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

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 automatizar la generación de cuentas de correo en tiempo real, respaldado por sus sistemas de origen.

Motivación

Todo trabajador o estudiante al momento de ingresar en la Universidad, dígase al realizar el contrato en recursos humanos u ofrecer sus datos en secretaría docente, debe esperar un plazo de al menos 24 horas hasta que el sistema vigente actualice todos sus datos, generando molestias e inquietudes en los usuarios.

Por otra parte, el sistema actual 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 proceso de Transformación Digital que está siendo llevado a cabo por nuestra Universidad.

Antecedentes

El funcionamiento del sistema vigente consta de dos fases. La primera está implementada en directorio y obtiene toda su información realizando una copia parcial de los sistemas originales, borrando y recreando cada noche todos sus usuarios. La segunda fase hace uso del Protocolo Ligero de Acceso a Directorios (en inglés: Lightweight Directory Access Protocol, también conocido por sus siglas como LDAP). Este sistema es dependiente directamente del anterior y por tanto se considera una segunda capa. También replica el proceso de la misma forma: eliminando todos los datos y reconstruyéndolos.

Problemática

Este sistema ofrece autenticación múltiple con tecnologías obsoletas por lo cual todos los navegadores clientes en la actualidad rechazan su conexión a no ser que una excepción manual sea generada. Esto genera brechas de seguridad no permisibles hoy en día.

El procedimiento anteriormente descrito tiene problemas estructurales y funcionales, por lo que es propenso a errores. Entre los problemas más destacados se encuentra el mal manejo de recursos de hardware causando que el servicio se congele. Mantener la consistencia de los datos es una de las tareas más complejas. Crear, borrar y actualizar datos en tiempo real debe ser tolerante a fallas en la comunicación y en los servidores.

Otro problema del sistema es el no uso de encriptación para almacenar los datos, lo cual representa otra vulnerabilidad. El sistema debe cumplir los protocolos de seguridad y ser resistente a ataques externos. También, dada la sensibilidad de la información con la que trabaja, se debe proteger la privacidad de los usuarios.

Objetivo

Objetivo General

- Diseñar e implementar un sistema integrador de todos los usuarios de La Universidad de La Habana.

Objetivos Específicos

- Integrar las fuentes institucionales de usuarios existentes — Assests y Sigenu — de forma extensible a futuras fuentes de usuarios.
- Automatizar la generación de cuentas en tiempo real, respaldado por sus sistemas de origen.
- Permitir el manejo de usuarios excepcionales y/o casos externos no incluidos en las fuentes de datos estándar.
- Implementar la gestión semi-automatizada del control de roles según los metadatos descriptores del usuario.
- 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

Capítulo 1

Estado del Arte

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