Séptima Conferencia de Directores de Tecnología de Información y Comunicación en Instituciones de Educación Superior: Gestión de las TICs para la investigación y colaboración
Migración, sincronización e interoperabilidad entre diversos Servicios de Directorio Activos: Caso de éxito de la Universidad de Costa Rica

José Valverde Cerdas, Luis Loría Chavarría

Centro de Informática, Ciudad Universitaria Rodrigo Facio, Universidad de Costa Rica,
San Pedro, Montes de Oca, Costa Rica
jose.valverde@ucr.ac.cr, luis.loria@ucr.ac.cr

Resumen. La Universidad de Costa Rica migró su servicio de Directorio Institucional basado en el Protocolo Ligero de Acceso a Directorio (LDAP). Este servicio provee a la Comunidad Universitaria, actualmente cerca de 85,000 usuarios, de un medio de autenticación a los servicios y sistemas institucionales.

El servicio cuenta con un clúster multimaestro-consumidor, balanceo de carga y alta disponibilidad basado en el protocolo LDAP, además de un sistema web para la administración de cuentas y gestión de directorios activos desarrollado en Java y una base de datos basada en PostgreSQL. El sistema de web gestiona la sincronización e interoperabilidad entre varios servicios LDAP de diversos proveedores de software tanto privativo como basado en Software Libre y Código Abierto.

El desarrollo de la solución responde a las necesidades puntuales de depuración, gestión y unificación de cuentas de usuario, la migración a plataformas de código abierto y la integración del Directorio Institucional dentro del proyecto de la Nube Académica Computacional (NAC) de la Universidad de Costa Rica.

Palabras Clave: Migración entre Directorios Activos, LDAP, Nube Computacional, PostgreSQL.

Eje temático: Infraestructura y desarrollo de software.

1 Introducción

Las instituciones de educación superior, dada la cantidad de usuarios de servicios informáticos con que cuentan, requieren de repositorios de cuentas de usuario robustos, de fácil implementación y que permitan la escalabilidad tanto horizontal como vertical. Asimismo, dichos repositorios deben permitir una fácil adaptabilidad a las necesidades y características específicas de cada institución, además de ser fácilmente gestionables e interoperables con los servicios y sus protocolos.

El presente trabajo tiene como fin mostrar el proceso de migración que efectuó la Universidad de Costa Rica (UCR) en el servicio de Directorio Institucional. Para esto es importante contextualizar la Universidad con un vistazo general sobre la institución, así las cosas, se debe tomar en consideración que esta universidad es pública y está conformada aproximadamente por 40.580 estudiantes, 9.000 docentes y/o administrativos distribuidas en 6 sedes universitarias, 6 recintos y más de 40 centros e institutos de investigación, además de otras instancias ubicadas a lo largo del territorio nacional. Siendo la Sede Rodrigo Facio la principal y ubicada en San José. La UCR cuenta con una de las mejores infraestructuras para una institución académica universitaria en el país, distribuyendo conectividad de red e Internet en todas las instalaciones a lo largo de Costa Rica, un total de 626.370,16 m² de área constructiva y 8.455.354,69 m²[1] en total.

Se ofrecen más de 600 opciones académicas entre profesorados, diplomados, bachilleratos, licenciaturas y posgrados en sus 13 facultades. El financiamiento es básicamente gubernamental y ronda para el 2017 los $554.237.740,00 según datos del sitio de transparencia y Gobierno Abierto institucional. La universidad se relaciona con otras universidades e instituciones dentro y fuera del país, ya sea por investigación, docencia, acción social, convenios de cooperación o relaciones meramente consultivas que van desde compartir experiencias académicas, hasta transferencias tecnológicas y proyectos conjuntos.

Así las cosas este directorio consta de un repositorio de cuentas de cerca de 150,000 usuarios entre los que se cuentan estudiantes, docentes, personal administrativo, personal jubilado y otros grupos menores y aproximadamente 2,000 cuentas para distintas unidades académicas y/o administrativas que son parte activa de las dinámicas universitarias.

Este documento está compuesto por las siguientes secciones:

- Antecedentes, donde se presentan las características del estado anterior del Directorio Institucional que motivaron la migración.
- Diseño, donde se presenta la topología física y lógica, así como cada componente de software que integra toda la solución implementada.
- Repositorio de cuentas de usuario, donde se describen en detalle las estructuras de datos y la distribución de servidores.
- Implementación de la alta disponibilidad, donde se explica la solución para provisionar el servicio de alta disponibilidad y balanceo de cargas.

---

[1] Tomado de http://www.ucr.ac.cr/acerca-u/ucr-en-cifras.html, acá se consideran las áreas de reservas naturales y zonas de investigación.

- Implementación del sistema de gestión de cuentas, que detalla los componentes de software que interactúan con la gestión adecuada (CRUD) de cuentas, desde el punto de vista de los gestores de datos.
- Trabajo futuro y retos, donde se describen en forma general, las actividades derivadas de este proyecto.

2 Antecedentes

El Directorio Institucional se encuentra en producción desde el año 2007 y provee un servicio único de autenticación para varios servicios institucionales, entre ellos el correo electrónico institucional y el sistema de expediente único para los funcionarios.

Básicamente existían dos tipos de cuentas:

- Cuentas de personas con la siguiente información:
    - Datos personales (nombre, apellidos, dirección de residencia, identificación personal, entre otros).
    - Datos de sistemas institucionales, requeridos para su adecuada operación o configuración (cuotas de casillero de correo electrónico, listados de contactos, entre otros).
- Cuentas de servicios, utilizadas por los servicios existentes para consultar y autenticar a usuarios desde esos servicios. Existen cerca de 60 servicios/sistemas institucionales que utilizan el Directorio Institucional para la autenticación de sus usuarios. Básicamente, poseen un identificador de cuenta y una contraseña. Estas cuentas están ligadas a listas de control de acceso, por medio de las cuales se determinan las cuentas de usuario que utilizan dichos servicios.

2.1 Características de la plataforma tecnológica

La plataforma tecnológica anterior, 2007, se basaba en Sun ONE Directory Server 7, utilizando el Protocolo Ligero de Acceso a Directorios (LDAP), para la cual ya en el 2013 no se contaba con mantenimiento y soporte por parte de SUN Microsystems.

El servicio ejecutaba el sistema operativo Solaris 10, en dos servidores físicos, sin un ambiente de desarrollo ni de pruebas.

La seguridad lógica de la plataforma era otro factor a considerar, ya que el servicio se encontraba accesible desde cualquier parte de la red de datos institucional y corría a través del protocolo LDAP inseguro (puerto 389 TCP).

2.2 Sobre los datos de usuario

La gestión de datos del usuario se llevaba a cabo utilizando una serie de scripts de sistema operativo y una aplicación desarrollada en Power Builder. Esos componentes

de software carecían de respaldo técnico, por lo que su mantenimiento se volvió altamente costoso. Esto también contribuyó a que los datos rápidamente perdieran vigencia.

Asimismo, si una persona era estudiante y empleado al mismo tiempo, el sistema le asignaba dos cuentas de usuario, una para cada rol. En algunos casos, si a un estudiante se le asignaba un nuevo código de estudiante, el sistema era incapaz de reconocer si la información correspondía a una misma persona, por lo que le asignaba una cuenta nueva. De esta forma esas personas debían gestionar al menos dos cuentas distintas.

La mayoría de los datos registrados en cada cuenta correspondían a parámetros de configuración de otros servicios. Esto generó una dependencia tecnológica entre plataformas de servicios y la plataforma LDAP, además de que cada cuenta de usuario terminó por contener datos en su mayoría irrelevantes, repetidos y desactualizados.

2.3 Sobre los procedimientos de gestión

La información de las nuevas cuentas de usuario era entregada a las personas en forma impresa en soporte papel, con la contraseña en texto plano, de forma que si una persona perdía ese reporte, corría el riesgo de que su cuenta fuera accedida por terceros.

Los períodos de creación masiva de cuentas para estudiantes de primer ingreso, se generaba una cantidad cercana a 8,000 cuentas, es decir la misma cantidad reportes de contraseñas.

Una grave ausencia de ese sistema era la localidad, es decir, ante la perdía de la contraseña de un usuario, este debía acudir al Centro de Informática, en la Sede Rodrigo Facio para la recuperación de la misma.

Por otra parte, la gestión de cuentas de usuarios era compleja ya que la inserción se realizaba en forma semiautomatizada, se carecía de edición de datos y no existía control si una persona ya poseía una cuenta.

3 Plan de trabajo

El plan de trabajo para la implementación de la nueva solución se dividió en las siguientes fases:

- Análisis del directorio existente, que incluyó análisis del contenido de los datos, arquitectura existente, equipos físicos, procedencia y formato de datos, análisis de los procesos y los componentes de software existentes.
- Documentación de requisitos, tanto para el sistema de gestión de cuentas como para el nuevo servidor de directorio, además del diseño de la base de datos relacional.

- Análisis de soluciones, la cual incluyó la elección del servidor para el directorio, lenguajes de programación, sistemas gestores de bases de datos, desarrollo casero versus outsourcing.
- Depuración de datos, que incluyó la definición de formatos de datos, eliminación de datos irrelevantes, depuración de los existentes y análisis y unificación de cuentas de usuario duplicadas.
- Fase de desarrollo, donde se incluyó la codificación, ejecución de pruebas, corrección de errores, implementación del servidor de directorio y ejecución de pruebas de autenticación con sistemas de prueba.
- Fase de migración, que incluyó la gestión de datos en el directorio viejo y el directorio nuevo, la asesoría y acompañamiento a los gestores de sistemas/servicios institucionales en la migración al nuevo directorio, migración de sistemas y servicios propiamente dicha.
- Fase de análisis de riesgos y gestión de la continuidad del servicio, que incluyó análisis y calificación de riesgos, definición de controles y pruebas de recuperación del servicio.

4 Descripción de la solución

Con el análisis del directorio existente y las necesidades universitarias se determinó que se requiere enfocar la solución sobre tres ejes principales: el servicio de directorio basado en LDAP, el sistema web para gestión de usuarios basado en las reglas de negocio de la Universidad de Costa Rica y el rediseño de procesos técnico-administrativos. Pero, dentro de las soluciones y requerimientos se detectó la necesidad de prever la conectividad de la solución con diversos sistemas LDAP tales como Active Directory de Microsoft, 389 Directory Service y FreeIPA, así entonces como parte de la solución se crea un componente de conectividad hacia diversos directorios activos de proveedores de software diferentes e implementaciones de LDAP diferentes basada en la versión actual del protocolo, la LDAPv3 definido en los RFCs 2251, 2256, 2829, 2830 y 3377 [2], donde se cuenta con funciones CRUD típicas, una organización jerárquica en forma de árbol, y un robusto mecanismo de control de acceso basado en permisos y roles, entre otros [1].

4.1 Sobre las fuentes institucionales de datos de usuario

La información para generación y mantenimiento de cuentas de usuario proviene de varias fuentes, entre las cuales se pueden citar las siguientes:

- Sistema de Aplicaciones Estudiantiles (SAE). Proporciona los datos básicos de estudiantes que se encuentran activos al momento de realizar la consulta.
- Sistema de Información de Recursos Humanos (SIRH). Proporciona los datos de funcionarios activos, funcionarios pensionados y funcionarios cesados.

- Sistema de Becados al Exterior (SIBEX). Proporciona datos de becados al exterior.
- Datos de personal contratado. Son personas que no forman parte de la planilla de Recursos Humanos, sino que son contratados a través de proyectos de investigación.
- Cuentas departamentales. Se denomina así a las cuentas de usuario que utilizan las dependencias universitarias para envío de correos electrónicos relacionados con su quehacer diario, realización de eventos (congresos, seminarios, etc.), entre otros.
- Otras fuentes. Son datos para la creación de cuentas de usuario de casos especiales a solicitud de las dependencias universitarias.

Para todos los casos, existen procedimientos automatizados, ya sea mediante el acceso a bases de datos o ejecutando procesamientos de archivos separados por comas. La tabla 1 muestra las fuentes de datos a partir de las cuales se generan las cuentas de usuario, en la Universidad de Costa Rica.

Tabla 1. Fuentes de datos de los usuarios del Directorio Institucional.

Tipo de usuario	Fuente de datos	Cantidad de cuentas activas (Marzo 2017)
Estudiante	Oficina de Registro e Información (ORI)	67793
Empleado (docente, administrativo)	Oficina de Recursos Humanos (ORH)	9709
Personal jubilado	Oficina de Recursos Humanos (ORH)	2684
Becados al exterior	Oficina de Asuntos Internacionales (OAICE)	402
Cuentas departamentales	A solicitud de cada dependencia universitaria	2187
Otros	Varias fuentes	949
Total:		**83724**

4.2 Servicio de directorio basado en LDAP

Para elegir el software de servicio de directorio se tomaron como premisas indispensables las siguientes: Implementación en código abierto, configuración y administración sencilla, implementación de protocolo seguro (LDAPS, puerto 636 TCP) y escalabilidad.

Se analizaron los directorios 389 Directory Server y su "hijo" FreeIPA, en las versiones estables disponibles a octubre 2015. Se efectuaron pruebas de rendimiento asociadas a la creación, edición y eliminación de usuarios en distintos escenarios de tamaño de la base de datos del directorio. De esta forma, se probaron principalmente inserciones masivas de lotes de 10,000 usuarios separados en 2 ó 3 threads, en contextos en los que el directorio tuviera previamente registrados 40,000, 50,000 y 60,000 usuarios.

389 Directory Server presentó tiempos de ejecución de a lo sumo 10 minutos, mientras que FreeIPA presentó tiempos de ejecución de entre 17 y 29 horas.

Por ello, se escogió el servicio 389 Directory Server, un servidor LDAP desarrollado por Red Hat, el cual cumplió plenamente con los requerimientos básicos, principalmente por su facilidad y rapidez de implementación desde cero.

Se configuraron cinco servidores en un clúster multimaestro-consumidor, de acuerdo con la guía técnica en la documentación que Red Hat tiene disponible en la Internet [3].

4.2.1. Topología y componentes del servicio de directorio

Como se muestra en la figura 1, se pueden distinguir tres bloques de servicios bien definidos, a saber, servidores multimaestros, servidores consumidores y servicio balanceador.

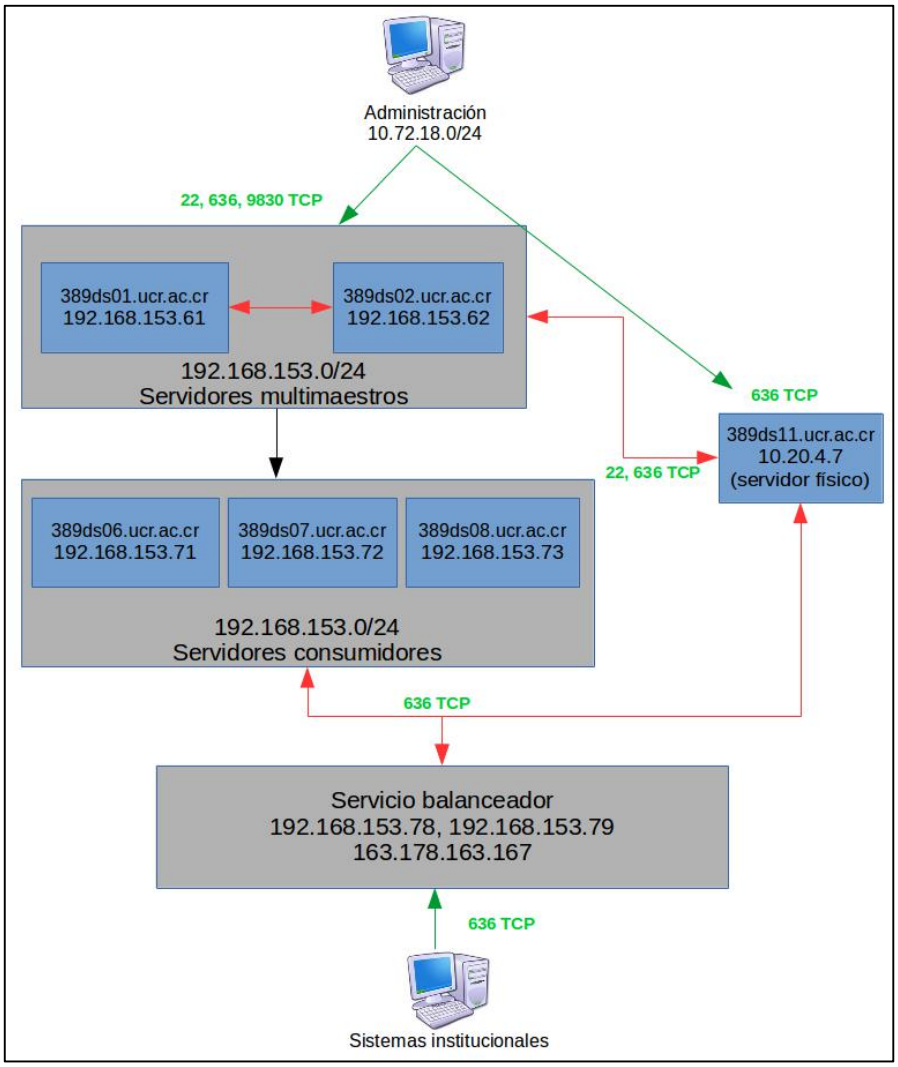


Fig. 1. Topología del servicio de directorio.

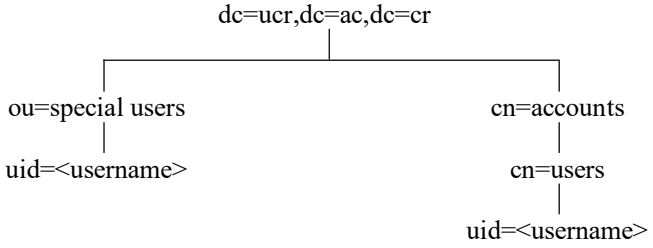
El servicio de directorio está integrado por los siguientes componentes básicos:

- **Servidores multimaestro**. Consta de dos servidores virtuales que permiten la inserción (ldapadd), modificación (ldapmodify), consulta (ldapsearch) y eliminación (ldapdelete) de cuentas de usuario y que se replican mutuamente los datos, creando un ambiente de redundancia y alta disponibilidad.
  Estos servidores solamente son accedidos desde el sistema web de administración de cuentas a través del puerto 636 TCP (operaciones CRUD), desde la red de administración a través de los puertos TCP 22 (para administración), 636 (pruebas de operación del servicio) y 9830 para gestión desde una consola gráfica remota.
- **Servidores consumidores**. Consta de tres servidores virtuales que literalmente "consumen" los datos de las cuentas de usuario desde los servidores multimaestro. Estos consumidores permiten operaciones de consulta (ldapsearch) de cuentas de usuario y son accedidos desde los servidores multimaestro a través del puerto 389 TCP (replicación), desde los servidores de balanceador por el puerto 636 TCP (ldapsearch), desde la red de administración a través de los puertos TCP 22 (para administración), 636 (pruebas de operación del servicio) y 9830 para gestión desde una consola gráfica remota.
- **Servidor físico de respaldo**. Este servidor opera en forma activo – activo con los multimaestros y puede ser accedido para consultas como un consumidor. De esta manera se brinda un ambiente alterno de respaldo en un sitio físico separado de los servidores virtuales.
  El acceso a este servidor es a través de los puertos indicados en los dos tipos anteriores. Sin embargo, el acceso por el puerto 22 está disponible únicamente desde esos otros servidores.
- **Servicio balanceador**. Consta de dos servidores virtuales con HAProxy [4]; actúan como balanceadores de carga de peticiones que llegan desde los sistemas/servicios de la solución y Keepalived [5], anunciando el servicio de directorio a través de una dirección IP virtual hacia los sistemas/servicios cliente.
  El acceso a este servidor está condicionado mediante instrucciones de IPtables. Y sólo los sistemas/servicios previamente autorizados y configurados pueden acceder al servicio, por el puerto 636 TCP.
  Las consultas llegan desde los sistemas/servicios hasta el servicio de balanceo, el cual las distribuye en los nodos consumidores utilizando un algoritmo round-robin.

En relación con los certificados de seguridad, los servidores consumidores proporcionan los certificados para la comunicación a través de LDAPS. Por su parte, el servicio balanceo utiliza un certificado público de la autoridad certificadora Let's Encrypt [6], lo cual permite que cualquier sistema debidamente registrado y autorizado, pueda realizar consultas al servicio de directorio sin necesidad de instalar certificados.

4.2.2 Estructura del directorio y organización de los datos de las cuentas de usuario

En cuanto a la estructura de jerarquía, se implementó el siguiente formato:



La rama derecha (cn=users,cn=accounts) corresponde al subdirectorio dentro del cual están todas las cuentas de usuarios. La rama izquierda (ou=special users) corresponde a todas las cuentas que utilizan sistemas/servicios institucionales para la consulta y autenticación de usuarios.

Se utilizaron atributos de las clases estándar de LDAP para el almacenamiento de datos. Sin embargo, debido a que la Institución requiere el almacenamiento de otros atributos específicos, se creó una clase de objeto llamada ucrUserInformation, para la definición de los siguientes atributos:

- Carné de estudiante
- Número de empleado
- Correo electrónico alternativo
- Segundo apellido
- Identificación
- Tipo de identificación
- Descripción del estado de la cuenta del usuario
- Perfil del usuario (puede contener varios valores)
- Nombre “conocido como”
- Primer apellido “conocido como”
- Segundo apellido “conocido como”

4.3 Sistema web para gestión de usuarios

El Directorio Institucional cuenta con una aplicación web para la administración de las cuentas de usuarios, que permite realizar tareas básicas como creación, edición, consultas e inactivación de usuarios.

4.3.1. Funcionalidades

A continuación se describen las funcionalidades del sistema web:

- Inserción y modificación de cuentas de usuario, en forma individual o por lotes. En el caso de los trabajos por lotes, se realizan en forma automatizada mediante la conexión a las bases de datos de sistemas institucionales o por medio de archivos separados por coma (CSV).
- Inactivación de cuentas de usuario en forma individual o por lotes.
- Consulta de cuentas de usuario por varios criterios de búsqueda.
- Modificación de datos específicos, de acuerdo con requerimientos generados desde otros sistemas.
- Posibilidad de escribir datos y generar cuentas en varios tipos de directorios tal como se mencionó anteriormente: FreeIPA, 389 Directory Server y Active Directory entre otros.

4.3.2. Sistema gestor de bases de datos

Para el almacenamiento y gestión de datos se configuró el servicio de PostgreSQL en modo maestro-esclavo en equipos virtuales. La configuración de esquemas y tablas es la siguiente:

Base de datos: sdi	
Esquema:	cuentas
Tablas	
Datos de cuentas:	EstudiantesActivos FuncionariosActivos HistoricoRelacion RelacionUcr Usuarios
Catálogos:	Categorias MotivoCese TipoIdentificacion
Auditoría y gestión:	Bitacoras Perfiles
Sistema de menús y usuarios de sistema:	Items MenuPerfiles Parametros SistemaMenus UsuariosSistema

4.3.3. Sistema web propiamente dicho

La aplicación web fue desarrollada en lenguaje Java utilizando el patrón de arquitectura de software Modelo-Vista-Controlador. El proceso de análisis y diseño concluyó la necesidad de mejorar los procesos existentes e incorporar nuevos procesos; en la Figura 2 se presenta el diagrama de arquitectura del sistema. Las funcionalidades y el diseño se describen a continuación:

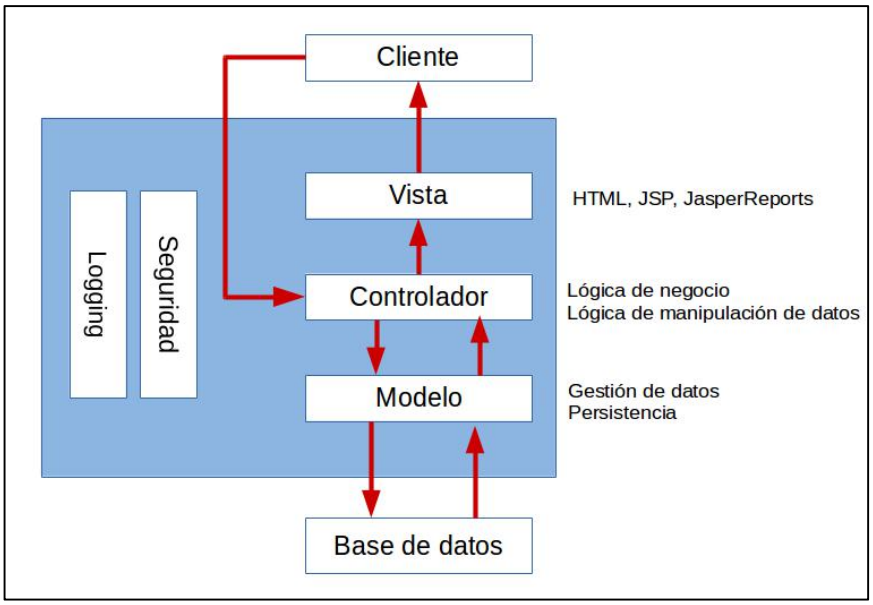


Fig. 2. Arquitectura del sistema empleando el modelo-Vista-Controlador.

Modelo: El mapeo objeto-relacional (ORM) se realiza utilizando Hibernate. Cada entidad en la base de datos tiene un objeto asociado en el modelo, con excepción de las entidades con llaves primarias compuestas por dos o más atributos, en cuyo caso el modelo presenta un objeto adicional para la llave primaria (Primary Key o PK) asociado al respectivo objeto. Cada objeto tiene sus respectivos métodos Get y Set para cada atributo.

Controlador: El controlador, por su parte, tiene un conjunto de clases de control que se comunican con las clases de servicio del modelo para acceder a la base de datos. También tiene un conjunto de clases que implementan la lógica de negocio, de acuerdo con las funcionalidades. El controlador se comunica con la vista mediante el envío de mensajes y resultados a través de una interfaz tipo Map que permite el almacenamiento de duplas parametro-valor, que son utilizadas por la vista para presentar los datos al usuario.

Por otra parte, el controlador se encarga de implementar las acciones necesarias para que el sistema operativo efectúe las operaciones de manipulación de las cuentas de usuario en el servidor de directorio (LDAP), mediante el uso la API de Java para acceso a directorios LDAP.

Vista: La aplicación utiliza las siguientes interfaces para generar resultados:

- Presentación web para captura de datos, presentación de resultados de procesamiento y de consultas, generación de mensajes de error, información y advertencia. Se utiliza HTML5, CSS 3 y JQuery.
- Reportes de resultados en formato ODF. Se utiliza JasperReports de Jasper Soft Studio.
- Mensajes de correo electrónico para envío de resultados a los usuarios del Directorio Institucional.

Seguridad a través de la aplicación: Acceso de usuarios al sistema: se cuenta con una administración de usuarios basada en roles. Cada usuario utiliza su nombre de usuario (username) y contraseña registrados en el Directorio Institucional (LDAP) para el ingreso al sistema.
Seguridad a nivel de equipos y red: se configuró muros de fuego en cada servidor, según las siguientes condiciones:

- El servidor de la aplicación y el sistema gestor de bases de datos están en segmentos de red distintos.
- El tráfico de red entre servidores solamente está garantizado para las direcciones IP de los equipos involucrados. Como excepción, solamente se autoriza el ingreso de las direcciones IP de las PCs de los usuarios administradores hacia el servidor de aplicación a través del puerto 8080 de TCP (Tomcat).
- El servidor de Directorio (LDAP) solamente será accedido desde el servidor de aplicación a través del puerto 636 de TCP.
- Las transacciones de base de datos se realizarán a través del controlador de la aplicación, de acuerdo con los principios de la arquitectura Modelo-Vista-Controlador.
- La aplicación web para administración será la única que accederá a los servidores multimaestros del Directorio Institucional.

4.4. Procesos administrativos

Los procesos que se mejoraron y crearon son los siguientes:

- Entrega de contraseñas a los usuarios: se estableció con carácter de obligatoriedad que cada usuario registre una cuenta de correo electrónico alterna a la institucional para que el sistema envíe información relacionada con su cuenta institucional, como por ejemplo el cambio de contraseña y otras notificaciones relativas al servicio; brindando mayor seguridad a la entrega de contraseñas, se sustituye la entrega de contraseñas impresas en soporte papel y se prevén nuevos procesos de recuperación de la clave de manera remota.
- Definición de perfiles de cuentas de usuario: se definen y crean nuevos perfiles de cuentas de usuario para limitar el acceso a los sistemas/servicios según el rol dentro de la Institución.
- Automatización del procesamiento de cuentas: con excepción de los procesos existentes para cuentas de estudiantes y funcionarios, se definieron nuevos procesos y reglas de negocio para la automatización de creación y edición de cuentas de otros perfiles de usuario.
- Segregación de componentes: los servicios institucionales almacenan sus parámetros en bases de datos propias. El Directorio Institucional solamente almacena datos relacionados a la identificación y autenticación de los usuarios.
- Reducción de datos almacenados en cada cuenta: como consecuencia de lo anterior, los datos almacenados en las cuentas de los usuarios se redujeron considerablemente lo cual mejora el rendimiento y gestión del Directorio.

- Unificación de datos, cuentas, para usuarios con dos o más cuentas con perfiles antiguos: se detectaron cerca de 7,500 usuarios que tenían dos o más cuentas registradas en el Directorio Institucional anterior, en su mayoría, como estudiantes y como empleados. Se ejecutó un procedimiento mediante el cual cada usuario indicara cuál de los nombres de cuentas usaría como definitiva. Los datos relacionados con las cuentas a eliminar se guardaron en la cuenta definitiva, a solicitud de los usuarios que así lo expresaran.
- Se documentó todo el proceso de continuidad del servicio, que incluyó el análisis y evaluación de riesgos, definición de controles, documentación y pruebas de los procedimientos de recuperación del servicio en caso de desastres. Esto implicó un proceso de capacitación arduo del área de investigación y desarrollo hacia el área de gestión de servicios dentro del Centro de Informática lo cual garantiza la adecuada gestión del servicio nuevo.

5. Proceso de migración

El proceso de migración entre la plataforma SunOne y la nueva plataforma 389 Directory Server involucró las siguientes etapas:

5.1. Comunicación y coordinación con gestores de TI

En sesiones de trabajo con los gestores de sistemas y servicios que se autentican con el Directorio Institucional se explicaron las indicaciones y las consideraciones necesarias para migrar los sistemas en producción al nuevo directorio. Los aspectos más importantes están los siguientes:

- Homologación de tipos de datos en los sistemas.
- Homologación de los nombres de los atributos en los sistemas con los existentes en el nuevo servidor de directorio.
- Activación de certificados de seguridad para la configuración de LDAP Seguro.
- La imperante e irrefutable ejecución de pruebas en las plataformas de desarrollo.

5.2. Gestión de datos simultánea en ambas plataformas

Con el fin de efectuar una migración lo más transparente posible, fue necesario configurar la aplicación web de gestión de cuentas para que realizara las inserciones y modificaciones en ambos directorios activos, el SunOne como en 389 Directory Server. De esta forma, se mantuvieron ambos directorios estrictamente sincronizados para facilitar el pase de los sistemas al nuevo directorio, sin afectar a los usuarios finales.

5.3. Proceso de migración de sistemas y servicios

El proceso de migración se realizó en primera instancia con un clúster de dos servidores de directorio, configurados de acuerdo con la documentación del producto. Así las cosas la migración de los sistemas se llevó a cabo en forma paulatina, con el

fin de ajustar el dimensionamiento del rendimiento planteado inicialmente para el servicio, según recibiera la carga de trabajo se podría ajustar. De esta forma, la migración se llevó a cabo en el siguiente orden:

- Sistemas y servicios de alto acceso: Se consideran así los servicios a los que tiene acceso el 100% de los usuarios.
    - Correo electrónico: dado que tiene varios componentes, cada uno de los cuales realiza autenticación con el servicio de directorio. Se migró cada componente por separado y con base en los resultados se determinó la necesidad de configurar un nuevo nodo de 389 Directory Server.
    - Servicio de red inalámbrica: se monitoreó el impacto en el servicio determinado la necesidad de ajustes en los tiempos de espera del servicio de red inalámbrica.
- Sistemas o servicios de mediano acceso: Se refiere a sistemas en los que la población meta es específica y limitada. El monitoreo no mostró efectos significativos de la migración de estos servicios sobre el rendimiento. Estos servicios son:
    - Expediente Único
    - Sistema de Información de Recursos Humanos
    - Aula Virtual
    - Servicios de información del Sistema de Bibliotecas (SIBDI)
- Sistemas o servicios de bajo acceso: Se refiere a servicios en que no se superan los 20 usuarios autenticados. Fueron cerca de 45 servicios/sistemas de este tipo. Cabe destacar que algunos de ellos corresponden a nuevos servicios, los cuales fueron implementados directamente contra la nueva plataforma.

6. Trabajo futuro y retos

El Centro de Informática y el Centro de Investigación en Tecnologías de la Información y Comunicación (CITIC) han estado desarrollando conjuntamente un proyecto para la implementación de la "Nube Académica Computacional" (NAC).

La NAC contará con servicios de autenticación basada en Kerberos, LDAP, SSO entre otros, por lo que el servicio de Directorio Institucional nuevo forma parte fundamental de dicho proyecto y se diseñó conceptualizando esta integración.

A raíz de ello, la plataforma de servicio de directorio descrita a lo largo de este documento, constituye la primera etapa del sistema de autenticación de la NAC, una pieza de un IDM o Gestor de Identidad.

Como segunda etapa se prevé la instalación y configuración de un clúster basado en el software FreeIPA, dejando como plataforma de respaldo la basada en 389 Directory Server existente, pero ambos conectados y sincronizados a la misma plataforma de gestión para el Directorio Activo.

Debido a que el proyecto de la NAC incluye servicios orientados a equipos con sistema operativo Windows, será necesario incluir la definición específica para la

conectividad con el servicio de Active Directory el cual precisamente es un elemento transcendental del proyecto donde se explota la utilización de Kerberos.

Como parte del mejoramiento continuo de la plataforma nueva, es necesario brindar mayor robustez al sistema gestor de bases de datos PostgreSQL por lo que se tiene en la hoja de ruta para mejoras la implementación del servicio como un clúster de alta disponibilidad (HA) empleando herramientas como pgPool o similares.

Finalmente, es indispensable finalizar el proceso de licenciar los productos del proyecto bajo licencias Creative Commons y GLPL para facilitar así la publicación y crecimiento público y abierto del desarrollo.

7. Conclusiones

La mejora tecnológica al Directorio Institucional de la Universidad de Costa Rica, acá expuesta, cumple con características de fácil gestión, fácil implementación y escalabilidad necesarias por el entorno dinámico e interoperable de la institución.

Las necesidades de interoperabilidad entre diversos directorios activos impulsaron la creación de este elemento de software que gestiona, controla y sincroniza cuentas de usuarios y sus variaciones contra las plataformas que cumplen con implementan el LDAP, el esfuerzo esta en crear el módulo que "traduzca" del LDAP estándar en las estructuras y formatos específicos de una implementación. Esta funcionalidad facilita procesos de migración e incluso actualización sin olvidar la necesidad que muchas organizaciones de orden universitario requiere de interoperabilidad.

Ese es el gran mérito del trabajo realizado, probado y en producción; el cual esta disponible para ser mejorado y adaptado por otros centros educativos según sea solicitado y mantengan el espíritu académico y libre de las implementaciones.

Ahora bien, no se puede obviar que las mejoras o migraciones aplicadas a los servicios en producción conllevan cambios en los procesos asociados a dichos servicios. Esos cambios deben cumplir las siguientes características:

- No reñir con las leyes del país ni la normativa de la organización.
- Ser aprobados por la alta gerencia.
- Ser adecuadamente comunicados a todas las partes.
- Ser adecuadamente entendidos por todas las partes.

A partir de allí es necesaria una adecuada gestión del cambio e ingeniería de requerimientos que involucre a todas las partes interesadas. En este caso se debe tomar en cuenta las jefaturas, los gestores de TI, los gestores de comunicación y el personal técnico directamente involucrado.

Referencias

1. Protocolo Ligero de Acceso a Directorios (LDAP), https://es.wikipedia.org/wiki/Protocolo_Ligero_de_Acceso_a_Directorios

2. Request for Comments. http://www.ietf.org/tools/
3. Red Hat Directory Server Documentation. Chapter 8. Managing Replication. https://www.centos.org/docs/5/html/CDS/ag/8.0/Managing_Replication.html
4. HAProxy. http://www.haproxy.org/
5. Keepalived. http://www.keepalived.org/
6. Let's Encrypt. https://letsencrypt.org/