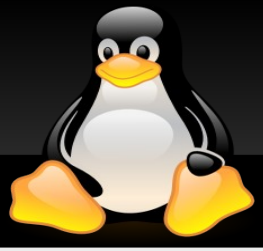
SERVIDORES LINUX



USANDO QUOTAS

- Limite de espaço que um usuário pode utilizar
- **quotas** tem "***hard limit***" e "***soft limit***"
  - O usuário pode exceder seu "*soft limit*" por um determinado período de tempo (grace time)
  - Um "*hard limit*" não pode ser ultrapassado
  - quota para blocos de dados
    - ***limita o espaço em disco para o usuário***
  - quota para inodes
    - ***limita o número de arquivos do usuário***

USANDO QUOTAS

- Instalação
  - **# apt-get install quota quotatool**
- Deve-se alterar arquivo /etc/fstab
  - Adicionar opção *usrquota* ou *grpquota* na partição
  - Exemplo:
    - /dev/hda6 /home auto defaults,usrquota,grpquota
- Depois deve-se remontar a partição ou reiniciar:
  - **# mount -o remount /home**

USANDO QUOTAS

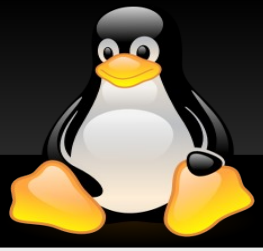
- Criar o arquivo de quotas vazio(na partição), com permissão de leitura e escrita apenas pelo root:
  - **# touch aquota.user**
  - **# chmod 600 aquota.user**
- Habilitando e desativando
  - **# quotaon -avug ou # /etc/init.d/quota start**
  - **# quotaoff -a ou # /etc/init.d/quota stop**
- Atualizar quotas(só deve ser feito com quotas desabilitadas)
  - **# quotacheck -avug**

USANDO QUOTAS

- Editando quotas para um usuário:
  - **# edquota -u mesquita**
- Após o comando acima, abre-se um vi para se editar as quotas,como abaixo:

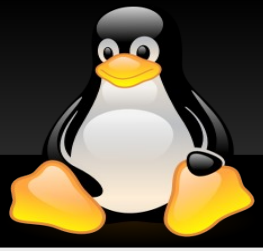
Disk quotas for user mesquita (uid 501):

Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/hda6	1024	0	0	12	0	0



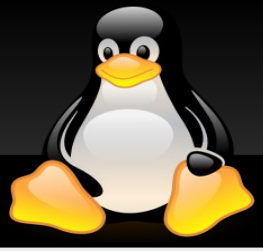
USANDO QUOTAS

- Parâmetros
  - **blocks**: espaço em KBytes ocupado pelos arquivos do usuário:
  - **inodes**: quantidade de arquivo atual do usuário.
  - **soft/hard**: os limites soft e hard do usuário para blocks e inodes.
- Configurando o grace time:
  - **# edquota -t**



USANDO QUOTAS

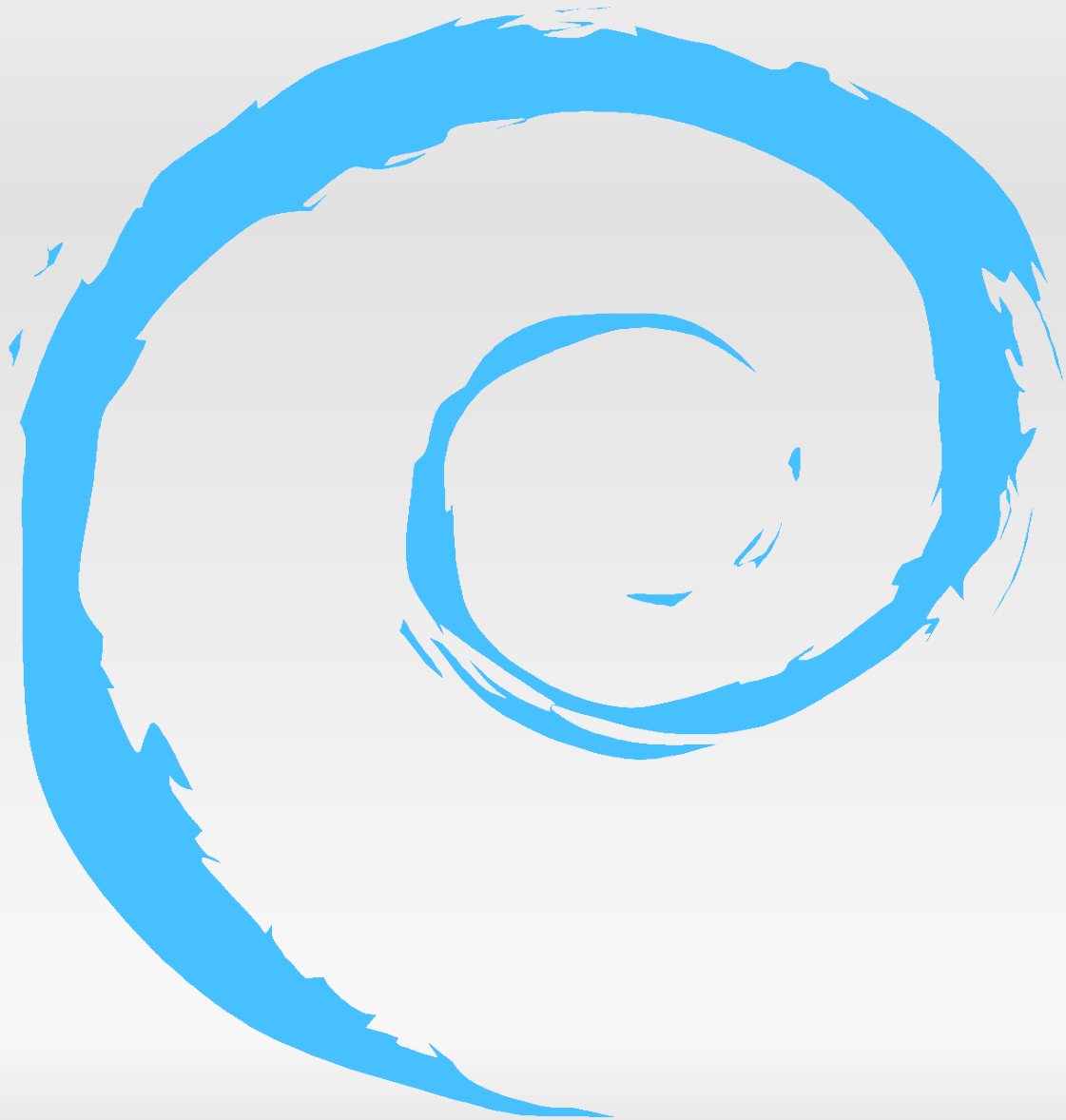
- Visualizando quotas
  - **# quota**
  - **# repquota -av**
- Copiando de um usuário para os outros
  - **# edquota -p user1 user2 user3**

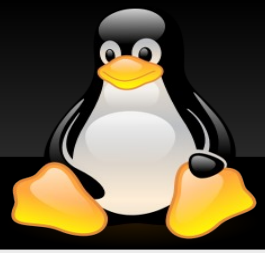


USANDO QUOTAS

- **Exercício**:
  - Criar uma partição /home no disco.
  - Criar 2 usuários na máquina.
  - Ativar quotas para a partição /home.
  - Definir 10MB de limite para um usuário .
  - Fazer o logon do usuário e verificar se o limite é respeitado.

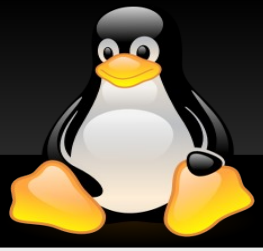
SERVIDORES LINUX





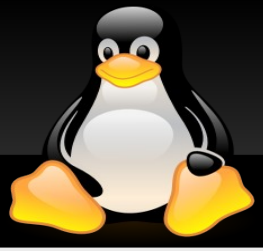
Servidor DHCP

- O servidor DHCP é aquele que tem por função fornecer a configuração de rede para um cliente da rede que solicita.
- A configuração básica fornece ao cliente os seguintes dados:
  - Endereço IP
  - Máscara de rede
  - Nome do domínio
  - Default gateway
  - Servidores DNS



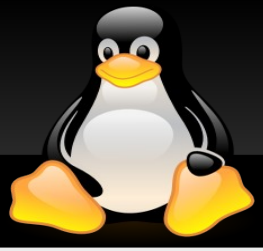
Servidor DHCP

- Outras informações fornecidas:
  - Tempo para solicitar renovação da configuração
  - Tempo máximo com aquela configuração
- **Instalação:**
  - ***# apt-get install dhcp3-server***
- **Arquivo de Configuração**
  - ***/etc/dhcp3/dhcpd.conf***



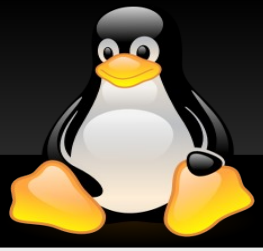
Exemplo dhcp.conf


```
subnet 192.168.0.0 netmask 255.255.255.0 {
        range 192.168.0.10 192.168.0.90;
        option routers 192.168.0.100;
        option subnet-mask 255.255.255.0;
        option domain-name “domain.org”;
        option domain-name-servers 192.168.0.1,
                192.168.0.2;
        default-lease-time 172800;
        max-lease-time 172800;
        }
```



Servidor DHCP

- Parâmetros de configuração:
  - **range:** faixa de valores Ips que será distribuído pelo servidor aos clientes.
  - **option routers:** IP do default gateway da rede(deve estar na mesma rede).
  - **option domain-name**: nome do domínio.
  - **option domain-name-servers**: IPs dos servidores de DNS separados por vírgula.
  - **option subnet-mask:** Máscara de sub-rede



Servidor DHCP

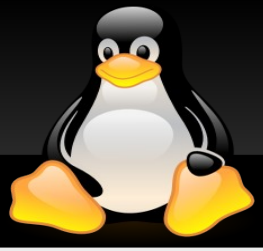
- Para configurar um endereço fixo para uma máquina, basta adicionar o seguinte:

```
host nome_maquina {
        hardware ethernet 00:ab:12:cd:34:ef;
        fixed address 192.168.0.99;
}
```

Arquivo dhcp.leases

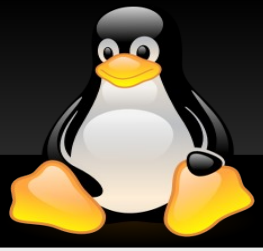
- Arquivo /var/lib/dhcp3/dhcpd.leases:
  - Guarda as informações sobre as máquinas que solicitaram configuração
  - Exemplo:

```
lease 192.168.0.20 {
        starts 4 2008/03/20 13:09:11;
        ends 4 2008/03/20 13:19:11;
        hardware ethernet 00:11:d8:08:20:dc;
}
```



Servidor DHCP

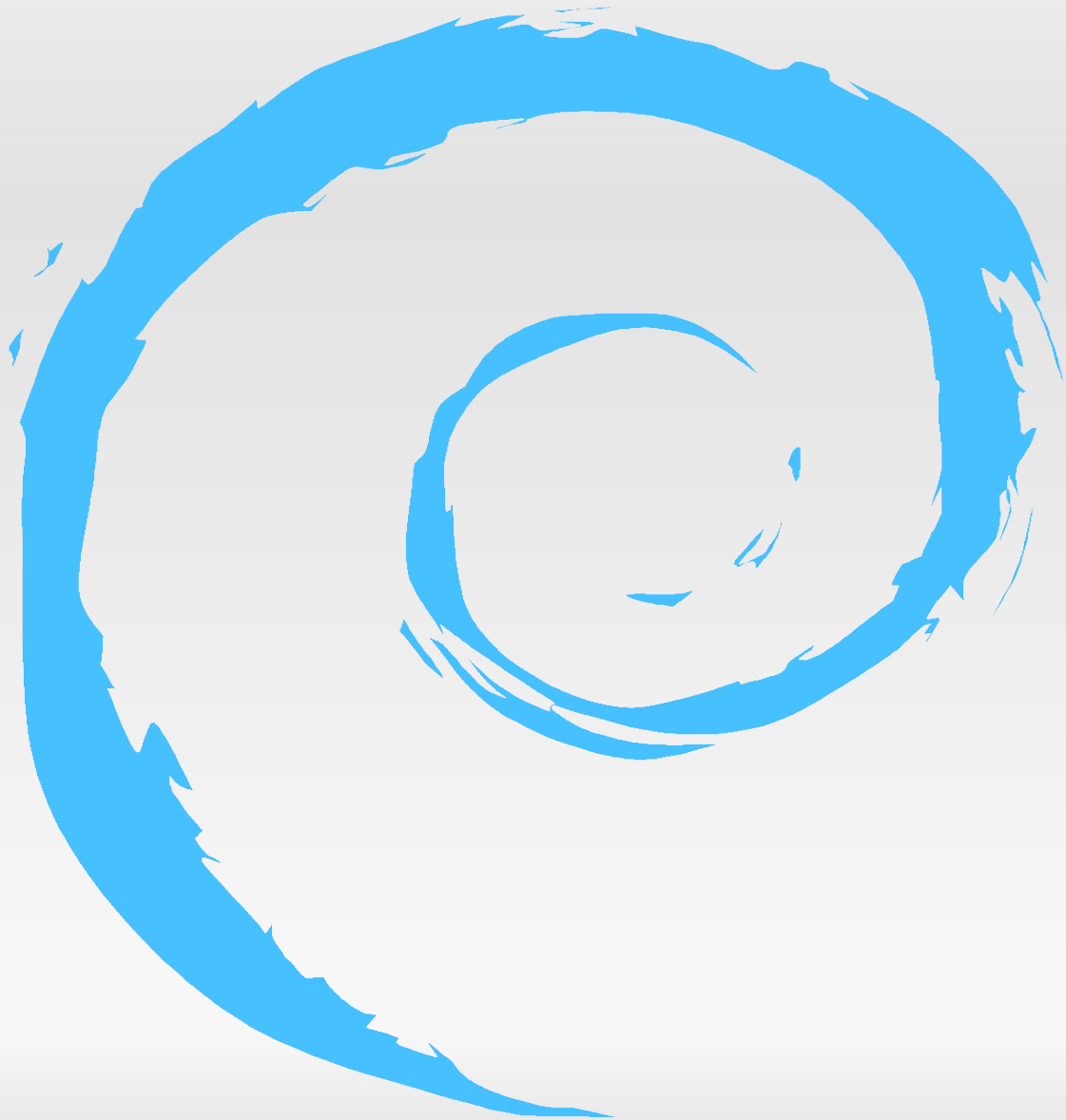
- **Cuidados** na configuração do arquivo dhcpd.conf.
  - Preste atenção às chaves e aos ponto-e-vígula e às aspas.
  - Verifique se o range está dentro da rede especificada.
  - Verifique se o default gateway está na mesma rede.
  - Verifique se está distribuindo ip na mesma rede.
  - Os erros citados acima são bastante comuns.
  - Verifique o arquivo de log, se na configuração houve erro, esse erro será indicado no log. Use o seguinte comando:
  - **# tail -30 /var/log/syslog**

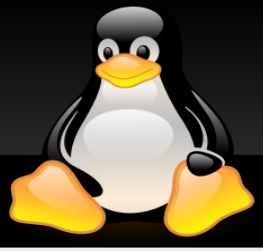


Servidor DHCP

- **Exercício**:
  - Criar um Servidor dhcp LOCAL.
  - Distribuir ip fixo através do Servidor dhcp.

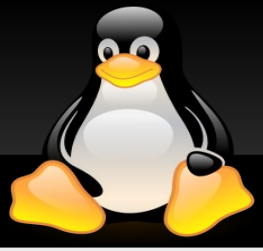
SERVIDORES LINUX





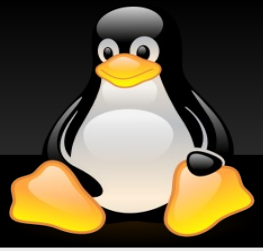
NAMED (BIND)

- **DNS**
  - Banco de dados distribuído e hierarquizado
  - Domínios
  - Nomes
  - Zonas
- Instalação:
  - ***# apt-get install bind9***



NAMED (BIND)

- **ARQUIVOS ASSOCIADOS AO DNS**
  - /etc/hosts
  - /etc/resolv.conf
  - /etc/nsswitch.conf
  - /etc/host.conf
  - /etc/bind/{*}
  - /var/named/{*}



NAMED (BIND)

- **COMPOSIÇÃO DA MENSAGEM DNS**
  - Cabeçalho
  - Pergunta
  - Resposta
  - Autoridade
  - Complementar

NAMED (BIND)

- Arquivo de configuração global : **/etc/bind/named.conf** ou **/etc/bind/bind.conf**
- Tipos de zonas
  - **master:** O próprio servidor é o responsável pela resolução dos endereços do domínio.
  - **slave:** O servidor faz o download do arquivo de zona do domínio de um servidor master.
  - **forward**: O servidor repassa a consulta para um outro servidor de nomes.
  - **hint:** Serve para especificar um conjunto de servidores raiz.
  - **stub:** O servidor mantém a lista de outros servidores com autoridade sobre domínios.

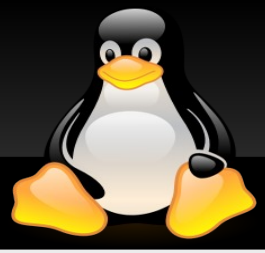
NAMED (BIND)

- **REGISTRO DE RECURSOS**
  - **Escopo:** O domínio ao qual o registro refere-se.
  - **TTL:** Tempo de vida dos registros armazenados em cache.
  - **Classe de operação**: Classes de recursos suportadas pelo Bind (IN – Internet; CH -Chaos; HS - Hesiod).
  - **Tipo de registro:** Refere-se aos registros suportados em da uma das classes (NS; SOA; PTR; A; CNAME).
  - **Valor:** O servidor mantém a lista de outros servidores com autoridade sobre domínios.

NAMED (BIND)

- Arquivo ***named.conf***

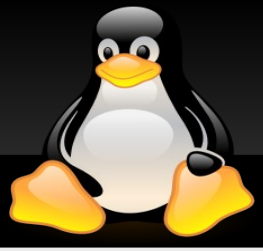
```
zone "." {
    type hint;
    file "/etc/bind/db.root";
}
zone "dominio.com.br" {
    type forward;
    forwarders { 192.168.4.12; };
};
```



NAMED (BIND)

- Arquivo ***named.conf***

```
zone "meudominio.com" {
    type master;
    file "meudominio.zone";
    allow-transfer { 192.168.4.14; };
}
zone "dominiodooutro.com" {
    type slave;
    file "dominiodooutro.com";
    masters { 192.168.4.12; };
};
```



NAMED (BIND)

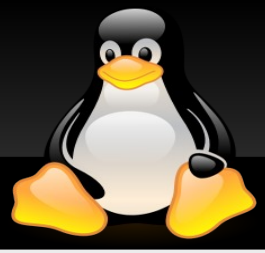
- Arquivo ***named.conf***

```
options {
    directory "/etc/bind";
    listen-on {192.168.2.1; 127.0.0.1;};
    allow-query { 192.168.2.0/24;};

    forwarders { 10.46.59.1;};
}
server 10.46.59.1 {
    minimal_responses yes;
    };
```

NAMED (BIND)

- Arquivo ***named.conf***

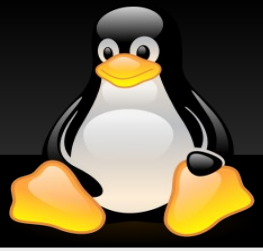
```
view "interno" {
    match-clients {192.168.2.0/24;}
    zone "meudominio"{
          type master;
          file "db.meudom";};

    zone "2.168.192.in-addr.arpa"{
          type master;
          file "db.2.168.192";
  };
```



NAMED (BIND)

- Arquivo ***named.conf***

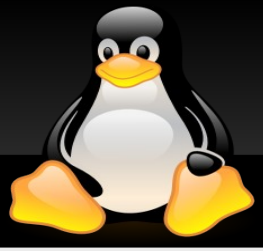
```
view "externo" {


    match-clients {any;};
    minimal_responses yes;
    zone "meudominio"{
            type master;
            file "db.meudom";};
  };
```



NAMED (BIND)

- Arquivo ***named.conf***

```
logging {
    channel "named_log";
    syslog local4;
    severity info;
  };

category "security" {
    "named_log";
    };
```



NAMED (BIND)

- Arquivo ***named.conf***

```
key rndc{
    // #dns-keygen -a hmac-md5 -b 512 -n
      "(user|host)" rndc
    algorithm hmac-md5;
    secret
      "l+FqrOfbs456USYHuGqsuYb7gpXLdf511XHyGD+om
      -M=";
    };
    controls {
          inet 127.0.0.1 allow {localhost;}
    keys {rndc};
    };
```

NAMED (BIND)

- Arquivo de configuração da zona:
  - Tipos de registros RR mais comuns
    - **A**: Indica o endereço IP de uma máquina.
    - **CNAME**: Indica um outro nome para a máquina.
    - **MX**: Indica um servidor de correio do domínio.
    - **NS**: Indica um servidor de nomes do domínio.
    - **SOA**: Indica a Autoridade pelo domínio.
- Pode-se se tomar como exemplo de arquivo de configuração de zona o arquivo /etc/bind/db.local. Basta fazer uma cópia:
  - **# cp db.local meudominio.zone**

NAMED (BIND)

- **Cuidados** na configuração do named.conf
  - Preste atenção às **chaves** que devem ser colocadas.
  - Preste atenção aos **pontos**, **pontos-e-vírgula** e às **aspas**.
  - Preste atenção ao nome dado ao arquivo de zona, esse deve ser o mesmo nome do arquivo a ser criado.
  - Os erros citados acima são bastante comuns.
  - Verifique o arquivo de log, se na configuração houve erro, esse erro será indicado no log. Use o seguinte comando:
    - ***# tail -30 /var/log/syslog***

NAMED (BIND)


```
$TTL    3600 ; default_ttl
@ IN SOA mercurio.5cta.eb.mil.br.
admin.5cta.eb.mil.br. (
2007052101 ; serial
8H ; refresh
4H ; retry
1000H ; expire
1D ; minimum_ttl
)
@ IN NS mercurio.5cta.eb.mil.br.
mercurio IN A 10.45.1.1
apolo IN A 10.45.1.2
mail IN CNAME mercurio.5cta.eb.mil.br.
```

NAMED (BIND)

- Ferramentas de análise do Servidor Bind:
  - named-checkconf
  - named-checkzone
  - host => ping => traceroute
  - nslookup => dig
  - ndc (8.0) => rndc (9.0)
  - dns-keygen
  - nsupdate

NAMED (BIND)

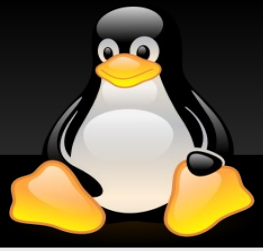
- Ferramenta de análise: host
  - host (Ferramenta de Resolução de Nome/IP)
  - Uso: host {nome consultado} {servidor de pesquisa}
  -
  - # host www.uol.com.br 10.45.1.60
  - # host 200.198.249.120 10.45.1.60
  -
  - # man host

NAMED (BIND)

- Ferramenta de análise: ping
  - ping (Ferramenta de verificação de conectividade)
  - # ping -c 5 10.45.1.60
  - # ping -a mail.5cta.eb.mil.br
- Ferramenta de análise: traceroute
  - traceroute (Ferramenta de verificação de conectividade)
  -
  - # traceroute www.registro.br

NAMED (BIND)

- Ferramenta de análise: named-checkconf
  - named-checkconf (Ferramenta de verificação da configuração do arquivo named.conf)
  - # named-checkconf /etc/bind/named.conf
  -
- Ferramenta de análise: named-checkzone
  - named-checkzone (Ferramenta de verificação da configuração do arquivo de zonas do dns)
  -
  - # named-checkconf meudominio /etc/bind/db.dom



NAMED (BIND)

- Ferramenta de análise: nslookup
  - nslookup (Ferramenta de Resolução de Nome/IP)
  - Uso: nslookup {nome consultado} {servidor de pesquisa}
  -
  - # nslookup www.uol.com.br (não-interativo)
  - # man nslookup

NAMED (BIND)

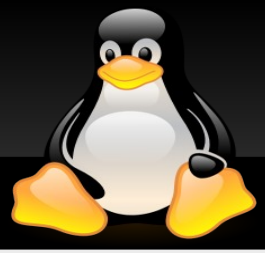
- Ferramenta de análise: nslookup (modo interativo)
  - nslookup> set type=any
  - nslookup> set type=ns
  - nslookup> set type=a
  - nslookup> set type=mx
  - nslookup> 5cta.eb.mil.br
  - nslookup> set domain=cmne.eb.mil.br
  - # man nslookup

NAMED (BIND)

- Ferramenta de análise: nslookup (modo interativo)
  - nslookup> server 10.47.24.7
  - nslookup> set type=ns
  - nslookup> cmne.eb.mil.br
  - nslookup> set type=any
  - nslookup> 5cta.eb.mil.br
  - nslookup> server 10.45.1.60
  - nslookup> set all
  - # man nslookup

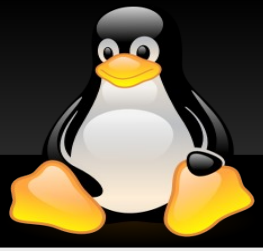
NAMED (BIND)

- Ferramenta de análise: dig [domain information groper]
  - dig (ferramenta flexível de resolução/conectividade)
  - Uso: dig [@server] [-c class] [-b address] [-f filename] [-k filename] [-p port] [-q name] [-t type] [-x addr] [-y [hmac]: name:key] [-4] [-6] name
  - # dig -x protweb.cmne.eb.mil.br
  - # dig @10.47.24.2 www.uol.com.br
  - # dig -x 200.176.2.173
  - # dig ns terra.com.br
  - # man dig



NAMED (BIND)

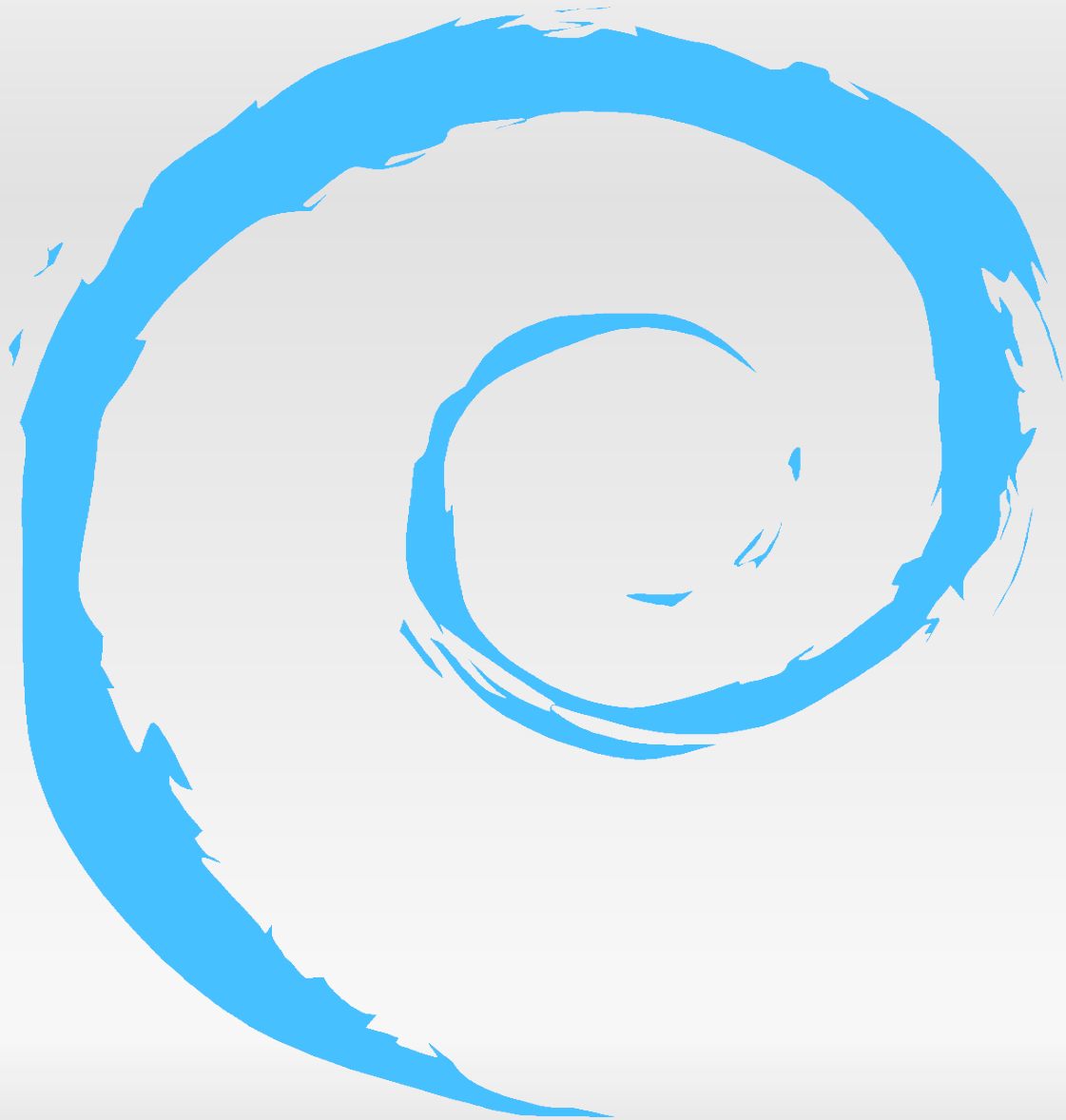
- **Cuidados** na configuração do arquivos das zonas.
  - Preste atenção ao ponto que deve ser colocado ao final do nome do domínio.
  - Não deixe um nome sem um IP correspondente.
  - Os erros citados acima são bastante comuns.
  - Verifique o arquivo de log, se na configuração houve erro, esse erro será indicado no log. Use o seguinte comando:
    - **# tail -30 /var/log/syslog**



USANDO DNS

- **Exercício**:
  - Criar um um arquivo customizado de domínio.
  - Incluir uma entrada de correio no arquivo.
  - Testar a resolução local e remota do domínio. respeitado.

SERVIDORES LINUX



Apache HTTP

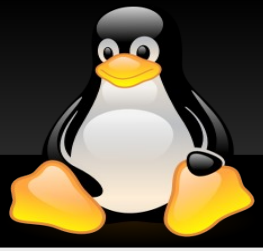
- Servidor poderoso, flexível, usado por milhões de servidores da Internet.
- Altamente configurável e extensível com módulos desenvolvidos por terceiros
- Possui código aberto e licença sem restrições.
- Roda em Windows, Netware, OS/2, Unix, e vários outros sistemas.
- Está constantemente sendo desenvolvido e aprimorado.

Apache HTTP

- Possui 2 versões em desenvolvimento.
  - Apache 1.3.x
  - Apache 2.x
- Instalação:
  - **#apt-get install apache**
  - **#apt-get install apache2**
- Arquivo de configuração principal:
  - **/etc/apache2/apache2.conf**

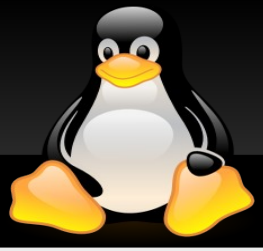
Apache HTTP

- Instala a seguinte estrutura de diretórios e arquivos:
  - /var/www/apache2-default (instalação de sites)
  - /etc/apache2 (configuração dos sites instalados)
- /etc/apache2:
  - **apache2.conf httpd.conf sites-enabled sites-available mods-available mods-enabled ports.conf envvars**
- Arquivo de configuração principal:
  - **/etc/apache2/apache2.conf**



Apache HTTP

- **Pincipais parâmetros de configuração:**
  - **DocumentRoot:** Indica o diretório raiz do apache
    - /var/www
    - Equivalente ao http://localhost/
  - **ServerRoot:** indica o local dos arquivos de configuração:
  - **User:** Usuário que o apache será executado.
  - **Group:** Grupo que o apache será executado.

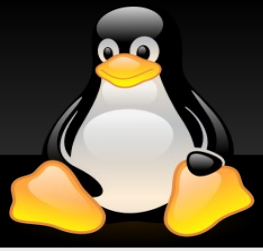


Apache HTTP

- **Pincipais parâmetros de configuração:**
  - **DirectoryIndex:** Indica nomes de arquivos que o apache procurará no diretório se o arquivo solicitado pelo usuário não for especificado.
  - **AcessFileName:** Nome do arquivo de controle de acesso ao diretório.
  - **AllowOverride**: usando para desabilitar o arquivo de controle de acesso.

Apache HTTP

- **Diretório /etc/apache2/sites-available:**
  - É um diretório onde deve ser criado um arquivo para cada *Virtual Host*(site) hospedado no servidor.
- **Diretório /etc/apache2/sites-enable:**
  - É um diretório onde devem ser criados links simbólicos para os arquivos do diretório ***sites-available***.
  - A existência do *link* indica que o site está disponível.



Apache HTTP

- Proteção do diretório no Apache
- Necessita do parâmetro AllowOverride All (é o padrão).
- Proteção baseada em IP
  - Arquivo ***.htaccess***

```
Deny from all
Allow from 127.0.0.1/32 10.45.0.0/16
```

Apache HTTP

- Proteção baseada em usuário:
  - Criação de um arquivo de senhas:

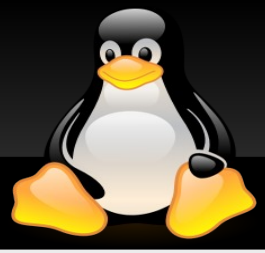
```
# htpasswd -c /etc/apache2/passwords usuario
```

  - Inclusão ou alteração no arquivo de senhas:

```
# htpasswd /etc/apache2/passwords usuario
```

  - Arquivo ***.htaccess***:

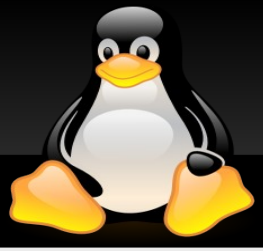
```
AuthType Basic
AuthName "Servidor Web"
AuthUserFile /etc/apache2/passwords
Require user usuario
```



Apache HTTP

- Arquivo ***.htaccess***:
  - Para permitir **qualquer usuário válido**:

```
AuthType Basic
AuthName "nome"
AuthUserFile /etc/apache2/passwords
Require valid-user
```



Apache HTTP

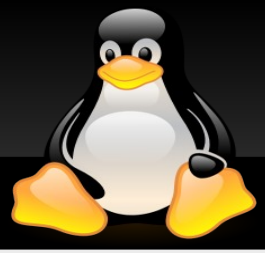
- **Pincipais comandos de configuração:**
  - { a2ensite, a2dissite, a2enmod, a2dismod }
  - a2dissite default
  - a2ensite intranet
  - a2enmod cgi php5 alias
  - a2enmod perl ssl dir
  - a2enmod proxy

Apache HTTP

- **Domínios virtuais**
  - Crie um arquivo dentro do diretório /etc/apache2/sites-available/ com o seguinte conteúdo:

```
<VirtualHost *>
ServerName intranet.dominio.com
DocumentRoot /var/www/intranet
</VirtualHost>
```

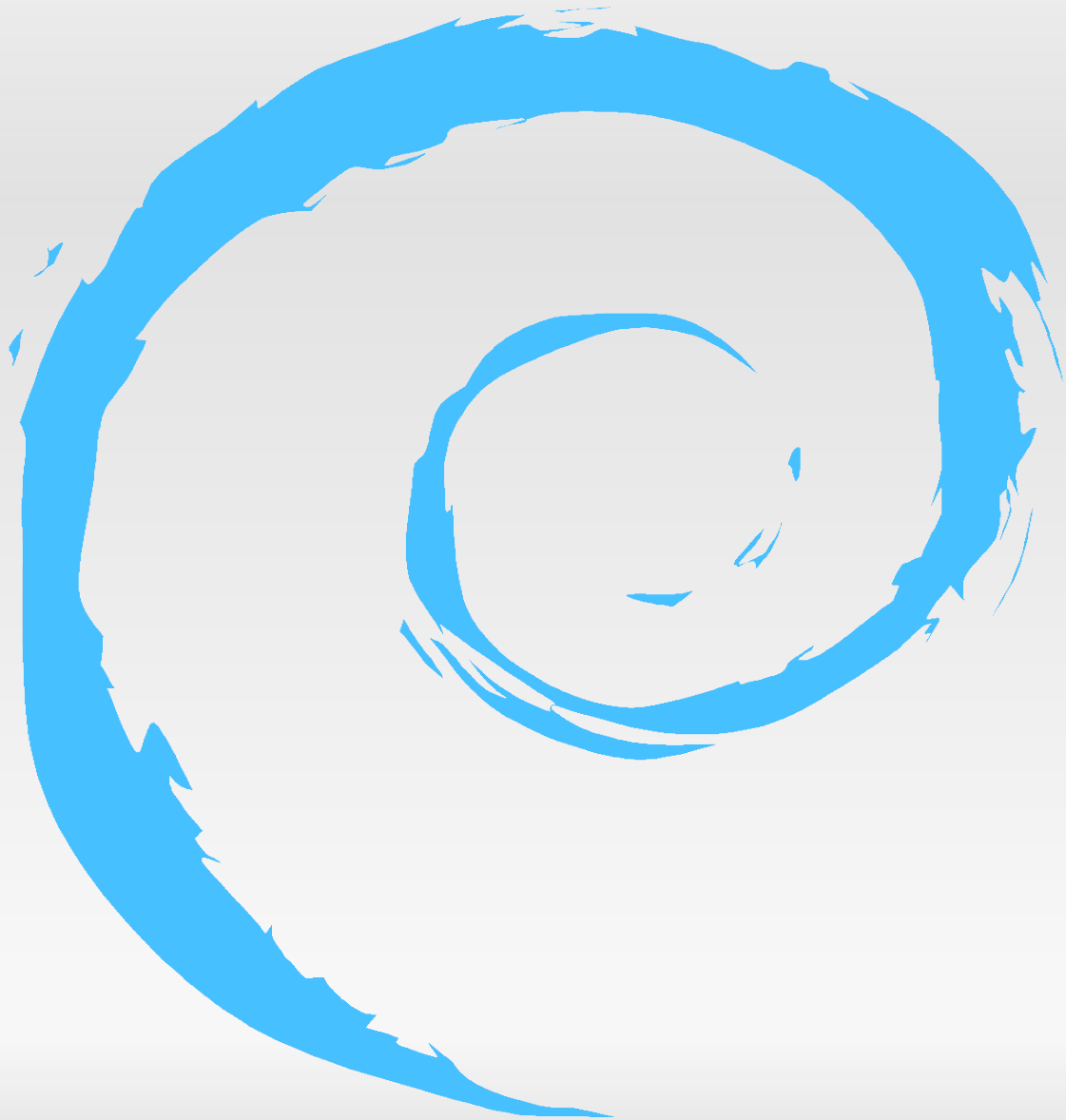
  - Crie um link simbólico dentro do diretório /etc/apache2/sites-enable/ apontando para o arquivo criado no passo anterior:
  - a2ensite intranet

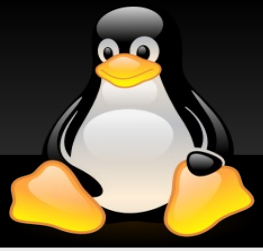


Apache HTTP

- **Exercício:**
  - Colocar o Apache no ar.
  - Configurar proteção de diretório baseada em usuário.
  - Configurar 2 entradas no servidor DNS para a máquina para dois sites fictícios.
  - Configurar 2 domínios virtuais no apache para os dois sites fictícios

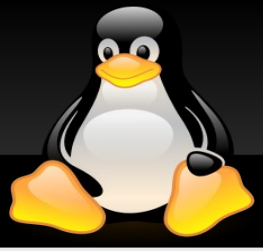
SERVIDORES LINUX





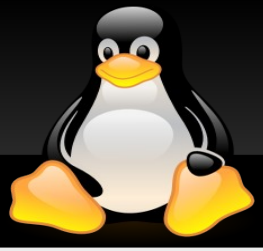
Banco de Dados

- **PostgreSQL**
  - http://www.postgresql.org/
- **MySQL**
  - http://www.mysql.com/



MySQL

- Características
  - Bom desempenho
  - Baixo custo
    - GPL ou licença comercial
  - Portabilidade
  - Acesso ao código fonte
  - Facilidade de uso
- Página oficial: http://www.mysql.com/

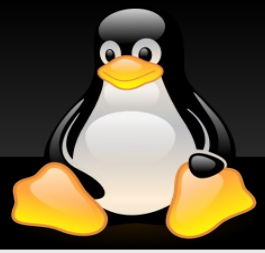


MySQL

- Linux
  - Instalação:
    - **# apt-get install mysql-client-5.0**
    - **# apt-get install mysql-server-5.0**
- Windows
  - Instalador

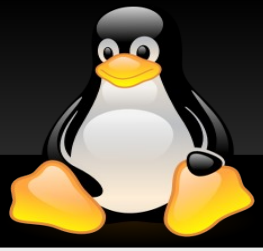
MySQL

- Iniciar/Parar/Reiniciar:
  - **# /etc/init.d/mysql {start/stop/restart}**
- Principais comandos
  - **mysql**
    - Cliente do mysql
  - **mysqladmin**
    - Para procedimentos administrativos (create database, drop database, shutdown, etc)



MySQL

- Principais comandos:
  - **mysqlshow**
    - Mostra a estrutura de uma base
  - **mysqldump**
    - Gera um dump das tabelas e/ou dados
    - Possibilita o backup
  - **mysqlimport**
    - Faz o restore de um backup



MySQL

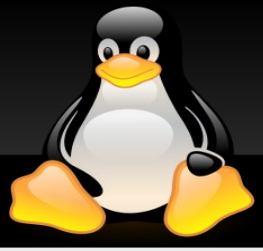
- Dois banco de dados
  - **mysql**
    - columns_priv
    - db
    - host
    - tables_priv
    - user
  - **information_schema**

MySQL

- Tabela ***user***
  - Nome do usuário
  - senha
  - Host (autorizado para a conexão)
  - Privilégios globais (todos os bancos de dados)
- Tabelas ***db*** e ***host***
  - Privilégios para os bancos de dados
- Tabelas ***columns_priv*** e ***tables_priv***
  - Privilégios de linha e coluna

MySQL

- Tipos básicos de colunas:
  - Numérico
  - data/hora
  - String
- Numérico
  - Inteiro ou float
- Inteiro
  - TINYINT(1), SMALLINT(2), MEDIUMINT(3), INT(4), BIGINT(8)



MySQL

- **String**
  - CHAR/VARCHAR
  - TEXT/BLOB
  - ENUM/SET

MySQL

- Data/hora
  - DATE
  - TIME
  - DATETIME
    - De 1000-01-01 00:00:00 até 9999-12-31 23:59:59
  - TIMESTAMP
    - A partir de 1970-01-01
    - Até o ano 2037

MySQL

- Acesso padrão
  - Usuário root / sem senha
- Acessando o banco
  - #mysql mysql
  - #mysql -h hostname -u root -p
  - #mysql>
    - #show databases;
    - #use <database>;
    - #show tables;
    - #desc <table>;
    - #select * from <table>;

MySQL

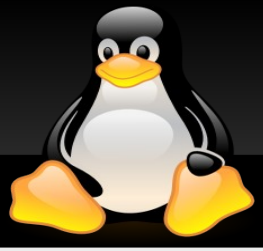
- Mudando a senha padrão do root
  - # mysqladmin -uroot password 'senhasecreta'
- Criando a base de dados:
  - #mysql mysql -p
  - mysql> show databases;
  - mysql> create database curso_linux;
    - mysql> show databases;
    - mysql> create database teste;
    - mysql> show databases;
    - mysql> rename database teste to ultimo_teste;
    - mysql> drop database ultimo_teste;

MySQL

- Acessado uma base de dados específica:
  - # mysql mysql -uroot -p
- Criando tabelas na base de dados:
  - mysql> show databases;
  - mysql> use curso_linux;
  - mysql> grant all privileges on curso_linux.* to usuario@'localhost' identified by 'senhapropria';
    - mysql> show databases;

MySQL

- Acessado uma base de dados específica:
  - # mysql -uusuario -p
- Criando tabelas na base de dados:
  - Mysql> use curso_linux;
  - mysql> create table alunos(nome varchar(20), email varchar(20), data date);
  - mysql> show tables;
  - mysql> desc alunos;
  - Mysql> select * from alunos;



MySQL

- Inserindo dados numa tabela da base de dados:
- # mysql -uusuario -p
- mysql> use curso_linux;
- mysql> show tables;
- mysql> select * from alunos;
- mysql> insert into alunos values('aluno1', 'aluno1@5cta.eb.mil.br','2009-06-05');
- Mysql > select * from alunos;

MySQL

- Inserindo dados numa tabela da base de dados:
- # mysql -uusuario -p
- mysql> use curso_linux;
- mysql> select * from alunos;
- mysql> insert into alunos values('aluno2', 'aluno2@gmail.com','2009-06-05');
- mysql> insert into alunos values('aluno3', 'aluno3@bol.com','2009-06-05');
- mysql> select * from alunos;

MySQL

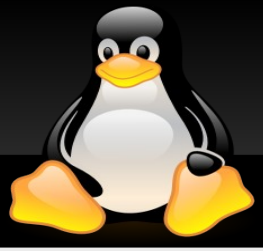
- Inserindo e atualizando dados numa tabela:
- # mysql -uusuario -p
- mysql> use curso_linux;
- mysql> select * from alunos;
- mysql> insert into alunos values('aluno4','aluno4@hotmail.com','2009-06-05');
- mysql> update alunos set email='aluno3@globo.com' where name='aluno3';
- mysql> select * from alunos;

MySQL

- Inserindo e deletando dados numa tabela:
- # mysql -uusuario -p
- mysql> use curso_linux;
- mysql> select * from alunos;
- mysql> insert into alunos values('alun4', 'aluno4@hotmail.com','2009-06-05');
- mysql> select * from alunos;
- mysql> delete from alunos where name='alun4';
- mysql> select * from alunos;

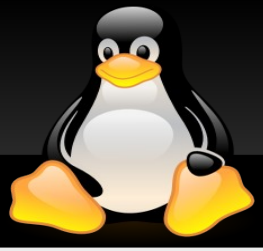
MySQL

- Consultando dados numa base mysql:
- mysql> use curso_linux;
- mysql> select * from alunos where name='aluno2';
- mysql> select * from alunos where name='aluno2';
- mysql> select * from alunos order by name;
- mysql> alter table alunos add column sexo varchar(1) after email;
- mysql> select * from alunos group by sexo;
- mysql> desc alunos;
- mysql> select * from alunos;



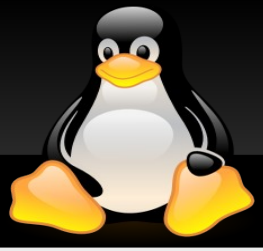
MySQL

- Modificando e protegendo dados numa base mysql:
- mysql> use curso_linux;
- mysql> create user gerente;
- mysql> grant all privileges on *.* to gerente@'localhost' identified by 'senhadogerente';
- mysql> flush privileges;



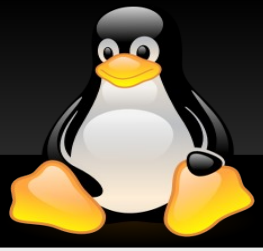
MySQL

- Segurança e proteção dos dados:
- mysql> lock table alunos read;
- # myisamchk -c *.MYI
- #myisamchk -r *.MYI
- #mysqldump curso_linux -u root -p > cursolinux.sql
- mysql> unlock tables;
- mysql> flush tables;
- #mysql -u gerente -p curso_linux < cursolinux.sql



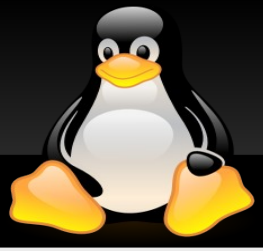
MySQL

- Modificando e protegendo dados numa base mysql:
- mysql> alter table alunos add column senha varchar(42) after sexo;
- mysql> insert into alunos values('aluna1','aluna1@bol.com.br','F','md5('senha')','2009-06-05');
- mysql> create user estagiario1;
- mysql> grant select on curso_linux.* to estagiario1@'localhost' identified by 'senha1';
- mysql> show grants for estagiario1@'localhost'';



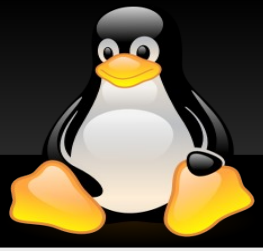
MySQL

- Modificando e protegendo dados numa base mysql:
- mysql> create user estagiario2;
- mysql> grant select on curso_linux.* to estagiario2@'%' identified by 'senha2';
- mysql> show grants for estagiario2@'%';
- mysql> flush privileges;
- mysql> revoke select on curso_linux.* from estagiario2@'%';
- mysql> flush privileges;



MySQL

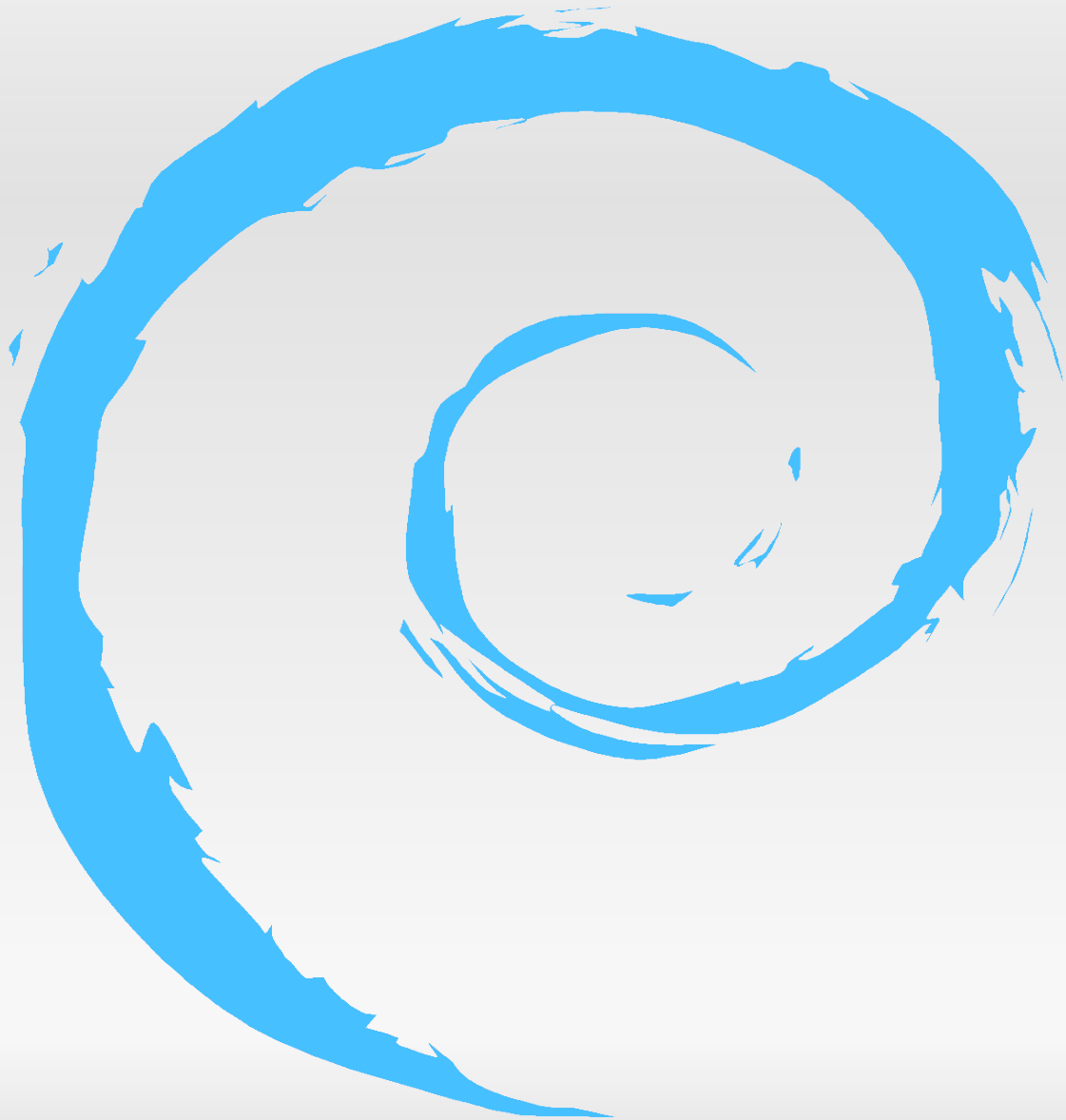
- Modificando e protegendo dados numa base mysql:
- mysql> revoke select on curso_linux.* from estagiario2@'%';
- mysql> set password for 'estagiario1' = password('novasenha');
- mysql> flush privileges;
- mysql> drop user 'estagiario2';



MySQL com phpMyAdmin

- Pacote de administração do MySQL via web
- Instalação:
  - **# apt-get install phpmyadmin**
- Site:
  - http://www.phpmyadmin.net
- Requisito: Servidor web no ar (apache) com suporte a PHP e MySQL
- Para acessar:
  - **http://localhost/phpmyadmin/**

SERVIDORES LINUX



Servidor SSH

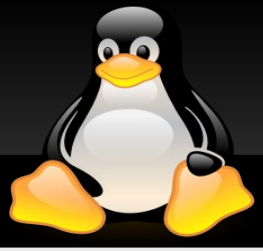
- O servidor ***ssh*** permite que o admistrador tenha acesso a um *shell* no servidor remotamente.
- Ele também permite a cópia de arquivos, através do comando ***scp***, que funciona de maneira semelhante ao ***cp***.
- Todo o tráfego entre o cliente e o servidor é criptografado.

Servidor SSH

- Instalar o OpenSSH-Server:
  - ***# apt-get install openssh-server***
  - ***# aptitude install openssh-server***
- Componentes do OpenSSH-Server:
  - ***{ sshd, ssh, scp, sftp, ssh-copy-id, ssh-keyscan, ssh-keygen, ssh-add, ssh-agent, keychain, ssh-vulnkey}***

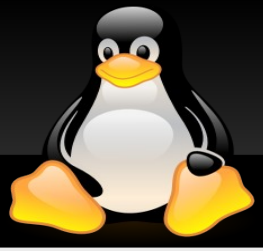
Servidor SSH

- FERRAMENTAS DE ADMINISTRAÇÃO:
- sshd: o servidor de shell seguro;
- ssh: o cliente para acesso remoto;
- scp: o cliente para tranferencia de dados criptografada;
- sftp: servidor seguro de ftp;
- Testando a configuração do Servidor:
- # sshd -t
- # ssh-keygen -t rsa -C “mailserver on 10.45.1.80”



Servidor SSH

- FERRAMENTAS DE MANIPULAÇÃO DE CHAVES:
- ssh-copy-id: programa utilizado para transferência segura de chave pública (*authorized_keys*);
- ssh-keyscan: programa para busca de chaves publicas compartilhadas na rede;
- ssh-keygen: programa gerador e administrador de chaves de autenticação DSA e RSA;
- ssh-vulnkey: programa criado para corrigir falhas em certificados gerados por versões inseguras do ssl.



Servidor SSH

- FERRAMENTAS DE AUTENTICAÇÃO:
- ssh-add: programa para adicionar identidades digitais ao chaveiro;
- ssh-agent: programa de gerenciamento de chaves digitais produzidas pelo servidor openssh;

Servidor SSH

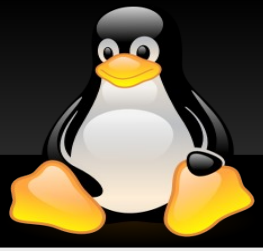
- Usando o cliente:
  - ***#ssh 192.168.0.1***
  - ***#ssh -l mesquita 192.168.0.1***
- Usando o scp:
  - ***#scp root@10.45.1.30:/etc/fstab /root***
  - ***#scp -r root@10.45.1.35:/home /dados***
  - ***#scp arquivo mesquita@192.168.0.5:/tmp***

Servidor SSH

- Gerando uma chave criptográfica:
  - ***# cd /etc/ssh***
  - ***# ssh-keygen -t dsa -f id_mailserver***
  - ***# chmod 400 /etc/ssh/id_mailserver***
- Transferindo uma chave de autenticação:
  - ***# ssh-copy-id -i id_mailserver.pub araujo@mailserver***
- *Trocando a frase de proteção:*
  - ***# ssh-keygen -p -f ~/.ssh/id_mailserver***

Servidor SSH

- Pode-se reforçar o Servidor SSH agregando-se a funcionalidade de portcknoking
- Arquivo de configuração do servidor:
  - **/etc/ssh/sshd_config**
- Principais parâmetros de configuração:
  - **PermitRootLogin**: o servidor aceitará conexões do usuário root.
  - **X11Forwarding:** o servidor repassará a aplicação gráfica para o cliente.
  - **RSAAuthentication**: o servidor aceitará autenticação usando chaves rsa.
  - **Port**: 22.

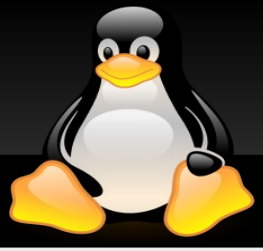


Servidor SSH

- Arquivo de configuração do cliente:
  - **/etc/ssh/ssh_config**
- Principais parâmetros de configuração:
  - **ForwardX11:** o cliente aceitará o encaminhamento de aplicações gráficas feitas pelo servidor.
  - **RSAAuthentication**: o cliente aceitará autenticação usando chaves rsa.

Servidor SSH

- Conferindo uma chave criptográfica:
  - ***# ssh-keygen -l***
- Acessando servidores com chaves individuais:
  - ***# ssh -F webserver 10.45.1.150***
  - ***# ssh -F mailserver 10.45.1.80***
- *Carregando ambiente gráfico remoto:*
  - ***# ssh -X 10.45.1.30***
- *Executando comandos remotos:*
  - ***# ssh -X araujo@10.45.9.8 sudo /etc/init.d/samba restart***



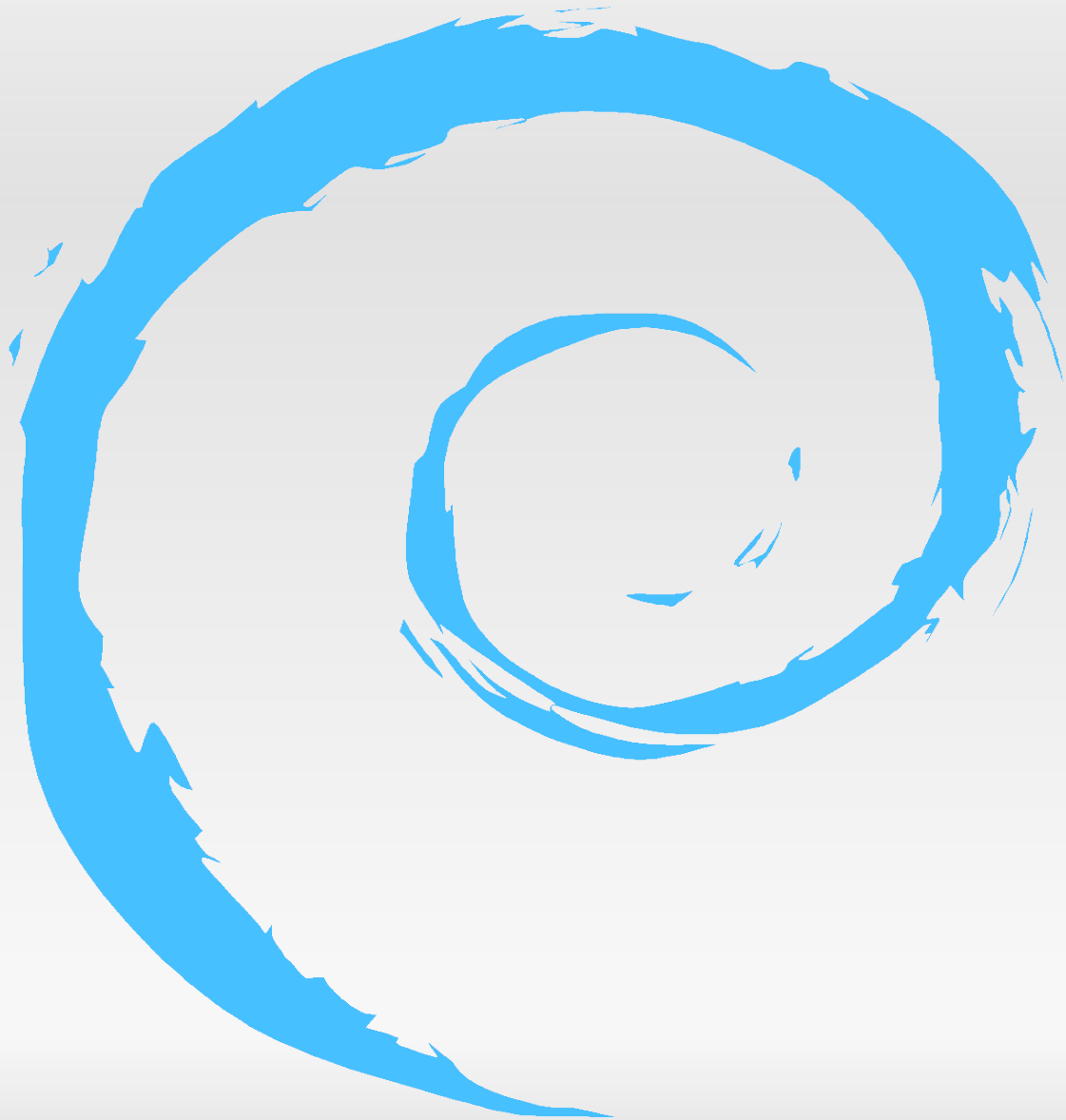
Servidor SSH

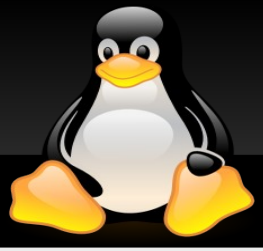
- Alterar a porta padrão do serviço
- Desabilitar o acesso do usuário root
- Utilizar o portcknoking
- Auditar os acessos indevidos:
  - apt-get install fail2ban
  - apt-get install denyhosts

Servidor SSH

- O arquivo ~/**.ssh/known_hosts** armazena as chaves publicas de todos os hosts conhecidos pelo cliente.
- Gerando uma chave RSA para autenticação:
  - **# ssh_keygen -t rsa**
  - A chave pública gerada fica no arquivo ~/**.ssh/id_rsa.pub**
- Essa chave RSA gerada deve ser copiada no servidor onde se deseja se conectar usando **apenas a chave (sem senha)**, no seguinte arquivo:
  - **~/.ssh/authorized_keys**

SERVIDORES LINUX



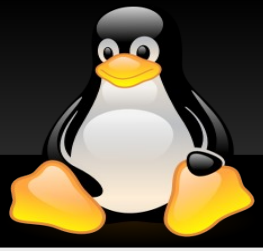


IP Forward (Gateway)

- ***IP forward*** é uma propriedade que habilita uma máquina a trabalhar como roteador.
- Normalmente a máquina deve ter duas ou mais placas de rede e ser o *gateway* padrão da rede local.
- O ***IP forward*** irá permitir a passagem de pacotes entre as redes, quando necessário.

IP Forward (Gateway)

- É usado por exemplo quando se quer **compartilhar o acesso à internet** com outras máquina.
- Ativar o IP forward via propriedades do kernel:
  - `# echo 1 > /proc/sys/net/ipv4/ip_forward`
- Ativar IP forward de **maneira permanente**, basta ativar a seguite opção no arquivo /etc/sysctl.conf:
  - **net.ipv4.conf.default.forwarding=1**
  - `#sysctl -p <ENTER>`



IPTABLES

- O ***Iptables*** está presente em kernels 2.4 e 2.6
- Ele pode verificar o cabeçalho de cada pacote, basicamente endereço IP, máscara, portas e tipos de protocolos, definindo o que ocorrerá com cada um.
- A configuração do ***Iptables*** é feita diretamente via terminal, bastando inserir as regras uma a uma.
- As regras se perdem ao reiniciar o micro, sendo necessário um script para que elas sejam recriadas automaticamente a cada inicialização.

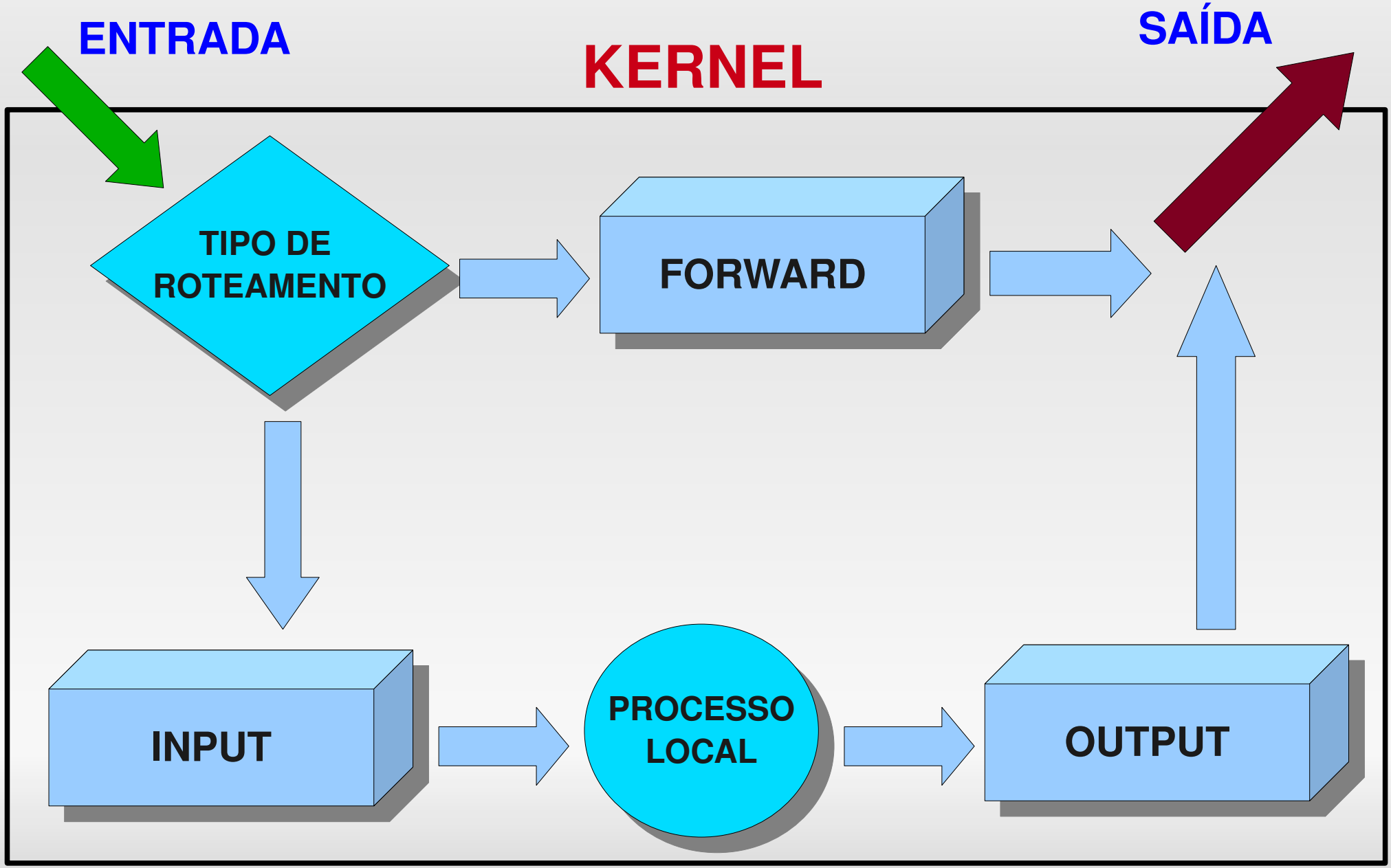
IPTABLES

- Funciona mediante regras estabelecidas, estruturadas em:
  - **tabelas -> chains -> regras**
- Existem 3 tabelas possíveis:
  - **filter**: é a tabela padrão. Quando não especificamos a tabela, a filter é utilizada. Refere-se às atividades normais de filtragem de pacotes. Possui as chains INPUT, OUTPUT e FORWARD.
  - **nat**: utilizada quando há NAT. Admite as chains PREROUTING, OUTPUT e POSTROUTING.
  - **mangle**: trabalha com a marcação de pacotes e QoS.
  - **raw**: tabela, inserida nos kernels 2.6 e superiores, destina-se a marcar pacotes que não devem ser manipulados.

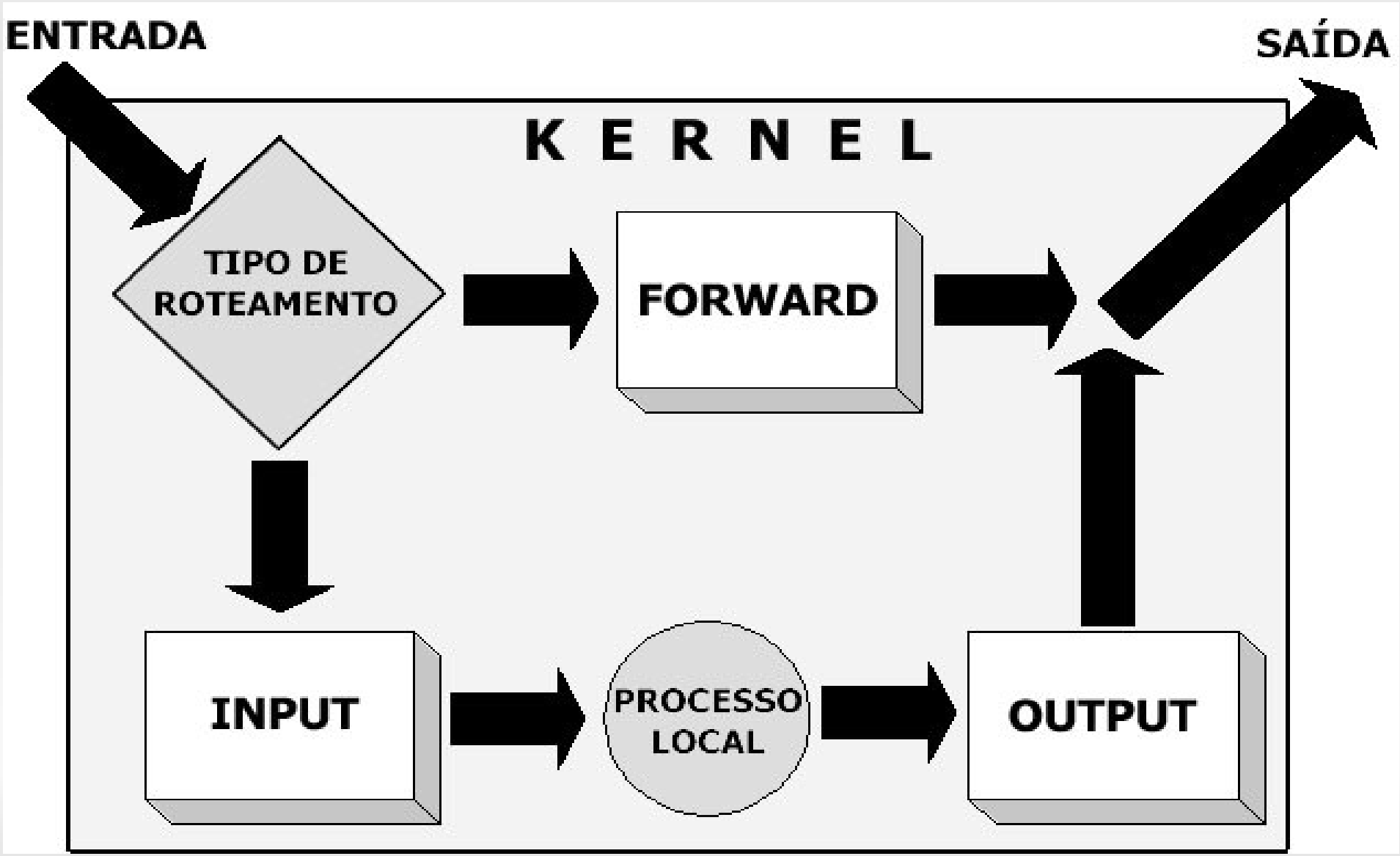
IPTABLES

- A tabela **FILTER** tem 3 ***CHAINS*** pré-definidas:
  - **INPUT**: para pacotes cujo destino é a própria máquina.
  - **OUTPUT**: para pacotes gerados pela máquina que devam sair para a rede
  - **FORWARD**: para pacotes que atravessam a máquina, ou seja, oriundos e direcionados a outras (ip_forward deve estar habilitado).

IPTABLES


ENTRADA
KERNEL
SAÍDA
TIPO DE ROTEAMENTO
FORWARD
INPUT
PROCESSO LOCAL
OUTPUT

IPTABLES

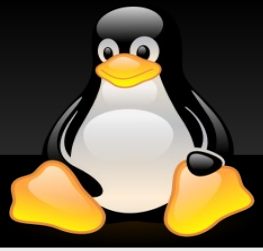

ENTRADA
SAÍDA
K E R N E L
TIPO DE ROTEAMENTO
FORWARD
INPUT
PROCESSO LOCAL
OUTPUT

IPTABLES

- Sintaxe básica

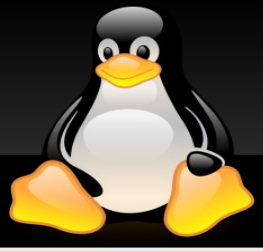
```
iptables [-t tabela] comando [chain]
  [especificação_regra] [-j ação]
```

- Exemplo:
  - # iptables -A INPUT -p udp -j DROP
    - adicionar na chain INPUT (-A INPUT)
    - protocolo UDP (-p udp)
    - Ação: descartar (-j DROP)
- Visualizar as regras existentes
  - # iptables -L -n
  - # iptables -L -n INPUT



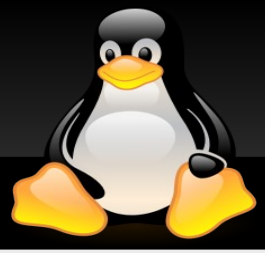
IPTABLES

- Apagar todas as regras:
  - **# iptables -F**
  - **# iptables -F FORWARD**
- Apagar uma regra
  - **# iptables -D INPUT 1**
- Alterar a política da chain. A política inicial de cada chain é ACCEPT.
  - **# iptables -P FORWARD DROP**
  - **# iptables -P INPUT ACCEPT**



IPTABLES

- Definindo uma regra:
  - **-s** (fonte): estabelece a origem do pacote.
    - -s 172.20.0.0/255.255.0.0
    - -s 172.20.0.0/16
  - **-d** (destino);
  - **-p** <protocolo>: especifica o protocolo a ser filtrado.
  - **-i** <interface>: interface de entrada.
    - ***-i ppp0***
    - ***-i eth+***



IPTABLES

- Definindo uma regra:
  - **-o** <interface>: interface de saída.
  - **!**: exclusão.
    - -s ! 10.0.0.1
    - -p ! tcp
  - **--sport** <porta>: porta de origem. Usado no caso do protocolo tcp ou udp.
    - -p tcp -–sport 80
  - **--dport** <porta>: porta de destino. Usado no caso do protocolo tcp ou udp.

IPTABLES

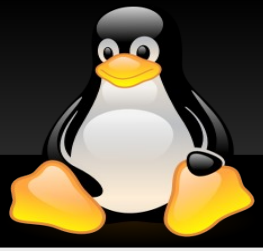
- Ações básicas:
  - **ACCEPT**: aceitar. Permite a passagem.
  - **DROP**: abandonar. Não permite a passagem do pacote, descartando-o.
  - **REJECT**: rejeitar. Igual ao DROP, mas avisa a origem sobre o ocorrido (envia um pacote *icmp unreachable*).
  - **LOG**: cria um log referente a regra e continua para a regra seguinte.
- Outras ações: MARK, MASQUERADE, REDIRECT, DNAT, SNAT...

IPTABLES

- Para compartilhar uma conexão com a Internet:
  - Habilitar o roteamento de pacotes
    - **net.ipv4.conf.default.forwarding = 1 no arquivo /etc/sysctl.conf**
  - Acrescentar uma regra na tabela NAT
    - **# iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**
  - Definir a regra na chain FORWARD liberando acesso ao tráfego estabelecido
    - **# iptables -A FORWARD -m state –state ESTABLISHED,RELATED -j ACCEPT**

IPTABLES

- As regras de iptables devem ser salvas de algum modo, ou se perderão quando a máquina for desligada.
- Uma forma de se fazer isso é com o comando iptables-save.
  - **# iptables-save > /etc/sysconfig/iptables**
- O carregamento poderá ser feito com o comando iptables-restore.
  - **# iptables-restore < /etc/sysconfig/iptables**
- A outra forma de salvar as regras é colocando-se dentro de um script shell, que poderá ser carregado pelo ***/etc/rc.local***

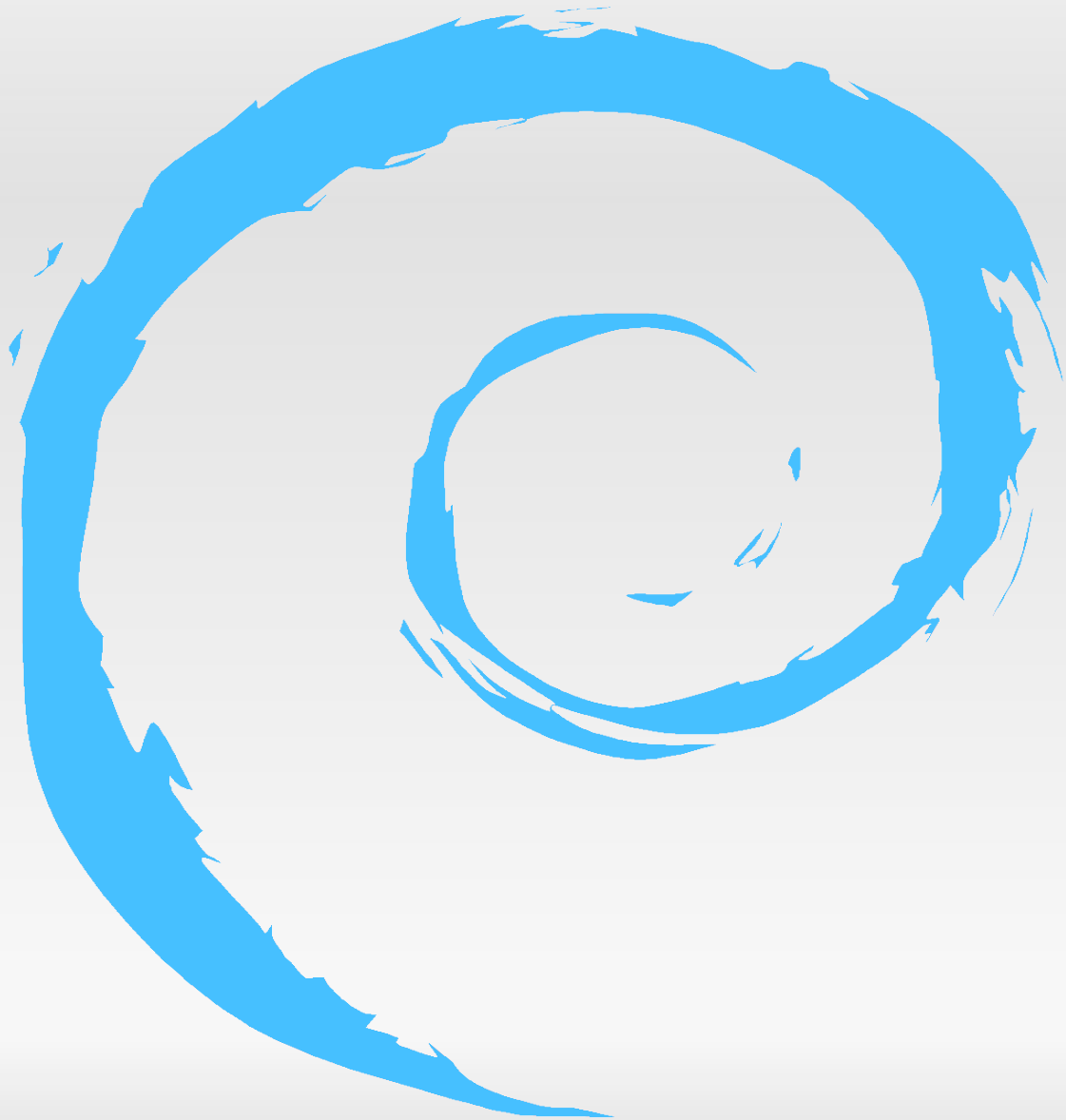


IPTABLES

- Carregando módulos
  - Módulo para conexões FTP modo ativo:
    - **# modprobe ip_conntrack_ftp**
  - Módulo para FTP modo ativo via NAT:
    - **#modprobe ip_nat_ftp**
- Configurando um firewall:

  #vim firewall.sh
- Carregando outro firewall:
  - **# apt-get install fwbuilder**

SERVIDORES LINUX



Proxy

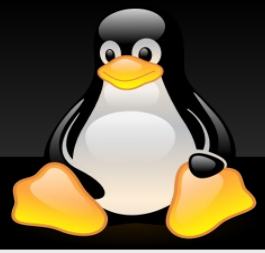
- **O que esperar de um proxy/cache ?**
- Podemos sumarizar os benefícios esperados em:
  - **velocidade de acesso**;
  - **disponibilidade**;
  - **transparência ou ostensividade**;
  - **simplicidade**.
- O **Squid** satisfaz todos esses pontos.

Proxy Squid

- **Squid** é um proxy-cache de alta performance para clientes web, que suporta os protocolos FTP e HTTP.
- O Squid mantém meta dados e objetos armazenados na RAM e “cacheia” buscas de DNS.
- Ele suporta SSL, listas de acesso complexas e logging completo.

Proxy Squid

- o Squid consiste em:
  - ***squid***: programa principal.
  - ***dnsserver***: sistema de busca e resolução de nomes.
  - Alguns programas adicionais para reescrever requests, fazer autenticação e gerenciar ferramentas de clientes.
- Podemos executar o Squid nas principais plataformas do mercado, como Linux, Unix e Windows.

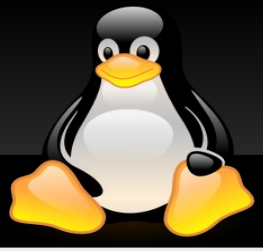


Por que utilizar um Proxy/Cache ?

- **controle de acesso**: navegação por sites não relativos ao seu trabalho primário ou que não condizem com a política da empresa, infecção de toda a rede da empresa com vírus e worms que são adquiridos em sites impróprios, ameaça de propagação de downloads de softwares piratas e músicas, entre outros.
- **performance**: a utilização de PROXY/CACHE pode gerar uma economia entre trinta e cinqüenta por cento nos horários de pico.

Por que utilizar o Squid ?

- Está continuamente melhorando sua performance.
- Implementação de novas funcionalidades.
- Excelente estabilidade em condições extremas.
- Possui compatibilidade com várias plataformas.
- Imensa gama de softwares para analisar logs, gerar relatórios, melhorar o desempenho.
- Possui ferramentas de administração simplificada e baseadas em *web* agregam grande valor ao produto.

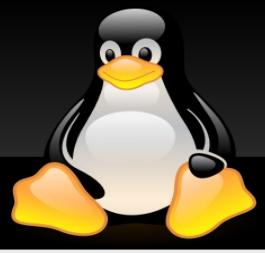


Proxy Squid

- O Squid busca por comunicação TCP ICP (Internet Cache Protocol) em portas específicas.
- O Squid trabalha apenas com FTP, gopher e http.
- Existe uma confusão muito comum entre pessoas que estão começando a trabalhar com o Squid em achar que poderão, através do Squid, configurar acesso a e-mails, ICQ, IRC, etc. **Isso é totalmente equivocado**.

Proxy Squid

- Instalação:
  - **# apt-get install squid**
- Arquivo de configuração
  - **/etc/squid/squid.conf**
- Antes de qualquer configuração é sempre bom gerar uma cópia do arquivo de configuração original:
  - **# cp squid.conf squid.conf.orig**

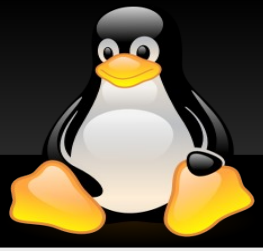


Proxy Squid

- Principais parâmetros de configuração:
  - **http_port:** o IP/porta que o squid aguardará conexões.
  - **cache**: indica se uma determinada ACL será “cacheada”.
  - **cache_mem:** quantidade de memória RAM a ser utilizada para cache.
  - **maximum_object_size**: o tamanho máximo de um objeto em cache. Objetos maiores do que esse limite não são salvos em disco.

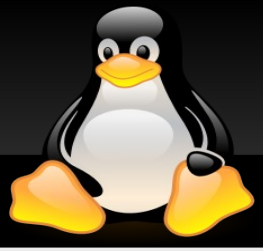
Proxy Squid

- Principais parâmetros de configuração:
  - **maximum_object_size_in_memory**: tamanho máximo do objeto cacheado em memória RAM.
  - **cache_dir**: diretório onde serão armazenados os objetos em cache no disco e o tamanho máximo que ocuparão.
  - **visible_hostname**: o nome do servidor.(Se não for configurado o Squid não inicializa)
  - **ACL**: definem um objeto que será usado nas regras de controle de acesso.



Proxy Squid

- Principais parâmetros de configuração:
  - **auth_param:** define como será a autenticação dos usuários.
  - **http_access:** permite ou bloqueia uma acesso baseado em ACLs. Usado para bloquear sites.
  - **reply_body_max_size:** tamanho máximo da resposta. Usado para limitar o tamanho do download.



Proxy Squid

- As regras de bloqueio do Squid são baseadas em listas de acessos(ACLs).
- Exemplo:
  - Suponha que a rede interna seja 192.168.5.0/24.

```
acl rede_interna src 192.168.5.0/24
http_access allow rede_interna
```

Proxy Squid - ACLs

- Principais opções usadas em ACLs:
  - **src:** ACL para o IP de origem de um pacote.
  - **dst:** ACL o IP destino de um pacote.
  - **dstdomain_regex:** ACL para o domínio de destino a partir de uma expressão regular. Útil para bloquear domínios (sites internos redirecionados).
  - **url_regex:** ACL para a URL inteira de destino a partir de uma expressão regular. Útil para bloquear sites.
  - **time:** definir dia da semana e intervalo de hora.
  - **proxy_auth:** usado para que o proxy use autenticação

Proxy Squid
Bloqueando sites indesejados

- As ***ACLs*** são muitos úteis para permitir trabalhar com níveis de acesso.
- Num Proxy é comum que a diretoria possa acessar qualquer site, a gerência não possa acessar determinados sites e os "peões" tenham acesso apenas ao site da empresa e de parceiros.
- Todas as configurações de usuários, grupos, horários e SITES são configuradas em ***ACLs***.

Proxy Squid
Bloqueando sites indesejados

- A ordem em que as regras aparecem é muito importante, por isso as regras que permitem devem aparecer antes das que bloqueiam.
- Criando os arquivos necessários:

```
# touch /etc/squid/sites_bloqueados.txt
```

```
# touch /etc/squid/sites_bons.txt
```

- O arquivo **sites_bloqueados.txt** conterá todos os sites e palavras que você deseja bloquear e o **sites_bons.txt** todas as exceções.

Proxy Squid
Bloqueando sites indesejados

- Criando as ACLs:
  - `acl sites_ruins url_regex -i "/etc/squid/sites_bloquedos.txt"`
  - `acl sites_bons url_regex -i "/etc/squid/sites_bons.txt"`
- Criando as regras de bloqueio:
  - `http_access allow sites_bons`
  - `http_access deny sites_ruins`

Proxy Squid
Autenticando usuários

- É um recurso bem interessante para controle pessoal de usuários.
- Isso permite que você crie ACLs individuais e gere LOGs de qualidade bem superior.
- Existem diversos métodos de autenticação, sendo interessante averiguar exatamente o que você irá precisar.
- Na maioria dos casos, o ***ncsa_auth*** resolve o problema.
- Outras opções são: ***pam_auth, ldap_auth e ntlm_auth***.

Proxy Squid
Autenticando usuários

- Para configurar basta descomentar as linhas para informar ao squid o tipo de autenticação a ser utilizada:

auth_param basic program /usr/lib/squid/ncsa_auth /etc/squid/passwd

auth_param basic children 5

auth_param basic realm Squid proxy-caching web server

auth_param basic credentialsttl 2 hours

auth_param basic casesensitive off

Proxy Squid
Autenticando usuários

- Criar a ACL:
  - **acl autenticacao proxy_auth REQUIRED**
- Criar a regra que permite apenas quem estiver autenticado:
  - **http_access allow autenticacao**

Proxy Squid
Exemplo de configuração


```
acl EB url-regex eb.mil.br

cache deny EB

cache_mem 32 MB

maximum_object_size 900000 KB

cache_dir ufs /var/spool/squid 200000 64 256

ftp_passive on

acl nossa_rede src 192.168.0.0/255.255.0.0
```

Proxy Squid
Exemplo de configuração


```
acl sexo url_regex -i "/etc/squid/sexo.txt"
acl som url_regex -i "/etc/squid/radios.txt"
acl chat url_regex chat batepapo bate-papo
acl expediente1 time MTWHF 09:00-12:00
acl expediente2 time MTWHF 13:30-17:00
http_access deny nossa_rede sexo
http_access deny nossa_rede som
http_access deny nossa_rede chat expediente1
http_access deny nossa_rede chat expediente2
http_access allow nossa_rede
cache_mgr adm@rede.com.br
```

Proxy Squid
Proxy Transparente

- Esse recurso é muito útil para evitar que seus usuários "burlem" o proxy removendo as configurações do *browser*.
- Eles serão obrigados a passar pelo proxy, mesmo que as máquinas não estejam configuradas para tal.
- Extremamente recomendado, principalmente em casos de bloqueio de *sites* ou limitação de banda.
- Para ser possível o uso de proxy transparente com o Squid, o firewall deve ser configurado adequadamente.

Proxy Squid
Proxy Transparente

- Esse recurso é muito útil para evitar que seus usuários "burlem" o proxy removendo as configurações do *browser*.
- Eles serão obrigados a passar pelo proxy, mesmo que as máquinas não estejam configuradas para tal.
- Extremamente recomendado, principalmente em casos de bloqueio de *sites* ou limitação de banda.
- Para ser possível o uso de proxy transparente com o Squid, o firewall deve ser configurado adequadamente.

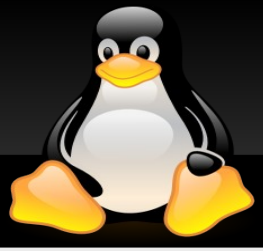
Proxy Squid
Proxy Transparente

- Deve-se inserir essa regra no iptables:

```
# iptables -t nat -A PREROUTING -i
  eth0 -p tcp --dport 80 -j REDIRECT
  --to-port 3128
```

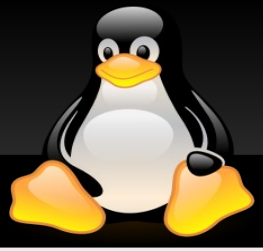
SARG

- Sigla para **Squid Analysis Report Generator**
- É um utilitário gerador de relatórios sobre os arquivos de log do Squid.
- Gera os relatórios em HTML ricos em detalhes.
- Instalação:
  - **# apt-get install sarg**
- Arquivo de configuração:
  - **/etc/squid/sarg.conf**



SARG

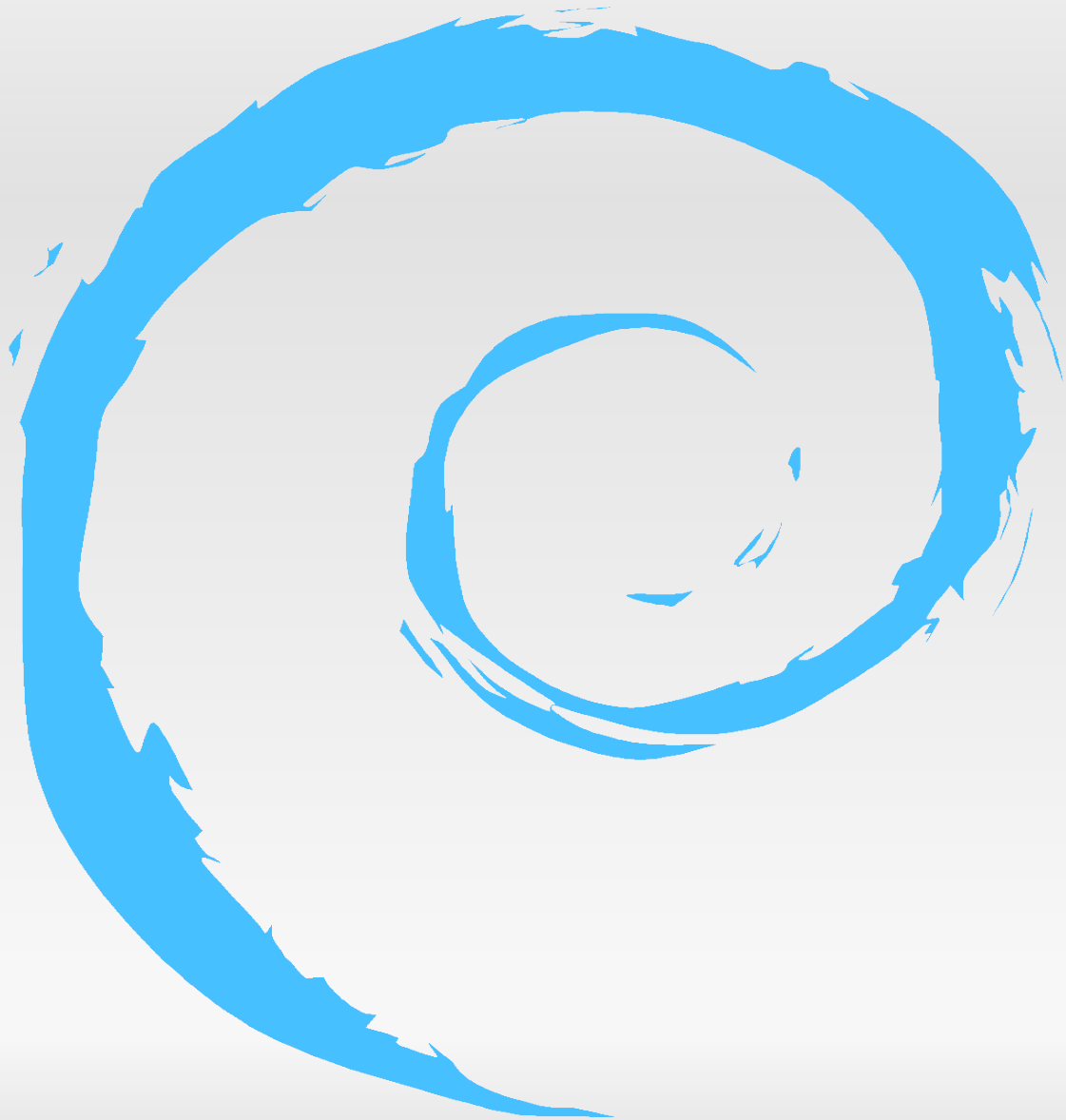
- Principais parâmetros de configuração:
  - **access_log**: arquivo de log do squid.
  - **language**: linguagem utilizada nos relatórios.
  - **output_dir**: diretório onde serão gerados os relatórios.
  - **date_format:** formato da data.



SARG

- No Debian, a instalação já gera um script no diretório ***/etc/cron.daily***, de forma que ele será executado diariamente pelo ***cron*** gerando assim o relatório.
- Comando para gerar relatório:
  - ***# sarg -d 23/03/2007-23/03/2007***

SERVIDORES LINUX

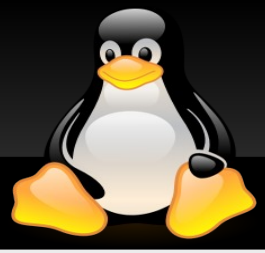


Network File System (NFS)

--- Linux NFS-HOWTO ---

O que é NFS ?

- O Network File System (NFS) foi desenvolvido para possibilitar a montagem de uma partição de um computador remoto, parecendo para o usuário que a mesma pertence ao HD Local.
- Dessa forma, o NFS permite o compartilhamento de arquivos de uma forma rápida, por meio de uma rede de computadores.
- O NFS também abre uma brecha de segurança, pois usuários indesejados poderão acessar um HD pela rede. Por isso é fundamental implementar o NFS da forma mais restritiva possível.

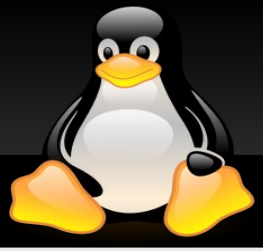


O que é NFS ?

- Existem outros sistemas que possuem a mesma funcionalidade. Dentre eles podemos citar:
  - Samba: http://www.samba.org;
  - Andrew File System (AFS);
  - Coda File System (CFS);
- Muitas das características do AFS e do CFS são esperadas na nova versão do NFS (versão 4).
- A grande vantagem do NFS é que já é uma ferramenta madura, padronizada, dominada e com suportada em várias arquiteturas.

NFS

- Instalação:
  - `# apt-get install portmap`
  - `# apt-get install nfs-common`
  - `# apt-get install nfs-kernel-server`
- Ao término da instalação o script de inicialização já estarão disponíveis no diretório /etc/init.d
- Você pode tirar dúvidas no site http://nfs.sourceforge.net



NFS - Configuração

- A configuração do NFS tem que ser realizada no servidor e no computador cliente.
- A configuração do servidor NFS envolve a configuração de alguns arquivos e a inicialização dos serviços NFS.
- Existem 3 (três) arquivos que necessitam ser configurados no servidor:
  - **/etc/exports;**
  - **/etc/hosts.allow;**
  - **/etc/hosts.deny**

NFS - /etc/exports

- Este arquivo contém uma lista de diretórios a serem compartilhados e o modo como serão compartilhados.
- Uma linha desse arquivo é da forma:

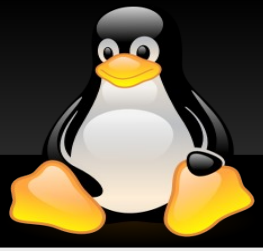
```
diretorio host1(opções) host2(opções)
```

- As principais opções são:
  - **ro**: somente leitura.
  - **rw**: leitura e escrita.
  - **no_root_squash**: permite que o root da máquina cliente acesse o compartilhamento, sobrepassando as permissões da pasta.
  - **sync** ou **async**: modo de transmissão de dados.

NFS - /etc/exports

- Exemplos de linhas do /etc/exports:

```
/home            192.168.0.1(ro) 192.168.0.2(rw)
/usr            192.168.0.0/255.255.255.0(ro)
/projects       192.168.0.0(rw,no_root_squash)
/usr/local       *.5cta.eb.mil.br(ro)
/tmp *(rw,all_squash,anonuid=150,anongid=100)
```



NFS - Lembretes

- Se um diretório for exportado seu diretório pai e os diretórios filhos não poderão ser exportados se não estiverem na mesma partição.
- É extremamente perigoso compartilhar com NFS diretórios formatados com FAT ou VFAT, pois esses sistemas de arquivo não foram projetados para trabalharem em sistemas multi-usuário e as permissões não funcionarão direito.
- A exportação de alguns dispositivos ou arquivos especiais não funcionam corretamente para clientes que não são Linux.

/etc/hosts.allow
/etc/hosts.deny

- Estes arquivos especificam os computadores que terão ou não acesso aos compartilhamentos.
- São processados na seguinte sequência:
  - primeiro é verificado o ***/etc/hosts.allow***;
  - depois o ***/etc/hosts.deny***;
  - se nenhuma regra se encaixou então o acesso é franqueado.

NFS
Inicialização dos serviços

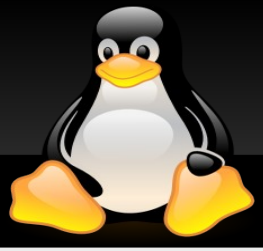
- Para funcionar o NFS precisa do *daemon* ***portmap*** iniciado.
- Uma forma de verificar se os scripts foram iniciados é com o comando:

```
# rpcinfo -p <host>
```

NFS
Alteração no /etc/exports

- As alterações realizadas no arquivo ***/etc/exports*** depois do início dos *daemons* só terão validade após o reinício do NFS ou depois da emissão do comando:

```
# exportfs -ra
```



NFS
Configuração do cliente

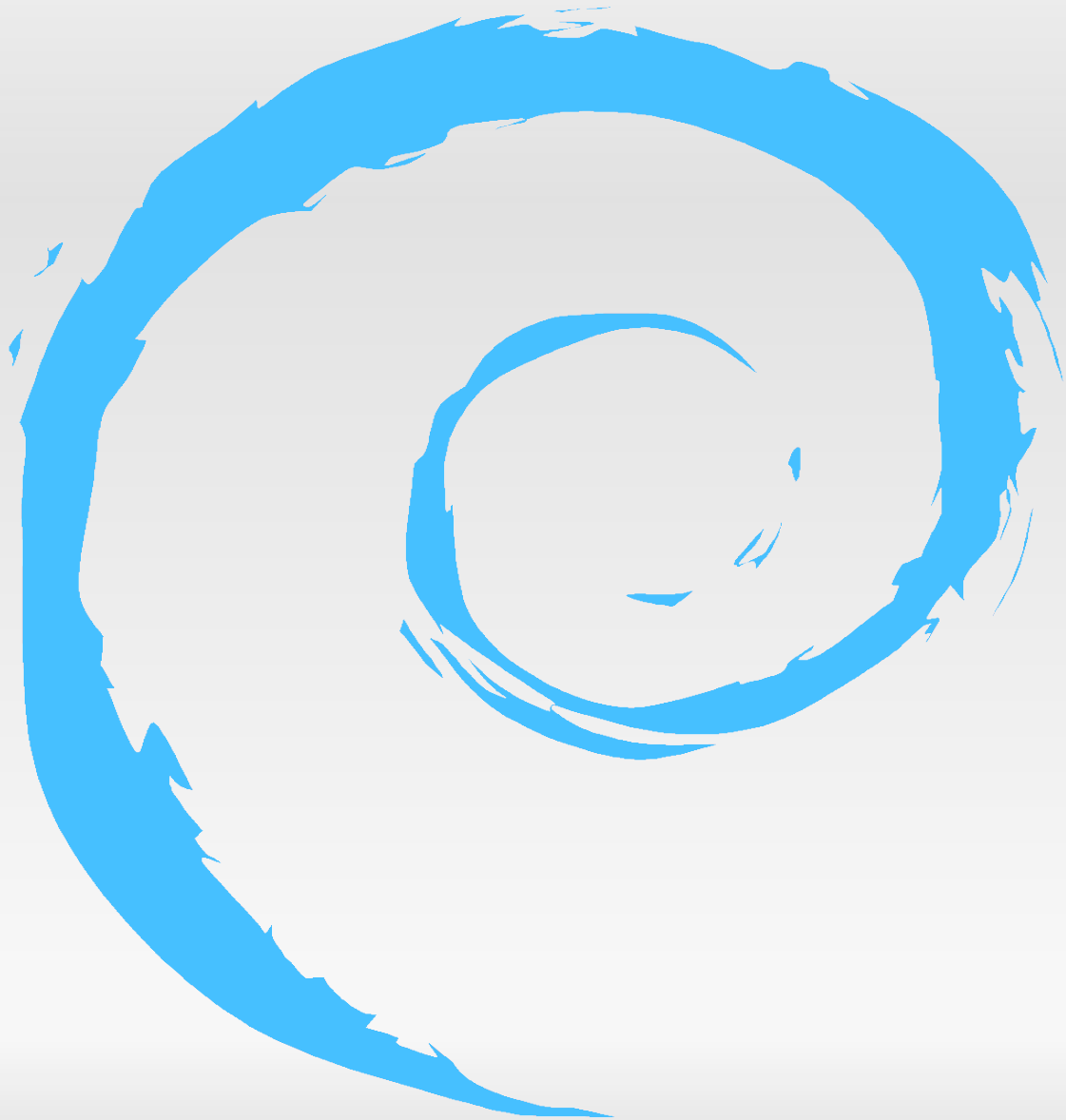
- Os daemon portmap, rpc.statd e rpc.lockd devem estar rodando.
- Você pode montar um diretório remoto com o comando mount:

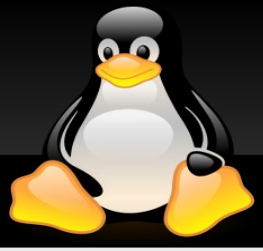
```
# mount -t nfs 192.168.0.1:/home /mnt/home
```

- Se desejar que seja montado no momento do boot do sistema basta acrescentar uma linha ao /etc/fstab:

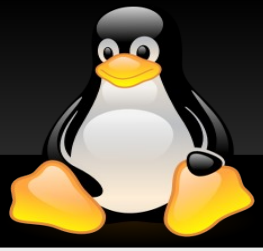
```
192.168.0.1:/home /mnt/home nfs rw 0 0
```

SERVIDORES LINUX



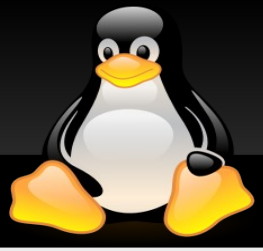


SAMBA



O que é o SAMBA ?

- Implementação aberta do protocolo ***CIFS*** (Common Internet File System)
- Pacote de ferramentas baseado no protocolo ***CIFS*** / ***SMB*** (Server Message Block)
- Pode ser implementado sobre TCP/IP, NetBEUI, IPX
- Possibilita acesso à rede MS
- Integra outros sistemas com estações da rede MS
  - Comunicação/Compartilhamento de recursos



O que é o SAMBA ?

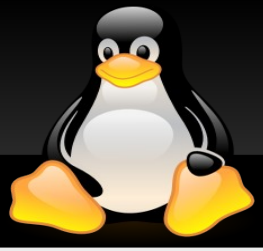
- De forma semelhante ao Linux, o Samba pode ser distribuído livremente sem ônus. Sua distribuição é regida pela licença GPL, da GNU
- Desenvolvido originalmente por Andrew Tridgell, na época (1991) estudante de Mestrado na Austrália, realizando engenharia reversa do protocolo SMB
- Ao ser perguntado sobre o nome do seu protocolo, fez uma pesquisa rápida por palavras com as letras “smb”
- Andrew é amigo de Linus Torwalds
  - Levou Linus ao Zôo, onde foi “bicado” por um pingüim, fato que motivou o símbolo do Linux

O que é o SAMBA ?

- O Samba possui dois programas chaves (***smbd*** e ***nmbd***), realizando 4 tarefas principais:
  - Compartilhamento de arquivos e impressoras
  - Autenticação e autorização
  - Resolução de nomes
  - Anúncio de serviços (browsing)
- Atualmente o protocolo é mantido por uma equipe de programadores de várias partes do mundo, sob a supervisão de Andrew Tridgell (Samba 4.0)
- Desenvolvimento auxiliado pela MS ao liberar o protocolo CIFS/SMB em 1996

SAMBA - Definições

- Grupo de trabalho (***workgroup***) - conjunto de máquinas que compartilham uma lista de recursos comum
- ***Domínio*** - um grupo de trabalho que inclui um servidor central de autenticação
- Controlador de domínio (***Domain Controller***) - a máquina no domínio que possui o banco de dados de autenticação
- ***Dominio NT/AD*** - grupo de máquinas com o mesmo controlador de domínio (Windows NT/200x)



SAMBA - Vantagens

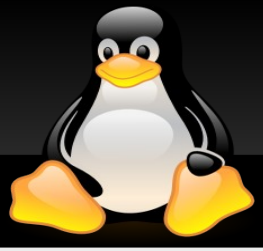
- Emula máquinas MS
- Hardware mais leve
- Maior robustez
- Mais rápido que máquinas MS (NT/2000)
- Livre de licença (software/clientes)

SAMBA
Algumas possibilidades (samba3)

- Servidor independente
- Membro de um domínio
  - NT
  - ADS
  - LDAP
- Controlador de domínio
  - PDC
  - BDC
- Servidor WINS

SAMBA - Restrições

- Samba é semelhante a um controlador de domínio NT4, com alguns detalhes a mais e outros a menos.
- Samba não é um Windows Server 200x
- Samba não funcionava como um servidor Active Directory (função incorporada na versão 4.0).
- Samba não funciona como PDC para um NT BDC ou vice-versa



SAMBA - Utilitários

- **nmbd**
  - daemon (udp/137 e 138) para os serviços de nomes e browsing
- **smbd**
  - daemon (tcp/139) para os serviços de arquivos e impressoras e autenticação local
- **winbindd**
  - daemon que permite que o samba trabalhe como membro de um domínio NT ou ADS

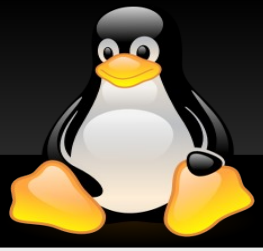
SAMBA - Utilitários

- **testparm**
  - Verifica o arquivo de configuração (**smb.conf**)

    # testparm -v **# testparm -s > smb.conf**
- **nmblookup**
  - resolve nomes NetBIOS em IP
- **smbpasswd**
  - muda a senha de usuários do samba
  - para o root, acrescenta/remove usuários do samba

SAMBA - Utilitários

- **smbstatus**
  - Apresenta o estado (conexões) do smbd
- **smbclient**
  - cliente para acesso a compartilhamentos
    - **smbclient -L localhost -U root**
- **smbmount**
  - monta um sistema de arquivos smbfs
    - **smbmount //servidor/compartilhamento /mnt/dir -o username=user**



SAMBA - Segurança

- O Samba foi escrito com atenção especial para a segurança. Oferece muito mais opções de segurança que outros pacotes para compartilhamento de arquivos
- Pode utilizar os serviços de um servidor NT para verificação de usuários
- Não se sobrepõe aos mecanismos de segurança do UNIX.
- Pode usar LDAP, MySQL, NIS+ ou um arquivo para armazenar senhas (***smbpasswd***)

SAMBA - Características

- O Samba foi escrito para ser portável e não requer alterações no kernel.
- Já foi portado para plataformas não UNIX como OS/2, Novell Netware, VMS e AmigaOS.
- O Samba cria um processo UNIX para cada usuário conectado.
- Cada usuário requer por volta de 600 a 800 k de memória dependendo do tipo de utilização feito.
- Usado por grandes, médias e pequenas organizações em todo o mundo.

SAMBA - Browsing

- Os protocolos de *browsing* permitem que a opção "***Network Neighborhood***" ou "Toda a Rede" vejam todos os servidores disponíveis
- Os protocolos de *browsing* são complexos e envolvem um sistema de eleição para decidir o "***browser master***" que é a máquina responsável por manter a lista de servidores visível
  - Utiliza principalmente a porta **UDP/ 138**

SAMBA - Configuração

- Arquivo de configuração
  - **/etc/samba/smb.conf**
  - Possui uma enorme quantidade de opções muito bem documentadas (**man smb.conf**)
  - A maior parte das definições padrão podem funcionar perfeitamente.
- Carregado no início do serviço
- Pode ser editado com o servidor no ar, as alterações valerão na próxima carga do Samba

SAMBA
Variáveis de Ambiente

- Exemplos:
  - **%u** Usuário UNIX (efetivo)
  - **%g** Grupo primário UNIX correspondente a %u
  - **%U** Usuário NetBIOS (pode ser diferente de %u)
  - **%G** Grupo primário de %U
  - **%H** Diretório-base do usuário %u.
  - **%v** Versão do Samba.

SAMBA
Variáveis de Ambiente

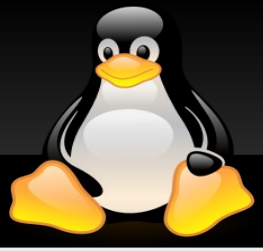
- Exemplos:
  - **%h** Nome DNS da máquina em que o Samba está rodando.
  - **%M** Nome DNS da máquina-cliente.
  - **%I** Número IP da máquina-cliente.
  - **%d** Número do processo (PID) do servidor corrente.
  - **%T** Data e hora correntes.

SAMBA
Seções do smb.conf

- **[global]**
  - Atributos globais do servidor
- **[homes]**
  - Pastas pessoais dos usuários
- **[printers]**
  - Impressoras compartilhadas
- **[<nome>]**
  - <nome> = nome do compartilhamento

SAMBA
Parâmetros do smb.conf [global]

- **workgroup**
  - Nome do grupo de trabalho ou domínio.
- **netbios name (*parâmetro opcional*)**
  - Nome do servidor na rede.
  - Será usado nos acessos aos compartilhamentos
  - O Workgroup e o nome da máquina/Netbios name devem ser diferentes.



SAMBA
Parâmetros do smb.conf [global]

- **encrypt passwords**
  - Permite o uso de senhas criptografadas
- Versões do windows que não suportam senhas criptografadas:
  - Windows 95 antes do OSR2 (win95a)
  - Windows NT 3.x
  - Windows NT 4 antes do SP4

SAMBA
Parâmetros do smb.conf [global]

- **security**
  - Parâmetro mais importante
  - Opções
    - **SHARE**:
    - **USER:**
    - **DOMAIN:**
    - **SERVER**
    - **ADS (samba 3.0/4.0)**

SAMBA
Parâmetros do smb.conf [global]

- **security = share**
  - Segurança a nível de compartilhamento
  - Cada recurso compartilhado possui uma senha e o cliente necessita apenas desta senha para acessar tais os recursos . Este foi o primeiro modelo de segurança oferecido pelo SMB
  - Equivalente a rede MS
  - Linux funcionará como estação Windows na rede com compartilhamento

SAMBA
Parâmetros do smb.conf [global]

- **security = user**
  - Segurança a nível de usuário
  - O acesso é controlado baseado nos privilégios garantidos a cada usuário. O usuário precisa se identificar previamente junto ao servidor
  - Equivalente a servidor de autenticação
  - Linux pode funcionar como PDC
    - Clientes XP/2000 podem ser adicionados ao domínio samba

SAMBA
Parâmetros do smb.conf [global]

- **security = server**
  - Autenticação com outro servidor SMB
  - Definir o parâmetro ***password server***
  - É preferível colocar o samba como membro do domínio
- **security = domain**
  - Integração com o domínio NT
  - Autenticação no PDC/BDC
  - Necessário antes adicionar a máquina samba ao domínio
    - ***net rpc join -U administrator%password***

SAMBA
Parâmetros do smb.conf [global]

- **domain master**
  - Configura o nmbd pra ser o servidor principal de browsing
  - Não deve ser configurado como yes se houver um PDC NT na rede
- **preferred master**
  - Força uma eleição ao iniciar o samba
- **os level**
  - Valor inteiro (default = 20)
  - peso para vitória em eleição

SAMBA
Parâmetros do smb.conf [global]

- **domain logons**
  - Habilita o samba ser servidor de logon ou PDC
- **logon script**
  - indica o nome do arquivo script
  - Caminho relativo ao path do [netlogon]
  - Executa-se em tempo de login
  - *DEVE SER UM ARQUIVO TEXTO TIPO **DOS***

SAMBA
Parâmetros do smb.conf [global]

- **logon script**
  - Exemplo:

```
@echo off
net use f: \\server\share
net use h: /home
net time \\server /set /yes
```

SAMBA
Exemplo do [homes]

- [homes]

  comment = Home Directories

  path = %S

  writeable = yes

  browseable = no

- [netlogon]

  comment = netlogon

  path = /home/samba/netlogon

  read only = yes

SAMBA
Exemplo de compartilhamento

- [publico]

  comment = diretorio publico

  path = /tmp/samba/publico

  public = yes

  writeable = yes

  browseable = yes

  veto files = /*.mp3/*.wma/*.wmv/*.avi/*.mpg/*.wav/

SAMBA
Exemplo de compartilhamento

- [diretorio]

  comment = diretorio compartilhado

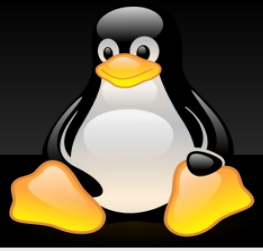
  path = /home/diretorio

  read only = yes

  write list = admin root @staff

  create mask = 0775

  directory mask = 0775



SAMBA

- Configurando o Samba como PDC:
  - Criar usuários no samba
  - Criar contas de máquinas
  - Configurar um compartilhamento público
  - Configurar um compartilhamento privado
  - Configurar um script de logon

SAMBA
Configurando PDC

- Exemplo dos parâmetros no ***smb.conf***:
  - **workgroup** = curso
  - **netbios name** = servidor
  - **security** = user
  - **encrypt passwords** = true
  - **smb passwd file** = /etc/samba/smbpasswd
  - **obey pam restrictions** = yes

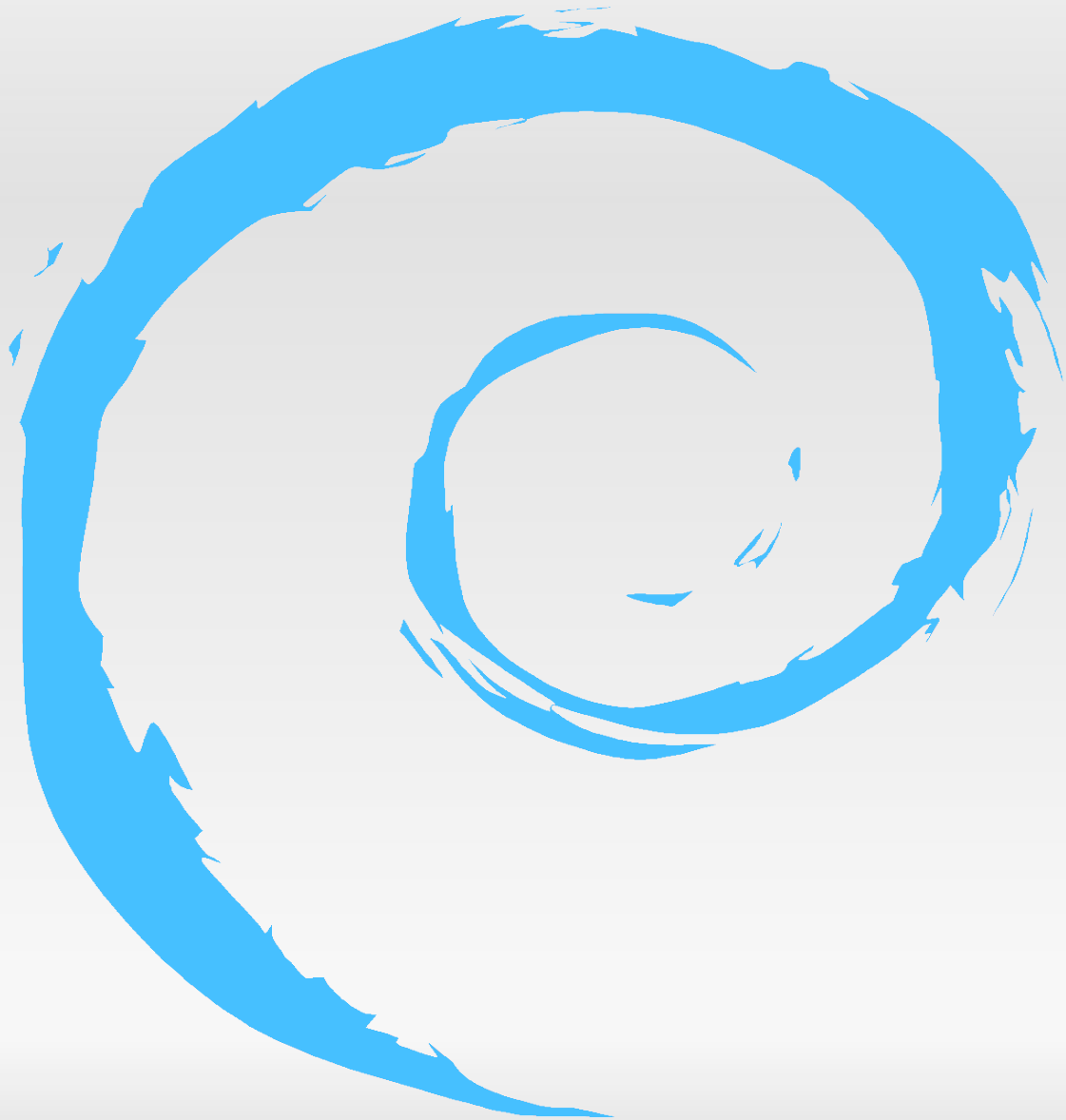
SAMBA
Configurando PDC

- Exemplo dos parâmetros no ***smb.conf***:
  - **domain logons** = yes
  - **domain master** = yes
  - **preferred master** = yes
  - **local master** = yes
  - **os level** = 100

SAMBA
Configurando PDC

- Inserindo usuário no PDC
  - **# adduser usuario**
  - **# useradd usuario -s /bin/false -d /dev/null usuario**
  - **# passwd usuario**
  - **# smbpasswd -a usuario**
- Alterando a senha de um usuário
  - **# smbpasswd usuario**
- Criação de um Servidor Samba PDC
  - **# vi samba_seguro.sh**

SERVIDORES LINUX



Winbind – Linux logando no SAMBA

- Objetivo
  - Logon no linux com contas do NT ou Samba
- Instalação
  - **# apt-get install winbind libpam-modules**
- Criação da conta de máquina:
  - **# useradd maquina$**
  - **# passwd -l maquina**
  - **# smbpasswd -a -m maquina**

Winbind – Linux logando no SAMBA

- Parâmetros do ***smb.conf***
  - **workgroup** = nome_dominio
  - **security** = domain
  - **wins server** = ip_do_pdc
  - **encrypt passwords** = true
  - **obey pam restrictions** = yes
  - **winbind enum groups** = yes
  - **winbind enum users** = yes

Winbind – Linux logando no SAMBA

- Parâmetros do ***smb.conf***
  - **winbind uid** = 10000-20000
  - **winbind gid** = 10000-20000
  - **winbind separator** = +
  - **template homedir** = /home/%U
  - **template shell** = /bin/false
  - **winbind use default domain** = yes

Winbind – Linux logando no SAMBA

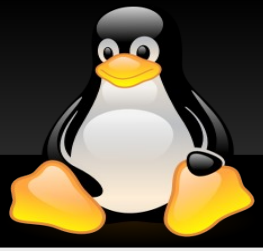
- Juntar-se ao domínio

  # smbpasswd -j DOM -r PDC -U admin (Samba2.0)

  ou

  # net rpc join -w DOM -S PDC -U admin (Samba3.0)

- Resposta:
  - Joined domain DOM



Winbind – Linux logando no SAMBA

- daemon
  - **winbind**
- Comandos
  - **wbinfo -u**
  - **wbinfo -g**
  - **wbinfo -t**
  - **getent passwd**
  - **getent group**

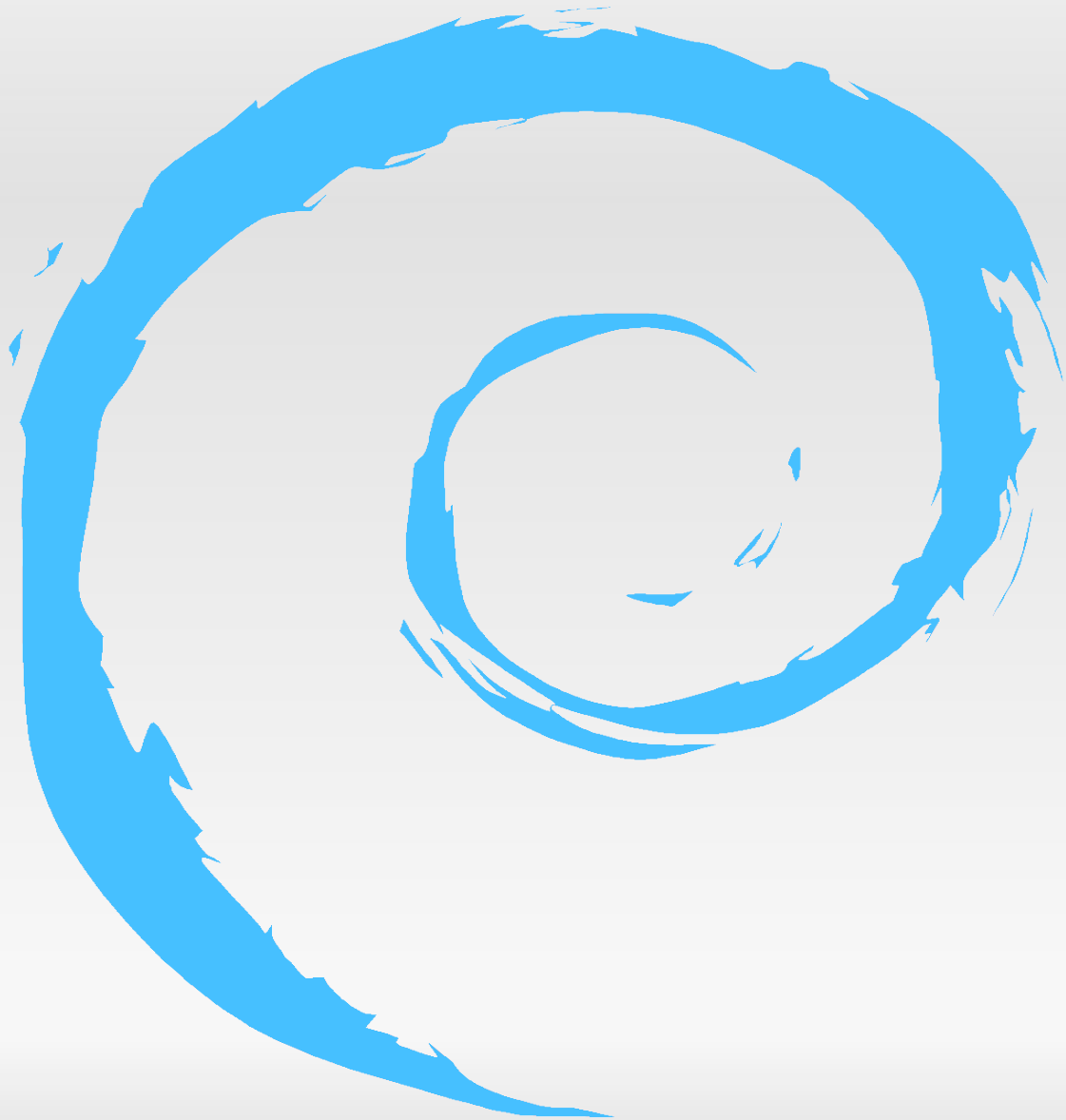
Winbind – Linux logando no SAMBA

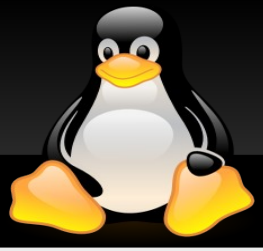
- Editar /**etc/nsswitch.conf**
  - **passwd**: files winbind
  - **group**: files winbind
  - **shadow**: files winbind
- Editar /**etc/pam.d/common-auth**
  - auth sufficient pam_unix.so nullok_secure
  - auth required pam_winbind.so use_first_pass

Winbind – Linux logando no SAMBA

- Editar **/etc/pam.d/common-account**
  - account sufficient pam_unix.so
  - account required pam_winbind.so use_first_pass
- Editar **/etc/pam.d/common-session**
  - session required pam_mkhomedir.so skel=/etc/skel umask=0022
  - session sufficient pam_unix.so
  - session required pam_winbind.so

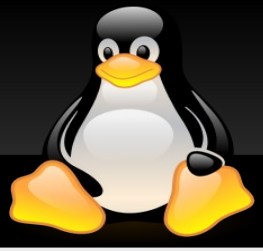
SERVIDORES LINUX





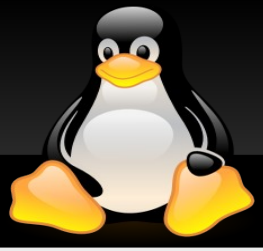
Servidor CUPS

- Instalando o Servidor CUPS
  - # apt-get install cups cups-common
  - # apt-get install cups-pdf
  - # apt-get install openprinting-ppds openprinting-ppds-extras linuxprinting.org-ppds linuxprinting.org-ppds-extra
- Acessando o Servidor CUPS
  - # konqueror http://localhost:631
  - Drivers locais: /usr/share/cups/drivers



Servidor CUPS

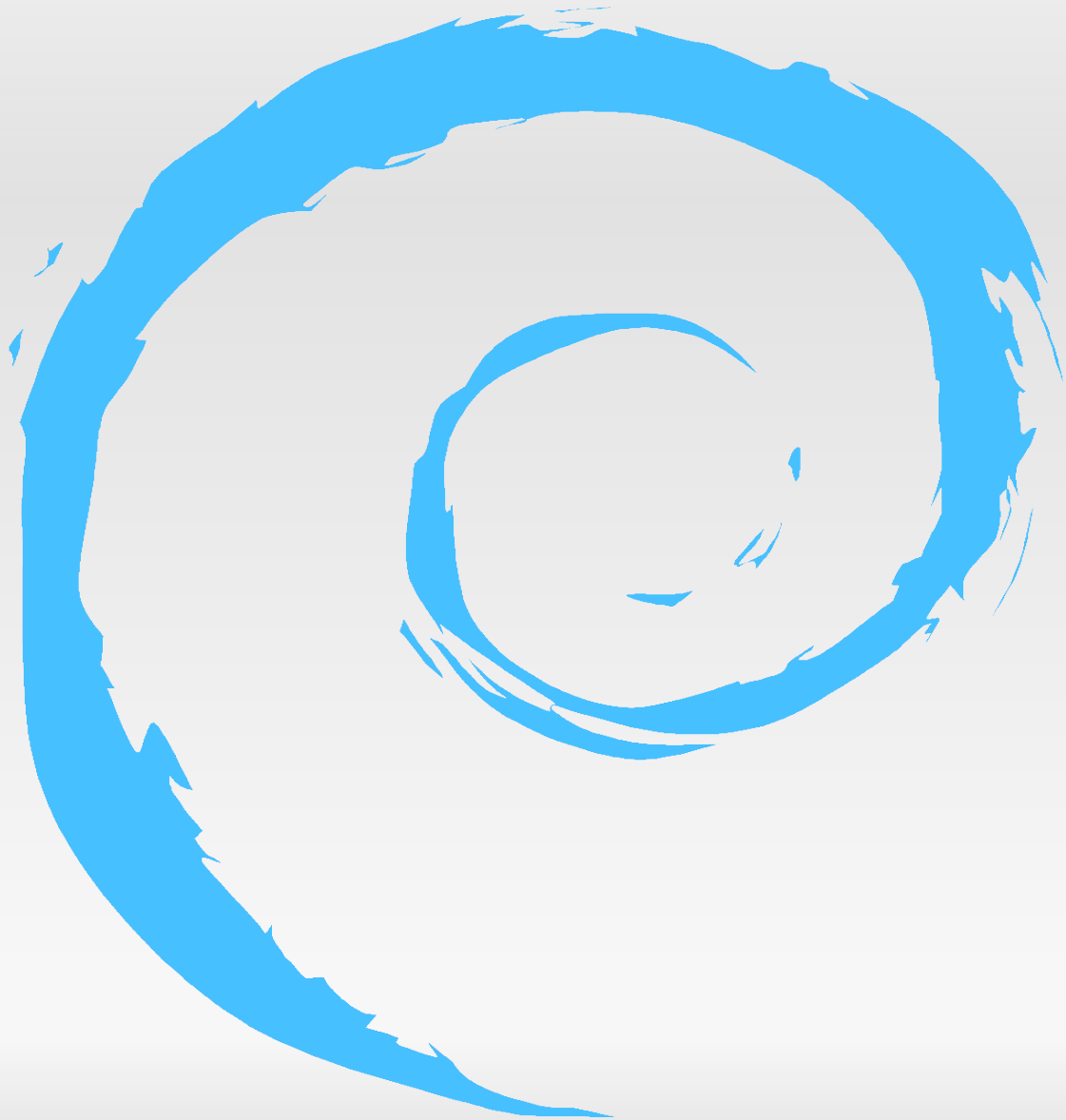
- Administrando impressora local e remota
  - konqueror http://localhost:631/admin
  - konqueror http://localhost:631/printers
- Imprimindo a partir do Windows
  - Driver ippprint.exe (suporte à impressão via web)
  - Impressora de Rede
  - Drivers locais



Servidor CUPS

- Instalando impressora do windows
  - konqueror smb://ipmaqwindows/impressora
  - Driver local do Linux
  - Usuário cadastrado no windows
- Obtendo informação sobre novos drivers
  - http://www.openprinting.org

SERVIDORES LINUX



SERVIDORES LINUX