

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

Introducción	1
1. Estado del Arte	3
2. Propuesta	4
3. Detalles de Implementación y Experimentos	5
Conclusiones	6
Recomendaciones	7

Índice de figuras

Ejemplos de código

Introducción

No se habla de la autenticación

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 secretaría 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

Qué son Sigenu y Assets?

Todo trabajador o estudiante al momento de ingresar en la Universidad, dígame 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.

El sistema actual es poco eficiente y requiere de intervención humana constantemente para corregir y/o restablecer el apropiado funcionamiento de los servicios de autenticación. Esto genera tiempos elevados de respuesta y ~~contradice de esta forma~~ el proceso de Transformación Digital que está siendo llevado a cabo por nuestra Universidad.

dificulta

Antecedentes

Donde entran sigenu y assets aquí?

fases

El funcionamiento del sistema vigente consta de dos momentos: el primero está implementado en directorio, el cual obtiene toda su información realizando una copia parcial de los sistemas originales, borrando y recreando cada noche todos sus usuarios. Este sistema ofrece autenticación múltiple con tecnologías obsoletas por lo cual todos los navegadores clientes en la actualidad refutan su conexión a no ser que una excepción manual sea generada, todo esto genera brechas de seguridad no permisibles en la actualidad. Por otra parte, el segundo momento se encuentra en el uso de LDAP, este sistema es dependiente directamente del anterior y por tanto se considera una segunda capa, con lo cual, además se está replicando el proceso de la misma forma:

protocolo ligero de acceso a directorios (en inglés: Lightweight Directory Access Protocol, también conocido por sus siglas de LDAP)

Qué es directorio?
¿qué problema resuelve?

Qué¹ es LDAP y cómo se usa en el nodo?

eliminando todos los datos y reconstruyéndolos. ~~Es necesario mencionar lo propenso a errores que se encuentra el procedimiento descrito anteriormente, desde problemas estructurales hasta funcionales, entre ellos, los más destacados son: mal manejo de recursos de hardware causando que el servicio se congele, el desuso de codificación para almacenar datos, causando que metadatos se escriban en código, entre otros.~~

encriptación lo cual representa una vulnerabilidad de seguridad

Reescribir último párrafo y moverlo para problemática

Problemática

Mantener la consistencia de los datos es una de las tareas más complejas. Crear, borrar y actualizar datos en tiempo real ~~es~~ debe ser tolerante a fallas en la comunicación y en los servidores. El sistema debe cumplir con 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

1. Autenticación (copiar de arriba)
2. Seguridad (copiar desuso de encriptación de arriba y añadir el sistema debe cumplir...)
3. propenso a errores y estados inconsistentes
4. Eficiencia

Objetivo General

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

Objetivos Específicos

- Integrar todas las fuentes de usuarios de los servicios institucionales: ~~Assets, Sigenu.~~ Integrar las fuentes institucionales de usuarios existentes — Assests y Sigenu — de forma extensible a futuras fuentes de usuarios
- Automatizar ~~el acceso de~~ la generación de cuentas en tiempo real respaldado ~~con~~ por sus sistemas de origen.
- Controlar el manejo de casos excepcionales y/o casos externos no aplicables a las fuentes de datos estándares. 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 metadatos descriptores del usuario.
- Generar los servicios de autenticación con compatibilidad en todas las tecnologías existentes y previstas en la institución. con
- Implementar la gestión de controles de acceso para los diferentes servicios y la simplificación del proceso de añadir nuevos.

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

Recomendaciones

Recomendaciones