Universidad de La Habana
Facultad de Matemática y Computación

Implementación de un sistema de autenticación de usuarios basado en LDAP

Autor: Eric Nordelo Galiano
Lian Ulloa Mc-kion

Tutor: **Lic. Gilberto Garcia**

Tutor: **Lic. Darío Álvarez Arteaga**

Trabajo de Diploma
presentado en opción al título de
Licenciado en Ciencias de la Computación

Junio de 2019

Agradecimientos

Opinión del tutor

Resumen

Abstract

Índice general

Índice de figuras

Introducción

La necesidad de desarrollar los medios de comunicación y la transmisión de información es una de las características que distingue a nuestra civilización desde hace milenios. Desde que se inventó la imprenta hace aproximadamente 6 siglos, la humanidad ha generado incontables volúmenes de texto para almacenar conocimiento de todo tipo. No obstante, no es hasta la década de 1960, con la adopción y proliferación de las computadoras y el mantenimiento de registros digitales, que se alcanzaría una verdadera revolución en los medios de almacenamiento, transmisión y en la accesibilidad a la información a escala global. Esta revolución conocida como Revolución Digital o Era de la Información gira en torno a las nuevas tecnologías e Internet, siendo la catalizadora de una enorme explosión tecnológica, produciendo grandes transformaciones en una sociedad donde la automatización de los procesos ya no solo industriales, tambien cotidianos,

Aqui separa oraciones como: . Esta automatizacion, mejora considerablemente ...

mejora considerablemente la calidez

Creo que quisiste decir calidad.

, rapidez y robustez de los mismos, y donde el surgimiento de las redes de dipositivos facilita la comunicación y la organización de personas y organismos.

Una de las ventajas que trae consigo el establecimiento de redes de dispositivos es la posibilidad de descentralizar el almacenamiento de información sin comprometer el acceso a la misma. Actualmente la red de la Universidad de La Habana cuenta con varios servicios consumidores y fuentes de diferentes tipos de información relacionada con el

No pongas el departamento, pon los departamentos. Cada unidad presupuestada tiene un departamento de RH diferente.

departamento de Recursos Humanos, careciendo de un servicio que ad-

ministre de manera adecuada el flujo de comunicación entre los mismos. De estos servicios se benefician no solo las facultades pertenecientes a la Universidad, también se benefician otras instituciones asociadas a la misma como el Instituto Superior de Diseño (ISDI) y el Instituto Superior de Ciencia y Tecnología Aplicada (InSTEC)

Si quieres puedes mencionar tambien a IFAL, JBN y la DOM

. La gran mayoría de estos servicios requiere que el la verificación previa del usuario que solicita acceder o agregar información a los mismos, por lo que con el objetivo de centralizar el proceso de verificaciónse han ido acumulando sobre un dominio web (directorio.uh.cu) varias actualizaciones aisladas que conforman lo que se conoce como "Directorio Único de la Universidad de La Habana"para poder integrar y administrar servicios que funcionan sobre diferentes tecnologías. Esto trae consigo dificultad a la hora de integrar nuevos servicios al directorio, así como inestabilidady falta de robustez en el servicio de verificación y solicitud de información almacenada.

El párrafo del la explicación del problema debería ser re escrito para su mejor comprensión.

Dicho esto, el objetivo de este proyecto es proveer a la Universidad de La Habana de un servicio que se encargue de administrar estos procesos de manera confiable y eficiente, que además sea fácil de integrar y fácil de modificar (implementar mejoras).

Para lograr esto surgen varias preguntas a responder como por ejemplo: ¿qué método se debería utilizar para almacenar la información?, ¿qué método se debería utilizar para acceder a la misma?, ¿qué método usar para mantener la informacón actualizada?...

Como respuesta a la primera pregunta, después de analizar distintos métodos para gestionar información, debido a las características del problema que enfrentamos llegamos a la conclusión que lo mejor es almacenarla en una estructura de directorios. La principal ventaja de esto sobre las bases de datos relacionales (y no relacionales) es la velocidad para realizar consultas sobre grandes volúmenes de datos (perdiendo en velocidad de modificación de los mismos, tanto en actualizaciones, como en inserciones y eliminaciones).

Si vas a usa esto como un objetivo general, 'estos procesos' debe ser claramente definido. Cuales son los procesos?

Este es el punto de conducir la investigación, es mejor desarrollar una separación lógica de estas preguntas mas que presentar-

Decidido esto y después de analizar diversas maneras de manejar una estructura de directorios optamos por el LDAP (Lightweight Directory Access Protocol o Protocolo Ligero de Acceso a Directorios) como protocolo de acceso y OpenLDAP como implementación del mismo.

Este protocolo brinda un esquema similar al de una guía telefónica, implementando un enfoque jerárquico para el almacenamiento de la información. Además existe una interfaz de autenticación para la mayoría de los servicios que administran usuarios y permisos, que utiliza como fuente de información a servidores que implementen este protocolo. Partiendo de la problemática existente la autenticación de los servicios que se brindan en el recinto universitario, se ha formulado la siguiente hipótesis de investigación: mediante el sistema de autenticación basado en protocolo LDAP se solucionará la administración eficiente de la información y los servicios en la Universidad de La Habana.

Con esta tesis queremos sustituir el actual sistema de directorio único por un sistema de autenticación basado en el protocolo LDAP.

Para esto es necesario investigar sobre el estado del arte de los sistemas que implementan este protocolo, así como la disponibilidad que brindan. Además es necesario automatizar el proceso de recopilar la información provista por estas fuentes, para lo cual se diseñará una esquema de base de datos, guiado por el protocolo LDAP, que se adapte a la estructura de los datos almacenados actualmente. Por último, se plantea implementar una *API* acorde con el protocolo OpenId para facilitar la autenticación para futuros servicios.

Evitemos usar **Debido a esto** y **Decido esto**, se puede reformular como **Habiendo analizado las ventajas de usar una estructura de directorio se decidió ...**

En la introducción no toca explicar el protocolo LDAP. Tiene que haber una sección del capitulo 2 para explicar el concepto de LDAP y como funciona.

Esto esta aqui para plantear algun objetivo?

Generar la hiposteis a partir

Notes

Capítulo 1

Directorio Único

1.1. Surgimiento del Directorio Único

Directorio Único es un servicio, que fue implementado con el objetivo de acceder a los datos del personal de la Universidad de la Habana. En el momento de su surgimiento, se hacia necesario disponer de un sistema que unificara las principales fuentes de datos de trabajadores y estudiantes. De esta manera sería factible presentarlas a través de una misma interfaz. Desde su creación se han implementado, sobre dicha interfaz, varios servicios de manera escalonada. Entre los principales servicios implementados, podemos destacar la implementación de un mecanismo de autenticación OAuth para los sitios de la intranet. Todos los servicios implementados sobre directorio funcionan hasta hoy. Otros servicios permiten denegar o permitir el acceso de los usuarios a determinados recursos brindados por la Universidad. Se puede tomar como ejemplo, el acceso al servicio que administra la asignación de viajes internacionales al personal de la Universidad. Otro ejemplo, un poco más palpable, lo tenemos en el servicio que decide la cuota de internet asociada a cada usuario. Este se basa tanto, en el año que cursa, en caso de ser estudiante, como en el cargo que ocupa o departamento en que trabaja, en el caso de los trabajadores.

Todos estos servicios, se implementaron sobre una misma base, debido al proceso de centralización iniciado hace ya 4 años. Dicha centralización nos provee de ciertas ventajas, ya que representa una fuente de información de todo el personal de la Universidad de La Habana. Con este enfoque, la información queda más accesible y más fácil de administrar.

Sin embargo, esta información no se genera de forma centralizada, sino que se encuentra esparcida entre distintas fuentes. Primeramente contamos

con el Sistema de Gestión para la Nueva Universidad (SIGENU). La información almacenada en esta, es administrada por las secretarias de las respectivas facultades y es referente solo a los estudiantes. También se consume información de los trabajadores de la Universidad de La Habana, la cual se maneja por los departamentos de recursos humanos de cada una de las unidades presupuestadas de la Universidad (UH, IFAL, JBN, UPA, ISDI, INSTEC). Sobre esta no se tiene total acceso debido a que, para su creación y luego su administración, se utiliza un software privativo.

Entre los datos más relevantes, almacenados en el Directorio Único, se encuentran aquellos que permiten la restricción y/o concesión de acceso a los servicios brindados. Es decir, las credenciales de los usuarios de la red. Esta información permite:

1. **Autenticar al usuario:** Comprobar que la persona que solicita un servicio es quien dice ser.
2. **Administrar el acceso:** En correspondencia del nivel de privilegio de un usuario ,permitir o no el acceso a ciertos servicios.

Una parte de la información almacenada, contiene información personal de los usuarios, estando esta más asociada a los trabajadores y externos. Entre la misma sobresalen:

1. Año que cursa (en caso de ser estudiante)
2. Dirección Particular
3. Departamento al que pertenecen
4. Datos sobre la nomina
5. Puesto que ocupa
6. Cargos importante (si es que los posée)

A los datos que actualmente se mantienen en el sistema, se le asocia información adicional para conocer la actividad realizada por el usuario. Dicha información, la almacenad el nodo de la Universidad en otro sistema aparte. Durante su estancia en la red, podemos registrar los momentos en que se autentica , en que sistema lo hace, la cantidad de cuota de internet consumida, etc.

En el listado siguiente, se encuentra un ejemplo de una posible respuesta ofrecida por el directorio cuando se consultan los datos de un trabajador de la UH.

```
<TrabajadorInfoCuote>
<Id>15869</Id>
<CatOcupacional>técnicos docentes principal</CatOcupacional>
<Docente>Si</Docente>
<CatDocenteInvestigativa>Instructor</CatDocenteInvestigativa>
<Contrato>Indeterminado</Contrato>
<Cargo>INSTRUCTOR</Cargo>
<Adiestrado>No</Adiestrado>
<AdministradorArea>No</AdministradorArea>
<Tecnico>Si</Tecnico>
<TecnicoInformatico>No</TecnicoInformatico>
<EspecialistaPrincipal>No</EspecialistaPrincipal>
<Cuadro>No</Cuadro>
<Asset>1</Asset>
<Departamento>DIRECCION DE INFORMATIZACION</Departamento>
</TrabajadorInfoCuote>
```

1.2. Problemas del sistema actual

El sistema, tal y como existe en este momento, presenta varios problemas. Esta tesis pretende brindar una propuesta de solución, así como su implementación. Los problemas son presentados a continuación:

1.2.1. Mantenimiento y extensión del Sistema

Debido a la naturaleza del surgimiento del Directorio Único, es decir, el acoplamiento de varios servicios de manera escalonada sobre la idea inicial, cada componente es demasiado dependiente de la forma en que las demás brindan sus correspondientes funcionalidades. Esto se debe a que la interacción entre las mismas ha sido configurada mediante un enfoque estático. El propio sistema no dispone de herramientas que permitan su modificación de una manera cómoda para los encargados de su mantenimiento. Dicho enfoque dificulta enormemente las tareas de actualización del sistema, las cuales son necesarias para poder adecuar el mismo a las nuevas condiciones y necesidades que van surgiendo en la red a través de los años. De hecho, actualmente el personal encargado del mantenimiento de Directorio no puede responder a las necesidades de actualización. La principal causa de esta desatención, es que los desarrolladores de Directorio perdieron muchos de los cambios en su historial de código. Tan importante es la pérdida de este

historial que imposibilita la recuperación de la lógica del Directorio actual partiendo solamente del código almacenado.

1.2.2. Desuso de datos almacenados

Desde el surgimiento del Directorio Único, se han ido incorporando nuevos campos a las fuentes de información del sistema. Estos cambios han tenido como objetivo suplir las necesidades que ocupan a la Universidad en cada nuevo período escolar.

Actualmente muchos de esos campos han dejados de ser útiles para la Universidad. Como consecuencia de la rigidez del Directorio, cualquier cambio, sobre todo aquellos cuya repercusión y alcance no se conocen, podrían significar la caída del sistema por tiempo indefinido. De ahí que se siga la filosofía de que "... lo que funciona no se toca...". Pero mantener este enfoque, provoca una sobrecarga innecesaria para el sistema, que aunque pueda ser pequeña, no deja de ser significante. Dicha sobrecarga se refleja sobre todo en el espacio ocupado por la información en disco.

1.2.3. Incumplimiento de políticas de baja de usuarios

Este es otro problema en el cual se incurre con bastante frecuencia en la Universidad. Debido a la volatilidad de algunos contratos concertados con personal ajeno a nuestro centro de altos estudios.

Sucede frecuentemente que al dar de baja a estos usuarios, sus cuentas son eliminadas con efecto casi inmediato, lo cual va en contra de los protocolos usualmente implementados en estos casos. Generalmente se debe espera una cierta cantidad de días para implementar la eliminación total de las cuentas. De esta manera se puede prevenir la pérdida de acceso a servicios críticos, como son el correo, el proxy y la nube recientemente despliega en la intranet de la Universidad. Muchas veces estos servicios son desarrollados, administrados y mantenidos por agentes externos a la Universidad.

1.2.4. Carencia de protocolos comunes para servicios externos

A menudo, se implementan nuevos servicios en la red de la Universidad. Generalmente estos servicios necesitan tener control de acceso sobre los recursos que brindan a sus usuarios. Esto implica el tener que desarrollar para cada nuevo servicio, un mecanismo de autenticación de usuarios. Este mecanismo además tiene que ser capaz de brindar una funcionalidad para administrar los roles o grupos a los que pertenecen dichos usuarios. Un

enfoque más útil, es el de delegar esta tarea a un sistema externo y centralizado. De esta forma se evita el tener que repetir el desarrollo de la misma funcionalidad para cada servicio.

Teniendo esto en cuenta, es que se pretende implementar una API Rest que permita modificar la lógica detrás de la información brindada, sin que esto implique modificar todos los servicios que consuman información de nuestro sistema.

1.3. Propuesta de solución

Con el objetivo de subsanar dichos problemas, pretendemos desarrollar un sistema capaz de sustituir el Directorio Único. Nuestro enfoque va orientado a desplegar un servidor que implemente el protocolo LDAP. Este protocolo define un servicio de directorio optimizado para las operaciones de búsqueda. Además posee facilidades para la organización de los datos, asociándolos a entidades, grupos y cualquier otra unidad organizacional en la que se necesiten agrupar a los datos. Dichos datos serán consumidos directamente de las mismas fuentes de las que se alimenta Directorio Único. Existirá, para esto, un capa de software intermedio capaz de transformar los datos a un formato compatible con el protocolo LDAP, específicamente el formato LDIF. Dicho formato propone la declaración de los atributos, que componen la información de un usuario, a través de pares de llaves y valores. A continuación se puede observar, como ejemplo, una entrada del servidor LDAP expresada en este formato. La misma representa la información comúnmente almacenada con respecto a un usuario que no está directamente asociado a la Universidad.

```
dn: uid=labf@fq.uh.cu,ou=Externo,dc=uh,dc=cu
area: N/D
assets: 1
cargo: JEFE DE DEPARTAMENTO (ADM FACULTAD)
categoriadocenteinvestigativa: N/D
centrodegraduacion: N/D
ci: 38081015203
ciudadania: N/D
cn: Luis Enrique
correo: labf@fq.uh.cu
cuotainternet: 0
dependencia: UH: FACULTAD DE QUIMICA
direccion: N/D
```

```
direcciondelcentro: N/D
edad: 23
esbaja: FALSE
escuadro: TRUE
fechadecreacion: 1486962000
fechadebaja: 2145889787
fechaderegistro: 1484542800
gradocientifico: N/D
lugardenacimiento: N/D
municipio: N/D
objectclass: Externo
objectclass: top
provincia: N/D
raza: Blanca
sexo: M
sn: brahin Fuente
tienechat: TRUE
tienecorreo: TRUE
tieneinternet: TRUE
uid: luis.enrique.brahin.fuente_182711
ujc: FALSE
userpassword: {SSHA}n9+lgnpEQv63Ky7smvxyISK1Gb3dq
```

En caso de ser necesario guardar alguna información que no este incluida en las fuente, es en esta capa donde será generada.

Actualmente existe muchos servicios que saben como comunicarse directamente con el protocolo LDAP. Pero no todos incluyen esta funcionalidad. Por esta razón, es necesario implementar una interfaz, una capa de abstracción entre LDAP y el resto de los servicios, que permita su comunicación. El protocolo de comunicación más común entre servicios web es el de HTTP. Por eso pretendemos implementar una RESTFUL Api para garantizar la interacción de nuestro sistema, con todos los servicios que necesiten consumir la información que almacenaremos. Los servicios que brindara dicha Api son los siguiente:

1. Consultar la información acerca de cualquiera de las usuario almacenados en el sistema.

2. Agregar la información nuevos usuarios, así como asignarles una cuota de internet y un usuarion de correo.

3. Actualizar la información de los usuarios, tanto de estudiantes, como de trabajadores y externos.

4. Definir preguntas de seguridad para cada usuario, que le permitan al mismo recuperar sus credenciales.

   no se si las puse muy genericas? se me queda algo fuera?

Realizar cualquiera de estas acciones, requiere pasar el proceso de autenticación de dicha API y poseer los permisos necesarios para la funcionalidad correspondiente.

Antes de decidir el enfoque a seguir para la implementación de la solución propuesta, se tuvo en cuenta varias tecnologías. A continuación las presentamos y argumentamos nuestra elección.

Capítulo 2

Estado del arte

2.1. LDAP

2.1.1. ¿Qué es el protocolo LDAP?

LDAP (Lightweight Directory Access Protocol) es un protocolo perteneciente a la capa de aplicaciones [1], tanto para servidores como para clientes. Es abierto y multiplataforma. Está pensado para la implementación de servicios de directorio, como son: **IBM Security Directory Server**, **Active Directory**, **Oracle Internet Directory** y **OpenLDAP**; facilitando el acceso rápido a la información almacenada. Presenta una estructura arbórea, la cual organiza la información en ramas y permite realizar búsquedas de manera eficiente, debido a que la cardinalidad de las posibles repuestas se reduce a medida que se avanza por cualquiera de estas ramas. Es una versión ligera del protocolo DAP (Directory Access Protocol)[2], el cual a su vez es parte del estándar para servicios de directorios en la red: X.500 [3].

[1] TANENBAUM, ANDREW S. Redes de computadoras PEARSON EDUCACIÓN, México, 2003 ISBN: 970-26-0162-2

[2] `https://es.wikipedia.org/wiki/Directory_Access_Protocol`

[3] `https://es.wikipedia.org/wiki/X.500`

2.1.2. Conceptos Importantes dentro de LDAP

Servidor de Directorio

Un servidor de directorio, no es más que un tipo de base de datos pensada para ser utilizada directamente en la red. A diferencia de las bases de datos tradicionales[4], que representan los datos en tablas y cada instancia es una fila, en este cada entrada en el directorio es un árbol de entradas, donde cada árbol puede contener datos o ser una hoja (un árbol vacío)

Entradas

Cada entrada en un servidor de directorio representa una colección de información referente a cierta entidad. Está compuesta principalmente, por un nombre distinguido, que es el identificador unívoco de la misma. Además cuenta con un conjunto de atributos y de clases de objetos los cuales definen la estructura y el comportamiento de la entrada.

Nombre Distinguido

Este es el identificador unívoco de la entrada. Esta compuesto por lo que se conoce en la literatura como 'Nombres distinguidos relativos' o 'RDN' por sus siglas en inglés. Estos RDN no son más que un conjunto ordenado de pares atributo-valor. Usualmente se escogen los atributos más representativos de cada entrada para la representación del DN.

Artibutos

Los atributos son los encargados de guardar la información de cada entrada y tiene asociados un tipo, un conjunto de opciones.

Los atributos representan una parte importante del esquema del directorio LDAP. A través de estos podemos definir nuevas clases de objetos para poder suplir las necesidad de almacenamiento de información. Para poder definir tanto atributos como clases de objetos es necesario proveerle a ambos un identificador, el cual presenta un formato similar al siguiente: `1.3.6.1.4.1.<Identificador global>.1.5` . A continuación podemos ver un ejemplo de como se puede definir un nuevo atributo.

[4]Bases de datos relacionales, definidas por Edgar F. Codd en su artículo: A Relational Model of Data for Large Shared Data Banks

```
1  dn: cn=UHAccount,cn=schema,cn=config
2  objectClass: olcSchemaConfig
3  cn: UHAccount
4  olcAttributeTypes: ( 1.3.6.1.4.1.53027.1.1 NAME 'assets'
5  DESC 'assets'
6  EQUALITY integerMatch
7  SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 )
```

Este listado presenta el formato de un archivo ldif, con los cuales se administra tanto las configuraciones como los datos almacenados en el servidor LDAP. De la línea 1 a la 3, se configura bajo cuál entrada del directorio LDAP se agrega la configuración correspondiente. Luego se describe la inclusión de un nuevo atributo llamado 'assets'.

El identificador global, como se puede ver en el listado, no es más que un nímero de serie que distingue a la implementación del protocolo LDAP utilizada a nivel global. Este se puede obtener realizando una solicitud a IANA(Internet Assigned Numbers Authority) [5].

Clases de Objetos

Estos también representan una parte importante del esquema del protocolo LDAP. No son más que conjunto de atributos que definen la información almacenada en cada entrada. Pueden ser de dos tipos: estructurales o auxiliares. Cada entrada puede tener asociada una clase de objetos estructural y cero o más clases auxiliares. En el listado siguiente tenemos un ejemplo de como definir una nueva clase de objeto.

```
1  olcObjectClasses: ( 1.3.6.1.4.1.53027.2.1 NAME '
       UHAccount'
2  DESC 'Base user account for UH's authentication system'
3  SUP person
4  MUST (userPassword $ email )
5  MAY (givenName $ NoCI $ assets $ isAdmin ))
```

Filtros

Los filtros representan el mecanismo utilizado para realizar consultas al directorio. La lógica utilizada para filtrar las entidades almacenadas en el servidor se define a través de reglas de comparación, las cuales, a su vez se definen en los atributos.

[5] `https://www.iana.org`

2.1.3. Implementaciones más utilizadas

IBM Security Directory Server

Este servicio implementa las especificaciones de Internet Engineering Task Force (IETF) LDAP V3. Permite la comunicación con clientes basados en IETF LDAP V3. Esta alternativa presenta una amplia variedad de funcionalidades que facilitarían la integración con el sistema de la Universidad , pero esta herramienta es de pago, por lo que no podemos utilizarla [6].

Active Directory

Esta es la implementación que brinda Microsoft[7] del protocolo LDAP. Entre las principales ventajas que presenta esta implementación, se encuentra la integración que brinda con los propios programas de Microsoft como por el ejemplo el Outlook. En este caso no es necesario proveer las credenciales para utilizar estos servicios. Pero peca de los mismo que la mayoría de los programas de Microsoft. Es dependiente del sistema operativo por lo que necesita del sistema Windows Server. Para poder utilizar este sistema, es necesario comprar la correspondiente licencia y posiblemente mejores servidores que sean capaz de soportarlo.

Oracle Internet Directory

Oracle Internet Directory es un servicio de directorio de proposito general que facilita realizar consultas rápidas y administración centralizada de la información almacenada sobre los usuarios que utilizan la red. El mismo combina el protocolo LDAP en su version número 3 con el eficiente funcionamiento, escalabilidad y robustez de una base de datos de Oracle [8].

[6] https://www.ibm.com/support/knowledgecenter/en/SSVJJU_6.3.1/com.ibm.IBMDS.doc_6.3.1/admin_gd13.htm

[7] https://support.microsoft.com/es-es/help/196464

[8] https://docs.oracle.com/cd/B14099_19/idmanage.1012/b14082/intro.htm#i1001669

OpenLDAP

OpenLDAP es la alternativa de software libre que implementa el protocolo LDAP. Como la mayoría de las implementaciones de servicios asociados a la ideología del software libre, esta variante se ejecuta sobre sistemas basados en el kernel de Linux [9]. Esto facilita su despliegue en el ecosistema de la red universitaria, ya que la mayoría de los servidores, ejecutan sistemas basados en dicho kernel. Además esta implementación se encuentra disponible en los repositorios de las distribuciones más populares entre la comunidad de software libre, lo cual facilita la elección de uno u otro sistema base en dependencia de las necesidades.

Junto al programa de instalación, se encuentran predefinidas varios tipos de atributos y clases de objetos. Estos pretenden suplir las necesidades más comunes de aquellos que necesitan utilizar un servicio de directorio. Podemos destacar:

1. Asignar grupos a los usuarios registrados y de esta manera controlar su rango de acceso.

2. Estructurar la información almacenada de manera que simule las áreas y departamentos que componen a la Universidad.

3. Definir, sin mucho esfuerzo, aquellos atributos que se suelen almacenar sobre una persona como recurso humano o como internauta o directivo, etc.

4. Facilitar la integración con distintos sistemas de autenticación a través de las clases predefinidas.

Además de incluir estos esquemas por defecto, es fácilmente extensible. Brinda, dentro de sus funcionalidades, la capacidad de definir nuevos tipos de atributos y de clases de objetos. Incluso es posible extender los ya existentes a través de mecanismos simples de herencia de clases, así como definir campos obligatorios u opcionales.

Con respecto al apartado de seguridad, OpenLDAP permite la encriptación de la información almacenada a través de distintos métodos. Para algunos brinda soporte de manera nativa, para otros realiza el proceso de encriptación a través de la libreria CRYPT [10].

[9] `https://es.wikipedia.org/wiki/Núcleo_Linux`

[10] `https://ftp.gnu.org/old-gnu/Manuals/glibc-2.2.3/html_node/libc_650.html`

El soporte nativo lo brinda para:

1. **MD5**[11] **:** Codificación basada en el algoritmo MD5
2. **SMD5:** Codificación basada en el algoritmo MD5 con un secuencia aleatoria de caracteres conocida como salt
3. **SHA**[12]**:** Codificación basada en el algoritmo SHA-1
4. **SSHA:** Codificación basada en el algoritmo SHA-1 con un secuencia aleatoria de caracteres conocida como salt

A través de CRYPT y el formato PHC string [13] brinda soporte para:

1. **MD5:** Codificación basada en el algoritmo MD5
2. **Blowfish / bcrypt:**
3. **NTHASH:**
4. **SHA-256:**
5. **SHA-512:**
6. **Solaris MD5:**
7. **PBKDF1 with SHA-1:**

Existe además, una interfaz web ya implementada conocida phpLDAPadmin [14] que permite administrar de manera básica, el contenido del servidor LDAP. La misma permite listar los datos almacenados, modificarlos, añadir nuevas entradas, etc. En resumen, permite realizar las operaciones usuales sobre un conjunto de datos.

2.1.4. Modos de empleo usuales

DNS

LDAP es usualmente utilizado con una estructura de DNS. Las clases de objetos que existen por defecto en el esquema de OpenLDAP, permite simular una estructura de delegación de zonas, arborea, similar a la del

[11] `https://www.ietf.org/rfc/rfc1321.txt`
[12] `https://www.ietf.org/rfc/rfc3174.txt`
[13] `https://github.com/P-H-C/phc-string-format`
[14] `http://phpldapadmin.sourceforge.net/wiki/index.php/Main_Page`

DNS. Esto da la oportunidad de brindar las mismas funcionalidades de servicio de nombres de dominios y a la vez utilizar las ventajas de búsqueda y modificación de los LDAP.

Sistema de Autenticación

Esta implementación también brinda ventajas a la hora de implementar un sistema de autenticación de usuarios. Esto se debe principalmente al amplio soporte que tiene el protocolo LDAP para varios servicios. La posibilidad de agrupar a los usuario mediante unidades organizativas (Organizational Unit [OU]) y de representar su pertenencia a determinados grupos, permite administrar fácilmente el acceso que cada uno de los usuarios debe tener a los servicios ofrecidos por la universidad. Este modo de organizar la información de los usuarios se asemeja bastante a la manera en que se asigna permisos a un usuario en los sistemas operativos basados en Linux. De hecho, una de las funcionalidades implementadas como cliente de este protocolo, permite autenticar un usuario en una máquina, ya sea virtual o física, a pesar de que realmente no exista en el sistema. Basta con que el usuario exista en el servidor LDAP. En el caso específico de OpenLDAP, cuenta con dos clases de objetos que permiten este comportamiento. Se trata de la clase posixAccount y shadowAccount. Entre ellas guardan información referente a los atributos de un usuario en un sistema basado en linux. Las principales son: el directorio "home"del usuario, el número que lo identifica en el sistema, el grupo al que pertenece.

2.2. Docker

TODO: Revisar la longitud y ajuste al tema de las oraciones. Argumentar con ejemplos, idealmente con imagenes también. Argumentar la selección de la herramienta OpenLDAP. Abordar el análisis del lenguaje para la implementación del API. Argumentar cual es el framework utilizado para implementar el API. Descripción completa de la selección de herramientas para implementar la solución.

2.3. EA3

2.4. EA4

2.5. EA5

Capítulo 3

Implementación del sistema

3.1. Consideraciones previas

Es importante que en el capítulo de implementación se explique como solicitamos nuestro identificador global a IANA (Lian hizo esto si no recuerdo mal.)

3.2. SI2

3.3. SI3

3.3.1. SI3.1

3.3.2. SI3.2

3.3.3. SI3.3

3.4. Desarrollo de la solución

Capítulo 4

Experimentación y Resultados

Recomendaciones

Conclusiones

Bibliografía