Hugo González

@hugo_glez

http://atit.upslp.edu.mx/~hugo/

10 años UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

CONSOL

2008

Autenticación con LDAP para aplicaciones web.

Hugo Francisco González Robledo

hugo.gonzalez@upslp.edu.mx

presenta:

El problema:

- Existen multitud de aplicaciones web libres desarrolladas en varios lenguajes de programación, pero cada una trae su propia forma de autenticarse
  - Claro que existen sus excepciones ..
- Cuando tratas de implementar una solución abierta, debería poder funcionar una sola fuente de autenticación

Propuesta 1

- Base de datos Federada
  - La tabla que maneja las autenticaciones de las diferentes aplicaciones es compartida o ligada a una tabla general que almacena toda la información.
- Pros: No hay que modificar las aplicaciones
- Cons: Hay que tocar las bases de datos, y con el incremento de alguna otra aplicación, modificar la tabla que almacena la información.
  - Aplicaciones que almacenen contraseña en formato

Propuesta 2

- El famoso “single sign on”, una sola autenticación y te valida para diferentes aplicaciones. Esto sería lo ideal pero :
- Hay que modificar las aplicaciones, de manera que puedan usar esta ventaja, generalmente relacionada con el manejo de cookies, puede haber rollos de seguridad ...
- Esto es la panacea desde hace mucho tiempo.

Single Sign On

- Is a method of **access control** that enables a user to **authenticate once** and **gain access to** the resources of **multiple software systems**. Single sign-off is the reverse process whereby a single action of signing out terminates access to multiple software systems.
- The term enterprise reduced sign-on is preferred by some authors because they believe single sign-on to be a misnomer: "no one can achieve it without a

sigue ...

- In a **homogeneous** IT infrastructure or at least where a single user entity authentication scheme exists or where a user database is centralized, single sign-on is a visible benefit. All users in this infrastructure would have a single set of authentication credentials, e.g. in an organization which stores its user database in a **LDAP** database. All information processing systems can use such an LDAP database for user authentication and authorization, which in turn means single sign-on has been achieved organization-wide.

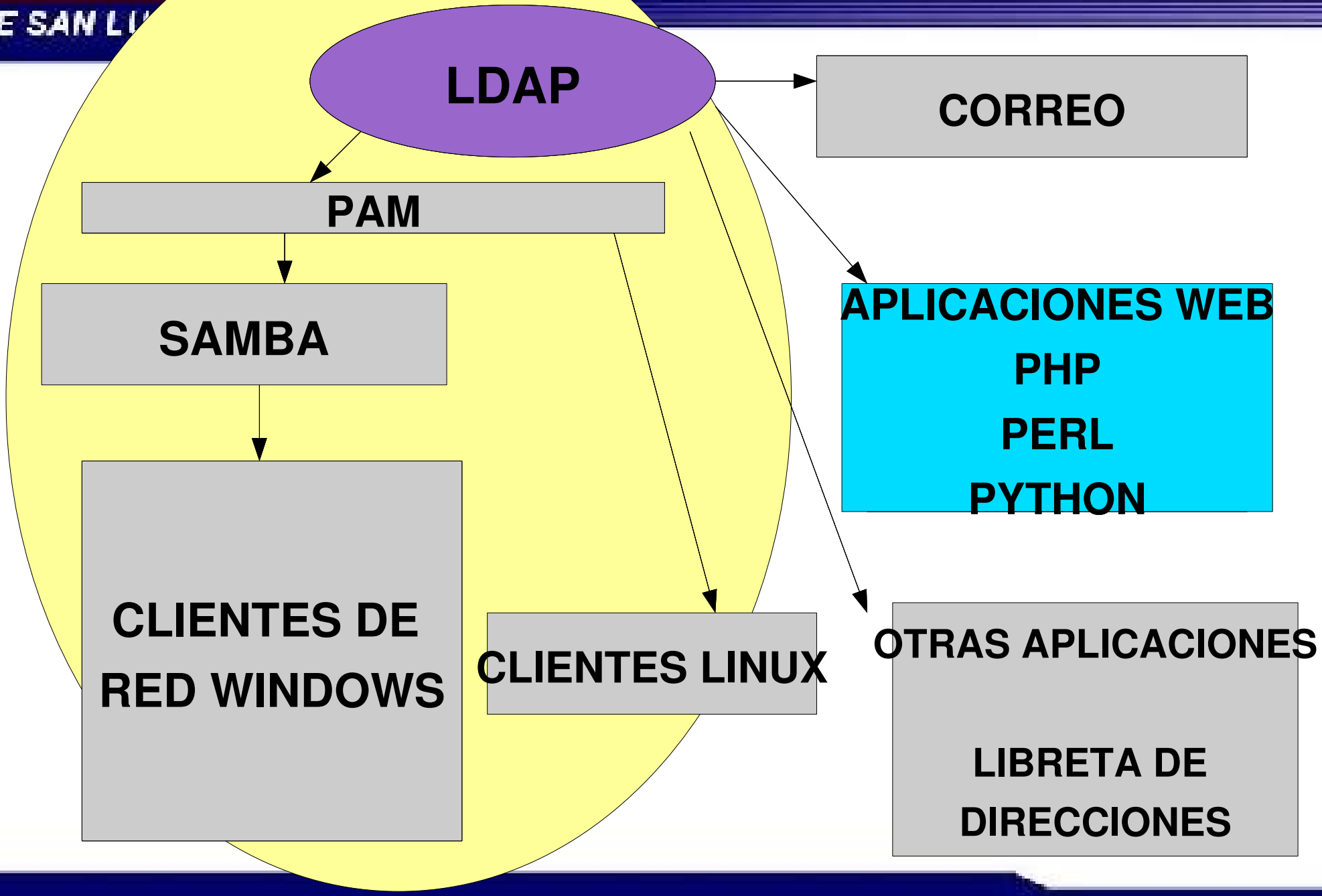
Mi opinión (del autor y no necesariamente del expositor)

- No es necesario que sea un ambiente homogéneo para simplificar la administración, se puede hacer con “estándares”, como el mismo artículo sugiere, utilizando LDAP, aunque sin llegar al Single Sign On, si unificando usuarios y contraseñas de una manera centralizada.

Ambientes posibles

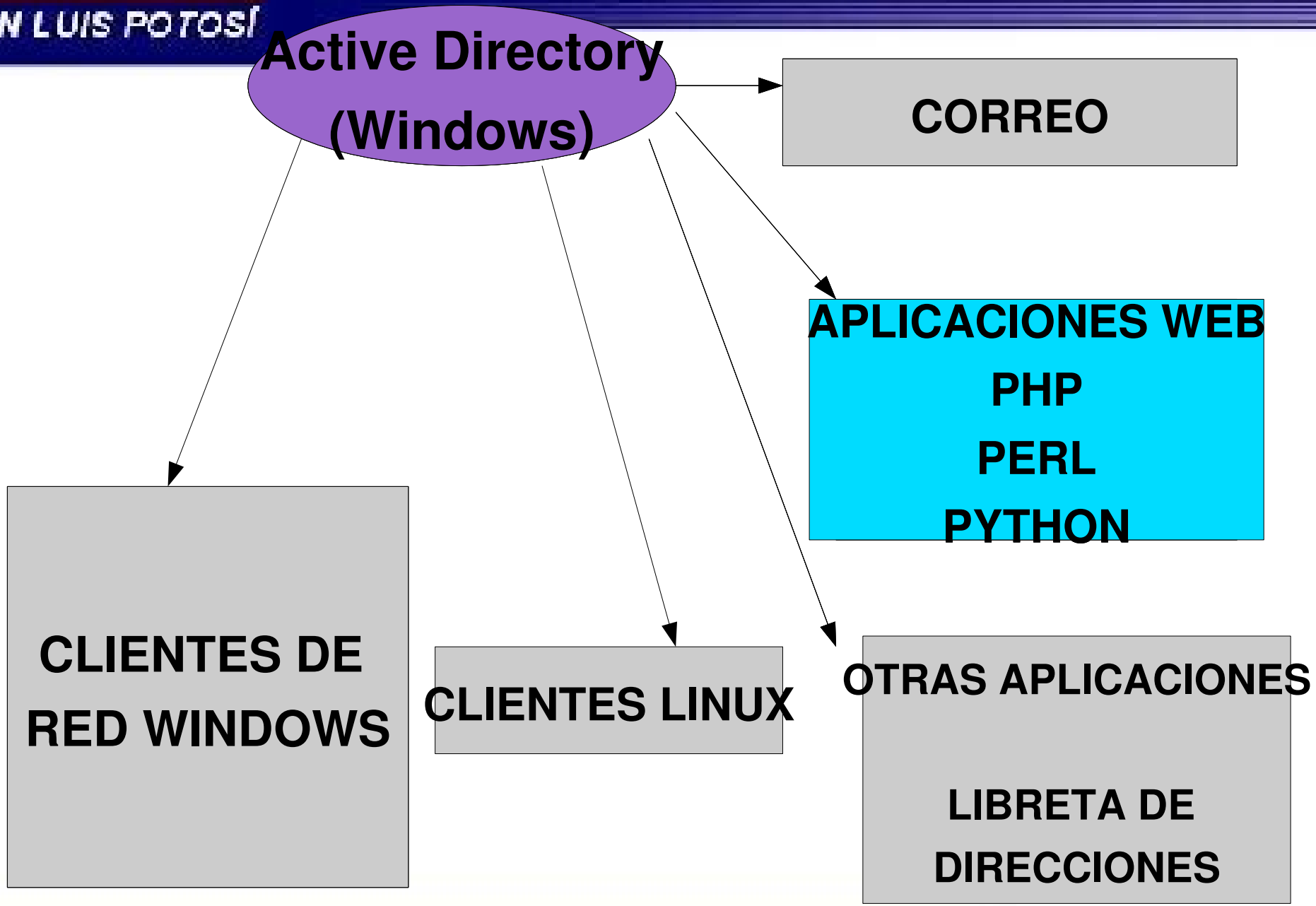
- En la siguiente diapositiva se presenta un esquema de la presentación "*Montando un servidor Samba + ldap para administrar usuarios en un laboratorio de cómputo*" en el Consol 2006, y que sigue vigente y ahora con más aplicaciones !!!

ESTO YA SE EXPLICO !!!



Ambientes posibles

- En la siguiente diapositiva se presenta un esquema de la presentación "*Montando un servidor Samba + ldap para administrar usuarios en un laboratorio de cómputo*" en el Consol 2006, y que sigue vigente y ahora con más aplicaciones !!!
- El otro ambiente es con un repositorio centralizado utilizando Active Directory (no me gusta pero en muchos lados lo utilizan)


Active Directory (Windows)
CORREO
APLICACIONES WEB
PHP
PERL
PYTHON
CLIENTES DE RED WINDOWS
CLIENTES LINUX
OTRAS APLICACIONES
LIBRETA DE DIRECCIONES

Propuesta

- Dotar a las aplicaciones web la opción de firmarse (o autenticarse) contra un servidor OpenLDAP o ActiveDirectory ...
- De esta manera sería transparente el poder integrar diversas aplicaciones para la industria o el sector productivo
- Sería un plus en el desarrollo de aplicaciones.

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Qué es OpenLDAP?

- OpenLDAP Software is an open source implementation of the Lightweight Directory Access Protocol.[1]
- Software del protocolo para transporte de acceso a información.
- No es Active Directory, pero tienen conceptos muy similares.
- Puedes almacenar información relacionada de muchos tipos.

[1] Extraido de la página de OpenLDAP: http://www.openldap.org/

Luego de este rollo ....

Ejemplos de implementación de diferentes lenguajes:

PHP, Perl, Ruby, C#, Python y JSP (Java)

“Algoritmo”

- Conectarse al controlador Active Directory o al OpenLDAP
- Intentar un bind
- **Si se consigue el usuario es válido**
- Desconectarse del controlador

PHP

Falta validar las entradas de usuario

Conectar al ActiveDirectory

```
$ad = ldap_connect("ldap://upslp.edu.mx") or die("Couldn't connect to AC!");
@$bd=ldap_bind($ad,$_POST['userBox'].'@upslp.edu.mx', $_POST['passBox']);
if($bd){
ldap_unbind($ad);
session_register("LOGGEDIN");^M
session_register("USER_NAME");
$_SESSION['LOGGEDIN'] = $_POST['userB
$_SESSION['USER_NAME'] = $_POST['use
```

Bind con los datos introducidos por el usuario

Si se logra el bind, el usuario es válido

Perl

Conectar al ActiveDirectory

```
use Net::LDAP;
$ldap = Net::LDAP->new ( "ldap.upslp.edu.mx" ) or die "$@";
$mesg = $ldap->bind ( "$userToAuthenticate",
                password => "$passwd",
                version => 3 );
if ($mesg->done) {print “Valid user\n”;
 $ldap->unbind;
```

Bind con los datos introducidos por el usuario

Si se logra el bind, el usuario es válido

C#, o mono

Crear conección

Conectar al ActiveDirectory

Bind con los datos introducidos por el usuario

Si se logra el bind, el usuario es válido

```
// C# Library namespace
using Novell.Directory.Ldap;

// Creating an LdapConnection instance
LdapConnection ldapConn= new LdapConnection();

//Connect function will create a socket connection to the server
ldapConn.Connect(ldapHost,ldapPort);

//Bind function will Bind the user object Credent
ldapConn.Bind(userDN,userPasswd);
```

Ruby on Rails

```
require 'active_ldap'
class LdapUser < ActiveLdap:Base
    ldap_mapping :prefix => "cn=users"
    def self.login(username, password)
      ActiveLdap::Base.connect \
        :host => "ldap.yourserver.com",
        :port => 389,
        :base => "dc=your,dc=base",
        :bind_format =>
"uid=#{username},cn=users,dc=your,dc=ldap,dc=binding,dc=config,dc=com",
        :password_block => Proc.new { password },
        :allow_anonymous => false

      return true
    rescue ActiveLdap::AuthenticationError
      return false
    ensure
```

Conectar al ActiveDirectory

Bind con los datos introducidos por el usuario

Si se logra el bind, el usuario es válido

Python

```
import ldap
l=ldap.open('hostname')
#set which protocol if you do not like the default
l.protocol_version = ldap.VERSION3
l.simple_bind('user','password')
```

Conectar al ActiveDirectory

Bind con los datos introducidos por el usuario

Si se logra el bind, el usuario es válido

JSP

Incompleto, pero esa es la idea

```
import java.util.*;
import javax.naming.*;
import javax.naming.directory.*;

try {
    Hashtable ldapEnv = new Hashtable(11);
    ldapEnv.put(Context.INITIAL_CONTEXT_FACTORY,
"com.sun.jndi.ldap.LdapCtxFactory");
    ldapEnv.put(Context.PROVIDER_URL,  "ldap://" + serverIP + ":636");
    ldapEnv.put(Context.SECURITY_AUTHENTICATION, "simple");
    ldapEnv.put(Context.SECURITY_PRINCIPAL, "cn=ldapadmin"
baseName);
    ldapEnv.put(Context.SECURITY_CREDENTIALS, "xxxx");
    ldapEnv.put(Context.SECURITY_PROTOCOL, "ssl");
    ldapContext = new InitialDirContext(ldapEnv);
    }
    catch (Exception e) {
      System.out.println(" bind error: " + e);
```

Conectar al ActiveDirectory

Bind con los datos introducidos por el usuario

Si se logra el bind, el usuario es válido

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Conclusiones

- Podemos utilizar un sistema centralizado para autenticar usuarios a diferentes niveles usando OpenLDAP o AC a través de “casi” cualquier lenguaje de programación.
- La integración de nuestras aplicaciones web podría ser menos dolorosa
- **Voluntarios para escribir módulos para aplicaciones comunes para usar esta autenticación ????**

Recursos:

OpenLDAP

- http://www.openldap.org
- http://www.yolinux.com/TUTORIALS/LinuxTutorialLDAP.html
- http://www.linuxjournal.com/article/6266

PHP

- http://mx.php.net/ldap
- http://adldap.sourceforge.net/

Perl

- http://ldap.perl.org/
- http://ldap.perl.org/FAQ.htm
- http://www.linuxjournal.com/article/7086

JSP

- http://forum.java.sun.com/thread.jspa?threadID=574610&messageID=2863697
- http://today.java.net/cs/user/view/cs_msg/1269

Java

- http://www.openldap.org/jldap/

C#

- http://www.novell.com/coolsolutions/feature/11204.html
- http://www.thescripts.com/forum/thread426214.html

Samba + openldap

- http://www.howtoforge.com/openldap-samba-domain-controller-ubuntu7.10

UNIVERSIDAD POLITÉCNICA DE SAN LUIS POTOSÍ

Preguntas ?

hugo.gonzalez@upslp.edu.mx