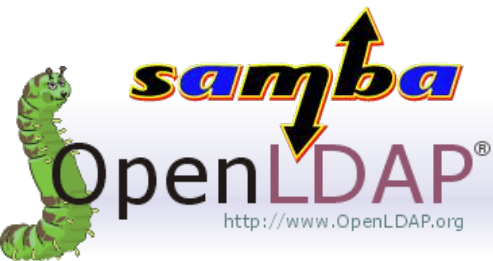


SAMBA3 e LDAP

**Base sólida para
redes heterogêneas.**

Felipe Augusto van de Wiel (faw)

Brasil, São Paulo, 06 de novembro de 2004.



Quem sou eu?

"No mundo"

Admin. Redes e Sistemas

Instrutor Rede Conectiva de Treinamentos

Contato com GNU/Linux em 1998

Contato com Debian em 2002

Voluntário

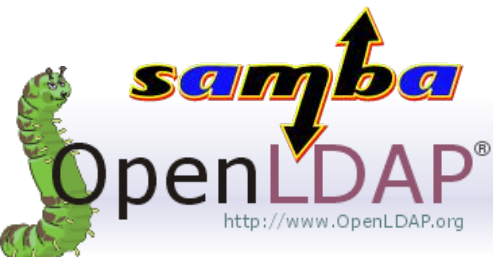
Projeto Debian-BR

Projeto Debian-PR

PHP Community

Certificado

**Conectiva (2x)
LPIC1**



Quem sou eu?

“No mundo Debian”

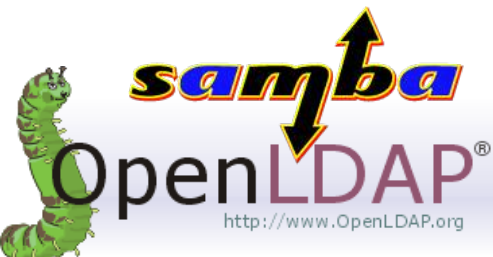
Administro Servidor Debian-PR

Moderador da lista debian-pr

Líder GUD-PR

Voluntário PSL-PR / MSL-PR / CGNU

Traduções e documentações



Nossos Objetivos

SAMBA

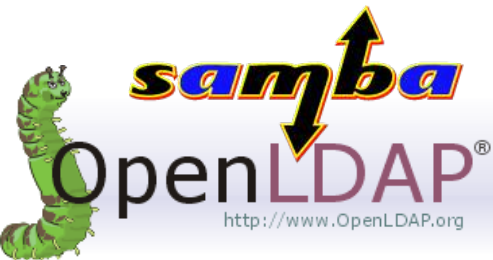
- História & Conceitos
- Samba 2.2 / 3.0 / 3.2 / 4.0 / HEAD

LDAP

- DAP, X.500 e AD
- LDAP e OpenLDAP

SAMBA3 e LDAP

- Integração
- Vantagens e Desvantagens



Opening Windows to a Wider World

Desde 1992!!!

Serviços de impressão e arquivos
para clientes SMB/CIFS

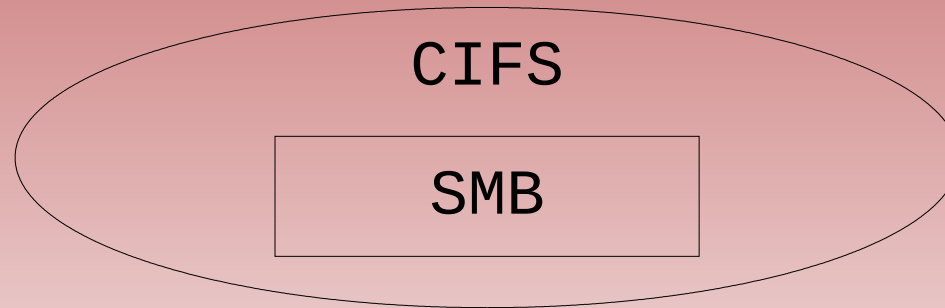
Interoperabilidade entre
Linux/Unix e Windows

Andrew Tridgell (rsync)

CIFS/SMB

SAMBA

Common Internet File System (MS)



Server Message Block

NetBIOS - Network Input Output System

NetBEUI - NetBIOS Enhanced User Interface

Pontos Chave

SAMBA

smbd & nmbd

(A) Compartilhamento de arquivos e impressoras

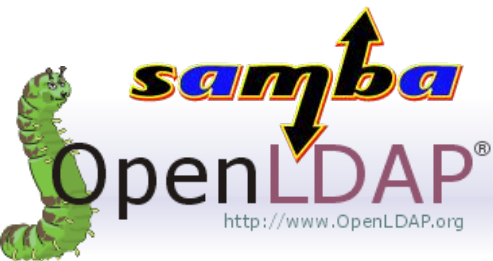
(B) Autenticação e Autorização

(C) Resolução de Nomes

(D) Anúncio (browsing)

SMB Daemon -> A; B(share/user)

NMB Daemon -> C; D



Festival de nomes

SAMBA

Domínio NT

Active Directory (AD)

Local Master Browser (LMB)

Domain Master Browser (DMB)

NetBIOS Name Service (NBNS)

Windows Internet Name Service (WINS)

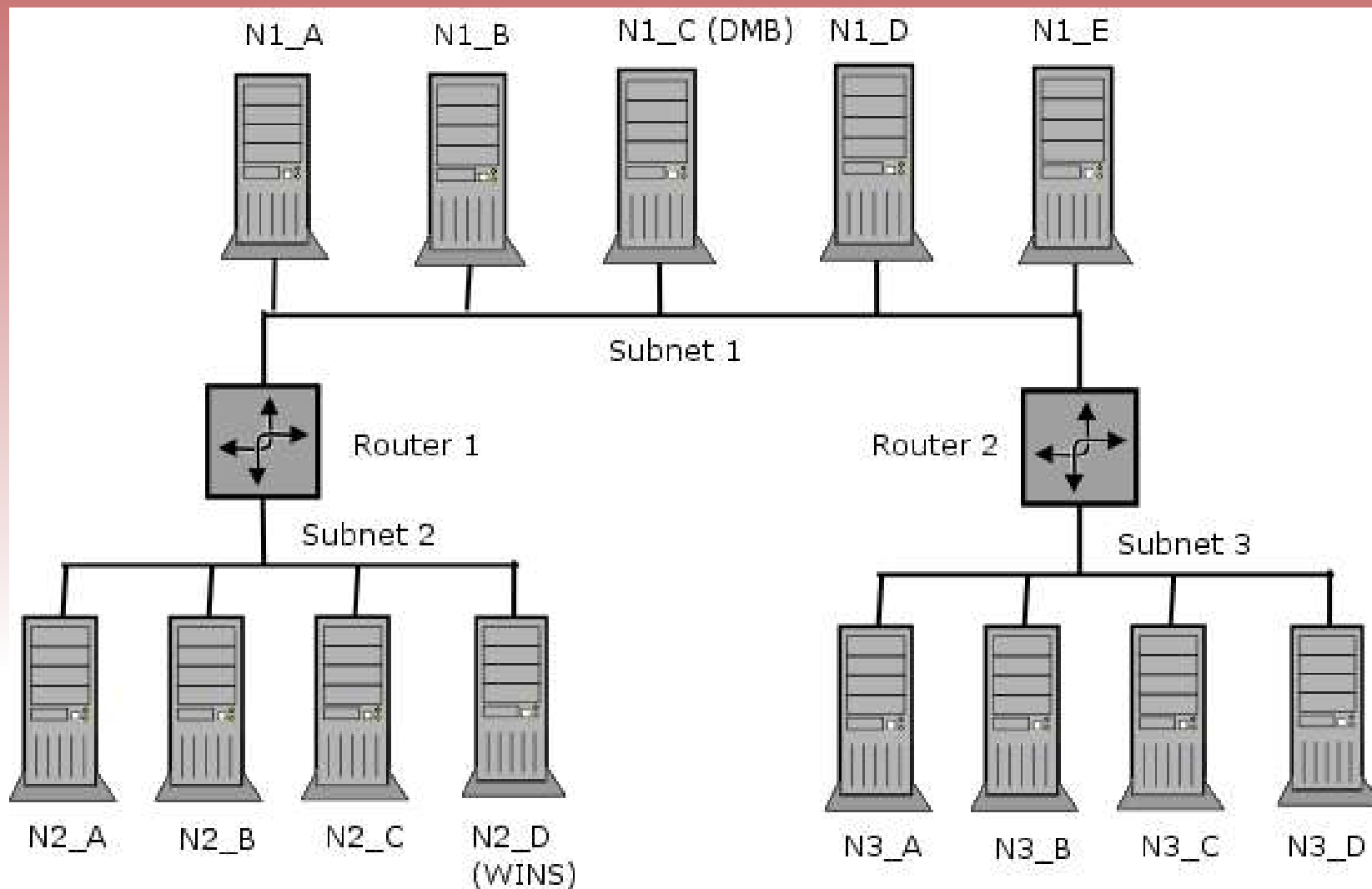
Primary Domain Controller (PDC)

Backup Domain Controller (BDC)



Visão Geral

SAMBA



Versões

SAMBA

2.2 obsoleto

3.0 atual

3.2 (final de 2004)

4.0 (...)

Implementação completa CIFS
Reorganização de código



Componentes

SAMBA

smb.conf

SMBD & NMBD

Repositório de senhas

LOGs

Recursos e Benefícios

SAMBA

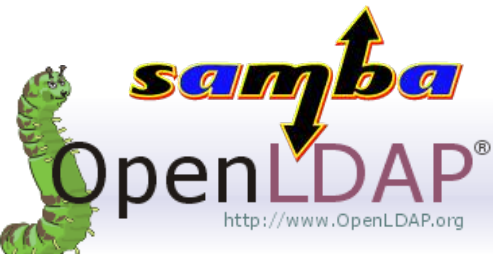
Samba3 pode substituir um NT4 (DC)

Interoperabilidade Domínios NT4 e AD

Confiança entre domínios NT4

Senhas podem ser replicadas e/ou distribuídas

Múltiplos backends de contas



Tipos de Servidor

SAMBA

Domain Controller

PDC

BDC

ADS DC

Domain Member

AD DS

NT4-style DS

Stand Alone

Modos de Segurança

SAMBA

Share

User

Domain

ADS

Server



Verificação de Senhas

SAMBA

Senhas criptografadas (challenge/response)

NTLMv1 NTLMv2

MD4 (unicode) - NT hash

upper(senha) - 14 bytes

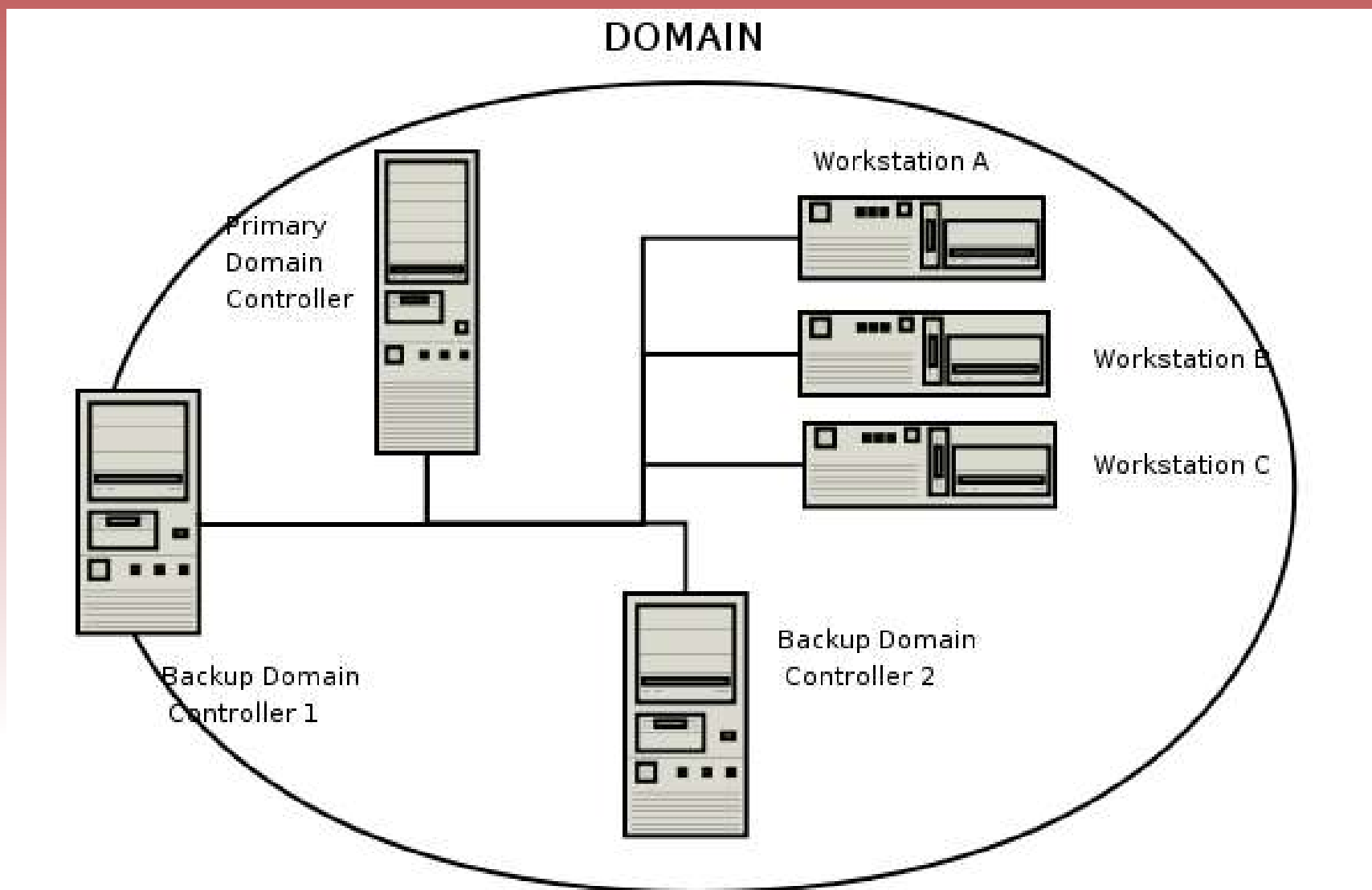
5 bytes NULL

Dividido em 2 chaves DES de 56bits

'magic' 8 bytes

16 bytes -> LanMan hash

Senhas texto puro



Lightweight Directory Access Protocol (LDAP)

Alternativa ao X.500 DAP

OpenSource

Universidade de Michigan

RFC 3377: LDAP (v3): Technical Specification
RFC 2251: LDAP (v3)
RFC 2252: LDAPv3: Attribute Syntax Definitions
RFC 2253: LDAPv3: UTF-8 String Representation of DN
RFC 2254: The String Repres. of LDAP Search Filters
RFC 2255: The LDAP URL Format
RFC 2256: A Summary of the X.500(96) User Schema...
RFC 2829: Authentication Methods for LDAP
RFC 2830: LDAPv3: Extension for TLS
RFC 3771: LDAP: Intermediate Response Message

LDAP version 2 (LDAPv2) é histórica (RFC 3494).

Objetivo

LDAP

Catálogo de Endereços
“phonebook”

Busca e navegação de informações

DNS

MTA

SAMBA

PAM

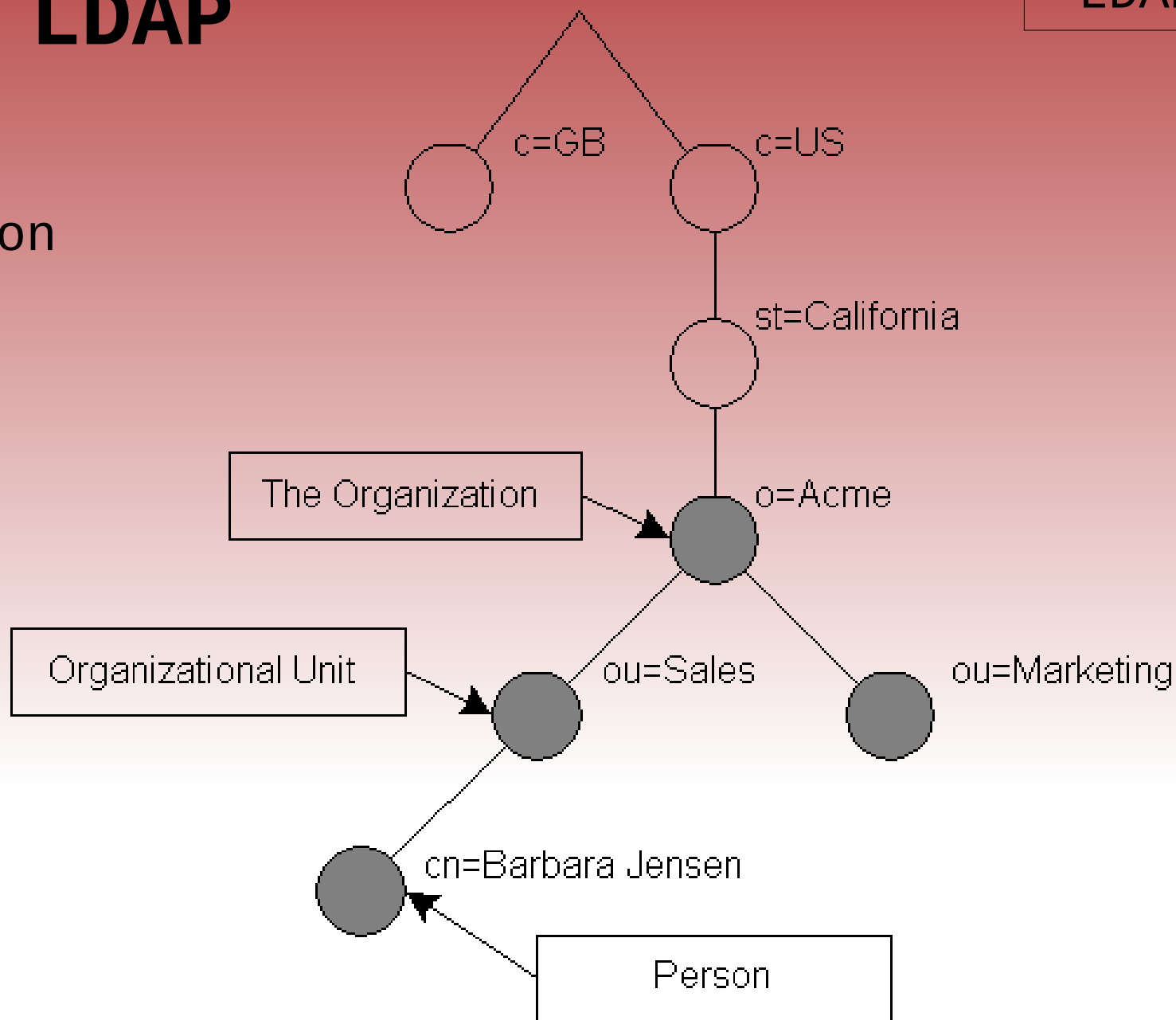
APACHE



Árvore LDAP

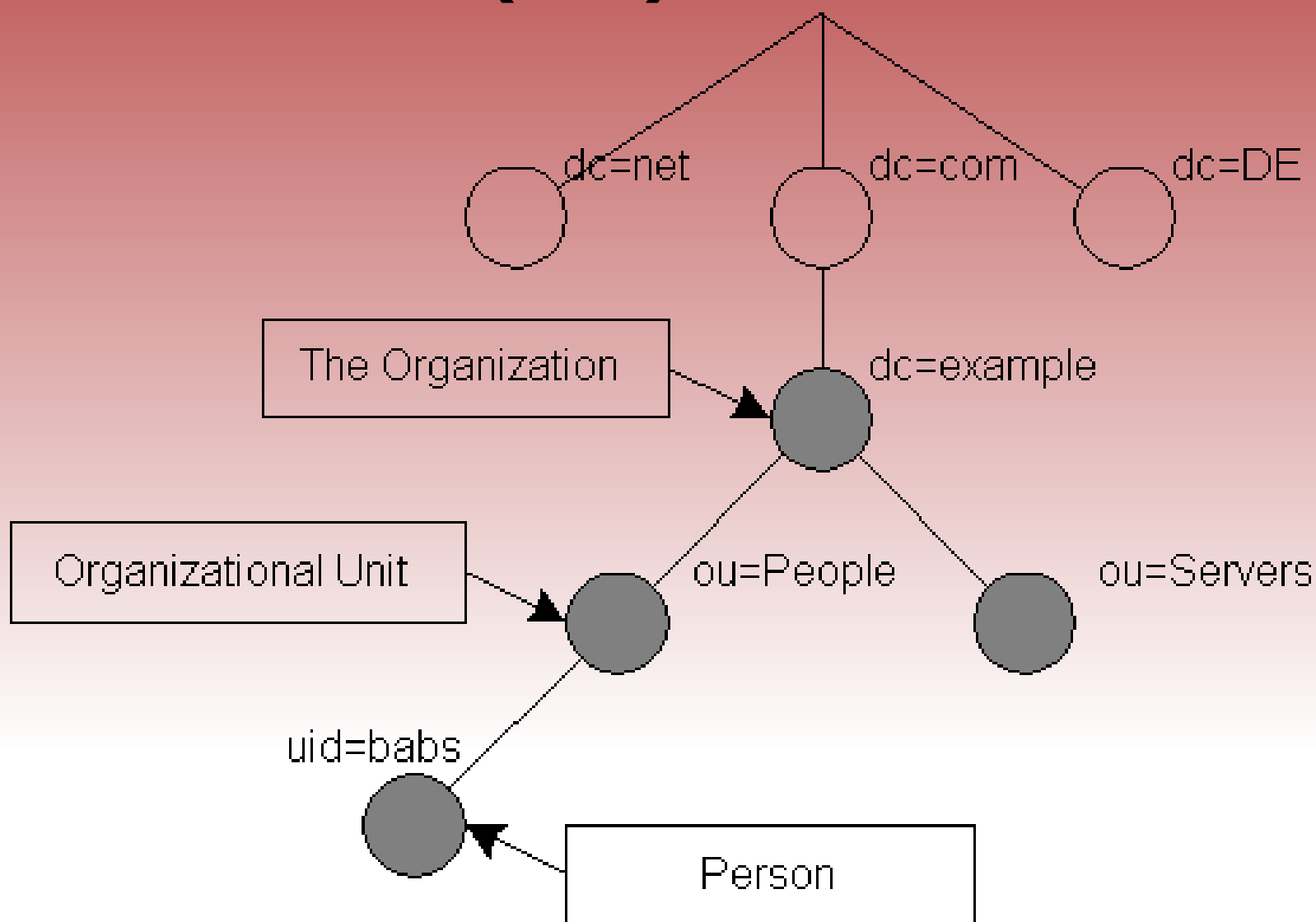
LDAP

Directory
Information
Tree



Árvore LDAP (dc)

LDAP



phpLDAPadmin

LDAP

GNU/GPL

Home / Commercial (\$ 49.95)

Livre

Agilidade

Tempo vs. Custo



phpLDAPadmin - CVS

[Request a new feature](#)[Report a bug](#)

Raider

[schema](#) | [search](#) | [refresh](#) | [create](#) | [info](#) | [import](#)

dc=example, dc=com (9)

- + cn=admin
- + cn=dave test
- + cn=MyGroup
- + cn=test
- + cn=test smith2
- + ou=automount
- + ou=People (22)
 - + cn=Funk Bob
 - + cn=Haberland felix
 - + cn=Joe2
 - + cn=Kazik Francuski
 - + cn=Smith Dave
 - + cn=thomas bob
 - + cn=Verónica (1)
 - + ou=People-copy8 (21)

Create Object

On server 'Raider', using template 'Custom'

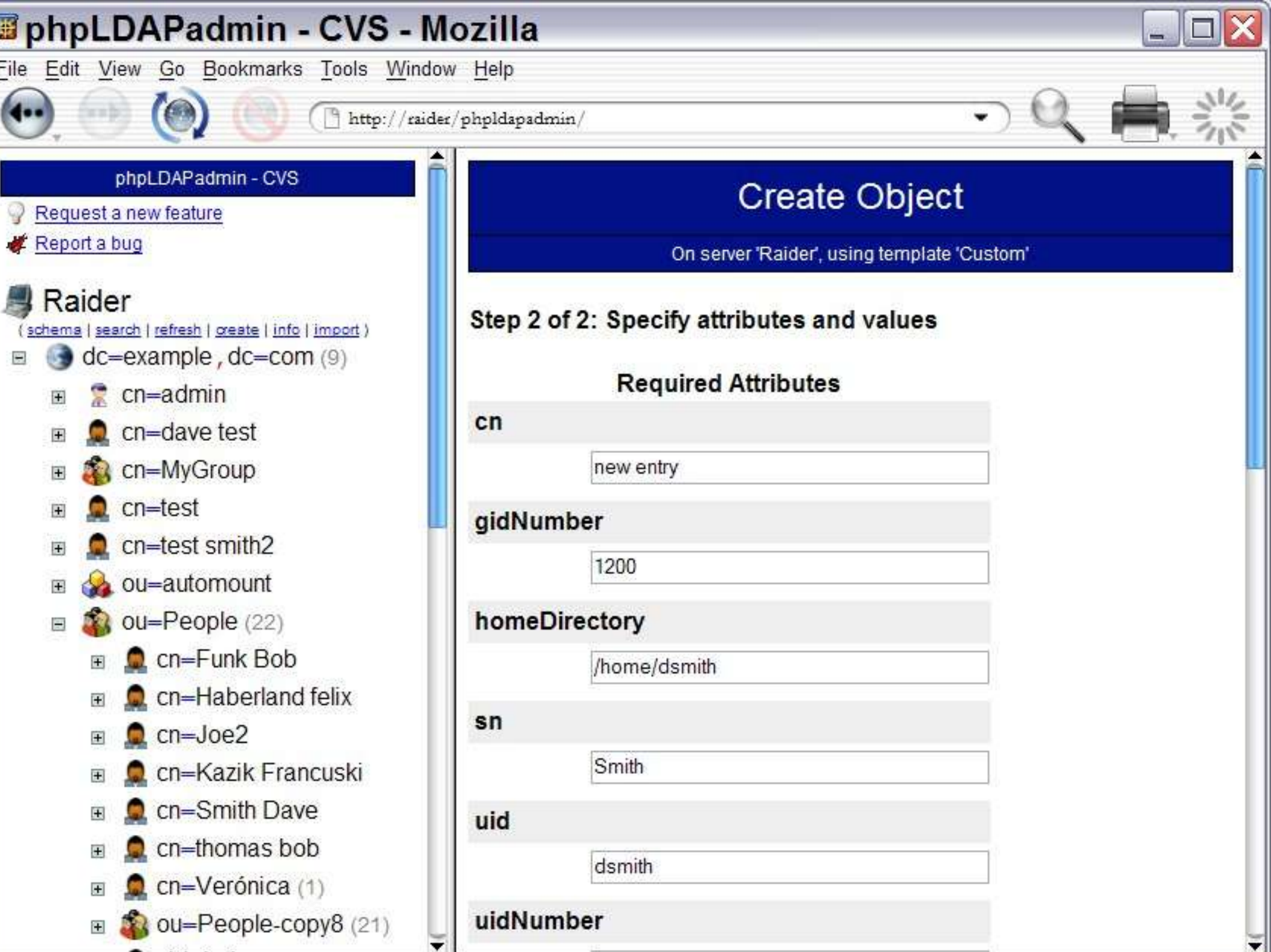
Step 1 of 2: Name and ObjectClass(es)

RDN: (example: cn=MyNewPerson)Container: [browse](#)

ObjectClasses

- oneOfpc
- OpenLDAPProotDSE
- organization
- organizationalPerson**
- organizationalRole
- organizationalUnit
- person
- pilotDSA
- pilotOrganization
- pilotPerson
- posixAccount**
- posixGroup
- qualityLabelledData
- referral
- residentialPerson
- REC822localPart

 Hint: You must choose at least one structural objectClass[Proceed >>](#)



phpLDAPadmin - CVS

[Request a new feature](#)

[Report a bug](#)

Raider

([schema](#) | [search](#) | [refresh](#) | [create](#) | [info](#) | [import](#))

dc=example, dc=com (9)

- + cn=admin
- + cn=dave test
- + cn=MyGroup
- + cn=test
- + cn=test smith2
- + ou=automount
- + ou=People (22)
- + ou=People2 (4)
- + ou=Roaming

★ Create New

Raider (session)

[Login...](#)

Raider (cookie)

Export

Export

Server Raider

DN ou=People,dc=example,dc=com

[browse](#)

Export format

- ☒ LDIF
- ☐ DSML V.1

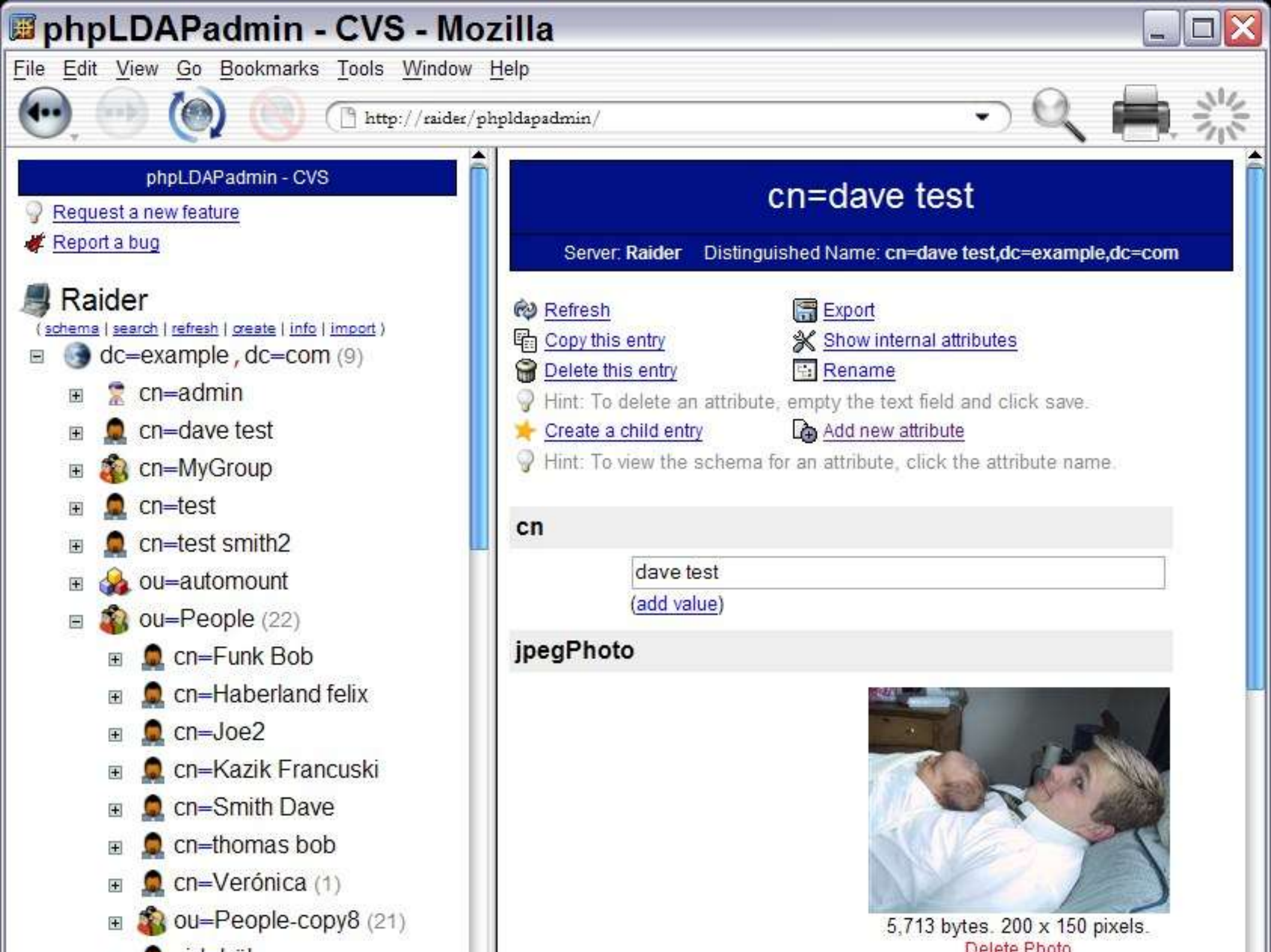
Line ends

- ☒ UNIX
- ☐ Macintosh
- ☐ Windows

Search Scope

- ☒ Base (base dn only)
- ☐ One (one level beneath base)
- ☐ Sub (entire subtree)

Proceed



phpLDAPadmin - CVS - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://raider/phpldapadmin/

phpLDAPadmin - CVS

Request a new feature

Report a bug

Raider

(schema | search | refresh | create | info | import)

dc=example , dc=com (9)

cn=admin

cn=dave test

cn=MyGroup

cn=test

cn=test smith2

ou=automount

ou=People (22)

cn=Funk Bob

cn=Haberland felix

cn=Joe2

cn=Kazik Francuski

cn=Smith Dave

cn=thomas bob

cn=Verónica (1)

ou=People-copy8 (21)

cn=dave test

Server: Raider Distinguished Name: cn=dave test,dc=example,dc=com

Refresh

Copy this entry

Delete this entry

Create a child entry

Hint: To delete an attribute, empty the text field and click save.

Hint: To view the schema for an attribute, click the attribute name.

Export

Show internal attributes

Rename

Add new attribute

cn

dave test

(add value)

jpegPhoto

5,713 bytes. 200 x 150 pixels.

Delete Photo

phpLDAPadmin - CVS

[Request a new feature](#)

[Report a bug](#)

Raider

([schema](#) | [search](#) | [refresh](#) | [create](#) | [info](#) | [import](#))

dc=example, dc=com (9)

cn=admin

cn=dave test

cn=MyGroup

cn=test

cn=test smith2

ou=automount

ou=People (22)

cn=Funk Bob

cn=Haberland felix

cn=Joe2

cn=Kazik Francuski

cn=Smith Dave

cn=thomas bob

cn=Verónica (1)



Use the menu to the left to navigate

[Credits](#) | [ChangeLog](#) | [Donate](#)

phpLDAPadmin - CVS - Mozilla

File Edit View Go Bookmarks Tools Window Help

http://raider/phpldapadmin/

phpLDAPadmin - CVS

Request a new feature

Report a bug

Raider

schema

search

refresh

create

info

import

dc=example, dc=com (9)

cn=admin

cn=dave test

cn=MyGroup

cn=test

cn=test smith2

ou=automount

ou=People (22)

cn=Funk Bob

cn=Haberland felix

cn=Joe2

cn=Kazik Francuski

cn=Smith Dave

cn=thomas bob

cn=Verónica (1)

ou=People-copy8 (21)

cn

Description	(no description)
OID	2.5.4.3
Obsolete?	No
Inherits	name
Equality	caseIgnoreMatch
Ordering	(not specified)
Substring Rule	caseIgnoreSubstringsMatch
Syntax	Directory String (1.3.6.1.4.1.1466.115.121.1.15)
Single Valued	No
Collective?	No
User Modification	Yes
Usage	(not specified)
Maximum Length	32,768 characters
Aliases	commonName
Used by	applicationEntity applicationProcess automount

phpLDAPadmin - CVS

[Request a new feature](#)

[Report a bug](#)

Raider

([schema](#) | [search](#) | [refresh](#) | [create](#) | [info](#) | [import](#))

dc=example, dc=com (9)

- + cn=admin
- + cn=dave test
- + cn=MyGroup
- + cn=test
- + cn=test smith2
- + ou=automount
- + ou=People (22)
 - + cn=Funk Bob
 - + cn=Haberland felix
 - + cn=Joe2
 - + cn=Kazik Francuski
 - + cn=Smith Dave
 - + cn=thomas bob
 - + cn=Verónica (1)
 - + ou=People-copy8 (21)
 - + uid=bäb
 - + uid=dsmith
 - + uid=esanford

Simple Search Form

([Advanced Search Form](#) | [Predefined Searches](#))

Server

Raider

Search for entries whose:

User Name

equals

*

Search

Searching...

Entries found: **900** (3.49 seconds).

Filter performed: (uid=*)

Showing results **1** through **50**.

« 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 »

[uid=vsanford](#)

dn uid=vsanford,ou=People,dc=example,dc=com
cn Victory
sn Sanford
uid vsanford

[uid=jjose](#)

dn uid=jjose,ou=People,dc=example,dc=com
cn JOAO
sn JOSE
Phone 123456789
uid jjose

[uid=lsanford](#)

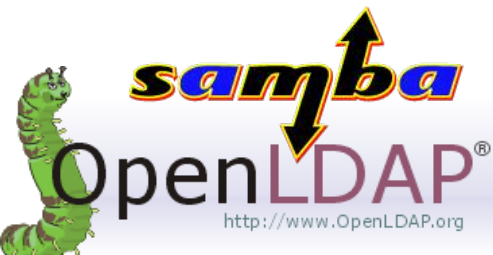
SAMBA + LDAP

SMB/LDAP

IDEALX (<http://www.idealx.{com,org}>)

smbldaptools

samba-console





IDEALX Management Console

Domain Configuration

- Authentication Options
- Account Policy
- Network Options
- Windows Networking Options
- Misc Options

Domain Management

- Manage Services
- Show Samba Server log
- Show NetBIOS log
- Show winbind log
- Show LDAP Server log
- Show System log

Account Management

- Manage user accounts
- Manage group accounts
- Manage computer accounts

Home > Domain Management

16-sep-2004



Server : localhost

Manager (logout)

— Account Properties —

Username Administrator

Rename

Full Name Administrator

Description

Password *****

Confirm Password

- ☐ User Must Change Password at Next Logon
- ☐ User Cannot Change Password
- ☐ Password Never Expires
- ☐ Account Disabled
- ☐ Account Locked

Submit Query

— Group Memberships —

PrimaryGroup Domain Admins

Set

Memberships

Domain Admins

Domain Users



SAMBA + LDAP

SMB/LDAP

PDC

BDC

Master LDAP

Slave LDAP

Central LDAP

Central LDAP

tdbsam

tdbsam
rpc net vampire

tdbsam

tdbsam
rsync

smbpasswd

smbpasswd



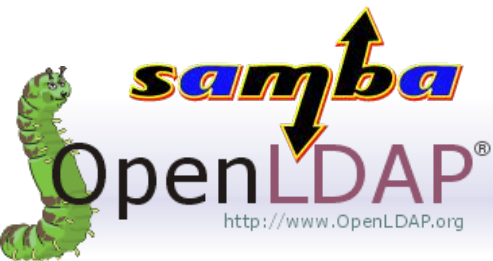
Agradecimentos

SAMBA
OpenLDAP

<http://www.samba.org>
<http://www.openldap.org>

Projeto Debian-PR e Debian-BR
Grupo de Usuários Debian-PR e Debian-BR

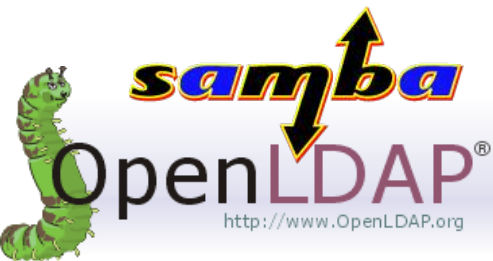
SEDU/PARANACIDADE
Conisli



Obrigado! :o)

Felipe Augusto van de Wiel

felipe@cathedrallabs.org
felipe.wiel@gmail.com



SAMBA

Andrew Tridgell (rsync)

NetBIOS – Network Basic Input/Output System

NetBEUI – NetBIOS Enhanced User Interface

Server Message Block (SMB)

Common Internet File System (CIFS)

TCP / UDP

