U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

[dcc]

LDAP
LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL

ADMINISTRAÇÃO DE SISTEMAS

2021/2022

ROLANDO MARTINS

Referências dos slides

- O conteúdo destes slides é baseado no livro da disciplina: “Unix and Linux System Administration Handbook (4ªEd)” por Evi Nemeth, Garth Snyder, Trent R. Hein e Ben Whaley, Prentice Hall, ISBN: 0-13-148005-7
- Assim como no livro “Essential System Administration”, Æleen Frisch, O’Reilly Media
- As imagens usadas têm a atribuição aos autores ou são de uso livre.

Objetivo

Lightweight Directory Access Protocol (RFC 4511)

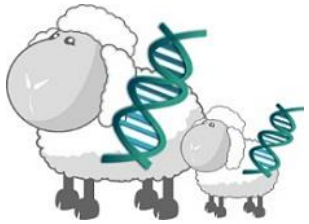
- Permite fazer a gestão de utilizadores e dos seus atributos
  - Email, telefone, perfil, etc.
- Permite ter UIDs e GIDs únicos num domínio (vários sistemas)
- Mais geralmente: Base de dados que armazena dados de forma hierárquica

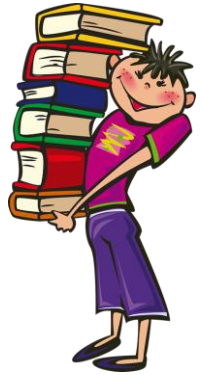
- **Microsoft usa como base o LDAP no Active Directory (AD)**

- Baseado originalmente em X.500 directory service

Características

- Dados são pequenos
- Replicação e cache
- Baseada em atributos
- **Lido muitas vezes, escrito poucas**
- Procura é uma operação frequente





Especificações

- De RFC 4510 LDAP: Specification Road Map
  - LDAP: The Protocol [RFC4511]
  - LDAP: Directory Information Models [RFC4512]
  - LDAP: Authentication Methods and Security Mechanisms [RFC4513]
  - LDAP: String Representation of Distinguished Names [RFC4514]
  - LDAP: String Representation of Search Filters [RFC4515]
  - LDAP: Uniform Resource Locator [RFC4516]
  - LDAP: Syntaxes and Matching Rules [RFC4517]
  - LDAP: Internationalized String Preparation [RFC4518]
  - LDAP: Schema for User Applications [RFC4519]

Aplicações do LDAP

- Repositório central de informação sobre utilizadores
- Aplicações podem aceder à informação centralizada para as suas funções
  - Ex.: servidor de email verificar endereços válidos
- Aplicações podem autenticar utilizadores
  - Ex.: Mooshak, codex, Proxmox, etc.
- Ferramentas para linha de comandos
  - Permite scripts
- Mudanças no LDAP são visíveis imediatamente

Servidores

- OpenLDAP 

  - Iniciado na Univ. de Michigan, agora open source
- 389 directory server 

  - Melhor documentação
  - Usam o mesmo código base
  - Em tempos era comercial
  - Consola gráfica

Ferramentas para gestão

- Lista em LDAP.com
- LDAP Admin

  - Open Source, suporta SAMBA
- web2ldap
  - Cliente LDAP via web
- phpLDAPadmin

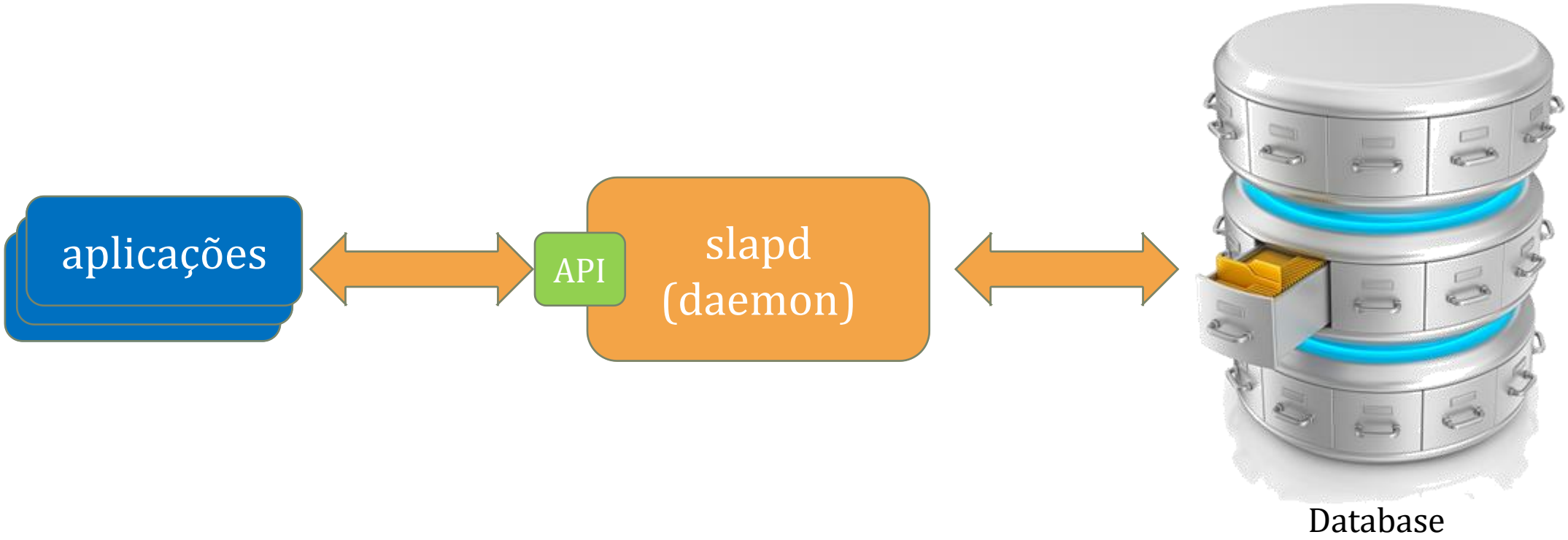
- MigrationApache Directory

  - Baseado em Eclipse RCP

MigrationTools

- Permite migrar estrutura existente para o LDAP.
  - Utilizadores e grupos
  - Hosts
  - Configuração de rede
  - `/etc/fstab`
  - etc.

Arquitetura



Arquitetura (cont)

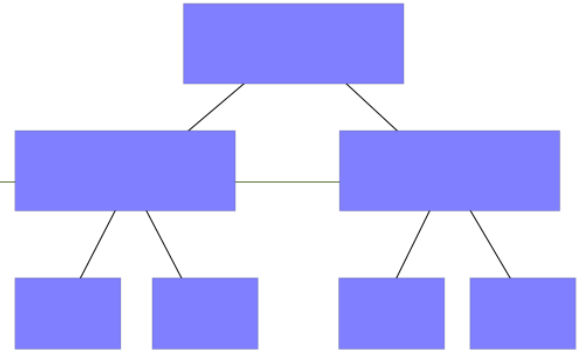
Daemon (slapd)

- Ficheiros de configuração
  - ~~`/etc/openldap/slapd.conf`~~
  - `/etc/openldap/slapd.d/`
- Utilitários
  - `slappaswd`, `slaptest`, `slapcat`, etc.

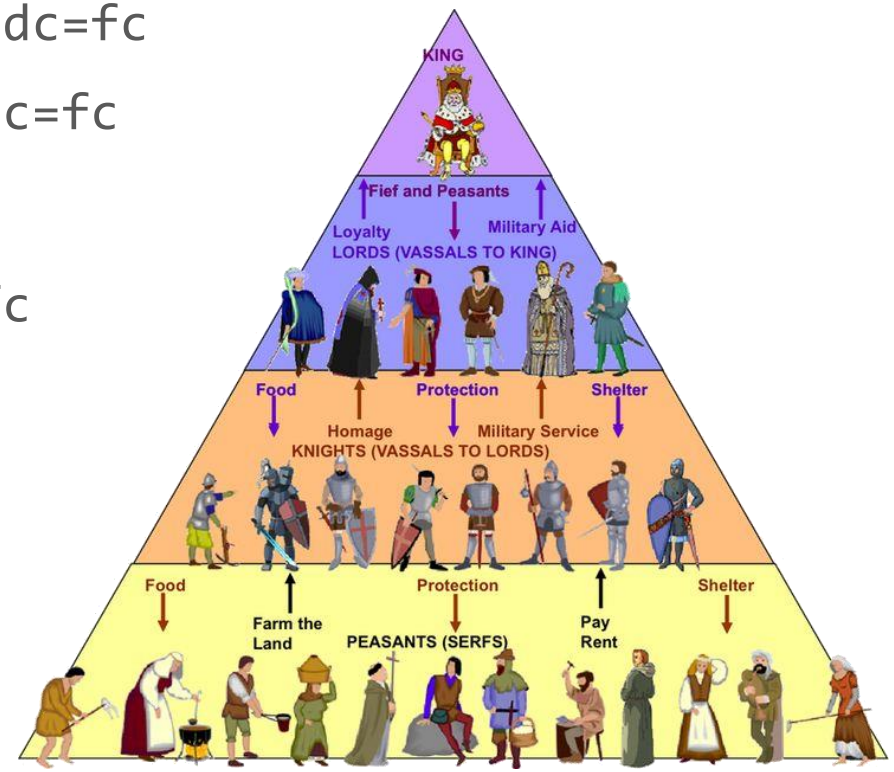
Base de dados

- Geralmente Berkeley DB
- Ficheiros de configuração
  - `/etc/openldap/schema/`
- Utilitários
  - `ldapadd`, `ldapsearch`, `ldapdelete`, `ldapmodify`, etc.

Hierarquia

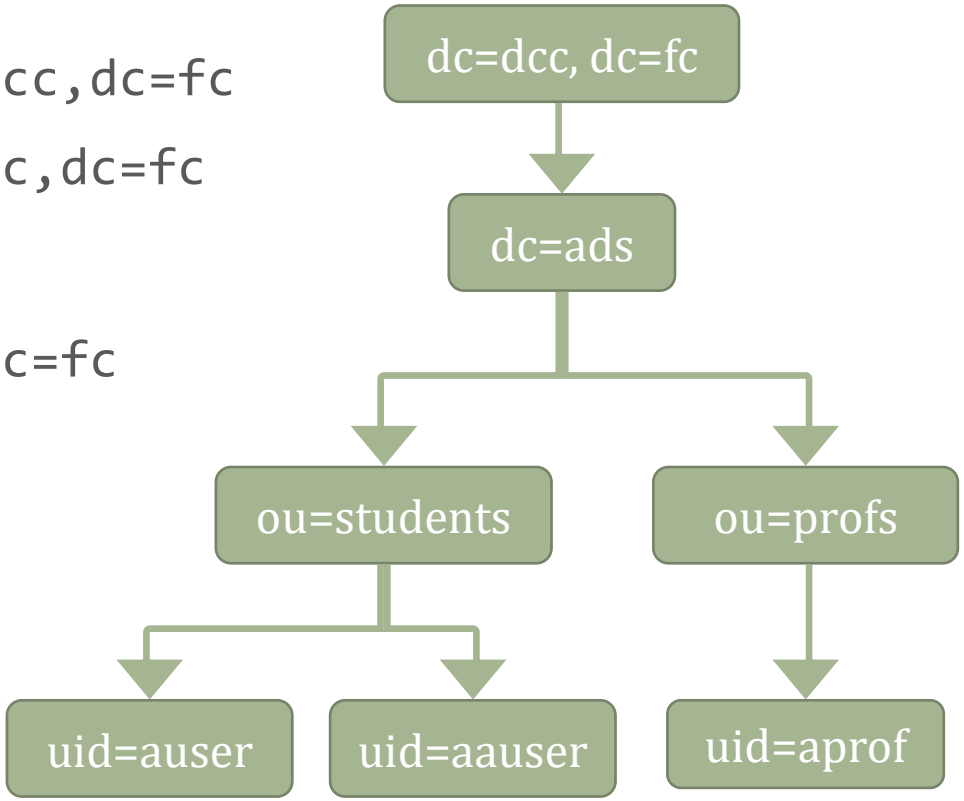


- dc=dcc,dc=fc
  - ou=Students,dc=ads,dc=dcc,dc=fc
    - uid=aauser,ou=Students,dc=ads,dc=dcc,dc=fc
    - uid=auser,ou=Students,dc=ads,dc=dcc,dc=fc
  - ou=Profs,dc=ads,dc=dcc,dc=fc
    - uid=aprof,ou=Profs,dc=ads,dc=dcc,dc=fc



Hierarquia (2)

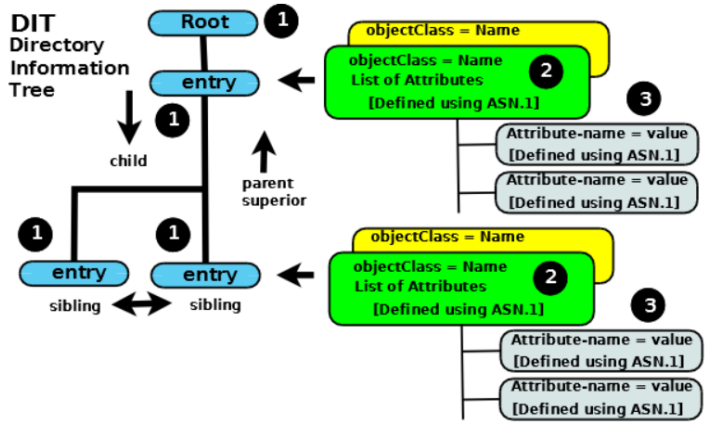
- dc=dcc,dc=fc
  - ou=Students,dc=ads,dc=dcc,dc=fc
    - uid=aauser,ou=Students,dc=ads,dc=dcc,dc=fc
    - uid=auser,ou=Students,dc=ads,dc=dcc,dc=fc
  - ou=Profs,dc=ads,dc=dcc,dc=fc
    - uid=aprof,ou=Profs,dc=ads,dc=dcc,dc=fc



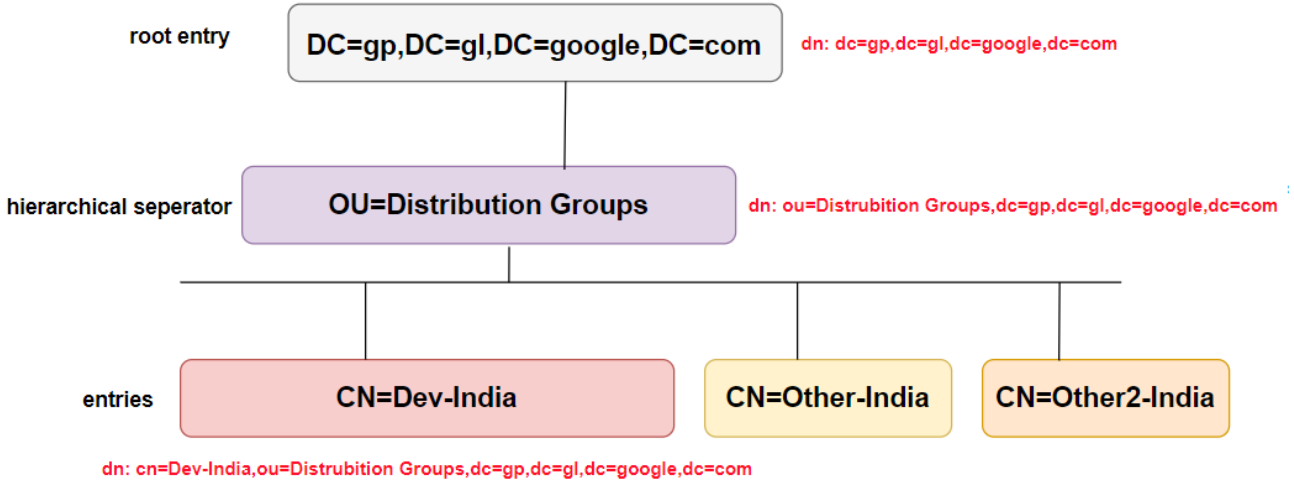
Hierarquia (3)

From https://stackoverflow.com/questions/18756688/what-are-cn-ou-dc-in-an-ldap-search

Technically, LDAP is just a protocol that defines the method by which directory data is accessed.Necessarily, it also defines and describes how data is **represented** in the directory service
Data is represented in an LDAP system as a hierarchy of objects, each of which is called an **entry**. The resulting tree structure is called a **Directory Information Tree (DIT)**. The top of the tree is commonly called the **root** (a.k.a base or the suffix).



LDAP DIT Information (Data) Model



Alguns atributos

- **dc**: domain componente
- **cn**: common name
- **ou**: organization unit

- Os atributos de uma entidade estão definidos na(s) ObjectClass(es) a que pertence

- **Ver mais em: http://www.zytrax.com/books/ldap/ch2/index.html**

Estrutura dos dados

Distinguished name, "chave na BD"

Tipo da entidade

Common Name

Entidade sobre uma conta de utilizador

Atributos :<identificador:valor>

Múltipla "herança"

```
dn: uid=aauser,ou=Students,dc=ads,dc=dcc
uid: aauser
cn: An admin User
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:
{crypt}$6$b8L.PFMUy9z8vejP$6l3bfLxvPP6.ywpuw/.
0eScm93M83Sg3vGyk4TopmLS/6RB9WfdQzcRwAMy4VQ2iu
FqVUK5b/zxpe96ngJ4M01
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/aauser
gecos: An admin User
```

organizational unit

Domain base: ads.dcc

Exemplo para utilizadores

Apenas ilustrado para um utilizador

Migration Tools

top is an abstract object class that is the parent of every LDAP object class. It is the one that defines that every object in LDAP must have an objectClass attribute.

- shadowLastChange - Indicates the number of days between January 1, 1970 and the day when the user password was last changed. (single-valued)
- shadowExpire - Indicates the date on which the user login will be disabled. (single-valued)
- shadowFlag - not currently in use.
- shadowInactive - Indicates the number of days of inactivity allowed for the user. (single-valued)
- shadowMax - Indicates the maximum number of days for which the user password remains valid. (single-valued)
- shadowMin - Indicates the minimum number of days required between password changes. (single-valued)
- shadowWarning - The number of days of advance warning given to the user before the user password expires. (single-valued)

```
# /usr/share/migrationtools/migrate_passwd.pl /etc/passwd
dn: uid=aauser,ou=People,dc=padl,dc=com
uid: aauser
cn: An admin User
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:
{crypt}$6$b8L.PFMUj9z8vejW$6l3bkLxvPP6.ywpuw/.0gScm03M82Sg3vGyk4Tam
mLS/6RB9WfdQzckwAMy4VQ2iuFqVUS0b/zxpe45ngF2M01
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/aauser
gecos: An admin User
```

Base por omissão das *tools*

Consultou o /etc/shadow

Esquemas (Schemas)

- Vários já definidos em:
  - `/etc/openldap/schema/`

- Exemplos:
  - `inetorgperson.ldif`
  - `nis.ldif`

Daemons

- **`slapd`** é o servidor do OpenLDAP
- **`slurpd`** serve para quando existem vários servidores LDAP para manter a replicação aos servidores súbditos (slaves).

Formato ldif (LDAP Data Interchange Format)

```
# commentário
dn: <distinguished name>
<attrdesc>: <attrvalue>
<attrdesc>: <attrvalue>
```

- Para continuar uma linha, ter espaço ou tab no início

```
dn: cn=Barbara J Jensen,dc=example,dc=
  com
cn: Barbara J
     Jensen
```

Fonte: The LDIF text entry format

Formato ldif (2)

- Valores múltiplos:

```
cn: Barbara J Jensen
cn: Babs Jensen
```

- Para ter espaço ou ":" no valor deve-se codificar em **base64** e ter 2x ":"
  - Texto " begins with a space"

```
cn:: IGJlZ2lucyB3aXRoIGEgc3BhY2U=
```

Fonte: The LDIF text entry format

Formato ldif (3)

olcRootDN: <DN> This directive specifies **the DN that is not subject to access control or administrative limit restrictions for operations on this database**. The DN need not refer to an entry in this database or even in the directory

- Mesmo ficheiro pode ter múltiplas entradas distintas (diferentes dn)
- Para modificação uma linha com "-" significa que se mantem no mesmo dn. Ex.:

```
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=Manager,dc=profs,dc=ads,dc=dcc
-
replace: olcRootPW
olcRootPW: {SSHA}IDx/NImy7xbOD8F1N008Op+e2mvHfLr8
```

MDB: A Memory-Mapped Database

https://www.zytrax.com/books/ldap/ch6/slapd-config.html

The numeric {<index>} may be provided to distinguish multiple databases of the same type

Fonte: The LDIF text entry format

Formato ldif (4)

Ver mais: https://www.openldap.org/doc/admin24/access-control.html

- A ordem da entrada num mesmo atributo pode ser especificada
  Ex.:

```
olcAccess: {0}to attrs=member,entry
        by dnattr=member selfwrite
olcAccess: {1}to dn.children="dc=example,dc=com"
        by * search
olcAccess: {2}to dn.children="dc=com"
        by * read
```

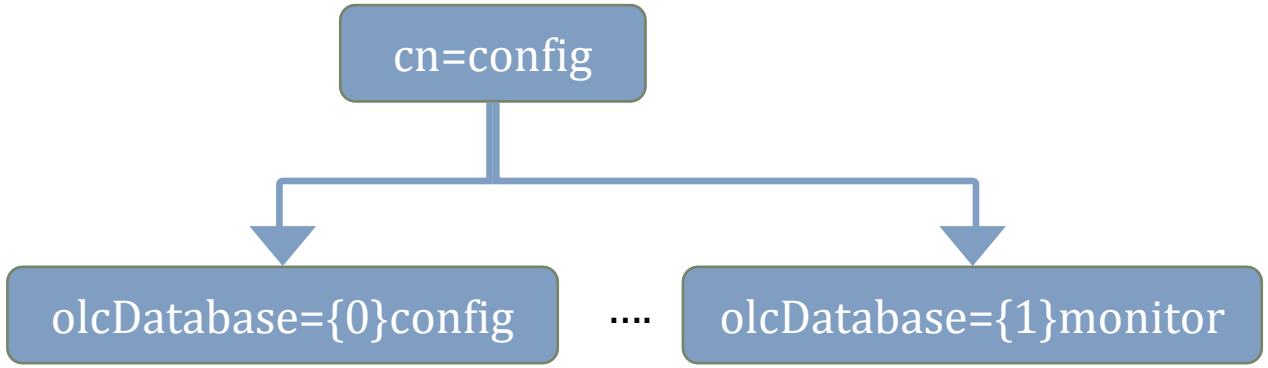
Basic ACLs
Generally one should start with some basic ACLs such as:
access to attrs=userPassword
by self =xw
by anonymous auth
by * none

Fonte: Access Control Ordering

“Duas” bases de dados

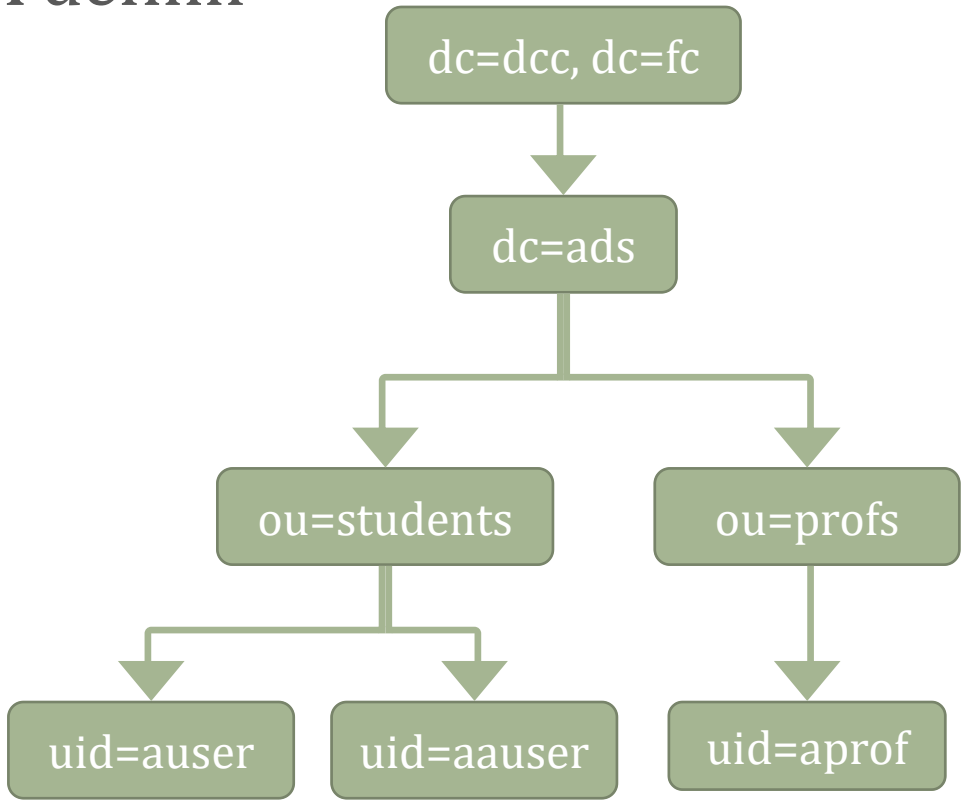
Configuração do LDAP

- Já existente
- Modificar/adicionar atributos ➔configuração



Base com os dados

- A definir



Controlo de acesso

- Definição em ldif para limitar o acesso

```
olcAccess: {0}to attrs=userPassword,shadowLastChange
    by dn="cn=Manager,dc=profsvb,dc=ads,dc=dcc" write
    by anonymous auth
    by self write
    by * none
olcAccess: {1}to dn.base=""
      by * read
```

O que se restringe o acesso a

O acesso permitido

A quem se permite/restringe o acesso

Entrada 0 e 1 no array de olcAccess.

A quem: especificar as entidades

Specifier	Entities
*	All, including anonymous and authenticated users
anonymous	Anonymous (non-authenticated) users
users	Authenticated users
self	User associated with target entry
dn[.<basic-style>]=<regex>	Users matching a regular expression
dn.<scope-style>=<DN>	Users within scope of a DN

Acesso: nível

Level	Privileges	Description
`none =`	0	no access
`disclose =`	d	needed for information disclosure on error
`auth =`	dx	needed to authenticate (bind)
`compare =`	cdx	needed to compare
`search =`	scdx	needed to apply search filters
`read =`	rscdx	needed to read search results
`write =`	wrscdx	needed to modify/rename
`manage =`	mwrscdx	needed to manage

--Adicionar atributos a uma entrada

```
# changeBDpw.ldif
dn: olcDatabase={0}config,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}rVdhYTyjPcggsPHmAp25EsbTe8dYmyGo
```

- Executar passando o ficheiro ldif acima

```
# ldapmodify -Y EXTERNAL -H ldapi:/// -f changeBDpw.ldif
```

Ligações

URL	Protocol	Transport
`ldap:///`	LDAP	TCP port 389
`ldaps:///`	LDAP over SSL	TCP port 636
`ldapi:///`	LDAP	IPC (Unix-domain socket)

Buscas

OLC = "OpenLDAP Configuration"

```
# ldapsearch -Q -LLL -Y EXTERNAL -H ldapi:/// -b \
"olcDatabase={2}mdb,cn=config"
```

- -Q ser silencioso no output sobre a ligação
- -L formato do output
- -Y mecanismo para a autenticação SASL
- -H uri para ligação
- -b base de onde se inicia a busca

SASL - Simple Authentication and Security Layer

- Vários métodos para autenticação:
  - `EXTERNAL`: The SASL EXTERNAL mechanism makes use of an authentication performed by a lower-level protocol: usually TLS or Unix IPC
  - GSSAPI, KERBEROS_V4, DIGEST-MD5
  - Mapping Authentication Identities: autentica o utilizador indicado mapeando num utilizador LDAP
  - …

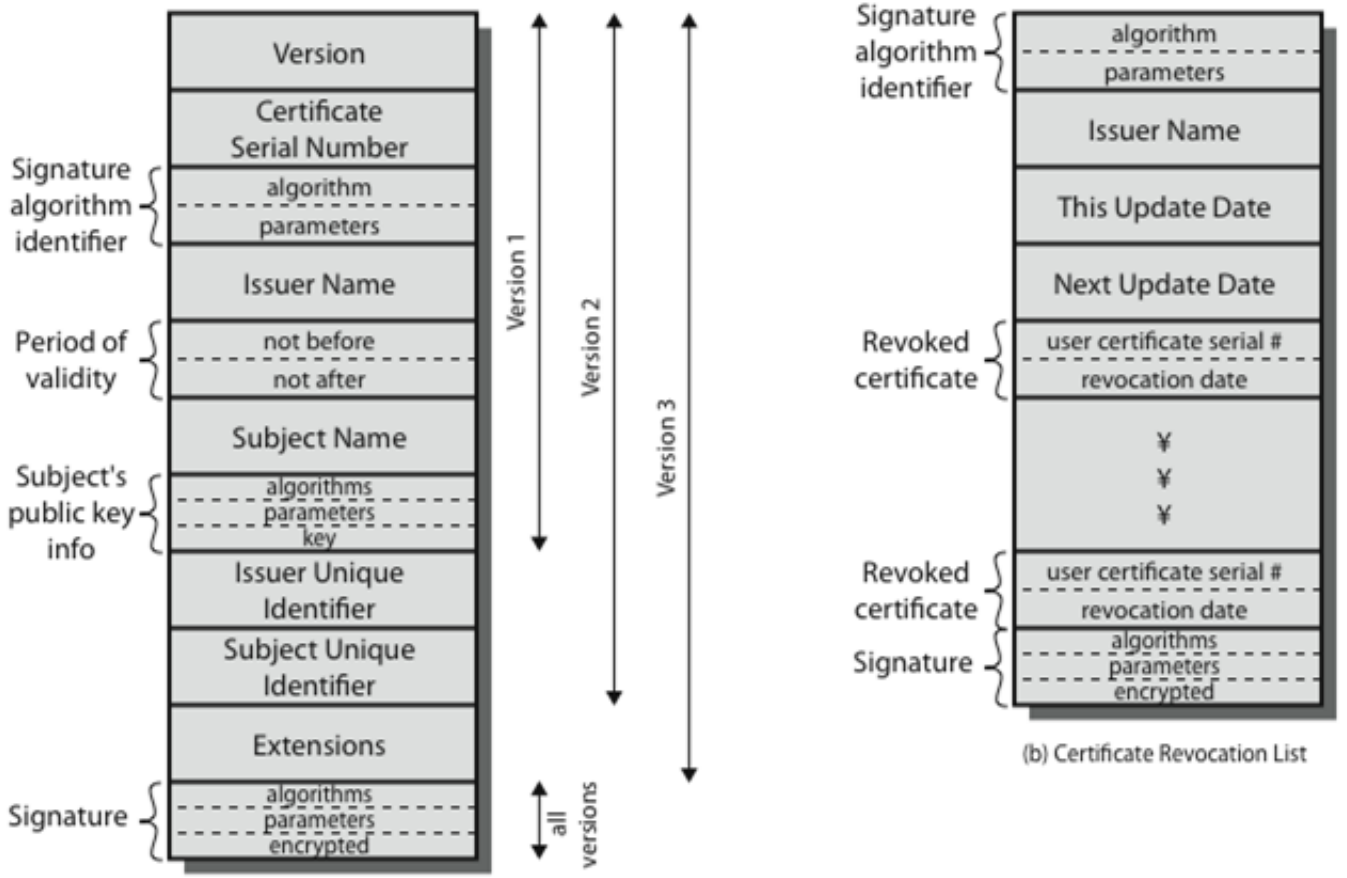
Procuras de entradas

```
# ldapsearch -x -L -W -D "cn=Manager,dc=profsvb,dc=ads,dc=dcc" -b
"dc=profsvb,dc=ads,dc=dcc" '(objectClass=account)' loginShell
homeDirectory uidNumber
```

- -x utilizar autenticação simples em vez de SASL
- -W pedir a password de acesso
- **-D usar a entidade (binding) para controlar o acesso**
- '(objectClass=account)' filtro para a busca
- `loginShell homeDirectory uidNumber` atributos que se quer ver
- **-b searchbase**

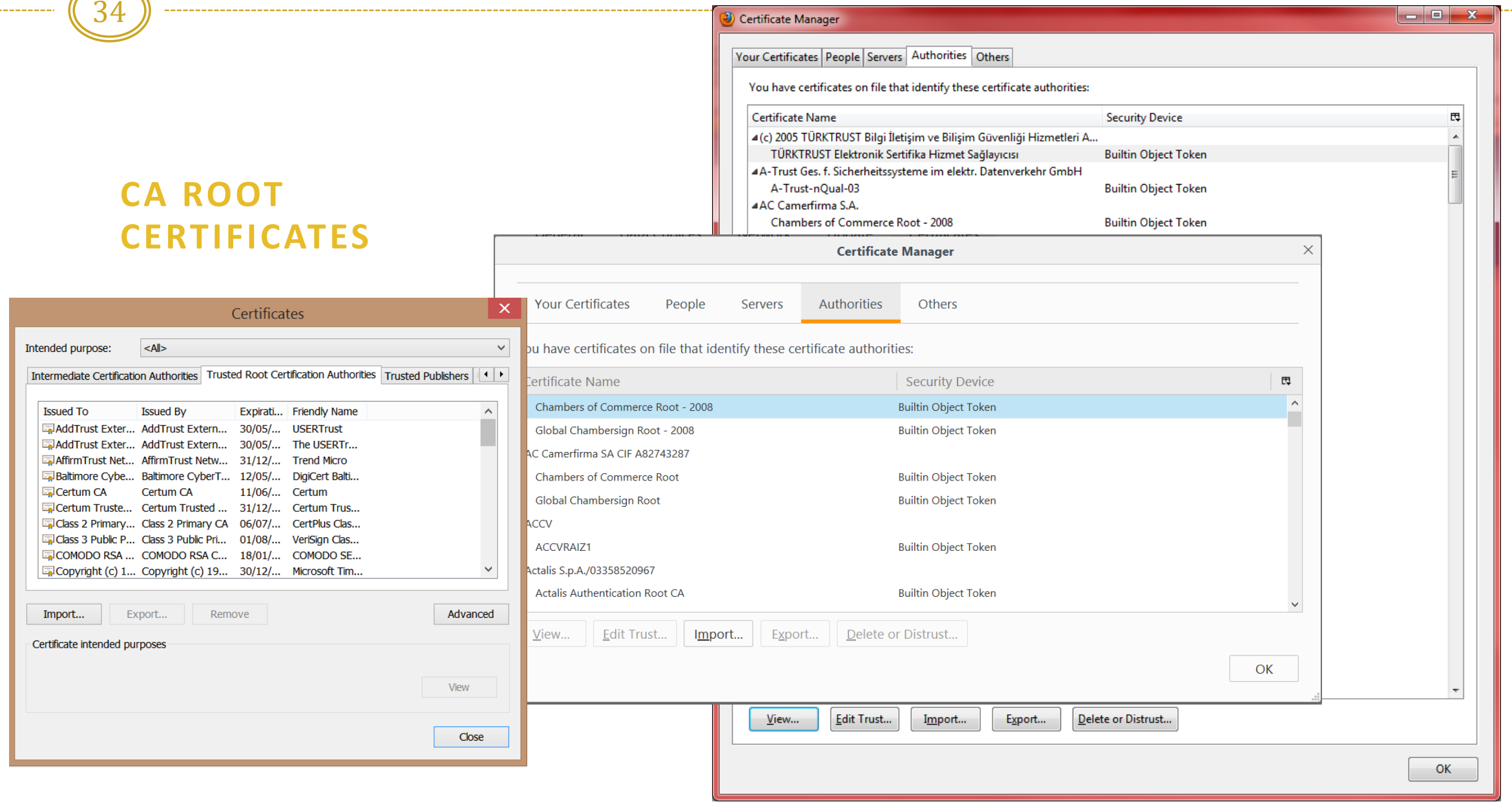
  Use searchbase as the starting point for the search instead of the default.

Breve interlúdio sobre certificados



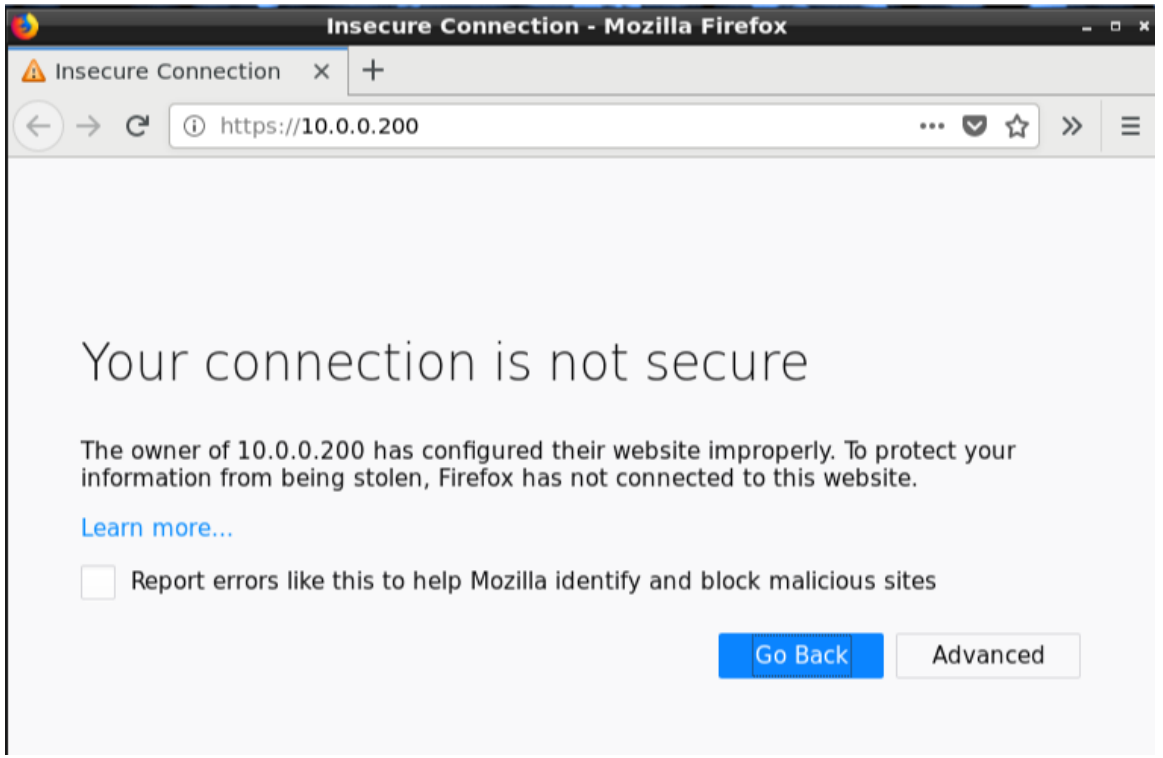
(b) Certificate Revocation List

CA ROOT CERTIFICATES



Certificados self-signed

- A chave privada do próprio certificado assina o certificado
- O CA (certificate authority) é a entidade do próprio certificado
- Necessariamente não confiável



Acesso do cliente

- Config:

  `/etc/openldap/ldap.conf`

- Confiar nos certificados não válidos
- Configurar o acesso ao servidor
  - Incluindo a base para acesso

Utilizadores

- Com o comando migrate (ou à mão) pode-se definir os utilizadores
- Adiciona-se com (supondo utilizador em user.ldif).

```
$ ldapadd -x -D cn=Manager,dc=profsvb,dc=ads,dc=dcc -W -f user.ldif
```

  - `-f` ficheiro com ldif a acrescentar
    - Poderia ser no stdin.
- Busca na máquina remota permite aceder aos mesmos dados

Interlúdio autenticação

- `authselect`
  - Permite configurar onde aceder a autenticação e identificação
  - Substitui `authconfig`
  - Define *profiles* para diminuir erros de mudar vários ficheiros

SSSD - System Security Services Daemon

- Daemon de gestão para consulta de diretórios de informação e autenticação

  /etc/sssd/sssd.conf

  /etc/sssd/sssd.d/

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/configuring_authentication_and_authorization_in_rhel/understanding-sssd-and-its-benefits_configuring-authentication-and-authorization-in-rhel

- Permite configurar diretório LDAP e o seu acesso

The **System Security Services Daemon** (SSSD) is software originally developed for the Linux operating system (OS) that provides a set of daemons to manage access to remote directory services and authentication mechanisms.[1] The beginnings of SSSD lie in the open-source software project FreeIPA (Identity, Policy and Audit).[2] The purpose of SSSD is to simplify system administration of authenticated and authorised user access involving multiple distinct hosts.[3] It is intended to provide single sign-on capabilities to networks based on Unix-like OSs that are similar in effect to the capabilities provided by Microsoft Active Directory Domain Services to Microsoft Windows networks.[4]

Autorização por LDAP

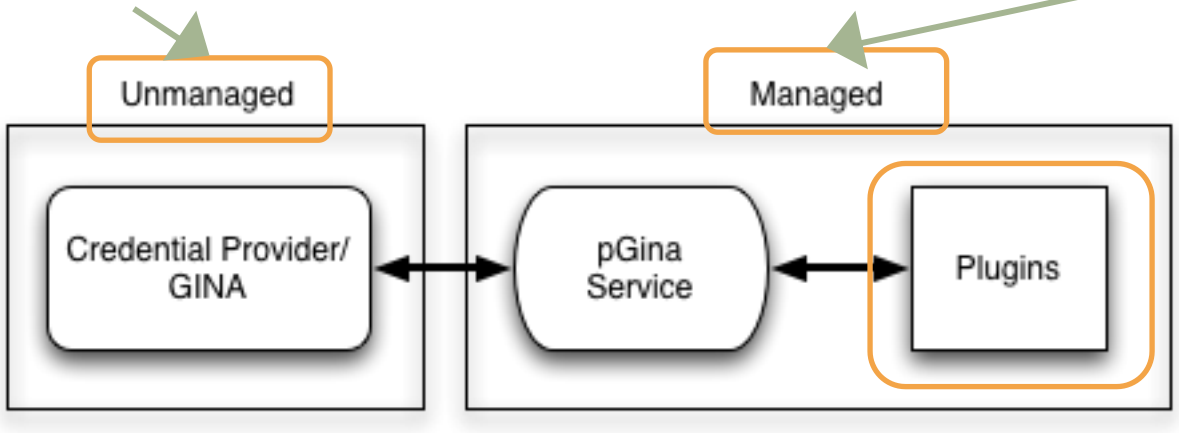
- Autenticação
  - `login`
- Mudança de passwd
  - `passwd`
- Detalhes sobre os utilizadores
  - `getent`, `id`

Autenticação Windows

- Utilização da ferramenta pGina fork (versão pGina original não tem sido atualizada)
- Permite configurar o servidor LDAP onde autenticar

Instalado, mas não será configurável

Instalado e configurável



Um dos quais: LDAP

Imagem de pGina User's Guide

Configuração pGina

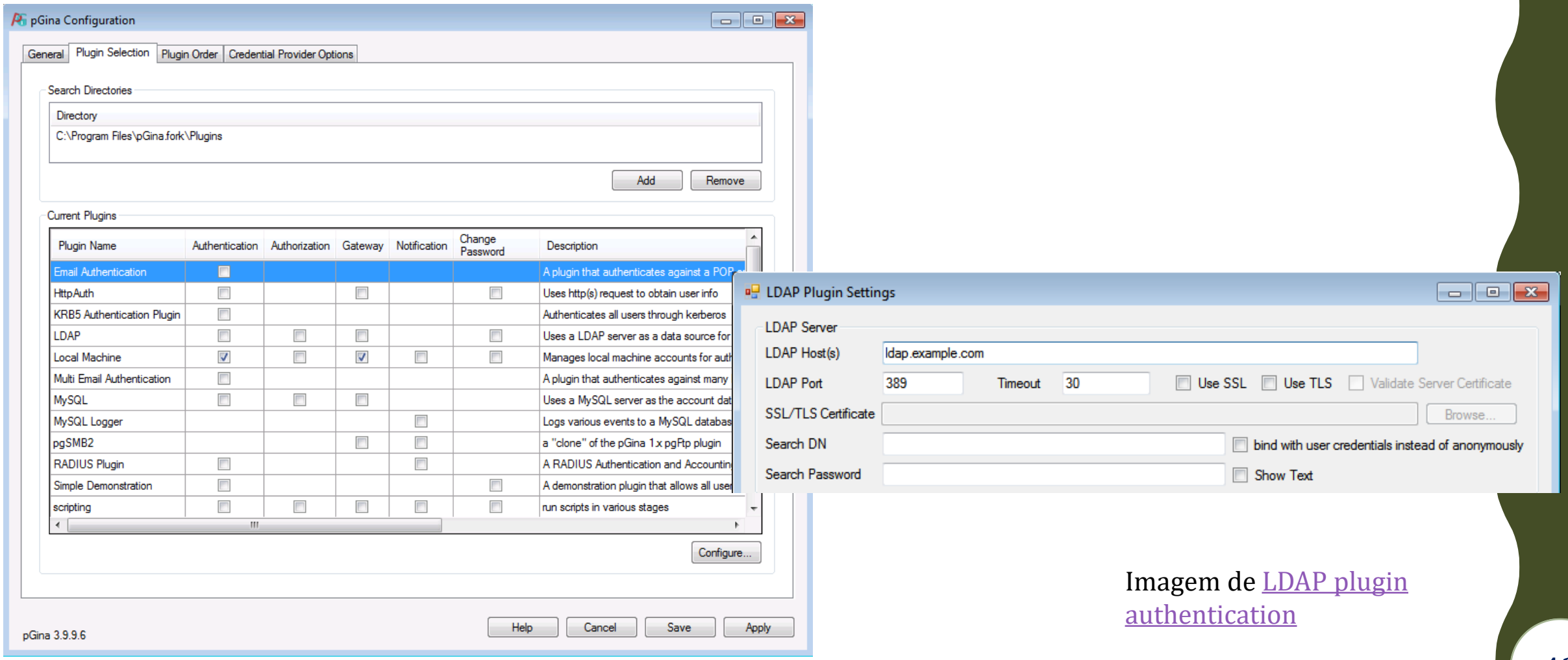


Imagem de LDAP plugin authentication

Imagem de pGina User's Guide

Resumo

- Especificações e ferramentas
- Arquitetura
- Formato LDIF
- Configurações e gestão
- Procuras
- Conexões (certificados e SSSD)
- Autenticação (Linux e Windows)

Referências

- OpenLDAP para Fedora 28
- OpenLDAP
  - What are the DB_CONFIG configuration directives?
  - Access Control
- Fedora Administrator Guide, Directory Servers
  - Várias ferramentas do slapd
- Understanding the LDAP Protocol, Data Hierarchy, and Entry Components
- LDAP for Rocket Scientists

[dcc]

U.PORTO

FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

QUESTÕES/ COMENTÁRIOS