Autenticación centralizada de los servicios digitales del ITC

José Jesús Sánchez Farías
Instituto Tecnológico de Celaya
jesus.sanchez@itcelaya.edu.mx

Oscar Grimaldo Aguayo
Instituto Tecnológico de Celaya
oscar.grimaldo@itcelaya.edu.mx

Luis Alberto López González
Instituto Tecnológico de Celaya
luislao@itcelaya.edu.mx

Juan Ignacio Cerca Vázquez
Instituto Tecnológico de Celaya
nacho@itcelaya.edu.mx

Resumen

En el artículo *"Autenticación centralizada para los sistemas de información de los Institutos Tecnológicos y Dgest"* publicado en el número 106 de esta revista, se planteó el problema de la autenticación de usuarios a nivel global dentro del sistema de Institutos Tecnológicos, y de cómo solucionar dicho problema en los sistemas de información ubicados en las Instituciones a nivel nacional. En este artículo se plantea una nueva solución que se puede implementar de manera local en las Instituciones, específicamente hablamos de los servicios digitales que ofrece hoy en día el Instituto Tecnológico de Celaya. Estos servicios incluye: Sistema Integral de Información, Red Inalámbrica Institucional, Sistemas de dosificación y Educación a distancia, así como cualquier otro sistema de información que se incorpore en un futuro a estos servicios.

Palabra(s) Clave(s): Autenticación de usuarios, servicios digitales, radius, freeradius.

1. Introducción

El Instituto Tecnológico de Celaya [1] cuenta actualmente con una gran variedad de servicios digitales que ofrece tanto a docentes, alumnos y personal administrativo. Entre estos servicios se pueden listar:

- **Sistema Integral de Información.** Este consiste en un sistema de información en el cual se lleva el control de los procesos administrativos de la institución.
- **Red Inalámbrica Institucional.** Es la red inalámbrica para acceso a internet que utilizan los alumnos y empleados de la institución.
- **Portal Web Institucional.** Es el sitio Web oficial de la institución, en el cual se publica información de las carreras, avisos importantes, así como información de los departamentos académicos y administrativos, entre otra información.
- **Correo electrónico Institucional.** Es el servicio de correo electrónico que ofrece la institución tanto para los empleados como para los alumnos.
- **Sistemas de dosificación y educación a distancia.** Son sistemas que están a servicio también de docentes y alumnos para llevar el control de los contenidos y seguimiento de las materias que se imparten semestre a semestre.

Estos servicios no necesariamente están comunicados entre sí, ni física, ni lógicamente, mucho menos comparten una base de datos centralizada para mínimo intercambiar información relacionada a los usuarios que los utilizan. Esto genera un descontento e incomodidad para los usuarios el tener que utilizar un nombre de usuario y contraseña diferentes para acceder a cada uno de estos servicios. Aunque resaltar que se ha avanzado en la integración de algunos de estos servicios como es el correo electrónico, red inalámbrica y sistema integral de información para acceder a ellos con el mismo usuario y contraseña. El problema de esta integración es que para lograrla se tienen que ejecutar muchos procesos internos que no llevan un estándar de autenticación y por lo tanto su labor se complica de manera exponencial, así tampoco se proporciona un método para que se integren nuevos sistemas o servicios.

El propósito entonces será plantear un esquema en el que todos estos servicios manejen un estándar de autenticación de usuarios, sea transparente y fácil de utilizar tanto para los usuarios finales como de los administradores del mismo.

Para lograr este propósito se utilizan una serie de herramientas y protocolos vigentes y perfectamente analizados y probados por compañías e instituciones alrededor del mundo. Hablamos específicamente del estándar de autenticación llamado *Radius* [2], motores de bases de datos como *MySQL* y Sistemas Operativos confiables y seguros como *Debian Linux*.

Todos estos elementos perfectamente instalados y configurados dan lugar a una infraestructura tecnológica que ofrece servicios de calidad a los usuarios finales. Las ventajas que se obtienen son:

- Seguridad en las cuentas de los usuarios.
- Se evita la duplicidad de cuentas.
- Los servicios están perfectamente sincronizados en cuanto a los usuarios y contraseñas que comparten.
- Al cambiar una contraseña para algún servicio, se refleja de manera inmediata en el resto.
- Evita al usuario manejar varias cuentas de usuario para acceder a los distintos servicios.

Protocolos AAA

El acrónimo AAA corresponde a los conceptos de Autenticación (Authentication), Autorización (Authorization) y Contabilización (Accounting). Estos no hacen referencia a un protocolo en particular, sino a un conjunto de ellos que ofrecen dichos servicios.

La autenticación es el proceso por el que una entidad demuestra que es quien dice ser, probando así su identidad frente a un sistema u otra entidad. En general, una entidad es un cliente, y la otra es un servidor ante el cual se requiere autenticación. La autenticación debe incluir las siguientes características: Fiabilidad, Factibilidad económica para una organización, Soporte a ciertos tipos de ataques informáticos y sobre todo ser aceptado por los usuarios finales.

La autorización se refiere a que, una vez que el usuario fue autenticado, pueda acceder a determinados recursos basado en los privilegios específicos que el sistema le provee.

Otras características:

- También pueden estar basadas en restricciones, tales como restricciones horarias, localización de la entidad solicitante, prohibición de logueos múltiples simultáneos del mismo usuario, etc.
- El proceso de autorización sirve para decir si la persona o dispositivo tiene permisos para acceder a los datos, funcionalidad o servicios del sistema.
- La mayoría de los Sistemas Operativos multiusuario incluyen proceso de autorización. Previamente, se realiza el proceso de autenticación, para identificar a los usuarios.

El Accounting o contabilización se refiere al seguimiento del consumo de los recursos de la red por un usuario. Los datos obtenidos pueden usarse para administración, planificación, facturación u otros propósitos. La contabilización puede ser en tiempo real o por lotes.

Radius

RADIUS es el acrónimo en inglés de Remote Authentication Dial-In User Server, el cual se utiliza para implementar los protocolos AAA y es quizás el más conocido. Utiliza el puerto UDP 1812 UDP y funciona como cliente-servidor. Su éxito residió, probablemente, en su implementación en proveedores de acceso a Internet (ISP), que fueron los que primero debieron incluir una instancia de autenticación remota a través de la red para validar las conexiones de sus clientes.

Radius es un servidor que blinda la seguridad de una red y protege diferentes servicios, usando protocolos.

Estos servicios pueden estar protegidos de diferentes formas, como es a través de usuario y contraseña para poder acceder a ellos (Autentificación), por otra parte, según el usuario, le autoriza unos servicios u otros según el rol de éste (Autorización) y finalmente, una vez que el usuario ha entrado, lo “vigila” para hacer un seguimiento de todo lo que hace (Accounting).

2. Métodos

En el departamento del Centro de Cómputo del Instituto Tecnológico de Celaya se lleva el control de la mayoría de los servicios digitales, tanto el área de redes como el área de desarrollo de software son los directamente responsables de llevar el funcionamiento de estos servicios. Cada uno de estos se lleva un procedimiento muy específico para incorporarlo al esquema de autenticación centralizada. Primeramente se debe realizar la instalación y configuración del servidor que actuará como punto central para laautenticación de usuarios, dentro de este se instalan los paquetes correspondientes a Freeradius y MySql para hospedar el servicio y base de datos, respectivamente.

Una vez instalado el servidor central, se procede a incorporar uno a uno de los servicios digitales. Para el caso del Sistema Integral de Información, programado en lenguaje PHP, se tiene que hacer cambios en el módulo específico de control de usuarios, indicándole que ahora la autenticación de estos la hará a través de un servidor Radius, adicionalmente se tiene instala un módulo para PHP llamado *php5-radius*.

La red inalámbrica institucional actualmente ya hace la validación de usuarios contra un servidor Radius, el problema es su integración con los demás servicios, para solventar este problema basta con redirigir la base de datos actual a la nueva base de datos que ahora ubicada en el servidor central de autenticación.

En el caso del sistema de educación a distancia llamado Lince Virtual [3], corresponde a un sistema que utilizan tanto docentes como alumnos, a estos se les proporciona un usuario y contraseña diferente al utilizado en los otros servicios digitales, en este sistema los docentes publican materiales para sus clases durante el semestre y el alumno puede consultar toda la información que se publique. Este sistema utiliza la plataforma de educación a distancia llamada Moodle [4], la cual está desarrollada en el lenguaje de programación PHP, lo cual facilita la incorporación al esquema centralizado, para lograr esto, es necesario instalar una serie de paquetes y librerías en el servidor físico que hospeda la plataforma, así como el módulo de Radius para Moodle. Entre los paquetes a instalar están *php5-radius, php-pear, php5-dev*.

Para el resto de los servicios como el portal del Instituto Tecnológico de Celaya, sistemas de dosificación y nuevos sistemas de información que pudiesen incorporarse en un futuro al esquema centralizado de autenticación, se propuso la solución de

"Instalación del módulo de Radius para Apache", este proceso consiste en instalar un módulo para el servidor de páginas web Apache, dicho servidor es el más popular y utilizado a nivel mundial en portales y sistemas web. El módulo para Apache es llamado *libapache-mod-auth-radius*.

Implementación

La implementación consiste en la instalación del servidor central de autenticación, así como de la incorporación de los servicios digitales al nuevo esquema. Estos se explican a continuación:

- **Servidor centralizado de autenticación de usuarios.** El procedimiento para realizar la instalación del servidor central es el siguiente:
  - ✓ **Instalación del Sistema Operativo.** Este es el paso inicial en el cual se debe instalar el Sistema Operativo Debian Linux, se recomienda este por su estabilidad, seguridad y facilidad en la instalación y configuración de los paquetes que se utilizarán. Para esto se debe descargar la imagen ISO de la página oficial de la distribución [5], y seguir el proceso estándar de instalación.
  - ✓ **Instalación de MySQL y FreeRadius.** Una vez instalado el sistema operativo, se prosigue a la instalación de los paquetes correspondientes al motor de base de datos MySQL y al servidor FreeRadius. Para se esto se ejecutan los siguientes comandos:

```
# apt-get install mysql-server
# apt-get install freeradius freeradius-mysql
```

  - ✓ **Configuración de MySQL y FreeRadius.**
    a. Habilitar la autenticación de usuarios por medio de la base de datos, para esto se modifica el archivo */etc/freeradius/radiusd.conf*:

```
# cd /etc/freeradius
# nano radiusd.conf
```

    y se descomenta la línea :

```
$INCLUDE sql.conf
```

    b. Generación de base de datos y carga de esquema de datos, esto se hace en el directorio */etc/freeradius/sql/mysql*:

```
# cd /etc/freeradius/sql/mysql
```

```
# mysql -u root -p
mysql> create database radius;
mysql> grant all on radius.* to radius@localhost identified by 'radius';
mysql> use radius
mysql> source schema.sql
mysql> show tables
```

c. Indicar a FreeRadius los parámetros de conexión a la base de datos:

```
# cd /etc/freeradius
# nano sql.conf
```

Se especifican los parámetros *"server, port, login, password y radius_db"*, de acuerdo a los establecidos en el paso anterior.

d. Modificar el archivo /etc/freeradius/sites-aviable/default, para indicar a los protocolos AAA que se basen en la base de datos creada:

```
# cd /etc/freeradius
# nano sites-aviable/default
```

Se buscan las secciones "*authorize y accounting"* y se descomenta donde aparezca la palabra "*sql"*.

e. En este punto se dan de alta todos los usuarios y contraseñas que deseamos sean parte del esquema de autenticación. Para esto se dan de alta en la tabla *radcheck* sobre la base de datos creada para tal propósito.

f. Es necesario indicar a FreeRadius que se harán conexiones remotas desde otros equipos, por ejemplo otros servidores que hospedan los servicios digitales. Para eso se edita el archivo */etc/freeradius/sql.conf*:

```
# cd /etc/freeradius
# nano sql.conf
```

Y se descomenta la linea "*readclients = yes".*

g. Cargar esquema de datos para las conexiones remotas, para esto:

```
# cd /etc/freeradius/sql/mysql
# mysql -u root -p radius
mysql> source ippool.sql;
mysql> source nas.sql;
```

Con el paso anterior se han generado una serie de tablas, entre ellas la tabla *nas*, que es en la que se introducen los clientes remotos. Los campos a introducir son los siguientes:

nasname: Dirección IP del cliente remoto, correspondiente al equipo que hospeda el servicio digital a integrar.

shortname: El nombre con el que queramos identificar al cliente remoto.

type: Utilizar valor *"other"*.

secret: Es la clave secreta que compartirán servidor y cliente (es el password que se configuró para el usuario *radius* de la base de datos *radius* y en el archivo *sql.conf*).

Con esto se concluye el proceso de instalación del servidor central. Cabe mencionar que cualquier cambio que se le haga a dicho servidor de FreeRadius, es necesario reiniciar el servicio con: # */etc/init.d/freeradius restart*

- **Sistema Integral de Información.** El procedimiento para incorporar el Sistema Integral de Información al esquema central de autenticación de usuarios es el siguiente:
  - ✓ **Instalar módulo de radius.** Al servidor donde está hospedado el sistema, se le debe instalar un módulo llamado *php5-radius*, esto es debido a que el sistema está desarrollado en el lenguaje de programación PHP y por lo tanto para que dicho lenguaje reconozca las instrucciones de conexión al servidor centralizado de autenticación, es necesario dicho paquete. Para instalar se ejecuta el siguiente comando desde una terminal con permisos de administrador:

```
# apt-get install php5-radius
```

  - ✓ **Modificar el módulo de autenticación.** El sistema está programado con el Framework de desarrollo llamado Yii [6], en este debe modificar el módulo correspondiente a la autenticación de usuarios para que ahora se conecte y autentique a los usuarios desde el servidor central, para esto se utilizan las siguientes instrucciones:

```
$radius = radius_auth_open();
$ip_address = "IP-SERVIDOR-CENTRAL";
$port= "1812"
$username = "nombre de usuario";
$password = "contraseña del usuario";
$shared_secret="radius"
```

```
radius_add_server($radius, $ip_address, $port, $shared_secret, 5, 3);
radius_create_request($radius, RADIUS_ACCESS_REQUEST);
radius_put_attr($radius, RADIUS_USER_NAME, $username);
radius_put_attr($radius, RADIUS_USER_PASSWORD, $password);
$result = radius_send_request($radius);
switch ($result) {
case RADIUS_ACCESS_ACCEPT:
  // La autenticación se hizo correctamente, ahora se puede redirigir a la página correspondiente.
  echo 'Autenticación exitosa';
  break;
case RADIUS_ACCESS_REJECT:
  // La autenticación a fallado, se manda mensaje de error al usuario de possible error de usuario y/o contraseña.
  echo 'Autenticación fallida;
  break;
default:
  die('Error durante el proceso de autenticación: ' . radius_strerror($radius));
}
```

En el código anterior habrá que adaptar variables a la situación actual del sistema para que recupere el usuario y contraseña que se conecta al sistema, así como pasar la dirección IP del servidor de autenticación, así como la llave de validación.

Adicionalmente se puede adaptar el módulo de autenticación del sistema para recuperar datos adicionales del servidor central de autenticación y guardarlos de manera local para futura referencia.

- **Sistema de Educación a Distancia**. El sistema de Educación a Distancia, mejor conocido como Lince Virtual, es una plataforma implementada bajo la herramienta Moodle. Para realizar la integración de este servicio al esquema central de autenticación, habrá entonces que hacer algunos ajustes a las configuraciones de Moodle, estas se describen a continuación:
  - ✓ En el equipo servidor donde se hospeda dicha plataforma, es necesario instalar algunos paquetes en el Sistema Operativo. Estos son *php5-dev php5-auth-pam php5-radius php-pear*, por lo que el comando a ejecutar en una terminal con permisos de administrador serán:

    ```
    # apt-get install php5-dev php5-auth-pam php5-radius php-pear
    ```
  - ✓ En seguida se instala el paquete Auth_RADIUS para pear [7]

```
# pear install radius Auth_RADIUS
```

- ✓ En seguida se agrega la siguiente línea al archivo *php.ini*

```
extension=radius.so
```

- ✓ Posteriormente se reinicia el servicio de Apache:

```
# /etc/init.d/apache2 restart
```

- ✓ Finalmente se accede a la herramienta administrativa de Moodle para realizar las configuraciones correspondientes a la autenticación de usuarios, en esta, se tiene que indicar la dirección IP del servidor de autenticación, puerto y clave de validación.

- **Resto de los servicios digitales**. Para el resto de los servicios que funcionan vía Web y a través del Servidor Web Apache, se recomienda hacer la autenticación al servidor central mediante un módulo propio de Apache, los pasos son los siguientes:
  - ✓ En el servidor que hospeda el servicio, poniendo como ejemplo el portal Web del Tecnológico de Celaya, se instala el siguiente paquete desde una terminal con permisos de administrador:

```
# apt-get install libapache-mod-auth-radius
```

  - ✓ Modificar archivo de configuración de Apache llamado *apache2.conf*, agregando las siguientes líneas:

```
AddRadiusAuth IP_SERVIDOR_CENTRAL:1812 radius 5
AddRadiusCookieValid 60
<Location /ubicacion_portal_web_itc >
 Options Indexes FollowSymlinks
 AuthType Basic
 AuthName "Autenticación central de Radius"
 AuthBasicAuthoritative Off
 AuthBasicProvider radius
 AuthRadiusAuthoritative on
 AuthRadiusActive On
 Require valid-user
</Location >
```

  - ✓ Se deben modificar algunos parámetros como la dirección IP del servidor de autenticación central, puerto y llave de validación, así también, indicar en *"/ubicación_portal_web_itc"*, la ruta completa hacia la carpeta que hospeda el portal Web o proyecto a proteger.

- ✓ Finalmente se reinicia el servicio de Apache con:

```
# /etc/init.d/apache2 restart
```

3. Resultados

El Instituto Tecnológico de Celaya actualmente tiene una matrícula de más de cuatro mil estudiantes, así como 500 empleados aproximadamente, esto dos da un total aproximado de cinco mil usuarios potenciales que todos los días acceden a los servicios digitales que la institución ofrece. Con la implementación de este esquema de autenticación centralizada, se verían beneficiados ese mismo total de usuarios, manejando un solo usuario y contraseña para acceder a todos los servicios y también a los nuevos que vayan surgiendo.

Otros beneficios que se obtienen son:

- Uso de una sola cuenta de acceso a los servicios digitales.
- Ahorro en tiempo para los usuarios al no tener que estar recordando o tratando de recuperar cuentas olvidadas o perdidas.
- Eficiencia en el servicio.
- Fácil administración para los administradores de los servicios digitales.
- Fácil integración de nuevos servicios y sistemas que surjan en un futuro.
- Ahorro en dinero al no ser necesario tener varios equipos validando usuarios, sino solamente uno, máximo dos como respaldo.
- Mejora en el rendimiento de los sistemas al delegar el proceso de validación de usuarios y contraseñas al servidor central.

4. Conclusión

El hecho que una empresa o institución sea de gran tamaño, así como la cantidad de servicios que ofrece a sus empleados o clientes, no refleja que estos sean de calidad, en ocasiones, al ser tantos, dificulta su administración así como la comunicación y coordinación entre ellos. Al final si los servicios ofrecidos no dejan satisfecho al usuario que los utiliza y no le solucionan un problema, por tantos que sean o el tiempo que se les haya dedicado en realizarlo, de nada habrá servido.

Es por eso que con el afán de ofrecer un mejor servicio a los usuarios de los sistemas digitales del Instituto Tecnológico de Celaya, se propone este nuevo esquema de validación y autenticación de usuarios, el impacto tecnológico que puede llegar a tener es enorme, así también el llegar a ser una de las pocas instituciones públicas a nivel nacional que ofrecen este tipo de servicios a sus empleados y alumnos.

5. Referencias

[1] Instituto Tecnológico de Celaya (ITC). http://www.itcelaya.edu.mx/

[2] Radius. https://www.gnu.org/software/radius/

[3] Lince Virtual. http://lincevirtual.itc.mx/2.7/

[4] Moodle. https://moodle.org/?lang=es

[5] Debian Linux. https://www.debian.org/distrib/

[6] Yii Framework. http://www.yiiframework.com/

[7] Pear Framework. http://pear.php.net/