Serviços de Rede

João Victor A. Di Stasi
jvictor@ufrj.br

17 de Outubro de 2006

1 DNS

2 LDAP

3 Correio
- Postfix
- Amavisd-new
- Spamassassin
- Clamav
- Greylisting
- SPF

História

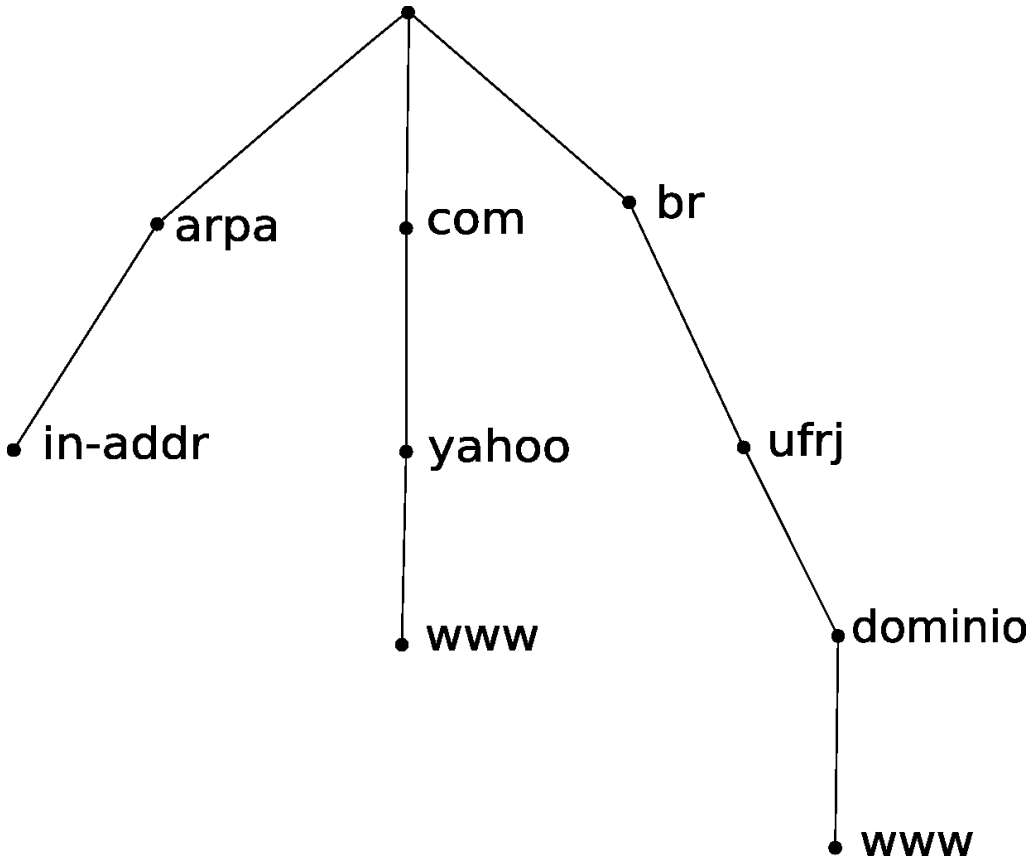
- Protocolo proposto por volta de 1980.
- Missão: resolver o problema do arquivo HOSTS.TXT.
- Estruturado de forma distribuída e redundante.
- Especificação original em 1983 pelas RFCs 882 e 883.
- Atualizadas em 1987 pelas RFCs 1034 e 1035.

História (continuação)

- Assim como HOSTS.TXT, o DNS provê a tradução de nomes para IP.
- Resolve o problema de escalabilidade do HOSTS.TXT.
- Cada organização agora é responsável por sua porção de informação.
- Extendido para manusear outros tipos de informações.

Framework do banco de dados distribuído do DNS

A informação é indexada pelo nome de domínio.



Framework do banco de dados distribuído do DNS

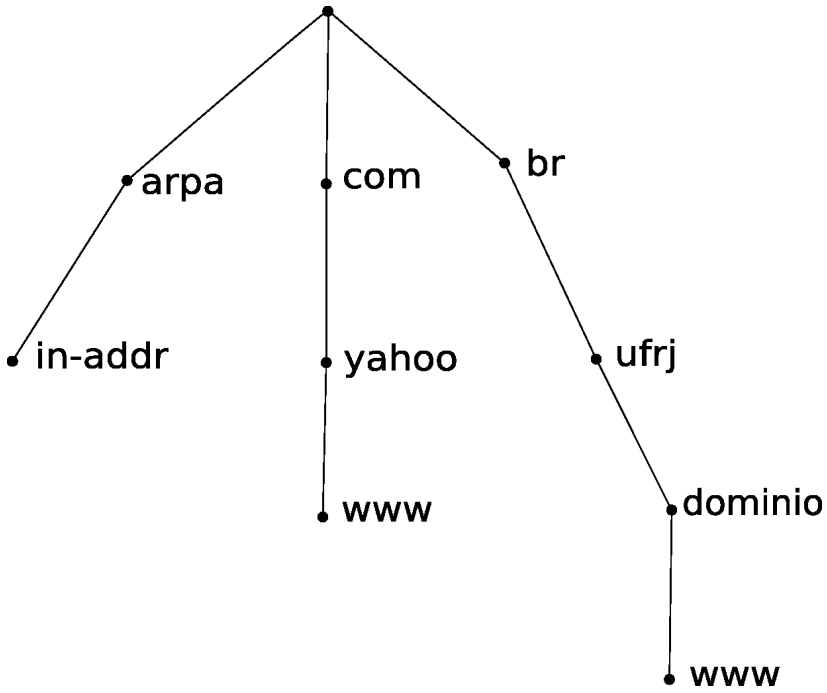
- Nós na árvore são chamados de nome de domínio.
  - Máximo de 63 caracteres.
    - ★ Case-insensitive.
    - ★ Permitido o uso de caracteres alfa-numéricos e '-' (hífen).
- Nós do mesmo nível na árvore devem ser únicos.
  - Esta regra evita qualquer tipo de colisão de nomes.
- Nós folhas continuam sendo nomes de domínio.
  - Também chamados de *hostnames*.

FQDN - Fully-Qualified Domain Name

- Representação completa do nome, separada por pontos.
- Identifica um nó de forma única.
- Máximo de 127 nós.
  Exemplo: maquina.dominio.ufrj.br.

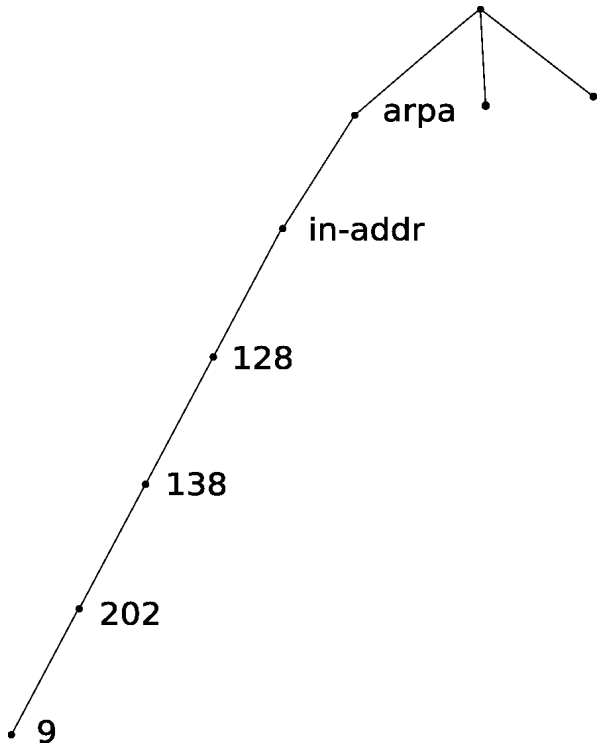
Domínio

- Uma sub-árvore do *namespace*.
- Normalmente chamado de zona.
  Exemplo: dominio.ufrj.br.



IN-ADDR.ARPA

- Sub-árvore de consultas reversas.
- Traduz IP para nome.



Zonas

- Pedaço da sub-árvore gerenciado por uma única entidade.
- Podem incluir sub-domínios.

Autoridade de zona

- Entidade que recebeu a delegação da zona na zona pai.
- Todas as respostas são confiáveis.
- Os servidores primário e secundários são autoridades.
- Pode modificar o mapa de *hosts*.
- Propaga a informação para outros servidores.

Tipos de pergunta DNS

Recursiva

- Executadas por aplicações clientes.
- O servidor local não conhece a resposta.
- O servidor local corre por toda a árvore DNS para obter a resposta.

Tipos de pergunta DNS

Recursiva

- Executadas por aplicações clientes.
- O servidor local não conhece a resposta.
- O servidor local corre por toda a árvore DNS para obter a resposta.

Não recursivas

- Executadas por servidores de nomes.
- As respostas geralmente são apenas referências para quem as possui.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"
- O servidor local pergunta para os servidores ROOT.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"
- O servidor local pergunta para os servidores ROOT.
  - A resposta é uma referência ao servidores de nome br.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"
- O servidor local pergunta para os servidores ROOT.
  - A resposta é uma referência ao servidores de nome br.
- O servidor local pergunta ao servidor de br.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"
- O servidor local pergunta para os servidores ROOT.
  - A resposta é uma referência ao servidores de nome br.
- O servidor local pergunta ao servidor de br.
  - A resposta é uma referência ao servidor de nome ufrj.br.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"
- O servidor local pergunta para os servidores ROOT.
  - A resposta é uma referência ao servidores de nome br.
- O servidor local pergunta ao servidor de br.
  - A resposta é uma referência ao servidor de nome ufrj.br.
- O servidor local pergunta ao servidor de ufrj.br.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"
- O servidor local pergunta para os servidores ROOT.
  - A resposta é uma referência ao servidores de nome br.
- O servidor local pergunta ao servidor de br.
  - A resposta é uma referência ao servidor de nome ufrj.br.
- O servidor local pergunta ao servidor de ufrj.br.
  - A resposta é uma referência ao servidor de nome dominio.ufrj.br.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"
- O servidor local pergunta para os servidores ROOT.
  - A resposta é uma referência ao servidores de nome br.
- O servidor local pergunta ao servidor de br.
  - A resposta é uma referência ao servidor de nome ufrj.br.
- O servidor local pergunta ao servidor de ufrj.br.
  - A resposta é uma referência ao servidor de nome dominio.ufrj.br.
- Finalmente, a pergunta é enviada ao servidor dominio.ufrj.br.

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"
- O servidor local pergunta para os servidores ROOT.
  - A resposta é uma referência ao servidores de nome br.
- O servidor local pergunta ao servidor de br.
  - A resposta é uma referência ao servidor de nome ufrj.br.
- O servidor local pergunta ao servidor de ufrj.br.
  - A resposta é uma referência ao servidor de nome dominio.ufrj.br.
- Finalmente, a pergunta é enviada ao servidor dominio.ufrj.br.
  - A resposta é o endereço IP de www.dominio.ufrj.br

Como funciona a resolução

- Ao apontar seu navegador para www.dominio.ufrj.br.
- Uma pergunta recursiva é enviada ao servidor de nomes local.
  - "Qual é o IP de www.dominio.ufrj.br?"
- O servidor local pergunta para os servidores ROOT.
  - A resposta é uma referência ao servidores de nome br.
- O servidor local pergunta ao servidor de br.
  - A resposta é uma referência ao servidor de nome ufrj.br.
- O servidor local pergunta ao servidor de ufrj.br.
  - A resposta é uma referência ao servidor de nome dominio.ufrj.br.
- Finalmente, a pergunta é enviada ao servidor dominio.ufrj.br.
  - A resposta é o endereço IP de www.dominio.ufrj.br
- O servidor local responde ao seu navegador.

Resource Records (RRs)

- Toda informação é armazenada na forma de *resource records*.
- Lista completa

  `http://www.iana.org/assignments/dns-parameters`

Registros importantes (Obrigatórios)

- SOA ("Start of Authority")
- NS (Name Server)

Resource Records (RRs)

Registros comuns

- A (Address)
- PTR (Pointer)
- CNAME (“Canonical Name”)
- MX (“Mail eXchange”)

Tipos de Servidores de nome

Primário

- Deve existir apenas 1.
- Também conhecido como “master”.
- É quem possui a cópia inicial da zona.

Tipos de Servidores de nome

Primário

- Deve existir apenas 1.
- Também conhecido como “master”.
- É quem possui a cópia inicial da zona.

Secundário

- Também conhecido como “slave”.
- Copia a zona do servidor primário (transferência de zona).
- Utiliza o registro SOA para ter conhecimento das alterações.

Tipos de Servidores de nome

Cache

- Não armazenam uma zona.
- Apenas armazena todas as respostas para perguntas por ele realizadas.
- Melhora a performance da rede local.

Informações de rede

- Servidores de nome escutam as portas.
  - 53/udp
    - ★ Perguntas ao servidor.
    - ★ Respostas do servidor.
  - 53/tcp
    - ★ Usado para transferências de zonas entre servidores.
    - ★ Respostas longas podem utilizar tcp.

Arquivo de zona (bind)

- São lidas pelos servidores de nomes.
- A maioria das entradas são RRs.
- $TTL deve ser a primeira diretiva.
- SOA deve ser a segunda diretiva.
- A ordem em que os RR ocorrem não importa (exceto SOA e $TTL).

Registros SOA

- Define:
  - Nome domínio (respostas com autoridade).
  - O servidor primário do domínio.
  - O contato para o domínio.
  - Número de série da zona.
  - Diversos tipos de 'time out', refresh, retry, expire, negative TTL.

Registros SOA (Continuação)

Exemplo:

```
@ IN SOA ns.dominio.ufrj.br. admin.dominio.ufrj.br. (
   20010421       ; Serial Number
      86400       ; Refresh - every 24 hours
       1800       ; Retry   - 30 minutes
    1209600       ; Expire  - 2 weeks
       7200 )     ; Negative answers - 2 hours
```

Exemplo de zona

```
$TTL 7200
@ IN SOA ns.dominio.ufrj.br. admin.dominio.ufrj.br. (
            20010421       ; Serial Number
               86400       ; Refresh - every 24 hours
                1800       ; Retry   - 30 minutes
             1209600       ; Expire  - 2 weeks
                7200 )     ; Negative answers - 2 hours

    IN      A      192.168.0.10
    IN      MX     10 mail.dominio.ufrj.br.
    IN      NS     ns.dominio.ufrj.br.
    IN      NS     ns2.dominio.ufrj.br.

localhost   IN     A      127.0.0.1

mail        IN     A      192.168.0.2
www         IN     A      192.168.0.3
ftp         IN     CNAME  www
```

BIND - Berkeley Internet Name Domain

- Servidor de nomes (named).
- Bibliotecas de resolução.
- Ferramentas para verificação de funcionamento.

/etc/named.conf

- Arquivo de configuração do named.

Configuração básica:

```
zone "dominio.ufrj.br" {
    type  master;  // ou slave
    file  "caminho/para/arquivo/zona";
};

zone "0.168.192.in-addr.arpa" {
    type  master;  // ou slave
    file  "caminho/para/arquivo/zona";
    masters {
        192.168.0.1;   //quando slave
    };
};
```

Ferramentas

- nslookup
- host
- dig
- sleuth
- dnsdoctor

1 DNS

2 LDAP

3 Correio
- Postfix
- Amavisd-new
- Spamassassin
- Clamav
- Greylisting
- SPF

O que é?

Banco de dados especializado e otimizado para:

- Ler
- Navegar
- Procurar

O que armazenar?

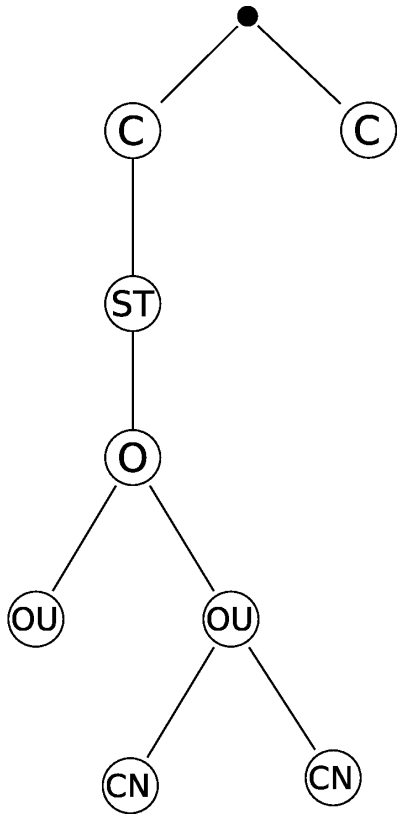
- Qualquer informação.
- Modelo baseado em entradas

Entrada

- Coleção de atributos.
- Possui um DN (único).
- Cada atributo possui: tipo e 1 ou mais valores.

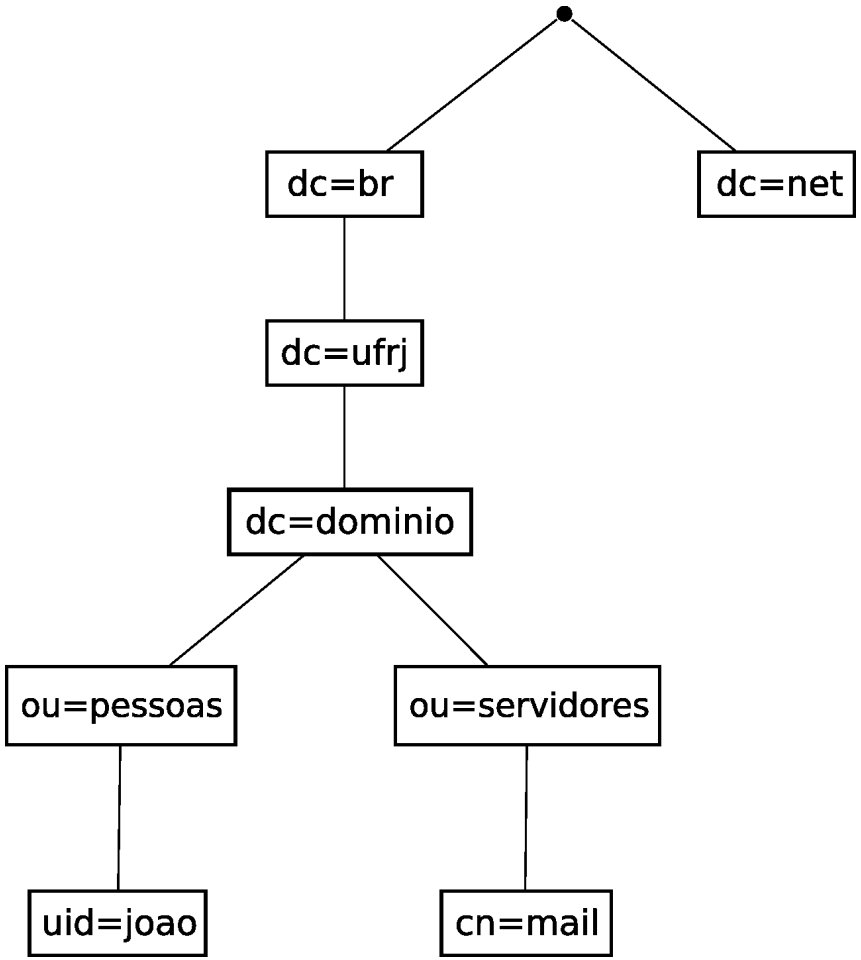
Organização

- Hierárquica.
- Projetado para ser distribuído.



Organização

Outro exemplo baseado em domínios:



Exemplo

EduPerson

- Iniciado pela Universidade de Wisconsin-Madison.
- Propõe uma lista de atributos e definições comuns instituições de ensino.

`http://www.educause.edu/`

Daemon

- slapd(8) - Daemon LDAP
  - 389/tcp
  - 636/tcp SSL
- slurpd(8) - Replicador

Instalação

```
apt-get install slapd

yum install openldap-servers

tar zxvf openldap-2.3.25.tgz
cd openldap-2.3.25
./configure
make
make install
```

Configuração

- slapd.conf(5)

/etc/ldap/slapd.conf

```
#Esquemas
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
schemacheck     on
```

Configuração (continuação)

```
pidfile         /var/run/slapd/slapd.pid
argsfile        /var/run/slapd.args
loglevel        0
allow bind_v2
modulepath      /usr/lib/ldap
moduleload      back_bdb
backend         bdb
database        bdb
suffix          "dc=dominio,dc=ufrj,dc=br"
rootdn          "cn=admin,dc=dominio,dc=ufrj,dc=br"
# Via slappasswd
rootpw          {SSHA}/fDalYsnPaoYqUktk83ed6JhWNNyMizW
```

Configuração (continuação)

```
directory       "/var/lib/ldap"
index           objectClass eq
lastmod         on
#ACLs
access to attrs=userPassword
        by dn="cn=admin,dc=dominio,dc=ufrj,dc=br" write
        by anonymous auth
        by self write
        by * none
access to dn.base="" by * read
access to *
        by dn="cn=admin,dc=dominio,dc=ufrj,dc=br" write
        by * read
```

Configuração - Inicializando a base

dominio.ldif

```
dn: dc=dominio,dc=ufrj,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
o: dominio
dc: dominio

dn: cn=admin,dc=dominio,dc=ufrj,dc=br
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword: {CRYPT}XKONnF5xArZ/s
```

Ferramentas

- ldapsearch(1)
- ldapadd(1)
- ldapmodify(1)
- ldapdelete(1)
- phpldapadmin
- Outras

Ferramentas - ldapsearch (1)

Sintaxe

```
ldapsearch -x -W -D "bindDN" -b "base" filtro
```

Base

A partir de que nó da árvore deseja buscar

```
"ou=pessoas,dc=dominio,dc=ufrj,dc=br"
```

Filtro

Qualquer coleção de atributos.

Ferramentas - ldapadd(1)

Sintaxe

```
ldapadd -x -W -D "bindDN" -f arquivo.ldif
```

Arquivo ldif

Depende de qual o tipo de objeto.

Ferramentas - ldapadd(1) (continuação)

Contas de usuário UNIX:

```
dn: cn=Nome do Usuario,ou=pessoas,dc=dominio,dc=ufrj,dc=br
cn: Nome do Usuario
objectClass: posixAccount
objectClass: shadowAccount
objectClass: inetOrgPerson
givenName: Nome
sn: do Usuario
uid: user
uidNumber: 1000
gidNumber: 5001
homeDirectory: /home/user
loginShell: /bin/bash
```

Ferramentas - ldapmodify(1)

Sintaxe

```
ldapmodify -x -W -D "bindDN" -f arquivo.ldif
```

Exemplo:

```
ldapsearch -x -W -D "bindDN" -b "base" filtro > arquivo.ldif
```

- Alterar o conteúdo de arquivo.ldif, e submeter a alteração.
- Cuidados:
  - Não alterar cn.
  - Não alterar dn.

Ferramentas - ldapdelete(1)

Sintaxe

```
ldadelete -x -W -D "bindDN" DN
```

Observação

-r Deleta uma entrada recursivamente

Ferramentas - phpldapadmin

- Gerenciamento via web.
- Cópia e deleção de objetos (recursiva).
- Diversidade de templates.
- `phpldapadmin.sourceforge.net`

Ferramentas - Outras

- Luma

  `http://luma.sourceforge.net`
- GOsa

  `http://gosa.gonicus.de/`

Linux como Cliente LDAP

- Informação de usuários:

  `libnss_ldap`
- Autenticação de usuários:

  `libpam_ldap`

libnss_ldap

/etc/libnss-ldap.conf ou /etc/ldap/ldap.conf

```
host 127.0.0.1
base dc=dominio,dc=ufrj,dc=br
ldap_version 3
```

libnss_ldap

/etc/libnss-ldap.conf ou /etc/ldap/ldap.conf

```
host 127.0.0.1
base dc=dominio,dc=ufrj,dc=br
ldap_version 3
```

/etc/ldap.conf

```
BASE    dc=dominio,dc=ufrj,dc=br
URI     ldap://localhost
```

libnss_ldap

/etc/libnss-ldap.conf ou /etc/ldap/ldap.conf

```
host 127.0.0.1
base dc=dominio,dc=ufrj,dc=br
ldap_version 3
```

/etc/ldap.conf

```
BASE    dc=dominio,dc=ufrj,dc=br
URI     ldap://localhost
```

/etc/nsswitch.conf

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
```

libpam_ldap

/etc/pam_ldap.conf

```
host 127.0.0.1
base dc=dominio,dc=ufrj,dc=br
ldap_version 3
rootbinddn cn=admin,dc=dominio,dc=ufrj,dc=br
pam_password md5
```

libpam_ldap

/etc/pam_ldap.conf

```
host 127.0.0.1
base dc=dominio,dc=ufrj,dc=br
ldap_version 3
rootbinddn cn=admin,dc=dominio,dc=ufrj,dc=br
pam_password md5
```

/etc/pam_ldap.secret

```
senha_do_rootdn
```

libpam_ldap (continuação)

/etc/pam.d/common-account

```
account sufficient      pam_ldap.so
account required        pam_unix.so
```

libpam_ldap (continuação)

/etc/pam.d/common-account

```
account sufficient      pam_ldap.so
account required        pam_unix.so
```

/etc/pam.d/common-auth

```
auth    sufficient    pam_ldap.so
auth    required      pam_unix.so nullok_secure use_first_pass
```

libpam_ldap (continuação)

/etc/pam.d/common-account

```
account sufficient      pam_ldap.so
account required        pam_unix.so
```

/etc/pam.d/common-auth

```
auth    sufficient    pam_ldap.so
auth    required      pam_unix.so nullok_secure use_first_pass
```

/etc/pam.d/common-password

```
password    sufficient  pam_ldap.so
password    required    pam_unix.so nullok obscure min=4 max=8 md5
```

Referências

- RedBooks IBM: http://www.redbooks.ibm.com/
  - Understanding LDAP Design and Implementation
  - TCP/IP Tutorial and Technical Overview (Cap. 8.4)
- LDP: Linux Documentation Project

1 DNS

2 LDAP

3 Correio
- Postfix
- Amavisd-new
- Spamassassin
- Clamav
- Greylisting
- SPF

SMTP (Simple Mail Transfer Protocol)

- Definido na RFC 821 em 1982
- Atualizado em 2001 pela RFC 2821
- Protocolo simples, baseado em texto.
- Utiliza 25/tcp
- Serviço de **entrega** de mensagens (**não resgata**)
- Não foi projetado pensando em segurança

Exemplo de comunicação

S: Servidor C: Cliente

```
S: 220 mail.dominio.ufrj.br ESMTP Postfix
C: HELO exemplo.com.br
S: 250 Hello smtp.exemplo.com.br
C: MAIL FROM:<remetente@exemplo.com.br>
S: 250 Ok
C: RCPT TO:<contato@dominio.ufrj.br>
S: 250 Ok
C: DATA
S: 354 End data with <CR><LF>.<CR><LF>
C: Subject: Mensagem teste
C: From: remetente@exemplo.com.br
C: To: contato@dominio.ufrj.br
C:
C: Ol^^e1,
C: Isto ^^e9 um teste.
C: At^^e9 logo.
C: .
S: 250 Ok: queued as 12345
C: QUIT
S: 221 Bye
```

Códigos de retorno

- 2xx
  - Sucesso
  - Pode proseguir
- 4xx
  - Erro temporário
  - Tente mais tarde
- 5xx
  - Erro fatal
  - Retorne o email ao remetente

Algumas definições

- MTA
  - Mail Transfer Agent
  - Exemplo: Postfix, sendmail, qmail
- MUA
  - Mail User Agent
  - Exemplo: Mozilla Thunderbird, Outlook, Eudora
- MDA
  - Mail Delivery Agent
  - Exemplo: Procmail, maildrop

1 DNS

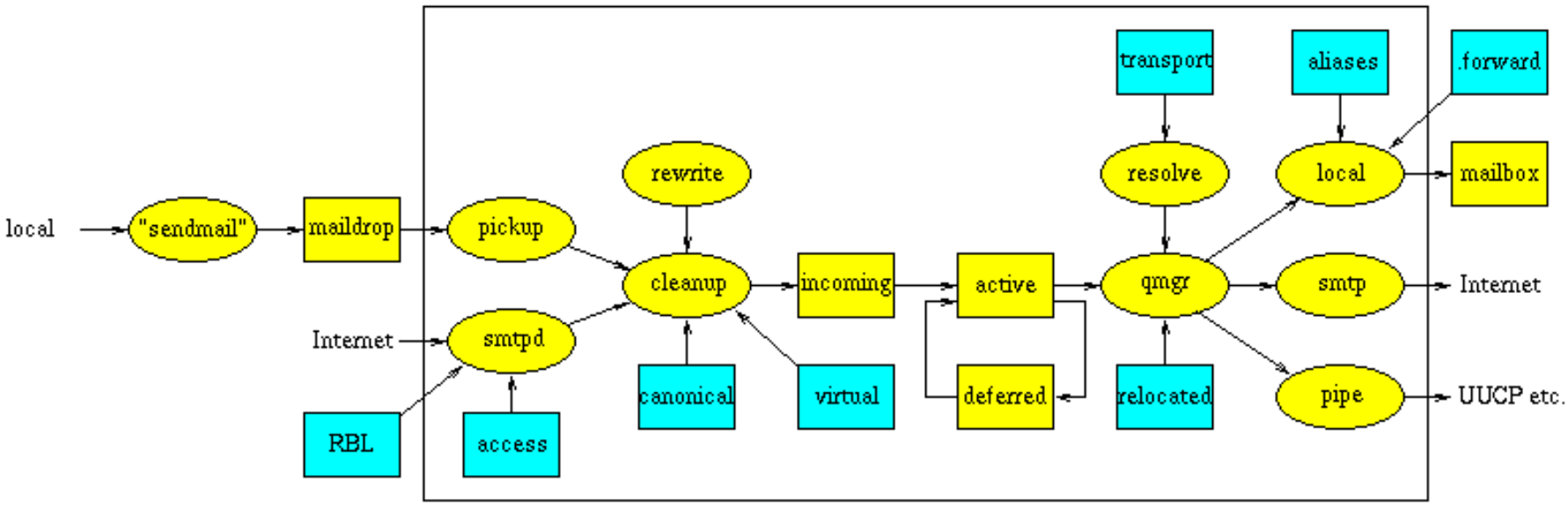
2 LDAP

3 Correio
- Postfix
- Amavisd-new
- Spamassassin
- Clamav
- Greylisting
- SPF

Introdução

- Projeto patrocinado pela IBM (IBM Secure Mailer)
- Alternativa ao Sendmail
- Propõe ser:
  - Seguro
  - Rápido
  - Modular
  - Fácil administração

Esquema


local
"sendmail"
maildrop
pickup
rewrite
cleanup
incoming
active
qmgr
transport
resolve
aliases
local
forward
mailbox
smtp
Internet
Internet
smtpd
canonical
virtual
deferred
relocated
pipe
UUCP etc.
RBL
access

Configuração Básica

/etc/postfix/main.cf

```
alias_database = hash:/etc/aliases
alias_maps = hash:/etc/aliases
config_directory = /etc/postfix
inet_interfaces = all
mydomain = dominio.ufrj.br
mydestination = $mydomain, localhost.localdomain, localhost
myhostname = mail.dominio.ufrj.br
mynetworks = 127.0.0.0/8, 192.168.0.0/24
myorigin = $mydomain
```

Restrições de entrega de mensagens

```
smtpd_helo_required = yes
disable_vrfy_command = yes
```

```
smtpd_client_restrictions = permit_mynetworks,
        permit_sasl_authenticated,
        check_client_access hash:/etc/postfix/access,
        reject_unknown_client,
        reject_rbl_client combined.njabl.org,
        reject_rbl_client sbl-xbl.spamhaus.org,
        reject_rbl_client bl.spamcop.net,
```

Restrições de entrega de mensagens (Continuação)

```
smtpd_helo_restrictions = permit_mynetworks,
     permit_sasl_authenticated,
     check_helo_access hash:/etc/postfix/helo_access,
     reject_invalid_hostname,
     reject_non_fqdn_hostname,
     reject_unknown_hostname,
```

```
smtpd_sender_restrictions = permit_mynetworks,
     permit_sasl_authenticated,
     check_sender_access hash:/etc/postfix/sender_access,
     reject_unknown_sender_domain,
     reject_non_fqdn_sender,
     reject_unauth_pipelining,
     reject_non_fqdn_sender,
```

Restrições de entrega de mensagens (Continuação)

```
smtpd_recipient_restrictions =
        check_recipient_access hash:/etc/postfix/access,
        permit_mynetworks,
        permit_sasl_authenticated,
        reject_non_fqdn_recipient,
        reject_unauth_pipelining,
        reject_unknown_recipient_domain,
        reject_unauth_destination,
```

1 DNS

2 LDAP

3 Correio
- Postfix
- Amavisd-new
- Spamassassin
- Clamav
- Greylisting
- SPF

Amavisd-new

- A MAil VIrus Scaner
- Interface entre o MTA e softwares antivírus e antispam
- Configuração simples (tudo pronto!)
- Detecta os módulos disponíveis na inicialização
- Muito versátil, suporta ldap, mysql, quarentena

Configuração

/etc/amavisd.conf (Editar as linhas)

```
$mydomain = 'dominio.ufrj.br';
$inet_socket_port = 10024
$final_virus_destiny      = D_DISCARD;
$final_banned_destiny     = D_BOUNCE;
$final_spam_destiny       = D_PASS;
$final_bad_header_destiny = D_PASS;

@av_scanners = (
...
### http://www.clamav.net/
['ClamAV-clamd',
  \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.ctl"],
  qr/\bOK$/, qr/\bFOUND$/,
  qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

Configuração do Postfix

/etc/master.cf

```
127.0.0.1:10025 inet n  -       n     -       -  smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o relay_recipient_maps=
    -o smtpd_restriction_classes=
    -o smtpd_client_restrictions=
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o mynetworks=127.0.0.0/8
    -o strict_rfc821_envelopes=yes
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
```

Configuração do Postfix (Continuação)

/etc/master.cf

```
smtp-amavis unix -      -       n       -       2  smtp
    -o lmtp_data_done_timeout=1200
    -o lmtp_send_xforward_command=yes
    -o disable_dns_lookups=yes
```

/etc/postfix/main.cf

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

1 DNS

2 LDAP

3 Correio
- Postfix
- Amavisd-new
- Spamassassin
- Clamav
- Greylisting
- SPF

Spamassassin

- Categorização de mensagens baseada no conteúdo (frases conhecidas)
- Testes de cabeçalho
- Aprendizagem através de usuários
- Filtros adaptativos (auto_whitelist)
- Configuração padrão funciona bem

1 DNS

2 LDAP

3 Correio
- Postfix
- Amavisd-new
- Spamassassin
- Clamav
- Greylisting
- SPF

Clamav

- Antivírus GPL
- Rápido e multi-threaded (escrito em C)
- Suporte a atualização de assinaturas de vírus (freshclam)
- Suporte a diversos tipos de arquivos compactados
- A configuração padrão funciona bem

1 DNS

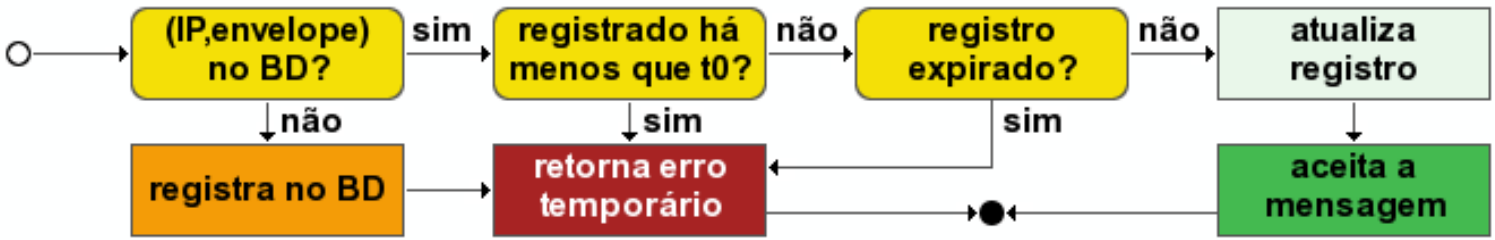
2 LDAP

3 Correio
- Postfix
- Amavisd-new
- Spamassassin
- Clamav
- Greylisting
- SPF

Greylisting

- Combate o envio de mensagens por mecanismos como vírus e *worms*.
- Basea-se na tríplice: **ip:remetente:destinatário**
- Consiste em recusar temporariamente uma mensagem e esperar por sua retransmissão
- Por que funciona?
  - e-mails válidos são enviados a partir de MTAs legítimos, que mantém filas e possuem políticas de retransmissão em caso de erros temporários;
  - spammers e códigos maliciosos raramente usam MTAs legítimos.
- Gera um atraso inicial na primeira comunicação.

Greylisting



1 DNS

2 LDAP

3 Correio
- Postfix
- Amavisd-new
- Spamassassin
- Clamav
- Greylisting
- SPF

SPF (Sender Policy Framework)

- Definido na RFC 4408
- Combate a falsificação de endereços de retorno de emails
- Define quais hosts podem enviar email para determinado domínio
- A publicação de registros SPF independem da checagem de SPF por parte do MTA do domínio
- Quebra o uso de redirecionamentos de emails (.forward)

Publicando a política SPF

```
dominio.ufrj.br. IN TXT  "v=spf1 a mx ip4:192.168.10.0/24 -all"
```

- Política
  - IP deve ser um RR tipo A do domínio dominio.ufrj.br (a);
  - MX do domínio dominio.ufrj.br (mx); ou
  - endereço IP pertencentes a rede 192.168.10.0/24 (ip4).
  - "-all" diz que devem ser recusados ("-", prefixo Fail) e-mails partindo de qualquer outro endereço IP (all).

Todo o mecanismo SPF está especificado em:
`http://new.openspf.org/RFC_4408`