Universidad de La Habana
Facultad de Matemática y Computación

Sistema de Autenticación Central

Autor:
Nadia González Fernández

Tutores:

Lic. Andy González Peña
Lic. Juan José Roque Cires

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

Noviembre de 2022

github.com/nala7/central_authentication_system

Dedicación

Agradecimientos

Agradecimientos

Opinión del tutor

Opiniones de los tutores

Resumen

Resumen en español

Abstract

Resumen en inglés

Índice general

Índice de figuras

Ejemplos de código

Introducción

Nowadays people use many different independent software systems and accumulate more and more identities. User identity is considered as a set of permanent or longlived temporal attributes associated with a user entity [Ceccarelli et al. 2015]. In order to access the service most of systems require the user to be registered and logged in. Quite often a user is registered in many web sites under the same user name and with the same or closely related passwords, which is not the best security practice. What is more they often forget their credentials, and the user management system have to send an unencrypted e-mail with these confidential data [Singer, Friedman 2013].
That is why the management of multiple user names and passwords is such an annoying aspect of the current Internet.
Taking into account all those security issues and the lack of the required competencies needed to fulfil them – more and more administrators of websites decide to outsource those management and authentication services to third parties, external entities specialized in that kind of activity. Such entities can solve those problems using different techniques. They can host, store, manage and secure user data on behalf of a particular service provider. They offer application programming interfaces (API), which can provide an access to user data for external applications. Such solutions enable to share user data among more than one web system, thus providing Single sign on (SSO) property for third party applications. The aim of the paper is to present an example of such a solution based on an internet platform for ~~gathering services dedicated to elderly people – ActGo-Gate (AGG).~~ *Aqui lo relaciono con la UH*
when users try to log in to any system, they are usually first requested to identify themselves with a user name and a password. Afterwards, the data input is checked against an existing user record to verify if the given combination is authentic. If so, the user becomes authenticated (i.e. the identification data he/she supplied previously is valid). Finally, a set of pre-defined permissions and restrictions for that particular login name is assigned to this user, which completes the final step, authorization. Usually authorization cannot be performed without any kind of authentication a [1]

El Nodo Central de la Universidad de La Habana tiene entre sus responsabilidades dar las credenciales digitales a todos los usuarios de la Universidad. Los trabajadores

y estudiantes de la institución registran sus datos personales en las bases de datos de recursos humanos y secretaria docente respectivamente. Esa información es utilizada más adelante para que los usuarios puedan autenticarse en los distintos servicios de la institución, respaldado por sus sistemas de origen.

La Universidad brinda servicios como correo, WI-FI, , FTP (*File Transfer Protocol*/Transferencia de Archivos) y alojamiento web. . En cada uno de estos el usuario debe autenticarse con una cuenta distinta.

Motivación

Actualmente vivimos en un mundo donde la tecnología tiene un papel protagónico. La Universidad de La Habana en los últimos años ha estado inmersa en el proceso de transformación digital que lleva a cabo nuestro país, como continuidad de la estrategia de informatización de la sociedad cubana, que pretende integrar las tecnologías digitales a todos los ámbitos de la sociedad.

En este sentido, nuestra sede universitaria ha avanzado en la digitalización de la información y los procesos y trabaja para facilitar el acceso a la red de todos sus estudiantes y trabajadores. A la par de estos avances, debe crecer también la seguridad de los sistemas para evitar brechas de información y asegurar la privacidad de los usuarios.

Garantizar un acceso seguro y sencillo a los recursos de la red es esencial para alcanzar este objetivo. Por consiguiente, se deben establecer mecanismos que cuenten con un alto nivel de seguridad y permitan identificar quién realmente está autorizado para acceder a los recursos del sistema.

La creación de una plataforma central de autenticación resolvería muchos de estos problemas y mejoraría la experiencia de los usuarios. Estos solo tendrían una cuenta para acceder a todos los servicios que ofrece la Universidad, por lo que no tendrían que lidiar con formularios de inicio de sesión cada vez que vayan a acceder a un servicio.

Antecedentes

Nota: Qué existe desde el punto de vista actual para autentificarte como usuario UH y sobre que esta soportado? qué problema trae ese soporte? existe en el mundo otros que pueden mejorar esas dificultades? Poner ejemplos.

Actualmente todos los usuarios de la Universidad de La Habana se almacenan en dos Protocolos Ligeros de Acceso a Directorios (en inglés: Lightweight Directory Access Protocol, también conocido por sus siglas como LDAP). En los dos directorios se guardan las cuentas de correo y los datos de sus usuarios. En uno ellos se registra la información de los estudiantes y en el otro la de los trabajadores. A partir de estos,

todos los sitios web y aplicaciones de la universidad, individualmente, verifican la pertenencia del usuario a la institución.

Cada aplicación y servicio tiene un servicio de autenticación individual que dependen de los dos mencionados directorios que contienen a los usuarios.

Problemática

El sistema implementado actualmente es poco eficiente y requiere de intervención humana constante para corregir y/o restablecer el apropiado funcionamiento de los servicios de autenticación. Esto genera tiempos elevados de respuesta y dificulta el mencionado proceso de transformación digital que está siendo llevado a cabo por nuestra Universidad.

Objetivo

Con el propósito de presentar una propuesta para solucionar la problemática expuesta anteriormente, se plantean los siguientes objetivos:

Objetivo General

- Diseñar e implementar un sistema de autenticación centralizada para todos los usuarios de La Universidad de La Habana.

Objetivos Específicos

- Generar los servicios de autenticación con compatibilidad con todas las tecnologías existentes y previstas en la institución.
- Implementar la gestión de control de acceso a todos los servicios ofrecidos por el Nodo Central de forma extensible a futuros servicios.

Estructura de la Tesis

Capítulo 1

Estado del Arte

En este capítulo se brindan las definiciones de herramientas utilizadas. También se realiza un estudio sobre el estado del arte de las mismas. Además, se brindan razones para incluir su utilización como parte de la solución propuesta.

estas son las unicas dos técnicas que existen?? no hay otras propietarias o no posible de utilzar por nosotros por el equipamiento que poseemos... en fin.
Al final debes decirme que tiene esa tecnica que no usas como defecto o como compatiblidad con la estructura existente en nuestra red.

Aqui en este capitulo debes hablar de la segurirdad que es algo importante para que no entrn intrusos que tecnica utilizas para ello-...

1.1. Autenticación

Authentication is about validating your credentials like User Name/User ID and password to verify your identity. The system determines whether you are what you say you are using your credentials. In public and private networks, the system authenticates the user identity via login passwords. Authentication is usually done by a username and password, and sometimes in conjunction with factors of authentication, which refers to the various ways to be authenticated. [4]

1.2. Inicio de Sesión Único

El Inicio de Sesión Único (en inglés *Single Sign-On* o también conocido por sus siglas SSO) has been widely adopted for online authentication due to its favorable usability and security.

1.3. OpenID Connect

A third protocol worth considering, is OpenID Connect – an authentication protocol based on OAuth 2.0 that provides a RESTful HTTP API and uses JSON as data format [Denis et al. 2015]. It is a simplified format that has gained large traction and is supported by many vendors, e.g. Google, IBM, Microsoft, Ping Identity etc. It extends pure OAuth 2.0 by providing user identity details in an efficient way so the requesting application knows not only the user's access rights to a particular asset, but also has a deep knowledge (to the given extent) about user identity. It also supports native apps like OAuth 2.0.
The OpenID Connect protocol, as it is based on OAuth 2.0, follows the same steps as OAuth (see again Figure 2), but the main difference is that OpenID connect provides an additional step to obtain information about user identity. Conceptually OAuth is developed for granting access to resources, not for authenticating the user. OpenID Connect provides an additional flow for providing id-token with some information about the user.[1]

1.3.1. Comparación

Ventajas:
-It resolves the potential security gaps of OAuth 2.0 and enhances the data by including user data (name, address etc.)
-Management & Configuration is simple.
VS Auth 2.0:
- tiene las ventajas de OAuth 2.0 - Architecture based security gaps have/ had to be solved in the implementations of it.
- It does not directly contain user information (name, address, etc.).
- Clients are moving away from OAuth 2.0 for new projects.[1]

1.4. LDAP

El Protocolo Ligero de Acceso a Directorios (en inglés: Lightweight Directory Access Protocol, también conocido por sus siglas de LDAP) es un conjunto de protocolos de licencia abierta que son utilizados para acceder a la información que está almacenada de forma centralizada en una red. Este protocolo se utiliza a nivel de aplicación para acceder a los servicios de directorio remoto.

LDAP está basado en estándares implementados sobre TCP/IP. Permite a los clientes interactuar directamente con los servidores de los directorios: almacenar y consultar información, buscar datos filtrados, autenticar usuarios, entre otros.

Este protocolo es utilizado actualmente por muchos sistemas que apuestan por el software libre al utilizar distribuciones de Linux para ejercer las funciones propias de un directorio activo en el que se gestionarán las credenciales y permisos de los usuarios y estaciones de trabajo en redes LAN corporativas en conexiones cliente/servidor.

Un directorio remoto es un conjunto de objetos que están organizados de forma jerárquica, tales como: nombre, claves, direcciones, etc. Estos objetos estarán disponibles para una serie de clientes conectados mediante una red, normalmente interna o LAN, y proporcionarán las identidades y permisos para esos usuarios que la utilicen.

LDAP está basado en el protocolo X.500 para compartir directorios, y contiene esta información de forma jerarquizada y mediante categorías para proporcionarnos una estructura intuitiva desde el punto de vista de la gestión por parte de los administradores.

Estos directorios se utilizan generalmente para contener información virtual de usuarios, para que otros usuarios accedan y dispongan de información acerca de los contactos que están aquí almacenados. Además es capaz de comunicarse de forma remota con otros directorios LDAP situados en servidores que pueden estar en el otro lado del mundo para acceder a la información disponible. De esta forma se crea una base de datos de información descentralizada y completamente accesible.

El sistema de autenticación vigente en el Nodo Central verifica sus usuarios con dos sistemas implementados con LDAP. Este protocolo se adapta a las necesidades y condiciones actuales de la Universidad ya que es *Open Source* (OSS o código abierto)
Por qué se utiliza LDAP?
R/
- ya se usaba en el nodo
- es open source: there are free LDAP server software solutions available (1. pq es bueno el open source? 2. se ajusta a las necesidades y posibilidades del nodo, existen pocos recursos)
- It is a mature, flexible, and well supported standards-based mechanism for interacting with directory servers. It's often used for authentication and storing information about users, groups, and applications, but an LDAP directory server is a fairly general-purpose data store and can be used in a wide variety of applications.
LDAP is a tool in the User Management and Authentication category of a tech stack.

1.5. Keycloak

Keycloak es un software de código abierto que permite el Single Sign-On o Inicio de Sesión Único (IdP) con Identity Management y Access Management para aplicaciones y servicios modernos. Esta herramienta facilita la protección de aplicaciones y servicios con poca o ninguna codificación. Un IdP permite que una aplicación (a menudo llamada Service Provider o SP) delegue su autenticación. [2]

Este software está escrito en Java y es compatible de forma predeterminada con los protocolos de federación de identidad SAML v2 y OpenID Connect (OIDC) / OAuth2. Está bajo licencia de Apache y es compatible con Red Hat. [2]

1.5.1. Características

Los usuarios se autentican en Keycloak en lugar de hacerlo en las aplicaciones. Esto significa que no es necesario que cada aplicación tenga un formulario de inicio de sesión, autentique a los usuarios o almacene sus datos. Una vez entren en Keycloak, los usuarios no tendrán que iniciar sesión en las demás aplicaciones conectadas al software. [2]

Lo mismo sucede cuando un usuario cierra sesión. Keycloak ofrece cierre de sesión único, lo cual significa que los usuarios solo tienen que desconectarse en una de las aplicaciones para salir de su cuenta en el resto. [2]

Otra prestación de Keycloak son las federaciones de usuarios, que facilitan la compatibilidad con LDAP y otros servidores de directorios activos. También admite la implementación de servicios propios para usuarios guardados en otros tipos de almacenamientos como en bases de datos relacionales. [2]

Keycloak ofrece como herramienta una consola de administración de cuentas, a través de la cual los usuarios pueden administrar sus propias cuentas. Pueden actualizar su perfil, cambiar sus contraseñas y configurar la autenticación en dos pasos. También pueden administrar sus sesiones y visualizar el historial de su cuenta. [2]

Otra característica es que es una herramienta extensible porque permite la eliminación, adición y modificación de las bases de datos de usuarios, los métodos de autenticación y los protocolos. Está basada en protocolos estándares y soportan OpenID Connect, OAuth 2.0 y SAML. [2]

1.5.2. Ventajas

Keycloak facilita añadir la autenticación y un servicio seguro a aplicaciones. Permite que los desarrolladores se centren en la funcionalidad empresarial al no tener que preocuparse por los aspectos de seguridad de la autenticación. También posibilita la unificación de los métodos de autenticación de distintas aplicaciones sin modificarlas.

Comparación Gluu:
Free open source access management suite with support for SAML and OpenID Connect SSO, and OAuth2 based web and API access management. The Gluu Server can include multiple components. Each one fulfills a different requirement, and can be included or excluded in individual deployments based on an organization's unique requirements. Gluu vs Keycloak:
- The Keycloak system requires 512 Mb of RAM and 1 GB of disk space, whereas the

Gluu system requires 8 GB of RAM and 40 GB of disk space.
- Gluu is less flexible to extend [3]

Capítulo 2

Propuesta

Capítulo 3

Detalles de Implementación y Experimentos

Conclusiones

Conclusiones

- El rendimiento del nuevo sistema es más eficiente ya que en cada iteración añade solo los nuevos usuarios en lugar de borrar y recrear cada noche todos sus usuarios. - El tiempo de activación de un usuario (el tiempo que transcurre entre que un usuario es dado de alta por recursos humanas y que el usuario tenga acceso a todos los servicios provistos por el Nodo Central como correo electrónico y acceso a internet) es más corto. - Sistema de autenticación más fiable

Recomendaciones

Recomendaciones

Bibliografía

[1] R. Kutera y W. Gryncewicz, «Single sign on as an effective way of managing user identity in distributed web systems. The ActGo-Gate project case study,» Informatyka Ekonomiczna, n.º 2 (40), 2016 (vid. págs. 1, 5).

[2] Keycloak Documentation, `https://www.keycloak.org/documentation` (vid. págs. 6, 7).

[3] G. Vassallo, S. Chiusano y D. Preuveneers, «Continuous authentication with behaviometrics on smartphones,» 2017 (vid. pág. 7).

[4] M. El Hajj Hussein, «Reproducible Examples for Integration with Keycloak,» inf. téc., 2019 (vid. pág. 8).