Centralizando la Autenticación y Autorización en la UNLP

Nuestra experiencia con SSO

Lic. Christian A. Rodriguez
car@cespi.unlp.edu.ar
@car_unlp

CeSPI
Centro Superior para el Procesamiento de la Información
UNIVERSIDAD NACIONAL DE LA PLATA

Roadmap

- Escenario
- Objetivo y alcance
- Alternativas tecnológicas
- Nuestra elección
- Selección de productos: servidor y librerías para desarrollo
- Desarrollos ad-hoc para sustentar el proyecto
- Complicaciones durante el desarrollo

Escenario

- En números:
  - 18 Unidades Académicas y 4 colegios
  - 109.000 alumnos
  - 12.000 docentes
  - 3000 administrativos
- Ya disponemos de un servicio web que integra tablas de referencia como: provincias, ciudades, tipo de documento, estado civil, y lo más importante **PERSONAS de la UNLP**
- Identificamos usuarios de las aplicaciones con roles implícitos:
  - Roles: alumnos, docentes y no docentes
  - Cada rol es en una dependencia
  - Un usuario puede tener más de un rol en cada dependencia

Escenario: aplicaciones que requieren autenticación y autorización

- Guaraní
- Moodle
- Licencias médicas
- Títulos
- Libretas estudiantiles sanitarias
- Albergue Universitario
- Becas
- Expedientes
- Liquidación de sueldos
- Recibos de sueldo
- Auditoría de cargos y descargos
- Proyectos de Extensión Universitaria
- ...

Escenario: los problemas conocidos

- Cada aplicación con su usuario
- La contraseña anotada en el monitor o compartida por toda una oficina
- Cuando alguien se desplaza en la organización, se dificulta mantener la autorización actualizada
- Políticas de seguridad distribuidas
- Los desarrollos siempre implementan la misma funcionalidad:
  - ABM de usuarios
  - Gestión de contraseña
  - Olvidé mi contraseña

Objetivos

- Un único usuario para todos los sistemas
- Una aplicación centralizada para autenticar los usuarios
- Una aplicación que permita gestionar la autorización a los sistemas
- Que los usuarios puedan utilizar sus cuentas institucionales y asociarlas a cuentas en redes sociales para la autenticación
- Que los nuevos desarrollos focalicen en la lógica de negocio y no en funcionalidad repetitiva
- Armar un repositorio de usuarios integrado a la API de integración de la UNLP permitiendo así:
  - Determinar usuarios por dependencia
  - Determinar usuarios que son alumnos, docentes o no docentes
  - Armar directorios virtuales para integrar servicios de infraestructura como por ejemplo: mensajería, email, radius, etc.

Alcance

- Análisis de tecnología y estándares vigentes
- Evaluación de productos
- Desarrollo y personalización de la infraestructura

Alternativas Tecnológicas

- Single Sign On en la organización
  - SAML
  - CAS
- Soluciones de autenticación alternativas
  - OpenID
  - Utilizar redes sociales: Facebook, Google, Twitter, Linkedin

Nuestra elección

- SAML como estándar
- Utilizar una fuente de autenticación de usuarios propia de la UNLP integrada con redes sociales

CeSPI

Evaluación de productos de código abierto

- **SimpleSAMLphp**
- CAS
- Shibboleth
- OpenAM

Librerías SAML para el desarrollo

- SimpleSAMLphp
- OneLogin
- Plugin para symfony 1.4
- Gema ruby-saml
- Plugin Redmine omniauth SAML
- Plugin Moodle SAML onelogin

Desarrollos y personalizaciones

- Fue necesario definir un esquema que permita
  - Representar los usuarios en la organización: un usuario pertenece a N dependencias, y en cada una puede tener roles implícitos
  - Representar las aplicaciones: las aplicaciones tienen entornos y permisos. Además automatiza la configuración de los service providers en SimpleSAMLphp
- Personalización de SimpleSAMLphp
  - Filtro que indica la fuente de autenticación: si es UNLP, o una red social. La aplicación determinará si es válida la fuente o requiere otra para su autenticación.
  - Filtro que agrega roles como atributos durante el login: se agregan los roles implícitos como los explícitos para una aplicación
  - Filtro de accounting y políticas de seguridad: ante la caducidad de una cuenta, se evita el login. Además se lleva el accounting de los accesos
- Aplicaciones ad-hoc
  - Gestor de usuarios, aplicaciones, permisos y notificaciones
  - Autoregistro
  - Gestor del perfil del usuario

Complicaciones durante el desarrollo

- Ambientes complejos en producción requiere una réplica compleja en desarrollo
  - Utilizamos Vagrant
  - Estamos pasando a docker
- Test de aplicaciones con ambientes similares
  - Se desarrolló la aplicación de gestión de aplicaciones con ambientes, permitiendo armar ambientes para los entornos de prueba diferentes a los de producción
- Necesidad de servicio web SSO
  - Las aplicaciones a veces requieren conocer datos de la infraestructura de SSO
  - Este servicio debe implementarse proveyendo entre otra información, qué usuarios tienen determinado rol

¿Consultas?