP, ya que al funcionar tendremos la oportunidad de mostrar a los demás, la forma de tener una red con clientes es muestra de seguridad y comodidad para los usuarios.

La creación del Servidor Centralizado de Contraseñas comprende las fases de Análisis, Planificación, Contenido, Diseño, Programación entre otras.

RESULTADOS

Al finalizar este proyecto podemos sentirnos satisfechos ya que este funcionó correctamente y sobre todo porque es una fuerte alternativa de uso libre ante los de uso privativo.

Durante el desarrollo de este realizamos pruebas para verificar su funcionamiento con Moodle, Moodle es una plataforma de aprendizaje diseñada para proporcionarles a educadores, administradores y estudiantes un sistema integrado único, robusto y seguro para crear ambientes de aprendizaje personalizados. Este funciona sin ningún problema, de igual forma este ha sido muy eficiente y a respondido con mucha facilidad y nos ofrece mucha seguridad.

Los requisitos para que este funcione son mínimos comparados con otros además de tener la opción de hacerlo con el directorio o la herramienta phpladapadmin, y este resulta más económico y fiable que otros sistemas.

CONCLUSIÓN

El propósito de este proyecto fue evaluar una solución de software libre que permitiera solucionar la problemática de la autenticación centralizada de usuarios.

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.

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.

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 Debian Strech usando OpenLDAP

El directorio OpenLDAP es la mejor alternativa en el aspecto económico, dado que ofrece una gran cantidad de beneficios.

Los requisitos de hardware son mínimos para poder instalarlo por lo que puede ser usado desde una pequeña oficina hasta una gran empresa.

RECOMENDACIONES

Es necesario que la población estudiantil conozca acerca de otras alternativas de estos directorios y así poderles dar uso ya que estas son gratuitas.

OpenLDAP no solo mantiene una lista de usuarios también puedes autenticar usuarios.

Conocer de las configuraciones de OpenLDAP para gestionar la centralización de contraseñas.

Identificar problemas comunes que pueden presentar este y así poderlos solventar.

El directorio OpenLDAP es una gran alternativa en el tema de seguridad y privacidad ya que este permite el control total de los usuarios, contraseñas seguras.

Es recomendable montar nuestro servidor centralizado de contraseña ya que este presenta muchas ventajas económicas y de acceso.

BIBLIOGRAFÍA

El Rincón De Juanjo. (2017/10/29). Instalación y Configuración de LDAP en Debian Stretch. 29/10/2017, de juanjoselo.wordpress.com Sitio web:https://juanjoselo.wordpress.com/2017/10/29/instalacion-y-configuracion-de-ldap-en-debian-stretch-con-directorio-ldap-basico/

ANTONIO S.C.. (SEPTIEMBRE 28, 2017). Instalar servidor LDAP en Debian 8. 2018, de CurseaMe Sitio web: http://www.cursea.me/tutoriales/instalar-servidor-ldap-en-debian-8/

P. Ruiz. (17 agosto, 2013). ¿Cómo funcionan LDAP y OpenLDAP? 17 agosto, 2013, de somebooks.es Sitio web: http://somebooks.es/12-6-como-funcionan-ldap-y-openldap/

Benjamin Coles. (2001-2019). Autenticación centralizada mediante OpenLDAP. 2019, de wiki Sitio web: https://wiki.gentoo.org/wiki/Centralized_authentication_using_OpenLDAP/es

Proyecto OpenLDAP. (2006). OpenLDAP. 27 mar 2019, de wikimedia Sitio web: https://es.wikipedia.org/wiki/OpenLDAP

Anónimo . (2008). Protocolo Ligero de Acceso a Directorios. 2018, de wikipedia Sitio web: https://es.wikipedia.org/wiki/Protocolo_Ligero_de_Acceso_a_Directorios

ANEXO

MANUAL DE PROGRAMADOR.

URL: https://drive.google.com/open?id=1v755ZDYVlmPayAN8Ih4ajA6893EpxlQc

MANUAL DE USUARIO

URL: https://drive.google.com/open?id=1n7uo9fPr5kSu0YjAVDeLwyNu-NqZFNJt

VIDEO TUTORIALES:

URL: https://youtu.be/04AzRJYVLZQ

URL: https://youtu.be/JekkHsrf37E