Validación centralizada con LDAP y PHP

Virginia Villanueva Velásquez

LDAP

(Lightweight Directory Access Protocol)

Descripción

- Protocolo de tipo cliente-servidor para acceder a un servicio de directorio.
- Basado en el estándar X.500.
- Soporta TCP/IP. Necesario para el acceso a Internet.
- Permite centralizar toda la información en un solo lugar.

Características de un directorio LDAP

- Es una clase especial de base de datos.
- Contiene información estructurada en forma de árbol.
- Se realizan lecturas mas que escrituras.
- Proporcionan una respuesta rápida.

Características de un servidor LDAP

Usos Prácticos

LDAP

- Directorios de información
- Sistemas de autenticación/autorización centralizada
- Sistemas de correo electrónico
- Sistemas de alojamiento de páginas web y FTP
- Servidores de certificados públicos y llaves de seguridad
- Autenticación única ó “single sign-on” para la personalización de aplicaciones
- Perfiles de usuarios centralizados.
- Libretas de direcciones compartidas

Administración de LDAP

Definición de términos:

Entradas → Es una colección de atributos que tienen un único y global Nombre Distintivo (DN)

DN → Se utiliza para referirse a una entrada sin ambigüedades

Administración de LDAP

Atributos → Son datos de un directorio y se presentan en pares acompañados de su valor

LDIF → Formato que se usa para Importar y exportar información De directorios entre servidores. Por sus siglas: **LDAP DIRECTORY INTERCHANGE FORMAT**

Objetos → La colección de atributos que pueden usarse para definir una entrada

Cómo se guarda la información

Similar a la estructura de directorios de los discos duros.

Referencia de un archivo en un subdirectorio:
/usr/local/misapps/docs

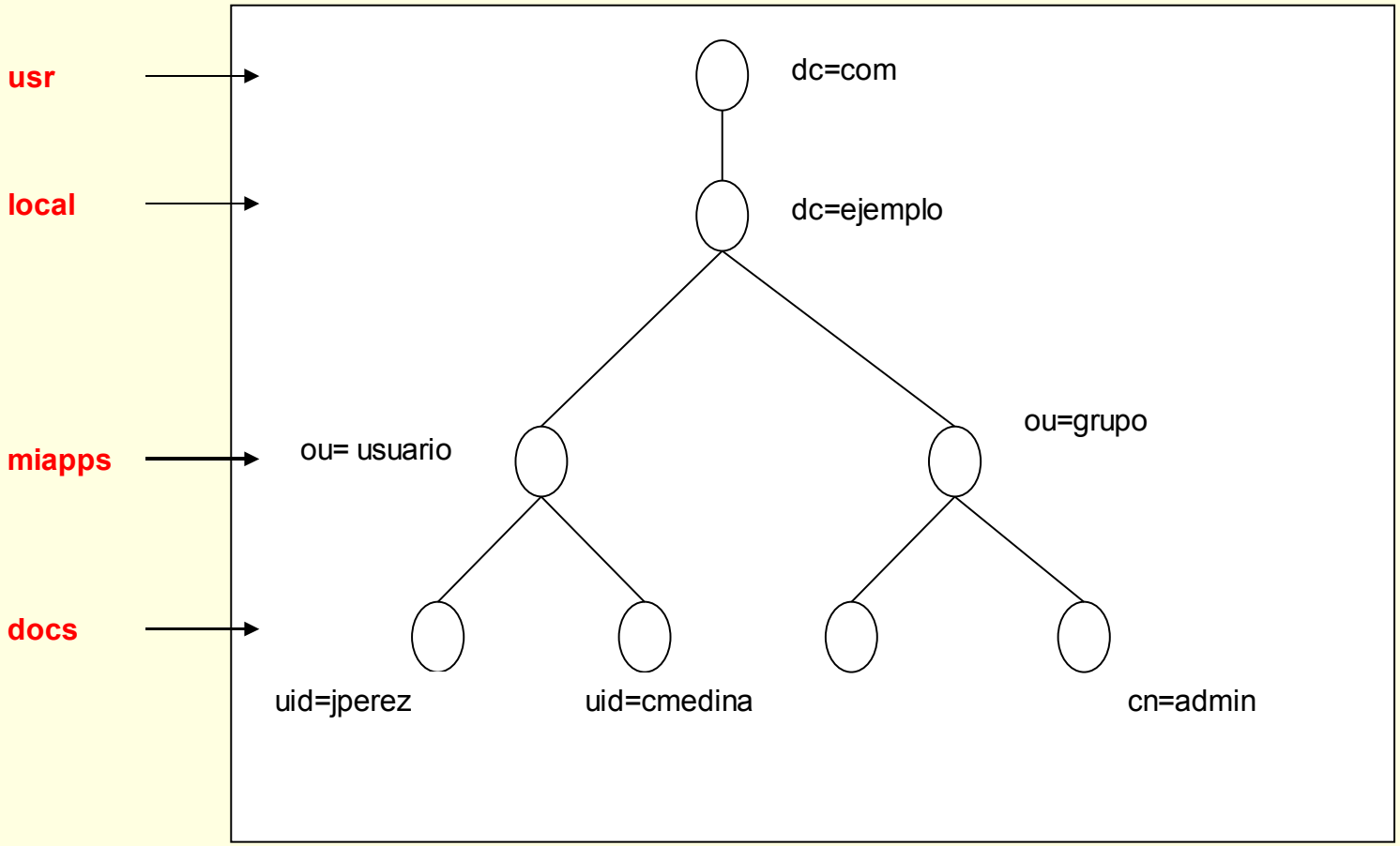
Equivalencia en LDAP:
"distinguished name" abreviado como "**dn**"

Un ejemplo de dn:

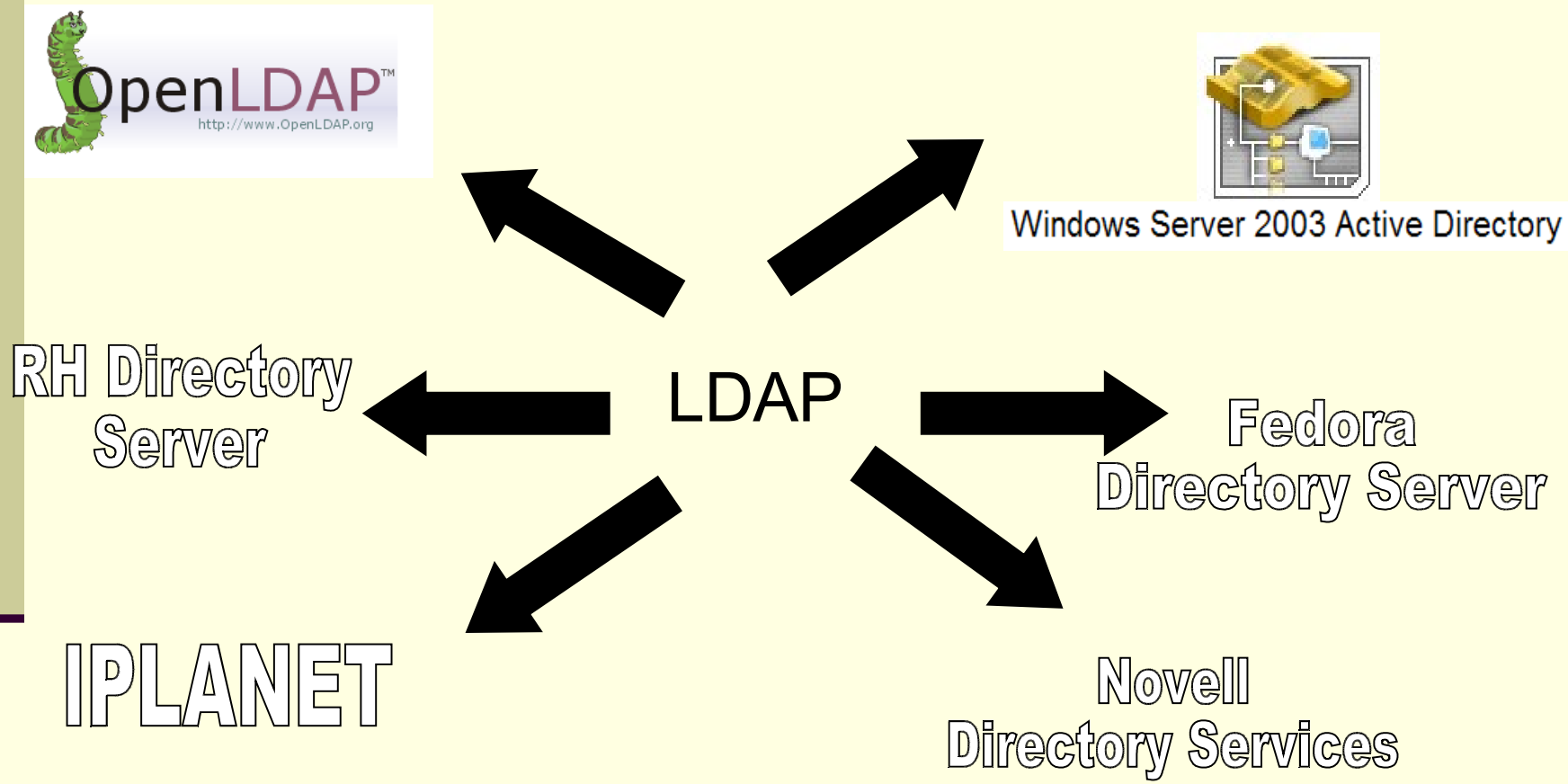
dn: uid=jperez,**ou**=usuario,**dc**=ejemplo,**dc**=com

/usr/local/misapps/docs

dn: uid=jperez,ou=usuario,dc=ejemplo,dc=com



Servidores LDAP



OpenLDAP

Descripción

- Implementación libre del protocolo LDAP
- Disponible en la mayoría de las distribuciones de GNU/Linux
- OpenLDAP se compone de varias partes:

slapd: El servidor LDAP.

slurpd: El servidor de replicación.

Requisitos para la instalación

Sistemas Operativos:

- Apple Mac OS X
- Linux: Debian, RedHat, Suse, Fedora, Centos, …
- FreeBSD
- IBM AIX
- Microsoft Windows 2000/NT
- NetBSD
- Solaris

Paquetes

OPENLDAP

OPENLDAP-CLIENTS

OPENLDAP-SERVERS

Configuración Básica

Parámetros fundamentales de **/etc/openldap/slapd.conf**

1. Sufijo: Base o raiz del directorio

suffix "dc=admon, dc=com"

2. Directorio de la base de datos:

directory /var/lib/ldap

3. Cuenta del administrador:

rootdn "cn=root, dc=admon, dc=com“

Configuración Básica

4. Contraseña del administrador

rootpw <CONTRASEÑA>

5. Niveles de acceso

access to dn=".*,ou=People,dc=admon,dc=com" attr=userPassword
by self write
by dn="cn=root,dc=admon,dc=com" write
by * auth

LDAP y PHP

Funciones principales

1. **ldap_connect() :** Inicializan los parámetros de conexión
2. **ldap_bind() :** Realiza la autenticación.
3. **ldap_modify() :** Modifica el valor de los atributos
4. **ldap_mod_add() :** Agrega atributos
5. **ldap_mod_del() :** Elimina atributos
6. **ldap_mod_replace()** : Reemplaza valores de atributos
7. **ldap_add() :** Agrega objetos al directorio.
8. **ldap_compare() :** Verificar pertenencia de atributos.
9. **ldap_search() :** Busca en un árbol LDAP

Conexión desde php

```
$servidorLdap = “ejemplo.com”;
$puertoLdap  = “389”;
$dnManager = “cn=Manager, dc=ejemplo, dc=com”;
$passManager = “secreto”;
$usuario = “prueba”;
$passUsuario = “pass”;

$ds = ldap_connect($servidor_ldap, $puerto_ldap);
$ r= ldap_bind($ds,$dnManager,"$passManager");
```

```
//Buscamos al usuario con ese código

$sr=ldap_search($ds, "ou=usuario,dc=ejemplo,dc=com", "uid=prueba")

$datosldap = ldap_get_entries($ds, $sr);

$dn = $datosldap[$i]["dn"];

$r=ldap_compare($ds,$dn,” userPassword”, $pass);
```

```
if ($r === -1)
{
        $msg = “Error datos"; //Contraseña incorrecta
}
elseif ($r === true)
{
    $datos[0]= $datosldap[$i]["cn"][0];
    $datos[1]= $ datosldap[$i]["givenname"][0];
    $datos[2]= $ datosldap[$i][“sn"][0];
    $datos[4]= $ datosldap[$i]["mail"][0];
 }
```