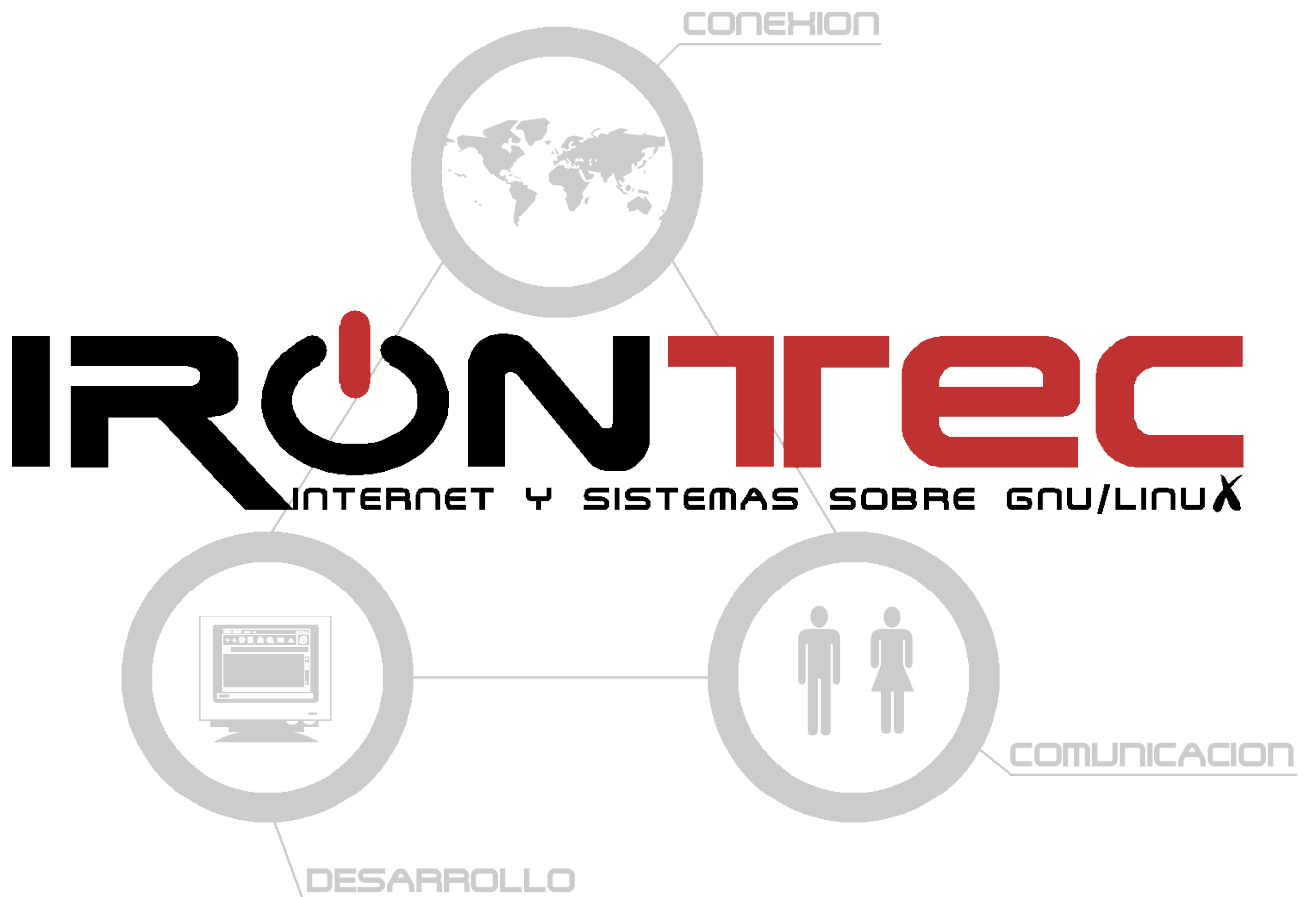


# Integración de Asterisk en LDAP



**## Astirectory: Usuarios SIP en Directorio LDAP ##**

*Versión 1.0*

11/07/06

## Índice de contenido

## Introducción ##	3
## LDAP ##	4
LDAP y bases de datos	4
## Astirectory ##	5
## Instalación y Configuración, Ejemplo Práctico ##	6
Escenario	6
Instalación de OpenLDAP	6
Instalación de PHPldapAdmin	6
Instalación y Configuración de Astirectory	7
Instalación	7
asterisk.schema	8
Configuración	8
Consultas en tiempo real	9
Configuración estática	9
Creación de usuarios	10
Integración de servicios	12
## Licencia ##	13

## ## INTRODUCCIÓN ##

Por defecto Asterisk emplea el fichero **sip.conf** para almacenar la información concerniente a los usuarios SIP. Este hecho acarrea ciertas limitaciones e inconvenientes:

- ◆ El fichero **sip.conf** contiene no solamente la información de los usuarios, sino también todo lo relacionado con la configuración de SIP: proveedores, NAT, IP/puerto, DNS, etc.
- ◆ Cualquier herramienta de administración de usuarios en Asterisk debería acceder al fichero **sip.conf** con permiso de escritura. Al operar directamente sobre un fichero de texto cualquier fallo de programación en la herramienta de gestión podría causar graves consecuencias en la configuración SIP de Asterisk y en los datos de los usuarios.
- ◆ No se permite integrar los datos de usuario para otros servicios como correo electrónico, agenda de contactos, servidor de ficheros, etc.

*Los datos del empleado X están almacenados en dos sitios independientes: en el fichero **sip.conf** para su uso por parte de Asterisk y en otro medio para su uso por parte del servidor de correo. Cualquier modificación de los datos empleado X requiere su actualización en 2 sitios.*

Existen otras modalidades de almacenamiento de usuarios disponibles en Asterisk, siendo la más extendida MySQL. La base de datos almacena la información relevante a los usuarios y permite ser administrada por cualquier herramienta de gestión (por ejemplo PHP+MySQL).

No obstante, existe un medio de almacenamiento más apropiado y efectivo de cara a mantener los usuarios de cualquier tipo de servicio: **LDAP**.

## ## LDAP ##

En un entorno de trabajo en red se vuelve transcendental el acceso rápido y eficaz a la información. Disponer de los datos de una manera desorganizada puede influir negativamente en el proceso de búsqueda dentro de la intranet de la empresa:

*¿Cuál es el teléfono del Sr. X en el departamento Y? ¿y su correo electrónico?*

*¿Qué empleado tiene la extensión XYZ?*

El servicio de directorio conforma la mejor respuesta a este problema, ofreciendo la información de forma sencilla y estructurada mediante acceso y atributos estandarizados y búsquedas eficientes.

LDAP es un protocolo de red que permite el acceso a un servicio de directorio. Hoy en día la mayor parte de los servicios soportan acceso LDAP (servicios de correo, ftp, compartición de ficheros, etc), pero también muchas aplicaciones cliente acceden a directorio LDAP (clientes de correo, de mensajería instantánea, agenda de contactos, etc).

### LDAP y bases de datos

A modo de resumen, las diferencias básicas entre ambos modelos serían:

- ◆ LDAP está diseñado para permitir lectura de datos muy rápida, no así la escritura. Ello lo convierte en solución idónea para almacenar información acerca de usuarios, a la que por norma general se realizan consultas mucho más que modificaciones.

*¿Con que frecuencia cambia la dirección de correo o la contraseña de un usuario?*

- ◆ LDAP propone una estructura jerarquizada de información frente a la organización relacional de una base de datos.
- ◆ LDAP no soporta complejos mecanismos de actualización o consulta. Las aplicaciones acceden al servicio de directorio LDAP de manera sencilla y eficiente.
- ◆ Por lo general, cualquier aplicación implementa acceso a servidor LDAP, no así a bases de datos.

*¿Puede un cliente de correo conectarse a una base de datos en un servidor remoto para búsqueda de contactos?*

*## ASTIRECTORY ##*

**Astirectory** es un módulo de Asterisk que permite delegar en un servidor LDAP los datos SIP de los usuarios, manteniendo la configuración general de SIP en el fichero **sip.conf**.

**Astirectory** facilita la integración de usuarios y la administración centralizada de los mismos. Gracias a **Astirectory**, Asterisk puede consultar los datos SIP de cada usuario de igual manera que un servidor de correo puede autenticar el acceso contra LDAP.

Astirectory ha sido desarrollado por **Asterisk e.V.**: <http://www.asterisk-ev.org>

## ## INSTALACIÓN Y CONFIGURACIÓN, EJEMPLO PRÁCTICO ##

### Escenario

Instalaremos un servidor **OpenLDAP** en una Debian Sarge (**192.168.0.100**) para mantener los datos de los empleados de la empresa. Instalaremos **Astirectory** en la máquina que alberga nuestro Asterisk (**192.168.0.1**) y lo configuraremos para que acceda al servidor LDAP.

### Instalación de OpenLDAP

El paquete Debian se llama **slapd**:

```
x apt-get install slapd
```

A continuación el gestor de paquetes DebConf nos realizará algunas preguntas:

- ◆ DNS domain name: **irontec.com** (nuestra raíz será **dc=irontec, dc=com**)
- ◆ Name of your organization: **Irontec**
- ◆ Admin password: **\*\*\*\*\***
- ◆ Database backend to use: **BDB**

Con esto ya tenemos nuestro servidor OpenLDAP funcionando.

### Instalación de PHPLdapAdmin

A continuación instalaremos **PHPLdapAdmin**, una aplicación web que permite gestionar de forma visual y sencilla los datos de nuestro servidor LDAP:

```
x apt-get install phpldapadmin
```

**Nota:** Si no tenemos Apache2 con PHP el propio paquete **phpldapadmin** forzará la instalación de las dependencias necesarias (Apache2, módulos PHP, etc).

**Importante:** Se recomienda configurar SSL en el servidor Apache2 para evitar el envío en texto plano de los datos de autenticación. No es objeto de este documento cómo configurar SSL en Apache2, pero se localiza fácilmente en Internet.

Una vez instalado entraremos vía web a la URL <https://192.168.0.100/phpldapadmin> (si no activamos SSL entraremos por http://) y nos autenticamos:

- ◆ Login DN: **cn=admin,dc=irontec,dc=com**
- ◆ Password: **\*\*\*\*\***

Crearemos una subrama **ou=People** para albergar los datos de los empleados. Para ello expandimos el árbol LDAP localizado en el marco izquierdo de la página, pulsamos en **Create new entry here**, elegimos **Organizational Unit** y lo nombramos **People**.

Hemos creado la subrama **ou=People,dc=admin,dc=irontec,dc=com**.

## Instalación y Configuración de Astirectory

### Instalación

- ◆ Descargamos la versión de **Astirectory** correspondiente a nuestra versión de Asterisk:  
<http://www.asterisk-ev.org/astirectory.php>

- ◆ Descomprimos:

```
x tar -zxvf astirectory-X.Y.tgz
```

- ◆ Descargamos **Asterisk Add-Ons**: <http://www.asterisk.org/download>

- ◆ Instalamos el paquete **LDAP devel** de la distribución:

```
x apt-get install libldap2-dev
```

- ◆ Parcheamos e instalamos:

```
x tar -zxvf asterisk-addons-1.2.X.tar.gz
x cd asterisk-addons-1.2.X
x patch -p1 < /path/to/astirectory.diff
x make
x make install (como root)
```

## *asterisk.schema*

Astirectory incluye su propio esquema LDAP que debemos activar en nuestro servidor OpenLDAP. Para ello copiamos el fichero **asterisk.schema** en el directorio **/etc/ldap/schema** y añadimos una línea al fichero **/etc/ldap/slapd.conf**:

```
x include          /etc/ldap/schema/asterisk.schema
```

## **Configuración**

- ◆ Creamos el fichero **/etc/asterisk/res\_ldap.conf** con la configuración de acceso al servidor LDAP:

```
x ldapuser = cn=admin,dc=irontec,dc=com
x ldapuri = ldap://192.168.0.100  (¡Ojo! en la documentación oficial
pone "ldaphost", pero está equivocado)
x ldappass = *****
x ldapbasedn = ou=People,dc=irontec,dc=com
```

**Nota:** no es suficiente con un *bind* anónimo ya que el proceso de registro de los teléfonos SIP o softphones necesita escribir en el servidor LDAP. El registro se realiza periódicamente, siendo su intervalo de tiempo configurable por el cliente (por norma general se realiza cada 3600 segundos).

**Importante:** En nuestro ejemplo accedemos al servidor LDAP autenticándonos como **admin**, lo que nos concede privilegios sobre todo el árbol del directorio (a nosotros y a quien, por un fallo de seguridad, consiguiese los datos de acceso). Sería recomendable crear un usuario **cn=asterisk,dc=irontec,dc=com** y dotarle de permisos de lectura y escritura únicamente dentro de la rama **ou=People,dc=irontec,dc=com** (esto se configura en el archivo **/etc/ldap/slapd.conf** y requiere de ciertos conocimientos en LDAP).

- ◆ Activamos el módulo **res\_config\_ldap.so** añadiendo lo siguiente en el archivo **/etc/asterisk/modules.conf**:

```
x preload => res_config_ldap.so
```

## Consultas en tiempo real

Las consultas a LDAP se hacen cada vez que se requieren datos, por lo que se pueden añadir o modificar usuarios en LDAP sin necesidad de reiniciar o recargar Asterisk.

- ◆ Para especificar que se quiere consultar LDAP para obtener datos SIP de los usuarios se añade lo siguiente en **/etc/asterisk/extconfig.conf**:

```
x sipusers => ldap,asterisk,sipuser
x sippeers => ldap,asterisk,sippeer
```

- ◆ Para que los usuarios en LDAP figuren al hacer **CLI> sip show peers/users** se debe indicar en el fichero **sip.conf** la opción:

```
x rtcachefriends=yes
```

## Configuración estática

La configuración no específica de SIP (*voicemail, queues, agents, meetme-rooms*) puede ser cargada desde LDAP de forma estática. Esto significa que dicha configuración requiere de un reinicio o recarga de Asterisk para cargar nuevos datos.

Para ello debemos añadir en el fichero **extconfig.conf**:

```
x voicemail.conf => ldap,/etc/asterisk/ldap_voicemail.conf,astVoicemail
```

De esta forma cargamos la información sobre *voicemail* desde LDAP en los objetos *astVoicemail*.

El fichero **/etc/asterisk/ldap\_voicemail.conf** sería un fichero de mapeo para cargar información desde distintos atributos especificados en el **asterisk.schema**. Algunos de los mapeos por defecto que se usan aunque no exista ningún fichero de mapeo serían:

x astVoicemailVoiceboxNr	VoiceboxNr
x astVoicemailPassword	Password
x astVoicemailEmailsubject	Emailsubject
x astVoicemailEmailbody	Emailbody
x astVoicemailEmaildateformat	Emaildateformat

- ◆ Si por ejemplo queremos que el número de buzón sea el mismo que el número de teléfono podemos mapearlo de la siguiente manera en el fichero `/etc/asterisk/ldap_voicemail.conf`:

```
x telephoneNumber          VoiceboxNr
```

- ◆ También podemos incluir información general de la configuración:

```
x astVoicemailGeneralConfig      ObjectClass_GeneralConfig
x astVoicemailVoiceboxNr         VoiceboxNr
x astVoicemailPassword           Password
x astVoicemailEmailsubject       Emailsubject
x astVoicemailEmailbody          Emailbody
x astVoicemailEmaildateformat    Emaildateformat
```

Ahora, al reiniciar o recargar Asterisk, el conector LDAP buscará el objeto `astVoicemailGeneralConfig` y usará sus atributos y valores como configuración general.

**Nota:** De la misma forma, podemos cargar desde LDAP la configuración para `queues.conf`, `agents.conf` y `meetme.conf`.

## Creación de usuarios

Una vez configurado todo el escenario sólo nos queda introducir los datos de los empleados en el servidor OpenLDAP. Lo haremos desde la propia aplicación web PHPLdapAdmin.

**Nota:** A efectos prácticos PHPLdapAdmin es una aplicación de carácter general y no constituye la forma más óptima de administrar los contactos. La solución más apropiada conllevaría el desarrollo de una aplicación a medida que tuviese en cuenta sólo los atributos y campos necesarios para detallar los datos de nuestros empleados.

Partiremos de este usuario de ejemplo:

```
dn: cn=Manolito Gafotas,ou=People,dc=irontec,dc=com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: astSipGeneric
objectClass: astSipUser
objectClass: astSipPeer
cn: Manolo Gafotas
```

```
sn: Gafotas
telephoneNumber: 301
astname: 301
astUsername: 301
astSecret: *****
astHost: dynamic
astContext: oficina
astLanguage: es
astQualify: yes
```

**Importante:**

- ◆ **astname** es el "userid" al que llamará Asterisk. La query LDAP se realiza precisamente en función de este atributo.
- ◆ **telephoneNumber** no tiene relación alguna con Asterisk, este dato NO será consultado durante la query LDAP. Lo lógico es que coincida con **astname** por comodidad.

Copiamos el texto anterior, vamos al navegador en <https://192.168.0.100/phpldapadmin> y pulsamos en **import** en el marco izquierdo. Pegamos el texto en el cuadro habilitado para ello y pulsamos **Proceder**.

Ahora vamos al marco izquierdo y pulsamos en **refrescar**, con lo que aparece nuestro primer usuario pudiendo modificar sus datos o añadir nuevos atributos.

Tal vez la forma más sencilla de gestionar los empleados con PHPLdapAdmin sea partir del usuario de ejemplo con todos los atributos necesarios y generar copias del mismo adecuando los atributos a cada empleado. Para ello, una vez seleccionado el usuario de ejemplo pulsaremos en **Copy or move this entry**, introduciremos el nombre y apellido del empleado en cuestión y modificaremos sus datos (teléfono, password, etc).

## Integración de servicios

Hemos organizado los datos de nuestros empleados en un servidor OpenLDAP. Las posibilidades de ampliación de este esquema son numerosas, por ejemplo:

Podemos instalar un servidor de correo para la empresa albergado en otra máquina, y configurarlo para que autentique y lea configuraciones de los empleados en el servidor OpenLDAP. Tan sólo habría que añadir en cada empleado los atributos LDAP requisito del servidor de correo.

Lo mismo para servidores de ficheros, mensajería instantánea (Jabber) y todo tipo de servicios habituales en una empresa. Incluso existen numerosas aplicaciones de tipo CRM que realizan consultas de personas a un servidor LDAP.

Las posibilidades son infinitas. Tal vez el único requerimiento sería disponer de una aplicación a medida (podría ser web) adecuada a nuestro entorno que permitiese fácilmente la administración de los datos de los empleados.

*## LICENCIA ##*

Este documento está protegido bajo la licencia **Attribution-ShareAlike 2.5** de **Creative Commons**:

<http://creativecommons.org/licenses/by-sa/2.5>

Copyright © 2006 Iñaki Baz Castillo <ibc@irontec.com>

Se permite la copia, modificación, distribución, uso comercial y realización de la obra, siempre y cuando se reconozca la autoría de la misma, a no sea ser que se obtenga permiso expreso del autor. El autor permite distribuir obras derivadas a esta sólo si mantienen la misma licencia que esta obra.

Esta nota no es la licencia completa de la obra, sino una traducción de la nota orientativa de la licencia original completa (jurídicamente válida).



<http://creativecommons.org/licenses/by-sa/2.5>