Administración de redes Linux

LDAP Básico

Iria Estévez Ayres

uc3m | Universidad Carlos III de Madrid

Departamento de Ingeniería Telemática

Marzo 2025

Índice

Apartado 1

Servicios de directorio

Servicio de directorio. Concepto

- Aplicación o conjunto de aplicaciones que organiza la información sobre los usuarios y recursos de red de una red de ordenadores.
- Permite a los administradores gestionar el acceso de usuarios a los recursos.
- Ofrece una capa de abstracción entre usuarios y recursos compartidos.
- Está especialmente diseñado para ofrecer búsquedas (*searching*), navegación (*browsing*), consultas (*lookup*) y actualizaciones (*updating*) a los datos.

Servicio de directorio. Introducción (I)

- Información descriptiva basada en atributos y soporte para realizar filtrados sofisticados.
- No son bases de datos
  - No soportan transacciones complicadas.
  - Las actualizaciones suelen ser cambios todo-o-nada (si se permiten).
- Diseñados para tener respuesta rápida a consultas (*lookup*) u operaciones de búsqueda en grandes volumenes de datos.
- Algunas implementaciones pueden usar réplicas para aumentar la disponibilidad y fiabilidad de la información, reduciendo también el tiempo de respuesta.
  - Si se replica la información de un directorio pueden aparecer inconsistencias temporales.
  - No importa, siempre y cuando se resuelvan en un tiempo determinado.

Servicio de directorio. Introducción (y II)

- Muchas formas diferentes de ofrecer un servicio de directorio.
  - Permiten almacenar diferentes tipos de información en el directorio.
  - Establecen diferentes requisitos sobre la forma en que esa información puede ser referenciada, consultada y actualizada.
  - Diferentes formas de protección contra el acceso no autorizado.
- Pueden ser:
  - Locales: prestan servicio a un contexto restringido (por ejemplo, el servicio `finger` en una sola máquina).
  - Globales: normalmente están distribuidos en varias máquinas que deben cooperar entre sí para ofrecer el servicio.
    - Espacio de nombres uniforme independientemente de la localización.

Servicio finger

- Permite hacer consultas sobre los usuarios del sistema
- Este ejemplo es en el servidor de cuentas profesores de `it.uc3m.es`

```
$ finger iria
Login: iria                             Name: Iria Manuela Estevez Ayres
Directory: /users/prof/iria             Shell: /bin/bash
Office: 4.1A06, x8746                   Home Phone: +34 91 624 8746
On since Mon Mar  4 15:28 (CET) on pts/0 from 83.33.21.107
   5 seconds idle
No mail.
No Plan.
```

Ejercicios a entregar (servicio finger)

Ejercicio 1

- En el aula virtual, haced `finger` de vuestro usuario.
- Copiad la salida en el documento a entregar.
- Conectaos con ssh a monitor02.lab.it.uc3m.es y volved a hacer lo mismo.
- Copiad la salida en el documento a entregar.

Apartado 2

LDAP. Conceptos básicos

LDAP

- LDAP: Lightweight Directory Access Protocol.
- Protocolo IETF, especificado en el `RFC 4510` *Lightweight Directory Access Protocol (LDAP) Technical Specification Road Map*.
- Protocolo ligero para acceder a servicios de directorio, específicamente a servicios de directorio basados en X.500.
- Funciona sobre TCP/IP u otros servicios orientados a conexión.
  - Es ligero en comparación con DAP (el protocolo de X.500) que estaba definido sobre la torre OSI.

LDAP desde el punto del vista del usuario (I)

¿Qué tipo de información puedo guardar?

- La información se basa en entradas (*entries*).
- Una **entrada** es un **conjunto de atributos** que tiene un Nombre Distinguido (DN) único a nivel global.
  - El DN identifica unívocamente a la entrada.
- Cada atributo es de un tipo y tiene uno o más valores.
  - Es un tipo: suelen ser cadenas mnemotécnicas, `cn` para el nombre común o `mail` para el correo electrónico.
  - Tiene uno o más valores: su sintaxis depende del tipo de atributo.

Ejemplo de entrada en LDAP

Mi usuario en LDAP de uc3m (entre otros atributos)

```
dn: uid=ayres,ou=INGENIERIA TELEMATICA,ou=Personal Docente e Investigador,
ou=Personal,ou=Gente,o=Universidad Carlos III,c=es
cn: IRIA MANUELA ESTEVEZ AYRES
sn: ESTEVEZ AYRES
description: ESTEVEZ AYRES, IRIA MANUELA
uc3mCorreoAlias: iria.estevez.ayres@uc3m.es
uid: ayres
mail: ayres@it.uc3m.es
irisMailAlternateAddress: iria.estevez.ayres@uc3m.es
irisMailMainAddress: ayres@it.uc3m.es
schacUserPrivateAttribute: none
givenName: IRIA MANUELA
uc3mEdificio: TORRES QUEVEDO
roomNumber: 4.1.A06
uc3mCampus: CAMPUS DE LEGANES
telephoneNumber: 8746
```

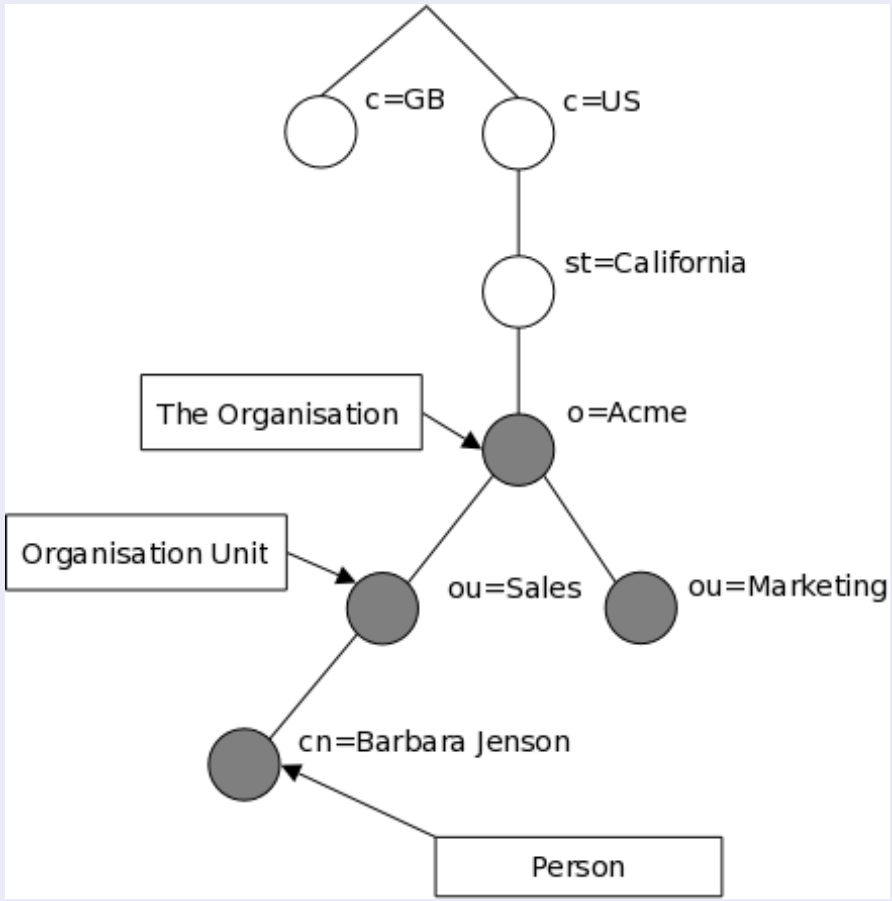
LDAP desde el punto del vista del usuario (II)

¿Cómo se ordena la información?

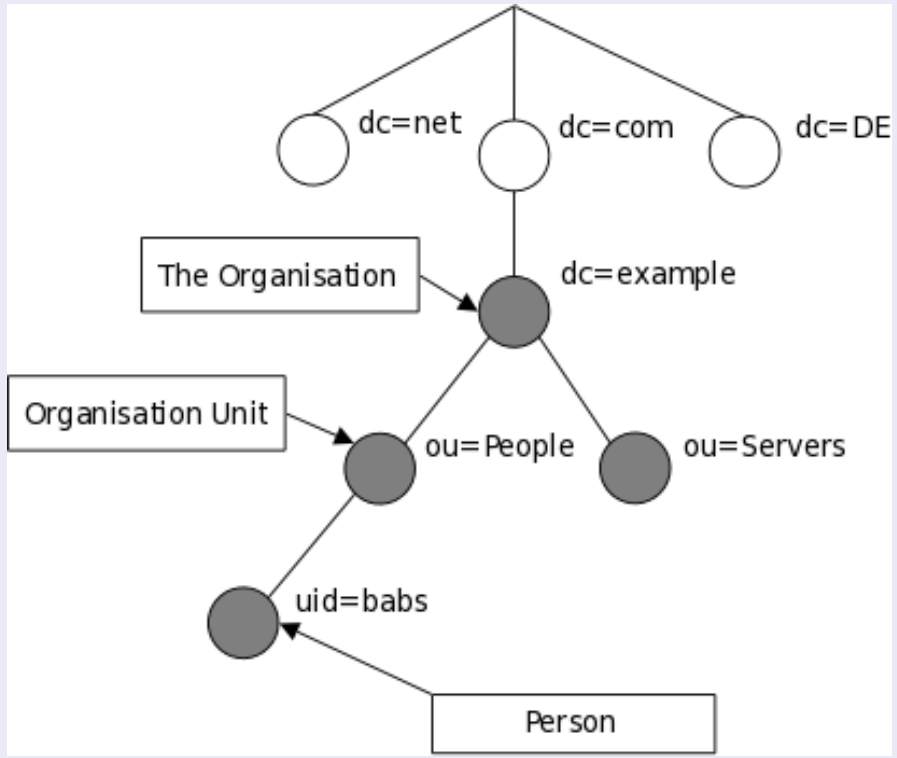
- Las entradas del directorio están organizadas en una estructura jerárquica de árbol.
- Tradicionalmente, esta estructura reflejaba los límites geográficos y/o de organización.
  - Las entradas que representan países aparecen en la parte superior del árbol.
  - Debajo de ellas están las entradas que representan estados y organizaciones nacionales.
  - Debajo de ellas pueden aparecer entradas que representan unidades organizativas, personas, impresoras, documentos o lo que se te ocurra.
- También organizarse en función de los nombres de dominio de Internet.
  - Enfoque cada vez más popular, ya que facilita localización con DNS.
- Los valores del atributo `objectClass` determinan las reglas del esquema que las entradas deben obedecer.

Ejemplo

Nombrado tradicional



Nombrado basado en dominio (estilo DNS)



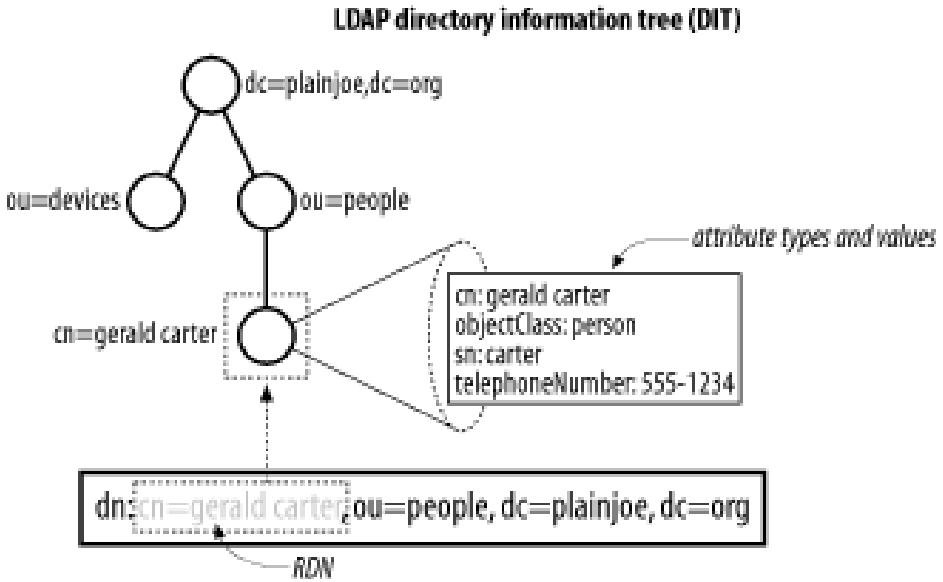
Tomado de la página `www.openldap.org`

LDAP desde el punto del vista del usuario (III)

¿Cómo se hace referencia a la información?

- Cada entrada se referencia por su Nombre Distinguido (DN).
- Se construye
  - Tomando el nombre de la propia entrada o nombre distinguido relativo (RDN).
  - Concatenando los nombres de las entradas de los ancestros.
- En los ejemplos anteriores:
  - En el ejemplo del árbol estilo DNS, la entrada de Barbara Jensen:
    - RDN: uid=babs
    - DN: uid=babs,ou=People,dc=ejemplo,dc=com
  - Mi usuario LDAP de uc3m:
    - rdn: uid=ayres
    - dn: uid=ayres,ou=INGENIERIA TELEMATICA,ou=Personal Docente e Investigador, ou=Personal,ou=Gente,o=Universidad Carlos III,c=es
- El RFC4514, *LDAP: String Representation of Distinguished Names*, describe el formato completo de un DN.

Ejemplo de RDN multivalor (I)



- Si tenemos dos *Jane Smith* en la organización, una en *Sales* y otra en *Engineering*.
- Si se usa como RDN sólo el atributo `cn` (*Jane Smith*), no sería unívoco.
- Si se usa como RDN sólo el atributo `ou` tampoco sería único (hay más personas en *Engineering*, por ejemplo)
- Se debe componer de varios atributos

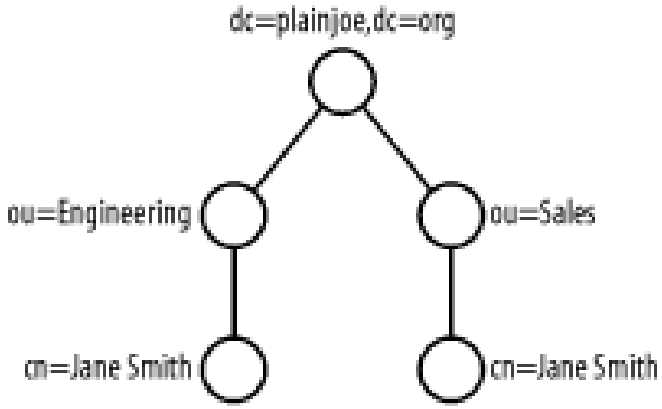
```
# Ejemplo de 2 entradas con un RDN multivalor
dn: cn=Jane Smith+ou=Sales,dc=plainjoe,dc=org
cn: Jane Smith
ou: Sales
<...resto de la entrada borrada...>

dn: cn=Jane Smith+ou=Engineering,dc=plainjoe,dc=org
cn: Jane Smith
ou: Engineering
<...resto de la entrada borrada...>
```

Ejemplo tomado de G. Carter *LDAP System Administration*, O'Reilly Media, 2003

Ejemplo de RDN multivalor (y II)

- Se deben evitar los RDN multivalor en la medida de lo posible.




```
dn: cn=Jane Smith,ou=Sales,dc=plainjoe,dc=org
<...resto de la entrada borrada...>
dn: cn=Jane Smith,ou=Engineering,dc=plainjoe,dc=org
<...resto de la entrada borrada...>
```

Ejemplo tomado de G. Carter *LDAP System Administration*, O'Reilly Media, 2003

LDAP desde el punto del vista del usuario (IV)

¿Cómo se accede a la información?

- LDAP define operaciones para:
  - Buscar información.
  - Actualizar el directorio:
    - añadir/eliminar entrada del directorio,
    - cambiar entrada existente
    - y cambiar el nombre de una entrada.
- Se usa mayoritariamente para buscar información en el directorio:
  - Uso de filtros para especificar criterios de búsqueda.
  - Se puede solicitar información de cada entrada que coincida con los criterios.

LDAP desde el punto del vista del usuario (V)

¿Cómo se protege la información contra el acceso no autorizado?

- Algunos servicios de directorio no ofrecen ninguna protección.
  - Permiten que cualquiera pueda ver la información
- LDAP permite que un cliente se autentique o pruebe su identidad a un servidor.

LDAP desde el punto del vista del usuario (y VI)

¿Cuándo debo usar LDAP?

- Cuando necesites que los datos estén gestionados y almacenados de forma centralizada y accesibles vía estándares.
- Algunos ejemplos:
  - Autenticación de máquinas
  - Autenticación de usuario
  - Grupos de usuarios/sistemas
  - Libreta de direcciones
  - Representación de la organización
  - Gestión de los recursos de los usuarios
  - Consultas de direcciones de correo electrónico
  - etc.
- Se pueden usar *Distributed Schema Files* preexistentes o crear nosotros uno.

¿Cuándo NO debo usar LDAP?

- Si sólo necesitas una aplicación para usar y manipular tus datos, quizás debes usar una BD.

Apartado 3

Búsqueda básica en un servicio de directorio

Herramienta **ldapsearch**

- Permite introducir una petición de búsqueda para localizar entradas en el directorio.
- Cada búsqueda incluye:
  - Localización servidor:
    - -h host
    - -p PUERTO
    - -H LDAP URI
  - Para autenticación:
    - -D bind
    - -w contraseña
    - -W: prompt para la contraseña
    - -x autenticación simple
  - Criterios de búsqueda.
- Cuando un cliente hace una búsqueda al servidor:
  - Se hace una petición de búsqueda a través de TCP/IP.
  - Se comprueba que el cliente es efectivamente un cliente autorizado:
    - Puede ser él mismo, otro usuario, administrador de directorio, o puede hacerse de forma anónima.
  - Se ejecuta la búsqueda y el servidor devuelve el resultado en formato LDIF.
  - Se cierra la conexión.

Buscando en el servicio de directorio de it

- Para los ejemplos se ha usado una cuenta de asignatura.
- Vosotros debéis usar vuestra cuenta de usuario de `lab.it.uc3m.es`

```
telematica@debian-mini:~$ ssh labgarl@monitor01.lab.it.uc3m.es
labgarl@monitor01.lab.it.uc3m.es's password:
monitor01:~> bash
labgarl@monitor01:~$ which ldapsearch
/usr/bin/ldapsearch
labgarl@monitor01:~$
```

Buscando todas las entradas

- Usaremos autenticación simple (`-x`)
- Usuario: anónimo (sin -D ni -W)
- Host: `-H ldaps://ldap.lab.it.uc3m.es`
- Base: `-b "dc=lab,dc=it,dc=uc3m,dc=es`

```
labgarl@monitor01:~$ ldapsearch -x -H ldaps://ldap.lab.it.uc3m.es\
-b "dc=lab,dc=it,dc=uc3m,dc=es" "(objectclass=*)"
# extended LDIF
#
# LDAPv3
# base <ou=Alum,dc=lab,dc=it,dc=uc3m,dc=es> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
.....
# search result
search: 2
result: 4 Size limit exceeded

# numResponses: 8066
# numEntries: 8065
labgarl@monitor01:~$
```

Limitando el número de respuestas

- En la anterior búsqueda se excedió el número máximo de respuestas.
- Podemos limitar el número de respuestas usando `-z num`
- Imprimimos sólo el dn añadiendo `1.1` al final de la búsqueda.

```
labgarl@monitor01:~$ ldapsearch -x -H ldaps://ldap.lab.it.uc3m.es -b "dc=lab,dc=it,dc=uc3m,dc=es"\
"(objectclass=*)" -z 2 1.1
# extended LDIF
#
# LDAPv3
# base <dc=lab,dc=it,dc=uc3m,dc=es> with scope subtree
# filter: (objectclass=*)
# requesting: 1.1
#

# lab.it.uc3m.es
dn: dc=lab,dc=it,dc=uc3m,dc=es

# admin, lab.it.uc3m.es
dn: cn=admin,dc=lab,dc=it,dc=uc3m,dc=es

# search result
search: 2
result: 4 Size limit exceeded

# numResponses: 3
# numEntries: 2
```

Ejercicios

Todos ejercicios deben hacerse **exclusivamente** con filtros de *ldapsearch*. No se pueden usar otros comandos.

2. Encuentra el `dn` de la asignatura con `uid` *labgdst*.
3. Muestra todas las cuentas de asignaturas. Indica el número de asignaturas.
4. Para cada asignatura, muestra sólo su dn
5. Para cada asignatura, muestra su homeDirectory y su nombre común (`cn`).
6. Busca tu usuario con un filtro de *ldapsearch*.
7. Muestra para tu usuario su home, su correo de uc3m y su titulación (está en el campo `gecos`).
8. Busca todos los estudiantes de tu titulación con cuenta en `lab.it.uc3m.es`. ¿Cuántos son?
9. Incluye `-s base` como opción. ¿Qué ocurre?
10. Incluye `-s one` y `1.1` como opciones. ¿Qué devuelve ldap?

Ejercicios

Todos ejercicios deben hacerse **exclusivamente** con filtros de *ldapsearch*. No se pueden usar otros comandos. Cuando se indica "buscar" también se debe indicar el número de entradas encontradas.

11. Busca todos los estudiantes que tengan el mismo (primer) nombre que tú.
12. Busca todos los estudiantes que tengan la subcadena GRA en su nombre.
13. Busca todos los estudiantes que tengan las subcadenas JU y MAR en su nombre.
14. Busca todos los estudiantes que tengan la subcadena MAR pero NO la cadena JU en su nombre.
15. Busca todos los estudiantes que tengan la subcadena JU, pero no la subcadena MAR en su nombre.
16. Incluye ahora en algunos de los comandos anteriores `-z 7` como opción ¿qué ocurre?
17. Busca todos los estudiantes que tengan la subcadena igual a tu primer apellido o igual a tu segundo apellido en su nombre (en mi caso, no devuelve entradas).
18. En un fichero escribe 3 uids, uno por fila. Añade a la búsqueda de todas las entradas, las siguientes opciones `"(uid=%s)" -f nombre_fichero` ¿Qué está ocurriendo? (Muestra el fichero usado y el resultado en los pantallazos)

Ejercicios

Todos ejercicios deben hacerse **exclusivamente** con filtros de *ldapsearch*. No se pueden usar otros comandos.
Este último ejercicio deberás hacerlo contra el ldap de la Universidad, con URL ldaps://ldap.uc3m.es

18. Busca todos **los estudiantes** que tengan el mismo (primer) nombre que tú, en el LDAP de la Universidad. Para ello deberás averiguar su estructura, realizando comandos previamente (echa un ojo a la transparencia 11). La búsqueda está limitada a devolver 50 resultados. Si te devuelve 50 resultados, deberás realizar una búsqueda más precisa, buscando cuańtos tienen el mismo nombre y algunas letras de tu segundo nombre o primer apellido que tú.
    - OJO: en mi caso, si busco los **estudiantes** cuyo nombre empiece por IRIA M me indica que hay 6 en toda la universidad. Si lo hubiese buscado en toda la Universidad, me indicaría que hay 8, pues hay dos personas que se llaman así y son profesoras.

Administración de redes Linux

LDAP Básico

Iria Estévez Ayres

uc3m | Universidad Carlos III de Madrid

Departamento de Ingeniería Telemática

Marzo 2025