

Linux Completo + Servidores

Aula 1: Introdução ao Linux

Apresentação

- Instrutor: Humberto F. Forsan
 - Pós Graduado em Segurança da Informação
 - Graduado em Redes de Computadores
 - Professor de cursos técnicos e cursos de pós graduação
 - Especialista em Segurança da Informação

Cronograma

Aula 1: Introdução ao Linux

Aula 2: Sistema de Arquivos

Aula 3: Instalação Linux

Aula 4: Comandos de Manipulação de Terminal

Aula 5: Editor de arquivos

Aula 6: Histórico e Edição dos Comandos

Aula 7: Criação e Manipulação de arquivos

Aula 8: Processos de Sistema

Aula 9: Usuários e Grupos

Aula 10: Instalação e Gerenciamento de Pacotes do Linux

Aula 11: Localizadores de Arquivos

Aula 12: Comando GREP

Aula 13: Compactadores de Arquivos

Aula 14: Gerenciamento de Sistemas de Arquivos

Aula 15: Montagem e Desmontagem de Sistemas de Arquivos

Aula 16: Monitorando e Consertando Sistemas de Arquivos

Aula 17: Permissões de Arquivos

Aula 18: Introdução a Redes de Computadores

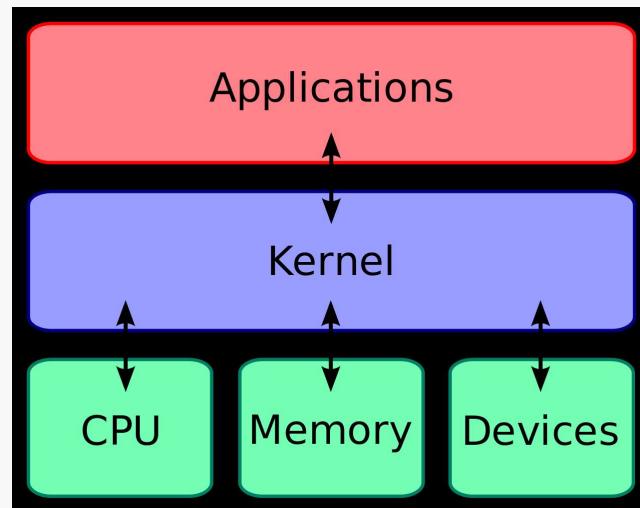
Aula 19: Modelo OSI

Cronograma

- Aula 20:** Protocolos de Rede Parte 1
- Aula 21:** Protocolos de Rede Parte 2
- Aula 22:** Redes Linux Parte 1
- Aula 23:** Redes Linux Parte 2
- Aula 24:** Prática Redes Linux
- Aula 25:** Servidor de Arquivos (SAMBA)
- Aula 26:** Servidor DHCP
- Aula 27:** Compartilhando a Internet
- Aula 28:** Servidor WEB (Apache2 + Php)
- Aula 29:** MariaDB e introdução a Banco de Dados
- Aula 30:** WordPress – Instalando e Administrando
- Aula 31:** Proxy Squid
- Aula 32:** Acesso Remoto
- Aula 33:** DNS – Bind Recursivo e Autoritativo
- Aula 34:** Firewall - Iptables
- Aula 35:** Controlador de Domínio (SAMBA) parte 1
- Aula 36:** Controlador de Domínio (SAMBA) parte 2
- Aula 37:** Controlador de Domínio (SAMBA) parte 3

O que é o Linux?

É o nome dado ao **Kernel** (núcleo) de um sistema operacional.



Criado por **Linus Torvalds**.

Lembre-se: O núcleo do sistema, em resumo é o coração do Sistema Operacional, é o Kernel que é responsável pela comunicação do Software com o Hardware, pelas informações de entrada e saída de dispositivos e interpretar os comandos inseridos pelos usuários.

Um Pouco de História

Transcrição do e-mail original enviado por Torvalds à lista comp.os.minix da USENET

From: torvalds@klaava.Helsinki.FL (Linus Benedict Torvalds)

Newsgroups: comp.os.minix

Subject: what would you like to see most in minix?

Message-ID: 1991Aug25.205708.95@klaava.Helsinki.FL

Date: 25 Aug 91 20:57:08 GMT

Hello everybody out there using minix.

I'm doing a (free) operation system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles is somewhat (same physical layout of the file-system(due to practical reasons) among other things). I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-)

Linus (torvalds@kruuna.helsinki.fi)

PS. Yes – it's free of any minix code, and it has a multi-threaded fs.

It is NOT protable (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.

Um Pouco de História

O Kernel Linux foi desenvolvido e lançado em 1991, baseado em uma distribuição Unix chamada Minix.

Devido ao descontentamento com essa distribuição, Linus resolveu desenvolver o seu próprio sistema.

Linux já possuía alguma melhoria sobre o Kernel do Unix, havia suporte ao disco rígido, tela, teclado e portas seriais, um sistema de arquivos e eram capaz de rodar o bash e o gcc ambos interpretadores de comando.

Um Pouco de História

Inicialmente, Torvalds lançou o Linux sobre uma licença de software livre que proibia qualquer uso comercial, mas isso foi mudado para a licença GNU “General Public License”.

Essa licença permitia que as modificações feitas a partir do Kernel Linux podem ser distribuídas e até mesmo vendidas, mas sempre com o código aberto.

Um Pouco de História

O Linux (Kernel) então é compilado no que nós chamamos de distribuições (Formando o Sistema Operacional).

As primeiras ficaram conhecidas como Debian e Slackware, ambas lançadas no Ano de 1993.

No início, eram difíceis de serem utilizadas, comparadas com o Windows 3.11 e 95, pois exigiam uma série de comandos para serem inicializadas.

Um Pouco de História

Em 1996, muitos integrantes da lista de discussão Linux estavam discutindo sobre a criação de um logotipo ou de um mascote que representasse o Linux.

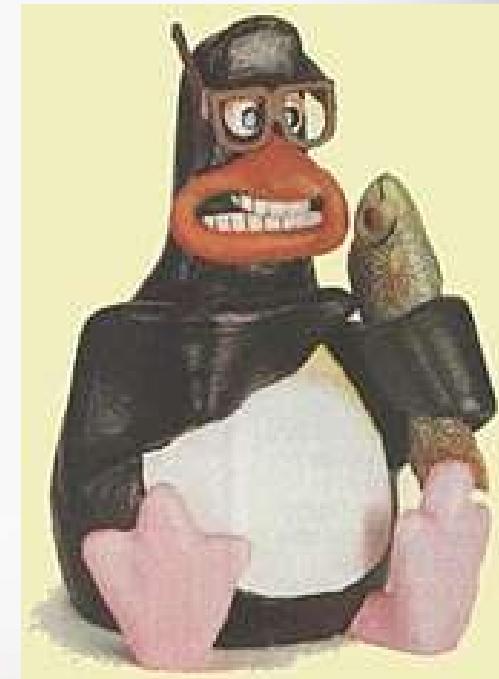
Muitas das sugestões eram paródias ao logotipo de um sistema operacional concorrente e muito conhecido.

Linus Torvalds acabou entrando nesse debate ao afirmar em uma mensagem que gostava muito de pinguins. Isso foi o suficiente para dar fim à discussão.

O mascote TUX Linux



Torvalds UniX.



A "imagem favorita de pinguim" de Linus Torvalds, usada como inspiração para o Tux

Distribuições

O Kernel é o núcleo do Sistema Operacional, ele precisa de uma interface de inserção de comandos, essa interface que pode ser uma tela de comando ou uma interface gráfica.

Essas interfaces criadas para comunicar o usuário ao Kernel são chamadas de **Distribuições**.



Linux Completo + Servidores

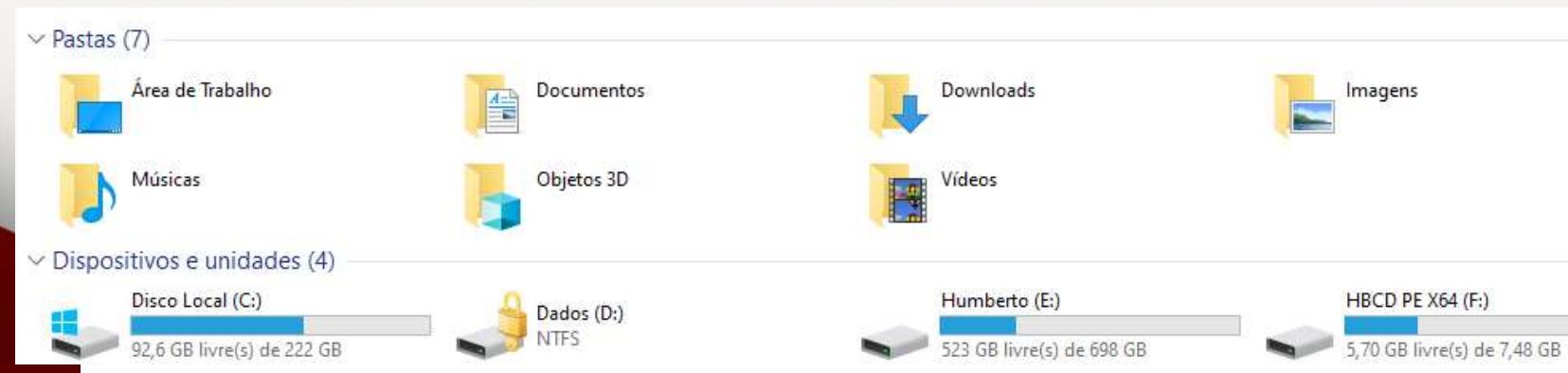
Aula 2: Sistema de Arquivos

Sistema de Arquivos



Se tratando de Windows!

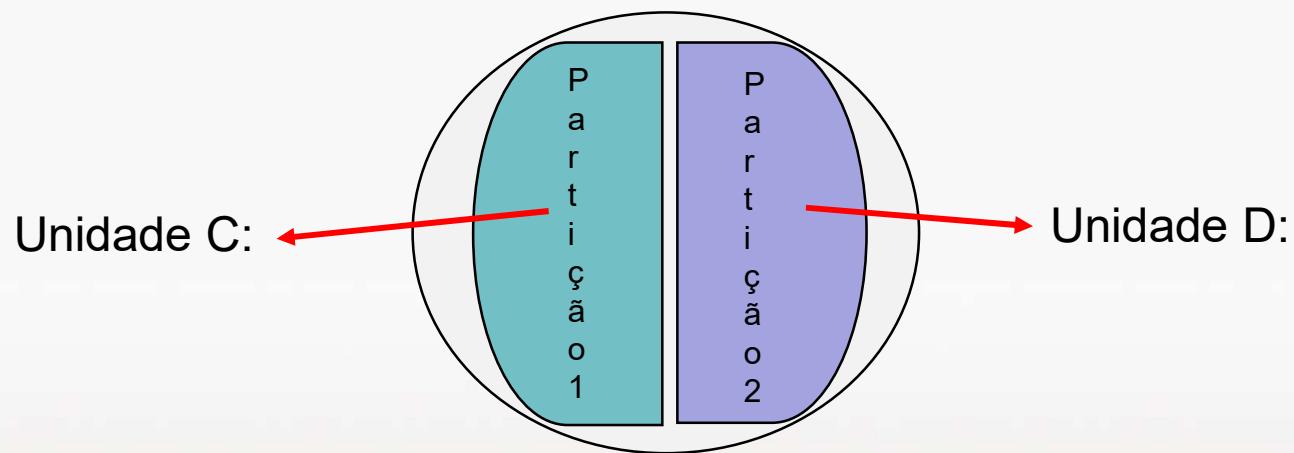
Está é uma visão macro, mas o usuário ainda sabe que ele tem que gravar dentro de um diretório (unidade) C:\D:\E: e em uma pasta



Sistema de Arquivos

Ainda se tratando de Windows!

As unidades de disco ou dispositivos de armazenamento conhecidos como C:\D:\E: ... Na verdade são “atalhos” para acessar uma parte física da sua HD, Pen Drive ou qualquer outros dispositivo de armazenamento e os chamamos de partições.



O Windows, trata suas unidades\partições como:

- A:** - unidade de disquete
- B:** - unidade de disquete
- C:** - unidade de disco rígido
- D:** - unidade de disco rígido
- E:** - unidade de disco rígido ou removível...

Sistema de Arquivos

Agora se tratando de Linux!

A principal diferença é como o Linux reconhece as suas unidades de disco.

Por padrão, o Linux define os arquivos de dispositivos **IDE** da seguinte maneira:

Master primário IDE: **/dev/hda**

Escravo primário IDE: **/dev/hdb**

Master secundário IDE: **/dev/hdc**

Escravo secundário IDE: **/dev/hdd**

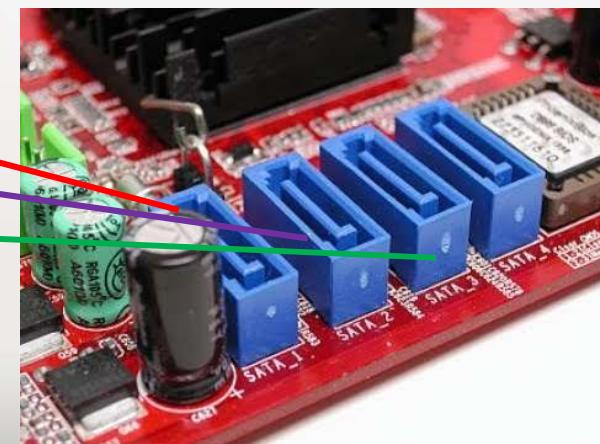


Os arquivos de dispositivos **SCSI ou SATA** são semelhantes, exceto pelo fato de que não há uma limitação de quatro dispositivos:

Primeiro drive SCSI: **/dev/sda**

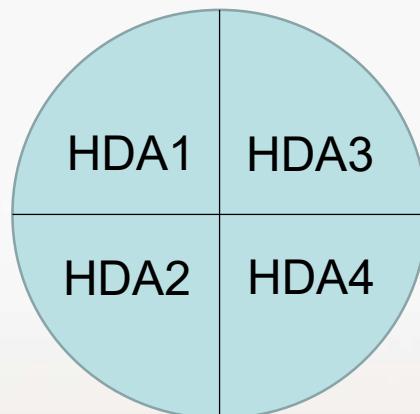
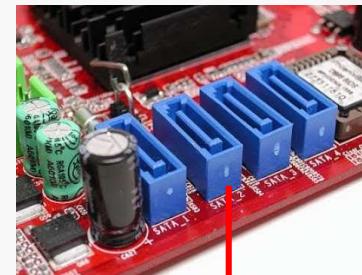
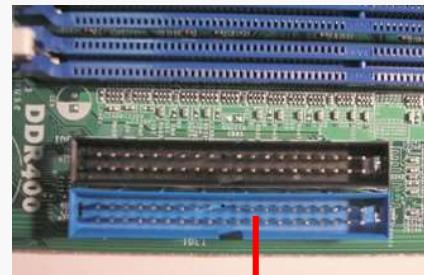
Segundo drive SCSI: **/dev/sbd**

Terceiro drive SCSI: **/dev/sdc**

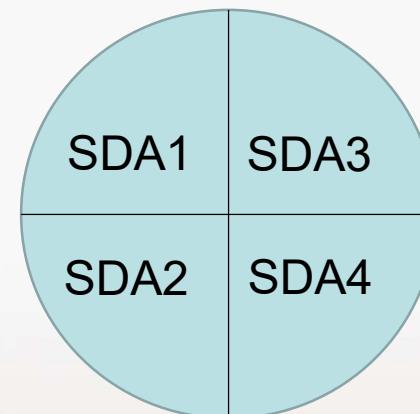


Sistema de Arquivos

Ainda se tratando de Linux!



HDA



SDA

Sistema de Arquivos

Para finalizar Pontos de Montagem\Diretórios

O Linux não trabalha com unidades de disco como o Windows (C:\D:)

O Linux trabalha com **diretórios (pontos de montagem)** e tudo começa com o diretório **/** (raiz)

```
root@debian:/# ls
bin      dev      initrd.img      lib32    lost+found    opt      run      sys      usr      vmlinuz.old
boot     etc      initrd.img.old   lib64    media        proc     sbin     teste     var
dados    home     lib            libx32   mnt         root     srv      tmp      vmlinuz
root@debian:/#
```

E cada um dos diretórios acima, poderia estar em uma partição separada!

```
root@debian:~# df -h -T
Sist. Arq.      Tipo      Blocos de 1K  Usado Disponível Uso% Montado em
udev          devtmpfs      490728       0    490728      0% /dev
tmpfs          tmpfs        101100     1712     99386      2% /run
/dev/sda2        ext4      9546944  871256    8171012     10% /
tmpfs          tmpfs        505528       0    505528      0% /dev/shm
tmpfs          tmpfs        5120        0      5120      0% /run/lock
tmpfs          tmpfs        505528       0    505528      0% /sys/fs/cgroup
/dev/sda1        ext4      89111    46344     36030     57% /boot
/dev/sda3        ext4     19091540   45096   18053576      1% /home
tmpfs          tmpfs       101104       0    101104      0% /run/user/0
root@debian:~#
```

Sistema de Arquivos

É por meio de um sistema de arquivos que ocorre a gravação e a recuperação dos dados em um dispositivo de armazenamento em um computador.

O sistema de arquivos é especificado pelo software do sistema operacional no momento da instalação.

É a forma de organização de dados em algum meio de armazenamento de dados em massa, frequentemente feito em discos magnéticos

O sistema de arquivo que faz o mapeamento do disco rígido permitindo a leitura e gravação.

Sistema de Arquivos

É necessário submeter o disco a um processo denominado formatação lógica para gravar uma estrutura de sistema de arquivos nele.

Esse formato especifica o modo como os arquivos são gravados e recuperados.

OBS: Durante a formatação pode-se encontrar blocos ruins no disco, chamados de blocos defeituosos (bad blocks).

Esses blocos defeituosos são marcados pelo sistema operacional como não utilizável. A presença de muitos blocos defeituosos indica a possibilidade de falha no dispositivo e recomenda-se sua troca.

Sistema de Arquivos (EXT)

É conhecido como “*Extended File System*”.

O sistema ext4 permite gravação de arquivos até 16TB e permite a criação de partições até 1Exabyte.

Suprime a **journaling** que dá suporte ao sistema operacional manter um log (*journal*), de todas as mudanças no sistema de arquivos antes de escrever os dados no disco.

Tipos de Sistemas de Arquivos

O Linux é capaz de montar uma série de sistemas de arquivos, como:

ext2

O sistema de arquivos padrão Linux.

ext3

Um sistema de arquivos com recursos de journaling.

ext4

Um sistema de arquivos com recursos de journaling.

ntfs

A partição nativa do MS Windows.

Tipos de Sistemas de Arquivos

EXT2

O sistema de arquivos ext2 é conhecido como "Second Extended FileSystem". Foi desenvolvido para ser mais "eficiente" que o sistema de arquivos "Minix", seu antecessor.

O Minix era muito utilizado nas primeiras versões do Linux, e foi utilizado por muitos anos.

O sistema de arquivos ext2 não possui journaling e foi substituído pelo ext3.

EXT3

O sistema de arquivos ext3 é uma versão do ext2 com suporte a journaling. Portanto, o ext3 tem características parecidas com o ext2, mas com suporte journaling.

Essa característica foi uma evolução e tornou o ext3 um sistema de arquivos muito estável e robusto.

O sistema ext3 permite gravação de arquivos até 16GB e permite a criação de partições até 2TB.

Tipos de Sistemas de Arquivos

EXT4

O sistema de arquivos ext4 também é atualização do ext3 com suporte a journaling. O sistema ext4 permite gravação de arquivos até 16TB e permite a criação de partições até 1 Exabyte.

Linux Completo + Servidores

Aula 3: Instalação Linux

Debian

Debian é um sistema operacional composto inteiramente de software livre.

O Debian foi lançado em 16 Agosto de 1993 por Ian Murdock, estudante universitário, que escreveu o Manifesto Debian que apelava à criação de uma distribuição GNU/Linux a ser mantida de uma maneira livre, segundo o espírito do GNU.

O Projeto Debian lançou suas versões 0.9x em 1994.

A primeira versão 1.x do Debian aconteceu em 1996, quando **dpkg** ganhou notoriedade.

Debian vem dos nomes dos seus fundadores, Ian Murdock e de sua esposa, Debra

O Debian é especialmente conhecido pelo seu sistema de gestão de pacotes, chamado APT, que permite: atualização, instalação quase sem esforço para novos pacotes e remoção limpa de pacotes antigos.

Debian

É mantido oficialmente pelo Projeto Debian.

O projeto Debian é mantido por meio de doações à organização sem fins lucrativos Software in the Public Interest (SPI).

Várias distribuições comerciais baseiam-se (ou basearam-se) no Debian, incluindo: Linspire (antigo Lindows), Xandros, Knoppix, Kurumin, BrDesktop e Ubuntu.

O Debian possui acesso á repositórios online que contem mais de 51.000 pacotes, fazendo este uma das maiores compilações de software. Oficialmente, Debian contem apenas softwares livres porem softwares não livres também podem ser baixados e instalados em seu repertório. Debian inclui programas populares como LibreOffice, Firefox web browser, K3b disc burner, VLC media player, GIMP image editor, e Evince document viewer.

<https://www.debian.org/distrib/>



Versões do Debian

O ciclo de desenvolvimento das versões do Debian passa por três fases:

"Unstable" - instável

"Testing" - teste

"Stable" - estável

Quando as versões estão na fase "testing" elas são identificadas por codinomes tirados dos personagens do filme Toy Story. Ao se tornarem "stable" as versões recebem um número de versão (ex: 5.0).

Versões, codinomes e datas em que se tornaram "stable":

10.0—Buster, 6 de julho de 2019
9.0—Stretch, 17 de junho de 2017
8.0—Jessie, 25 de abril de 2015
7.0—Wheezy, 4 de maio de 2013
6.0—Squeeze, 6 de fevereiro de 2011
5.0—Lenny, 15 de fevereiro de 2009
4.0—Etch, 8 de abril de 2007

3.1—Sarge, 6 de junho de 2005
3.0—Woody, 19 de junho de 2002
2.2—Potato, 15 de agosto de 2000
2.1—Slink, 9 de março de 1999
2.0—Hamm, 24 de julho de 1998
1.3—Bo, 2 de junho de 1997
1.2—Rex, 1996
1.1—Buzz, 1996

Linux Completo + Servidores

Aula 4: Comandos GNU e Unix

O Linux é **case sensitive**, ou seja ele faz diferença entre maiúsculas e minúsculas.

Usuário **root** (raiz) também representado por **#**

```
root@debian:/# su humberto  
humberto@debian:/$
```

ls	Lista o conteúdo do diretório
ls -l	Lista os arquivos por linha
ls -r	Inverte a ordem de seleção
ls -a	Lista os arquivos ocultos
ls more	Lista pausadamente os arquivos
ls *.extensão_do_arquivo	Lista somente arquivos com uma extensão.

cd nome_da_pasta	Abre uma pasta(diretório)
cd ..	Volta um diretório
cd /	Volta ao diretório padrão do sistema (/)
clear	Limpa a tela do prompt
pwd	Mostra o caminho completo do diretório
mkdir nome_da_pasta	Cria um pasta(diretório)
rmdir nome_da_pasta	Apaga uma pasta(diretório)
cat nome_do_arquivo	Visualiza o conteúdo do arquivo no modo texto

cp - Copia os arquivos

cp arquivo.extensão arquivo1.extensão

Copia o arquivo “**teste.txt**” para “**teste1.txt**”

cp arquivo.extensão /diretório

Copia o arquivo “**teste.txt**” para a pasta **/tmp**

cp * /diretório

Copia todos os arquivos do diretório atual para o diretório especificado.

cp -R /diretório/* /diretório

Copia todos os arquivos e subdiretórios para a pasta especificada.

mv - Move arquivos e diretórios.

mv arquivo.extensão /diretório

Move o arquivo selecionado para o diretório especificado.

mv /diretório/* /diretório

Move todos os arquivos do diretório para o outro especificado.

rm - Apaga um arquivo

rm arquivo.extensão Apaga o arquivo “teste.txt” no diretório atual.

rm *.extensão Apagam os arquivos do diretório atual com a extensão “.txt”

rm –rf diretório/sub-diretório/* Apaga todos os arquivos do diretório e sub-diretório.

rm –rf diretório/sub-diretório Apaga todos os arquivos e o diretório.

Linux Completo + Servidores

Aula 5: Editor de Arquivos

Editores de Arquivos

No Linux existem vários editores de arquivos, por padrão no sistema nós temos o vi.

O código original do vi foi escrito por Bill Joy em 1976, como o modo visual para um editor de linha chamado ex.

vi – Para criar ou abrir um arquivo já existente nós utilizamos o comando:

vi nome_do_arquivo

Opções: para fechar a opção pressionar ESC

i	insere texto a partir do cursor atual
a	insere texto depois do cursor atual
I	insere texto no início da linha
A	insere texto no final da linha
/Expressão	Procura Expressão (que pode ser qualquer palavra) no texto
n	Procura próxima ocorrência de Expressão no texto
N	Procura a ocorrência anterior
v	Seleciona o texto
yy	Copia linha atual do texto para memória
p	Cola conteúdo da memória no texto
dd	Apaga linha atual (e coloca na memória)
u	Desfaz última ação executada
.	Refaz última ação executada
:n	Pula para linha de número n
:w	Salva o arquivo atual
:wq	Salva o arquivo atual e sai do Vi
:q	Sai do Vi
:q!	Sai do Vi, independe de salvar o conteúdo atual

Linux Completo + Servidores

Aula 6: Histórico e Edição dos Comandos

Histórico e Edição dos Comandos

Trabalhando com um prompt de comando pode ser necessário e interessante consultar ou até mesmo repetir um determinado comando executado.

Os shells modernos, como o **bash**, incluem um importante conjunto de recursos chamados de histórico, expansão e edição dos comandos.

A primeira parte desse conjunto é o histórico.

A lista de históricos é controlada pela variável de shell HISTSIZE.

Por padrão é definida com 500 linhas.

Podemos consultar o tamanho da variável lendo ela com o comando:
echo \$HISTSIZE

```
root@debian:~# echo $HISTSIZE  
500
```

Para visualizar o seu histórico de comandos, use o comando **history**.

Haverá um número de linha antes de cada comando.

Esse número poderá ser usado posteriormente na expansão do histórico.

```
550 ps aux |more
551 ps aux | grep -i net
552 ps aux | grep -i samba
553 clear
554 ps aux | grep -i samba
555 dmesg |more
556 dmesg |more grep -i eth0
557 dmesg | grep -i eth0
558 clear
559 dmesg | grep -i eth0
560 dmesg | grep -i samba
561 dmesg | grep -i smb
562 dmesg | grep -i apache
563 dmesg | grep -i net
564*
565 dmesg | grep -i smb
566 echo $PS1
567 echo $PATH
568 echo $HISTSIZE
569 cd ~.
570 cd /
571 find -name bash*
572 find -name *history
573 history
root@saturno:/# history_
```

Designadores de expansão de histórico:

Designador	Descrição
!!	Refere-se ao ultimo comando executado
!n	Refere-se ao comando n do histórico, use o comando history para exibir esses números
!string	Refere-se ao comando mais recente que comece com string
!?string	Refere-se ao comando mais recente que contenha a string

Linux Completo + Servidores

Aula 7: Criação e Manipulação de arquivos

Digitando sequencia de comandos

Pode acontecer de surgir à necessidade de digitar dois comandos na mesma linha do prompt, o Linux permite essa opção, mas os comandos devem ser separados por ;

Exemplo:

```
# ls ; ps
```

touch

O comando **touch** é utilizado para criar arquivos vazios e alterar o registo de data e hora dos arquivos.

```
root@debian:~# touch teste  
root@debian:~# ls
```

Ele também pode criar vários arquivos de uma vez

```
root@debian:~# touch teste1 teste2 teste3 teste4  
root@debian:~# ls
```

touch

O comando **touch** modifica a data e hora de acesso e modificação de arquivos.

Você pode modificar tanto a hora de acesso quanto a hora de modificação dos arquivos, ou os dois ao mesmo tempo.

Legenda:

A - ano (é considerado a faixa de 1969-2068)

M - mês

D - dia

h - Hora

m - minutos

s - segundos

Para modificarmos a data e hora de acesso e modificação de um arquivo basta fazermos o seguinte:

touch -t AAAAMMDDhhmm arquivo

touch

```
root@terceiro:/dados# ls -l  
total 4  
-rw-r--r-- 1 root root 6 Dez 6 11:37 teste
```

```
root@terceiro:/dados# touch -t 198409201420 teste  
root@terceiro:/dados# ls -l  
total 4  
-rw-r--r-- 1 root root 6 Set 20 1984 teste
```

Para mudar a data e a hora de modificação para a atual, utilize a opção **-m**

Linux Completo + Servidores

Aula 8: Processos de Sistema

ps

O comando **ps** exibe informações sobre os processos que estão executando na máquina

Opções:

- a : mostra os processos de todos os usuários.
- A : mostra todos os processo.
- f : mostra a árvore de execução de comandos.
- x : mostra os processos que não foram iniciados no console.
- u : fornece o nome do usuário e a hora de início do processo.

```
root@debian:~# ps -au
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START  TIME COMMAND
root      380  0.0  0.3    6924  3396 tty1      Ss  11:53  0:00 /bin/login -p --
root      510  0.0  0.4    7652  4420 tty1      S   11:53  0:00 -bash
root      519  0.0  0.3    6924  3404 tty2      Ss  11:54  0:00 /bin/login -p --
humberto  530  0.0  0.4    7652  4464 tty2      S   11:54  0:00 -bash
humberto  533  0.1  0.3   10960  3616 tty2      S+  11:55  0:00 top
root      542  0.0  0.3   10632  3124 tty1      R+  11:58  0:00 ps -au
root@debian:~#
```

top

O comando **top** oferece uma saída semelhante à **ps**, porém em uma exibição continuamente atualizada.

Isso é útil em situações nas quais você precisa monitorar o status de um ou mais processos ou para ver como eles estão usando o seu sistema.

Opções:

-i

Ignora os processos ociosos, listando apenas os em execução.

top - 12:44:28 up 1:17, 1 user, load average: 0,00, 0,01, 0,03											
Tasks: 64 total, 1 running, 63 sleeping, 0 stopped, 0 zombie											
%Cpu(s): 0,0 us, 0,0 sy, 0,0 ni, 100,0 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st											
KiB Mem: 508892 total, 99916 used, 408976 free, 11520 buffers											
KiB Swap: 901116 total, 0 used, 901116 free, 52028 cached											
PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
16	root	20	0	0	0	0	S	0,3	0,0	0:01.86	kworker/0:1
2800	root	20	0	23172	1512	1128	R	0,3	0,3	0:00.31	top
1	root	20	0	10648	828	696	S	0,0	0,2	0:00.36	init
2	root	20	0	0	0	0	S	0,0	0,0	0:00.00	kthreadd
3	root	20	0	0	0	0	S	0,0	0,0	0:00.35	ksoftirqd/0
6	root	rt	0	0	0	0	S	0,0	0,0	0:00.00	migration/0
7	root	rt	0	0	0	0	S	0,0	0,0	0:00.08	watchdog/0
8	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	cpuset
9	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	khelper
10	root	20	0	0	0	0	S	0,0	0,0	0:00.00	kdevtmpfs
11	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	netns
12	root	20	0	0	0	0	S	0,0	0,0	0:00.04	sync_supers
13	root	20	0	0	0	0	S	0,0	0,0	0:00.00	bdi-default
14	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	kintegrityd
15	root	0	-20	0	0	0	S	0,0	0,0	0:00.00	kblockd
17	root	20	0	0	0	0	S	0,0	0,0	0:00.00	khungtaskd
18	root	20	0	0	0	0	S	0,0	0,0	0:00.00	kswapd0
19	root	25	5	0	0	0	S	0,0	0,0	0:00.00	ksmd

kill

Em sua simples forma o kill é usado para parar um processo imediatamente. Basta inserir o número do processo que tem que ser finalizado.

```
# kill 1000
```

```
root@terceiro:~# ps
  PID TTY      TIME CMD
 2472 tty1    00:00:00 login
 2625 tty1    00:00:00 bash
 2676 tty1    00:00:00 ps
root@terceiro:~# kill 2472
```

OBS: Ocasionalmente com o comando **ps** ou **top** um processo pode estar marcado como zumbi, são processos que ficaram travados ao tentar terminar, assim como nos filmes, não é possível matar um processo zumbi porque ele já está morto.

```
top - 19:33:28 up 2:11, 4 users, load average: 0.15, 1.00, 2.01
Tasks: 133 total, 3 running, 129 sleeping, 0 stopped, 1 zombie
Cpu(s): 4.0%us, 0.7%sy, 0.0%ni, 94.4%id, 0.7%wa, 0.0%hi, 0.3%si, 0.0%st
Mem: 1026516k total, 1005576k used, 20940k free, 18156k buffers
Swap: 1461904k total, 179036k used, 1282868k free, 540256k cached
```

free

Esse comando exibe a quantidade de memória livre e usada do sistema.

Opções:

-b

Mostra o uso da memória em bytes.

-k

Mostra o uso da memória em kilobytes.

-m

Mostra o uso da memória em megabytes

```
root@terceiro:/dados# free
              total        used        free      shared  buffers   cached
Mem:       508892       99908     408984          0     11520    52028
 -/+ buffers/cache:     36360     472532
Swap:      901116          0     901116
root@terceiro:/dados# free -m
              total        used        free      shared  buffers   cached
Mem:         496         97        399          0         11        50
 -/+ buffers/cache:     35        461
Swap:        879          0        879
root@terceiro:/dados# _
```

uptime

O comando **uptime** mostra as seguintes informações:

A hora atual, quanto tempo o sistema está rodando e quantos usuários estão logados no momento e as médias de carga no sistema (processamento) nos últimos 1, 5 e 15 minutos.

```
root@terceiro:/dados# uptime  
12:48:15 up 1:21, 1 user, load average: 0,00, 0,01, 0,03
```

Desligando e reiniciando o Linux modo texto

shutdown tempo_em_minutos -r	reiniciar
shutdown tempo_em_minutos -h	desligar
halt	para o sistema operacional
reboot	reinicializa o computador imediatamente

Linux Completo + Servidores

Aula 9: Usuários e Grupos

Usuários e Grupos

No Linux, existem 3 tipos de usuários: **Administrador**, **Comum** e de **Sistema**.

Um usuário **administrador** tem permissão total de utilização do sistema.

Esse usuário pode criar pastas/arquivos em qualquer diretório, além de poder editar e excluir qualquer arquivo de qualquer usuário ou de sistema.

Esse usuário pode executar, também, qualquer comando disponível no sistema operacional.

Um usuário **comum** tem algumas restrições na utilização do sistema, não podem executar todos os comandos, configurações ou acessar qualquer diretório.

Um usuário de **sistema** é um usuário criado durante a instalação de algum programa ou serviço para executar tarefas específicas daquele programa.

Não é possível logar no sistema utilizando este usuário.

Usuários e Grupos

adduser nome_do_usuário

cria um novo usuário

userdel nome_do_usuário

apaga um usuário

passwd nome_do_usuário

trocara ou define uma nova senha

logname

mostra o usuário logado no terminal aberto

users

mostra todos os usuários conectados no sistema

Usuários e Grupos

groupadd nome_do_grupo

Cria um novo grupo

adduser usuário grupo

Adiciona um usuário a um grupo

groups nome_do_usuário

Mostra os grupos desse usuário

As informações sobre os grupos e seus usuários ficam salvas em **/etc/group**.

Neste arquivo é possível adicionar um usuário a um grupo manualmente, é necessário colocar uma vírgula seguida do nome do usuário que deseja acrescentar:

```
root:x:0:  
daemon:x:1:  
bin:x:2:  
sys:x:3:  
adm:x:4:  
tty:x:5:  
disk:x:6:  
lp:x:7:  
mail:x:8:  
news:x:9:  
uucp:x:10:  
man:x:12:  
proxy:x:13:  
kmem:x:15:  
dialout:x:20:  
fax:x:21:  
voice:x:22:  
cdrom:x:24:humberto  
floppy:x:25:humberto  
tape:x:26:  
sudo:x:27:  
audio:x:29:humberto
```

Usuários e Grupos

Os usuários são cadastrados no sistema através do arquivo **/etc/passwd**.

Acessando este arquivo você verá as informações:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin.sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110.:/nonexistent:/usr/sbin/nologin
humberto:x:1000:1000:Humberto Forsan,,,:/home/humberto:/bin/bash
```

Usuários e Grupos

```
root:x:0:0:root:/root:/bin/bash
```

Descriptivo:

root – Nome de login do usuário

x – Indica que a senha do usuário está localizada no arquivo /etc/shadow (criptografada)

0 – UID do usuário

0 – GID do usuário

/root – Diretório HOME do usuário.

/bin/bash – Shell do usuário, o programa interpretador de comandos.

Para usuários comuns, ainda pode aparecer:

,,, – Informações do usuário, como nome, telefone...

Usuários e Grupos

O arquivo **/etc/shadow** é utilizado para armazenar as senhas dos usuários no linux, de maneira criptografada.

Também armazena informações sobre datas de expiração e validade das contas.

```
root:$6$Du2WOGD8isTyRwAo$3P9SxpjLF3gLnJi/oc631eY1yFK007h20SR6WGHajw9uIieGVbIx3KPEXHhp.u173XkqM7k51Gb
oJK2Gi3Kxo.:18422:0:99999:7:::
daemon:*:18422:0:99999:7:::
bin:*:18422:0:99999:7:::
sys:*:18422:0:99999:7:::
sync:*:18422:0:99999:7:::
games:*:18422:0:99999:7:::
man:*:18422:0:99999:7:::
lp:*:18422:0:99999:7:::
mail:*:18422:0:99999:7:::
news:**:18422:0:99999:7:::
uucp:**:18422:0:99999:7:::
proxy:**:18422:0:99999:7:::
www-data:**:18422:0:99999:7:::
backup:**:18422:0:99999:7:::
list:**:18422:0:99999:7:::
irc:**:18422:0:99999:7:::
gnats:**:18422:0:99999:7:::
nobody:**:18422:0:99999:7:::
_apt:**:18422:0:99999:7:::
systemd-timesync:**:18422:0:99999:7:::
systemd-network:**:18422:0:99999:7:::
systemd-resolve:**:18422:0:99999:7:::
messagebus:**:18422:0:99999:7:::
humberto:$6$GTmzmnI/RYT319mN$Dvf0ReaoWS/DnxFKSSTA4mAP2QTpW2oYB6RSbS/j6fI8q3nv4J09mydmZu20yggyzICacB0b
C4w0ubk94LqojQ.:18422:0:99999:7:::
:-coredump:!!!:18422:::::::
```

Usuários e Grupos

/etc/shadow

```
root:$6$Du2W0GD8isTyRwAo$3P9SxpjLF3gLnJi/oc631eYlyFK007h20SR6WGhAjw9uIieGVbIx3KPEXHhp.ui73XkqM7k51Gb
oJK2Gi3Kxo.:18422:0:99999:7:::
```

Desritivo:

root – Nome de login do usuário

\$6\$Du2W0... – Indica a senha do usuário criptografada.

18422 – Data da ultima alteração de senha, armazenada como o número de dias decorridos desde 01/01/1970.

0 – Dias até que a senha possa ser alterada novamente

99999 - Dias antes que uma alteração seja necessária.

7 - Dias de avisos antes da expiração da senha

Algumas distribuições podem ainda usar os 3 últimos campos que são, **Dias entre expiração e desativação**, **Data de expiração**, **Flag especial** (campo reservado).

Linux Completo + Servidores

Aula 10: Instalação e Gerenciamento de Pacotes do Linux

Gerenciar Bibliotecas Compartilhadas

Quando um programa é compilado no Linux, muitas das funções requeridas pelo programa são vinculadas a partir de bibliotecas de sistema que lidam com discos, com a memória e com outras funções.

Por exemplo, quando a função printf() da linguagem C padrão é usado em um programa, o programador não fornece o código fonte de printf(), mas, em vez disso, espera que o sistema já possua uma biblioteca contendo esse tipo de função.

Programas utilizam as rotinas do sistema, mas não incorporam o código das bibliotecas. Em vez disso, esse código é vinculado ao executável no momento da execução.

Esse processo de vinculação são compartilhadas entre muitos aplicativos e, por isso, são chamadas de bibliotecas compartilhadas.

Dependências de Bibliotecas Compartilhadas

Qualquer programa que esteja dinamicamente vinculado precisará de pelo menos algumas poucas bibliotecas compartilhadas. Se a biblioteca requerida não existir ou não puderem ser conectadas, o programa não poderá rodar.

Isso poderia acontecer, por exemplo, se você tentar rodar um aplicativo escrito para o ambiente gráfico GNOME sem ter instalado as bibliotecas GTK+ requeridas.

Instalar as bibliotecas corretas deve ser o suficiente para eliminar tais problemas.

l~~d~~~~d~~

O utilitário **l~~d~~~~d~~** pode ser usado para se determinar quais bibliotecas são necessárias para um executável específico.

Exemplo:

O **top** requer 12 bibliotecas compartilhadas:

```
root@debian:/bin# ldd top
    linux-vdso.so.1 (0x00007ffd6f8cb000)
    libprocps.so.7 => /lib/x86_64-linux-gnu/libprocps.so.7 (0x00007f8f63ad8000)
    libncurses.so.6 => /lib/x86_64-linux-gnu/libncurses.so.6 (0x00007f8f63aa8000)
    libtinfo.so.6 => /lib/x86_64-linux-gnu/libtinfo.so.6 (0x00007f8f63a78000)
    libdl.so.2 => /lib/x86_64-linux-gnu/libdl.so.2 (0x00007f8f63a70000)
    libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f8f638a8000)
    libsystemd.so.0 => /lib/x86_64-linux-gnu/libsystemd.so.0 (0x00007f8f63800000)
    /lib64/ld-linux-x86-64.so.2 (0x00007f8f63f50000)
    librt.so.1 => /lib/x86_64-linux-gnu/librt.so.1 (0x00007f8f637f0000)
    liblzma.so.5 => /lib/x86_64-linux-gnu/liblzma.so.5 (0x00007f8f637c8000)
    liblz4.so.1 => /lib/x86_64-linux-gnu/liblz4.so.1 (0x00007f8f637a8000)
    libgcrypt.so.20 => /lib/x86_64-linux-gnu/libgcrypt.so.20 (0x00007f8f63688000)
    libpthread.so.0 => /lib/x86_64-linux-gnu/libpthread.so.0 (0x00007f8f63660000)
    libgpg-error.so.0 => /lib/x86_64-linux-gnu/libgpg-error.so.0 (0x00007f8f63638000)
```

O **cat** requer 1 biblioteca compartilhada:

```
root@debian:/bin# ldd cat
    linux-vdso.so.1 (0x00007ffebcbcbeb000)
    libc.so.6 => /lib/x86_64-linux-gnu/libc.so.6 (0x00007f4ac41d8000)
    /lib64/ld-linux-x86-64.so.2 (0x00007f4ac43b8000)
```

Visão geral do gerenciamento de pacotes do Debian

Cada pacote do Debian contém arquivos de programas, configurações, documentação e indicação de dependências. Os nomes dos pacotes do Debian possuem três elementos em comum, incluindo:

Nome do pacote

Um nome de pacote do Debian é sempre curto e descritivo e quando várias palavras são usadas elas são separadas por hifens.

Número da versão

Cada pacote tem uma versão. A maioria das versões dos pacotes tem o mesmo número que o software que elas contêm.

Extensão do arquivo

Por padrão todos os pacotes do Debian terminam com a extensão .deb

Exemplo: nano-tiny_2.2.4-1_amd64.deb

Gerenciando os pacotes do Debian

No início havia o **.tar.gz**. Os usuários tinham de penar para compilar cada programa usado em seu sistema GNU/Linux

Quando o Debian foi criado, sentiu-se a necessidade de um sistema de gerenciamento de pacotes instalados no sistema.

Deu-se a esse sistema o nome de **dpkg**. Logo após a Red Hat resolveu criar seu conhecido sistema **rpm**.

Rapidamente outro dilema tomou conta das mentes dos produtores de GNU/Linux. Uma maneira rápida, prática e eficiente de se instalar pacotes, gerenciando suas dependências automaticamente e tomando conta de seus arquivos de configuração ao atualizar.

Assim, o Debian, criou o **APT** ou **Advanced Packaging Tool**

Gerenciando os pacotes do Debian

A ferramenta original de gerenciamento de pacotes do Debian é **dpkg**, que opera diretamente sobre os arquivos de pacotes **.deb** e pode ser usada para automatizar a instalação e a manutenção dos pacotes de software.

A ferramenta alternativa **apt** opera usando nomes de pacotes, obtendo-os a partir de uma fonte predefinida (CD-ROMS e sites FTP).

O comando **alien** permite o uso de pacotes não Debian, tais como o formato RPM do Red Hat.

dpkg

Sintaxe:

dpkg opções ação

O comando dpkg mantém informações sobre os pacotes em /var/lib/dpkg. Há dois arquivos que são de particular interesse:

available

É a lista de todos os pacotes disponíveis.

status

Contém atributos dos pacotes, tais como se um determinado pacote está instalado ou se está marcado para remoção.

Esses arquivos são modificados por **dpkg** e **apt-get**

dpkg

Opções:

-E

Instrui o comando a não sobrescrever um pacote instalado, da mesma versão.

-G

Instrui o comando a não sobrescrever um pacote instalado com uma versão mais antiga.

--configure package

Configura um pacote descompactado.

-i package_file

Instala o respectivo pacote.

--purge package

Remove tudo a respeito de package.

-r package

Remove tudo, exceto os arquivos de configuração.

-s package

Relata o status do package.

dpkg

Listando pacotes instalados com o dpkg:

```
# dpkg --get-selections
```

```
aspell-pt-br                               install
at                                         install
base-files                                install
base-passwd                               install
bash                                       install
bash-completion                           install
bc                                         install
bind9-host                                 install
bsd-mailx                                 install
bsdmainutils                             install
bsdutils                                  install
busybox                                   install
root@debian:/etc/apt# dpkg --get-selections |more
```

APT

Sintaxe:

`apt-get opções nome do pacote`

Ele não trabalha diretamente com os arquivos .deb como o dpkg, mas usa, em vez disso, nomes de pacotes .apt-get, além de fazer a configuração automática das dependências do pacote.

-d

Faz o download de arquivos, mas não instala.

-s

Simula os passos em uma modificação de pacotes, mas não modifica realmente o sistema.

-y

Responde “yes” as todas as perguntas do prompt.

-dist-upgrade

Faz upgrade do Debian.

install

Instala ou faz upgrade de pacotes mais novos.

remove

Remove os pacotes especificados.

update

Obtém uma lista atualizada de pacotes disponíveis para o APT-GET.

upgrade

Faz upgrade do conjunto de pacotes instalados no sistema.

APT

OBS: O apt-get usa o arquivo **/etc/apt/sources.list** para determinar de onde os pacotes deverão ser obtidos.

Exemplo Arquivo sources.list

```
# deb cdrom:[Debian GNU/Linux 10.3.0 _Buster_ - Official amd64 DVD Binary-1 20200208-12:08]/ buster
contrib main

#deb cdrom:[Debian GNU/Linux 10.3.0 _Buster_ - Official amd64 DVD Binary-1 20200208-12:08]/ buster c
ontrib main

deb http://deb.debian.org/debian/ buster main
deb-src http://deb.debian.org/debian/ buster main

deb http://security.debian.org/debian-security buster/updates main contrib
deb-src http://security.debian.org/debian-security buster/updates main contrib

# buster-updates, previously known as 'volatile'
deb http://deb.debian.org/debian/ buster-updates main contrib
deb-src http://deb.debian.org/debian/ buster-updates main contrib
~
~
~
```

APT

apt-cache search nome_do_programa

```
root@saturno:/bin# apt-cache search samba_
```

```
gnome-system-tools - utilitários de configuração interplataformas para o GNOME
ldap-account-manager - interface web para gerenciar contas num diretório LDAP
libwbclient0 - biblioteca do cliente Samba winbind
php-auth - módulos PHP PEAR para criar um sistema de autenticação
samba - servidor de login, impressão e arquivos SMB/CIFS para Unix
samba-common - arquivos comuns usados tanto pelo servidor quanto pelo cliente Sa
mba
samba-common-bin - arquivos comuns usados tanto pelo servidor quanto pelo client
e Samba
slapd-smbk5pwd - mantém senhas Kerberos e Samba em sincronia com slapd
smbclient - clientes SMB/CIFS em linha de comando para Unix
snort - sistema de detecção de intrusos de rede flexível
winbind - servidor de integração de serviços de nome Samba
root@saturno:/bin# _
```

ALIEN

Comando converte ou instala um pacote não Debian. Os tipos de pacotes suportados incluem o .rpm do Red Hat, o .slp do Stampede, o .tgz do Slackware, além de arquivos .tar.gz genéricos.

O RPM tem que estar instalado no seu sistema para poder fazer a conversão.

Opções:

- i Instala automaticamente o pacote gerado.
- r Converte o pacote para RPM.
- t Converte o pacote em um arquivo gzip tar.
- d Converte o pacote para DEB.

Exemplo:

Instalar automaticamente um pacote não Debian em um sistema Debian

alien –i package.rpm

Linux Completo + Servidores

Aula 11: Localizadores de Arquivos

find

O comando find, realiza a busca de arquivos pelo seu nome, podemos utilizar a sintaxe abaixo:

```
root@debian:/# find -name linux.doc  
./teste/linux.doc
```

Podemos listar todos os arquivos contidos em um diretório junto com os seus subdiretórios utilizando a sintaxe:

```
root@debian:/teste# find .  
.  
./humberto.doc  
./linux.doc  
./humberto2.doc  
./teste2  
./teste2/humberto.doc  
./teste2/humberto2.doc
```

find

Com o comando find também podemos listar somente arquivos ou somente diretórios com a opção -type f para arquivos e -type d para diretórios:

```
root@debian:/teste# find . -type f
./humberto.doc
./linux.doc
./humberto2.doc
./teste2/humberto.doc
./teste2/humberto2.doc
root@debian:/teste# find . -type d
.
./teste2
root@debian:/teste#
```

locate

O comando locate utiliza uma base indexada para localização de arquivos.

Antes de sua utilização é necessário construir esta base com o comando
updatedb.

Na primeira execução deste comando é criada a base e todo o hd é varrido para a construção da base e de sua indexação.

locate

Por questões de performance e segurança, este comando não indexa diretórios temporários, diretórios pessoais (/home, /root) e sistemas de arquivos remotos (mapeamentos).

Qualquer pesquisa realizada por qualquer usuário somente retornará os dados a que o usuário tiver permissão de acesso.

```
root@lpic101:/dados# locate **  
/dados/x.txt  
/dados/xh  
/dados/xy.txt  
/dados/xyz.txt  
/etc/X11/Xsession.d/35x11-common_xhost-local  
/lib/modules/3.2.0-4-486/kernel/drivers/usb/host/xhci-hcd.ko  
/lib/modules/3.2.0-4-486/kernel/sound/pci/pcxhr  
/lib/modules/3.2.0-4-486/kernel/sound/pci/pcxhr/snd-pcxhr.ko  
/usr/share/bash-completion/completions/xhost  
/usr/share/i18n/locales/xh_ZA  
/usr/share/locale/xh  
/usr/share/locale/xh/LC_MESSAGES  
/usr/share/locale/xh/LC_MESSAGES/iso_3166.mo  
/usr/share/locale/xh/LC_MESSAGES/iso_639.mo  
/usr/share/locale/xh/LC_MESSAGES/iso_639_3.mo  
/usr/share/locale/xh/LC_MESSAGES/newt.mo  
/usr/src/linux-headers-3.2.0-4-686-pae/include/config/snd/pcxhr.h  
/usr/src/linux-headers-3.2.0-4-686-pae/include/config/usb/xhci  
/usr/src/linux-headers-3.2.0-4-686-pae/include/config/usb/arch/has/xhci.h  
/usr/src/linux-headers-3.2.0-4-686-pae/include/config/usb/xhci/hcd.h
```

Linux Completo + Servidores

Aula 12: Comando GREP

grep

Muitas vezes, precisamos localizar um arquivo pelo seu conteúdo e não apenas pelo seu nome. Para isso utilizamos o comando grep.

grep

Sintaxe:

grep opções filtro-a-aplicar arquivo

Exemplo: Localizar a ocorrência “ldap” dentro do arquivo /etc/services:

grep “ldap” /etc/services

```
root@saturno:/etc# grep "ldap" /etc/services
ldap          389/tcp          # Lightweight Directory Access Protocol
ldap          389/udp
ldaps         636/tcp          # LDAP over SSL
ldaps         636/udp
root@saturno:/etc# _
```

grep

Outro exemplo pode se a pesquisa por ocorrências em letras maiúsculas ou minúsculas com a opção **-i**

```
grep -i "name" /etc/services
```

```
root@saturno:/etc# grep -i "name" /etc/services
nameserver      42/tcp          name          # IEN 116
whois           43/tcp          nickname
domain          53/tcp          hostname       # Domain Name Server
hostnames        101/tcp         cso-ns        # also used by CSD name server
csnet-ns         105/tcp         # NETBIOS Name Service
netbios-ns       137/tcp         # AppleTalk name binding
at-nbp           202/tcp         # Name Binding Protocol
#> Ports are used in the TCP [45,106] to name the ends of logical
nbp              2/ddp          # Name Binding Protocol
root@saturno:/etc# _
```

grep

Utilizando o grep também podemos destacar a cor do item procurado como no exemplo abaixo, utilizando **--color** :

```
root@debian:/teste# grep "teste" --color humberto.doc
teste
root@debian:/teste# grep -i "teste" --color humberto.doc
teste
TESTE
root@debian:/teste#
```

Também é útil saber em qual linha se encontra a ocorrência, para isso adicionamos a opção **-n**

```
root@debian:/teste# grep -i "teste" --color -n humberto.doc
5:teste
6:TESTE
root@debian:/teste#
```

Podemos ainda utilizar um caractere coringa como o * para realizar a busca em vários arquivos:

```
root@debian:/teste# grep -i "teste" --color -n *.doc
humberto2.doc:5:teste
humberto2.doc:6:TESTE
humberto.doc:5:teste
humberto.doc:6:TESTE
root@debian:/teste#
```

grep

Podemos realizar a pesquisa recursiva, isso é, realizando a busca em sub-diretórios **-r**:

```
root@debian:/teste# grep -r -i "teste" --color -n *.doc
humberto2.doc:5:teste
humberto2.doc:6:TESTE
humberto.doc:5:teste
humberto.doc:6:TESTE
root@debian:/teste#
```

Outro recurso do grep é a opção **-w** aonde será eliminado os resultados que conterem números, trazendo ocorrências que somente tiverem textos:

```
root@debian:/teste# grep -r -i -w "teste" --color -n *.doc
humberto2.doc:5:teste
humberto2.doc:6:TESTE
root@debian:/teste# grep -r -i "teste" --color -n *.doc
humberto2.doc:5:teste
humberto2.doc:6:TESTE
humberto.doc:5:teste1
humberto.doc:6:TESTE2
root@debian:/teste#
```

grep

Podemos solicitar que o comando grep conte o número de ocorrências da string com a opção **-c**

```
root@debian:~# cat teste1.txt
teste
Humberto
Linux
Debian

teste
TESTE

São Paulo

teste2
root@debian:~# grep -c teste teste1.txt
3
root@debian:~#
```

grep

-o mostra somente o texto que coincide com a string

```
root@debian:~# cat teste1.txt
teste
Humberto
Linux
Debian

teste
TESTE

São Paulo

teste2
root@debian:~# grep -o teste teste1.txt
teste
teste
teste
root@debian:~#
```

grep

-B "n" mostra as linhas N antes da string

```
root@debian:~# cat teste1.txt
teste
Humberto
Linux
Debian

teste
TESTE
São Paulo

teste2
root@debian:~# grep -B 2 Debian teste1.txt
Humberto
Linux
Debian
root@debian:~#
```

grep

-A "n" mostra as linhas N depois da string

```
root@debian:~# cat teste1.txt
```

teste

Humberto

Linux

Debian

teste

TESTE

São Paulo

teste2

```
root@debian:~# grep -A 3 Debian teste1.txt
```

Debian

teste

```
root@debian:~#
```

grep

-C uni as duas opções, pegando e imprimindo linhas antes e depois da linha que contem a string pesquisada.

```
root@debian:~# cat teste1.txt
teste
Humberto
Linux
Debian

teste
TESTE

São Paulo

teste2
root@debian:~# grep -C 3 Debian teste1.txt
teste
Humberto
Linux
Debian

teste
root@debian:~#
```

grep

-l Mostra somente o arquivo, não a string

```
root@debian:~# ls
nano-tiny_4.9.3-1_amd64.deb  nano.txt  teste1.txt  teste3.jpg
nano-tiny_4.9.3-1_i386.deb    teste      teste2.doc  teste5.txt
root@debian:~# grep -l Debian teste*
teste1.txt
root@debian:~#
```

grep

-L retorna os arquivos que não possuem a string pesquisada

```
root@debian:~# ls
nano-tiny_4.9.3-1_amd64.deb  nano.txt  teste1.txt  teste3.jpg
nano-tiny_4.9.3-1_i386.deb   teste      teste2.doc  teste5.txt
root@debian:~# grep -L Debian teste*
teste
teste2.doc
teste3.jpg
teste5.txt
root@debian:~#
```

grep

Com o grep, também é possível realizar buscas utilizando o que chamamos de Expressões Regulares

Para isso utilizamos a opção **-E**

```
root@debian:~# grep -E -i "teste|humberto" teste1.txt
teste
Humberto
teste
TESTE
teste2
root@debian:~#
```

```
root@debian:~# grep -E -lir "teste|humberto|araras" /root
/root/teste2.doc
/root/teste1.txt
/root/nano.txt
root@debian:~#
```

A opção | funciona como se fosse um “OU”

grep

```
root@debian:~# grep -E -lir "\.ste|humberto|araras" /root  
/root/teste2.doc  
/root/teste1.txt  
/root/nano.txt  
root@debian:~#
```

A opção **** funciona substituindo o texto.

```
root@debian:~# grep -E -lir "\.ste|humberto|araras" /root  
/root/teste2.doc  
/root/teste1.txt  
root@debian:~#
```

A opção **** funciona como um “escape” para que possa entender o **.** no exemplo

grep

Usando direto e com pipe

O comando grep pode ser utilizado junto com outro comando, utilizando o **pipe**

```
root@debian:~# cat teste2.doc | grep -i araras
Araras
root@debian:~#
```

Linux Completo + Servidores

Aula 13: Compactadores de Arquivos

Comando Tar (Compactador de Arquivos)

O Tar (Tape Archive) é o que faz o empacotamento com a extensão .tar

A sintaxe do Tar é a seguinte:

```
tar [parâmetros] [nome_do_arquivo_tar] [arquivos_de_origem]
```

EXEMPLO: tar -cf dados.tar arquivo1 arquivo2 trabalho.doc planilha.xls

Em parâmetros, é possível utilizar várias opções. Eis as principais:

- c Cria um novo arquivo tar
- t Exibe o conteúdo de um arquivo tar
- r Adiciona arquivos a um arquivo tar existente
- f Permite especificar o arquivo tar a ser utilizado
- v Exibe detalhes da operação
- w Pede confirmação antes de cada ação no comando
- x Extrai arquivos de um arquivo tar existente

Comando Tar (Compactador de Arquivos)

Exemplo:

1-Compactar arquivos:

tar -cf dados.tar arquivo1 arquivo2 arquivo3 (OBS: pode se usar o caractere curinga *)

2-Visualizar o conteúdo de um arquivo TAR.

tar -tf dados.tar

3-Descompactar um arquivo TAR.

tar -xf dados.tar

4-Adicionar um arquivo ao arquivo já compactado.

tar -rf dados.tar arquivo_novo

5-Compactar arquivos e pedir confirmação de arquivo por arquivo.

tar -cwf dados.tar *

bzip2

Compacta ou descompacta arquivos usando-se o algoritmo de compressão de texto que ordena blocos chamados Burrows-Wheeler e a codificação Huffman. Os arquivos compactados com bzip2 normalmente possuem a extensão .bz2.

Opções:

-d

Descompacta um arquivo .bzip2

-1 a -9

Define o tamanho do bloco para 100k, 200k, 300k,... 900k ao fazer compactação. Isso define os níveis de compactação.

Compactar um arquivo usando o nível mais alto de compactação.

bzip2 -9 *.doc

```
root@debian:/teste# ls
humberto2.doc  humberto.doc  linux.doc  teste2
root@debian:/teste# bzip2 -9 *.doc
root@debian:/teste# ls
humberto2.doc.bz2  humberto.doc.bz2  linux.doc.bz2  teste2
root@debian:/teste#
```

Descompactar um arquivo com a extensão .bz2

bzip2 -d *.bz2

```
root@debian:/teste# bzip2 -d *.bz2
root@debian:/teste# ls
humberto2.doc  humberto.doc  linux.doc  teste2
root@debian:/teste#
```

gzip e gunzip

Esses comandos servem para compactar e descompactar arquivos usando a codificação Lempel-Ziv, o gzip é um dos formatos de compactação mais comuns encontrados em sistemas Linux, embora esteja sendo substituído pelo bzip2 que é mais eficiente. Os arquivos compactados com gzip normalmente possuem a extensão .gz.

Opções:

-d

Descompacta um arquivo.

-r

Navega pela estrutura de diretórios recursivamente, compactando tudo.

```
root@debian:/teste# gzip humberto.doc
root@debian:/teste# ls
humberto2.doc  humberto.doc.gz  linux.doc  teste2
root@debian:/teste#
```

gzip e gunzip

Exemplo:

Descompactar o arquivo humberto.gz

```
# gunzip humberto.gz
```

Ou

```
# gzip -d humberto.gz
```

```
root@debian:/teste# gzip -d humberto.doc.gz
root@debian:/teste# ls
humberto2.doc  humberto.doc  linux.doc  teste2  teste.gz
root@debian:/teste# gunzip teste.gz
root@debian:/teste# ls
humberto2.doc  humberto.doc  linux.doc  teste  teste2
root@debian:/teste#
```

Linux Completo + Servidores

Aula 14: Gerenciamento de Sistemas de Arquivos

O gerenciamento do sistema de arquivos está entre as atividades mais importantes que você precisa realizar para manter um sistema Linux estável.

Em situações simples, após uma instalação com sucesso, você talvez nunca tenha um problema nem precise gerenciar detalhes específicos do sistema de arquivos.

No entanto, entender como configurar e fazer a manutenção dos sistemas de arquivos do Linux é essencial para gerenciar com segurança o seu sistema.

Partições de disco

Quase todos os sistemas operacionais têm suporte a um sistema para dividir um disco em dispositivos lógicos, chamados partições.

O Linux oferece suporte a diversos formatos de particionamento diferentes, mas, por padrão, usa o formato do MS-DOS.

A tabela de partição do MS-DOS permite até quatro partições primárias.

Uma dessas quatro partições primárias pode ser substituída por uma partição estendida, que pode conter até 12 partições lógicas, para um total de 15 partições possíveis (16 se você incluir o container da partição estendida.)

O tipo de partição, bem como o tipo de dispositivo, afeta o nome do dispositivo que o Linux usa para acessar a partição.

Partições de disco

Partições primárias em um disco IDE:

/dev/hda1

/dev/hda2

/dev/hda3

/dev/hda4

Partições estendidas:

/dev/hda1

/dev/hda2

...

As partições lógicas existem dentro da partição estendida são numeradas de 5 a 16.

Gerenciando partições

O Linux tem a opções básica para o particionamento de drives de disco.

O comando **fdisk** é um programa de modo texto fácil de usar e que existe em todas as distribuições do Linux.

fdisk

Sintaxe:

fdisk dispositivo

O comando fdisk manipula ou exibe a tabela de particionamento para dispositivo usando uma interface de texto interativa, dirigida por comandos.

Dispositivo é um disco físico, como **/dev/hda**, e não uma partição como **/dev/hda1**.

Os comandos interativos para fdisk são na forma de uma letra seguida por um retorno.

Os comandos não usam argumentos, mas iniciam um diálogo interativo.

Os comandos operam sobre partições irão pedir o número da partição, que é um número inteiro.

Ao fazer modificações à tabela de partição, fdisk acumula modificações sem escrevê-las em disco, até receber o comando write.

```
root@terceiro:~# fdisk -l
```

```
Disk /dev/sda: 21.5 GB, 21474836480 bytes  
255 heads, 63 sectors/track, 2610 cylinders, total 41943040 sectors  
Units = setores of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disk identifier: 0x0009f053
```

Dispositivo	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	2048	40136703	20067328	83	Linux
/dev/sda2		40138750	41940991	901121	5	Estendida
/dev/sda5		40138752	41940991	901120	82	Linux swap / Solaris

```
Disk /dev/sdb: 8589 MB, 8589934592 bytes  
255 heads, 63 sectors/track, 1044 cylinders, total 16777216 sectors  
Units = setores of 1 * 512 = 512 bytes  
Sector size (logical/physical): 512 bytes / 512 bytes  
I/O size (minimum/optimal): 512 bytes / 512 bytes  
Disk identifier: 0x00000000
```

```
O disco /dev/sdb não contém uma tabela de partições válida
```

```
root@terceiro:~$ fdisk /dev/sdb
O dispositivo não contém nem uma tabela de partições DOS válida nem um rótulo de
disco Sun, OSF ou SGI
Building a new DOS disklabel with disk identifier 0xd0931522.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Aviso: a opção inválida 0x0000 da tabela de partições 4 será corrigida por gravação (w)
```

```
Comando (m para ajuda): _
```

```
Aviso: a opção inválida 0x0000 da tabela de partições 4 será corrigida por gravação (w)
```

```
Comando (m para ajuda): m
```

```
Comando - ação
a    alterna a opção "inicializável"
b    edita rótulo BSD no disco
c    alterna a opção "compatibilidade"
d    exclui uma partição
l    lista os tipos de partição conhecidos
m    mostra este menu
n    cria uma nova partição
o    cria uma nova tabela de partições DOS vazia
p    mostra a tabela de partições
q    sai sem salvar as alterações
s    cria um novo rótulo de disco Sun vazio
t    altera a identificação da partição para o sistema
u    altera as unidades das entradas mostradas
v    verifica a tabela de partições
w    grava a tabela no disco e sai
x    funcionalidade adicional (somente para usuários avançados)
```

```
Comando (m para ajuda): _
```

Criando sistemas e arquivos

Uma vez particionado um disco, podem ser criados sistemas de arquivos nessas partições usando-se o utilitário **mkfs**.

O mkfs é uma ferramenta de criação de sistemas de arquivos, tais como mkfs.ext2 e mkfs.msdos, mkfs.ext3...

mkfs

Sintaxe: mkfs –tipo –opções dispositivo

O comando mkfs cria um sistema de arquivo, se o fstype for omitido, ext é usado por padrão (depende de qual distribuição estiver usando, por exemplo, o Debian 7 usa o ext4 como padrão).

É comum ver referencias a comandos, tais como mkfs.ext2, mkfs.ext4 que são alias para mkfs, especificando o tipo de sistema de arquivo desejado.

Opções:

-C

Verifica se existem bad blocks em dispositivo antes de criar o sistema de arquivo.

-L rótulo

Define o rótulo do volume para o sistema de arquivos (apenas sistemas de arquivos com base em ext).

-q

Usa mkfs em modo silencioso, resultando em uma saída bastante reduzida.

-j

Cria um arquivo de jornal ext3.

Exemplo:

Criar uma partição ext em /dev/sdb1:

mkfs /dev/sdb1

```
root@terceiro:~| mkfs -c /dev/sdb1
mke2fs 1.42.5 (29 Jul 2012)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
524288 inodes, 2096896 blocks
104844 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2147483648
64 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Checking for bad blocks (read-only test):  0.00% done, 0:00 elapsed. (0/0/0 errors)
done
Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

```
root@terceiro:~| mkfs -L dados /dev/sdb1
mke2fs 1.42.5 (29 Jul 2012)
Filesystem label=dados
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
524288 inodes, 2096896 blocks
104844 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2147483648
64 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done
```

Linux Completo + Servidores

Aula 15: Montagem e Desmontagem de Sistemas de Arquivos

Quando o Linux faz o boot, o kernel realiza uma verificação de todos os sistemas de arquivos de **/etc/fstab**.

Todos os sistemas de arquivos que não tenham sido desmontados de forma limpa são verificados.

Se essa verificação encontrar erros significativos, o sistema entra em modo de usuário único para que você possa executar o **fsck** manualmente.

Controlar a Montagem e a Desmontagem do Sistema de Arquivos

O Linux geralmente se compõe de várias partições, cada uma conectada ao sistema de arquivos root (/).

Sistemas de arquivos de mídia removível, como CD-ROMS, USB, ... , são conectados da mesma forma, mas geralmente de forma temporária.

Cada um desses sistemas de arquivos separados é montado no sistema na forma de diretório (ponto de montagem).

Os diretórios criados para serem pontos de montagem geralmente não contém arquivos nem outros diretórios.

Se uma diretório que já contiver arquivos for usado como um ponto de montagem, os seus arquivos serão obscurecidos e ficarão indisponíveis até que o sistema de arquivos seja desmontado.

Essas informações são registradas no arquivo **/etc/fstab**

O arquivo `/etc/fstab` é de texto simples e consiste de linhas com seis campos:

Dispositivo: Este campo especifica o arquivo de dispositivo da partição que armazena o sistema de arquivos (`/dev/hda1`). Ele pode ser tanto o nome do dispositivo, ou o UUID do dispositivo.

Ponto de montagem: Este campo especifica o diretório no qual o sistema de arquivos deve ser montado. Por exemplo, se `/dev/hda1` contiver o sistema de arquivos root, ele será montado em `/`.

Tipo do sistema de arquivos: Em seguida, é especificado o tipo do sistema de arquivos. Este pode ser do tipo `ext4`, `swap`, `iso 9660` (CD-ROM), entre outros.

Opções de montagem: Este campo contém uma lista de opções, separadas por vírgulas. Algumas opções são específicas de determinados tipos de sistema de arquivos.

Frequência de dump: O programa dump, um utilitário de backup padrão do Unix, consulta /etc/fstab para obter informações sobre a frequência com que ele deve fazer o dumping de cada sistema de arquivos.

Número de passe para fsck: Este campo é usado pelo **fsck** quando a opção **-A** é especificada, geralmente no momento do boot. Trata-se de um flag que pode conter apenas os valores 0, 1 ou 2.

1- instrui o fsck a verificar esse sistema primeiro.

2- Instrui o fsck a verificar os sistemas de arquivos correspondentes, após aqueles com um valor 1.

0- Instrui o fsck a não verificar o sistema de arquivos.

```
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options>          <dump> <pass>
# / was on /dev/sda1 during installation
UUID=bc48066c-a00a-410b-bc24-d89784872d60 /          ext4    errors=remount-ro 0      1
# swap was on /dev/sda5 during installation
UUID=eb42722c-2ec1-4b65-90ec-0281b202963a none        swap      sw      0      0
/dev/sr0      /media/cdrom0  udf,iso9660 user,noauto   0      0
~
```

O arquivo `/etc/fstab` é criado automaticamente quando o Linux é instalado e é baseado na configuração de particionamento e de ponto de montagem especificada.

Esse arquivo pode ser modificado a qualquer momento para adicionar dispositivos e pontos de montagem.

Há uma série de parâmetros disponíveis como opções para se montarem sistemas de arquivos.

Essas opções podem ser especificadas em **/etc/fstab**.

auto

Habilita a montagem automática na inicialização do sistema operacional.

defaults

Implica rw, exec, auto, nouser. É encontrada comumente em entradas de /etc/fstab para pontos de montagem ext2, ext3 e ext4.

exec

Habilita a execução de programas contidos na partição montada.

noauto

Proíbe a montagem automática. É geralmente especificada para mídias removíveis.

noexec

Proíbe a execução de programas executáveis, uma potencial medida de segurança.

nouser

Proíbe que usuários não root montem e desmontem o sistema de arquivos.

ro

Configura a partição para ser montada em modo de somente leitura.

rw

Configura a partição para ser montada em modo escrita.

users

Permite que qualquer usuário monte e desmonte o sistema de arquivos.

Montando Sistemas de Arquivos

Os sistemas de arquivos são montados usando-se o comando **mount**.

No momento do boot, os sistemas de arquivos com um número de passe diferente de zero em **/etc/fstab** são verificados e montados automaticamente.

Depois disso, você pode rodar **mount** manualmente para adicionar outros sistemas de arquivos do sistema.

mount

Sintaxe:

mount opções dispositivo diretório

Opções de linha de comando

-a

Monta todas as partições especificadas em /etc/fstab, exceto aquelas com a opção noauto.

-r

Monta o sistema de arquivos como somente leitura.

-v

Define o modo verbose.

-w

Monta o sistema de arquivos no modo escrita.

```
root@terceiro:/# mkdir dados2
root@terceiro:/# ls
bin      dados2  home       lib64      mnt      root     selinux   tmp     vmlinuz
boot    dev      initrd.img  lost+found  opt      run      srv      usr
dados   etc      lib        media     proc     sbin     sys      var
root@terceiro:/# mount /dev/sdb1 /dados2
```

Desmontando sistema de arquivos

Uma vez montado um sistema de arquivos, ele pode ser desmontado, liberando assim seu diretório ou dispositivo. Para desmontar é utilizado o comando **umount**.

Sintaxe:

umount opções dispositivo diretório

Opções:

-a

Desmonta todos os sistemas de arquivos descritos em /etc/fstab. Este arquivo é mantido pelos comandos mount e umount e contêm uma lista atualizada de sistemas montados.

-t fstype

Desmonta apenas sistemas de arquivos do tipo ftype.

Exemplo:

Desmontar o CD-ROM /dev/hdc montado em /mnt/cdrom:

umount /mnt/cdrom

Desmontar todos os sistemas de arquivos NFS:

umount –at nfs

Linux Completo + Servidores

Aula 16: Monitorando e Consertando Sistemas de Arquivos

Monitorar o espaço livre em disco

Um sistema de arquivos de leitura/escrita não é muito útil se ele crescer até o ponto em que não aceite mais arquivos novos.

Isso poderia acontecer se o sistema de arquivos tiver a sua capacidade totalmente preenchida.

O comando **df** lhe fornece as informações de que precisa sobre o status tanto da utilização do espaço em disco.

df

Sintaxe: df opções

Exibe informações gerais sobre a utilização do disco para sistemas de arquivos montados em arquivo.

Em geral, arquivo é um arquivo de dispositivo para uma partição, como
`/dev/hda1`

As informações para sistemas montados em todos os dispositivos ficam em
/etc/fstab.

Opções:

-h

Exibe os resultados em um formato legível, incluindo sufixos momo M (megabytes) e G (gigabytes).

-i

Exibe informações sobre os **inodes** restantes, em vez de as informações padrão sobre o espaço em disco.

Para cada arquivo existe um **inode**, que armazena informações sobre o arquivo relacionado. Essas informações, também conhecidas como Metadados, são importantes para administração do arquivo. O inode guarda informações como permissões, tempo, grupo e proprietário do arquivo.

Exemplo:

Verificar a utilização do espaço em disco de todos os sistemas de arquivos:

Sist. Arq.	Montado em	Tam	Usad	Dispon.	Us%
	rootfs	48G	2,4G	43G	6%
/		10M	0	10M	0%
udev		101M	404K	100M	1%
/dev					
tmpfs					
/run					
/dev/disk/by-uuid/0f3051fb-2aa0-485c-938b-2723e543882e		48G	2,4G	43G	6%
/					
tmpfs					
/run/lock		5,0M	0	5,0M	0%
is					
/shm		610M	0	610M	0%

Monitorando o uso do Disco

du

O comando du exibe informações de utilização de disco para diretórios. Se diretórios forem omitidos, a busca é feita no diretório de trabalho atual.

Sintaxe:

du opções diretórios

Opções:

-a

Mostra todos os arquivos, e não apenas diretórios.

-h

Exibe resultados em um formato legível, incluindo sufixos como M (megabytes) e G (gigabytes).

-s

Exibe um resumo para cada um dos diretórios especificados, em vez de totais para cada subdiretório encontrado recursivamente.

-S

Exclui subdiretórios de contagens e de totais, limitando os totais aos diretórios.

Exemplo:

Examinar a utilização de disco em /etc, incluindo os subdiretórios dentro dele:

```
# du -s /etc
```

```
root@saturno:/# du -s /etc
7028    /etc
```

Exibir um resumo de todos os subdiretórios de /home, com uma saída legível:

```
# du -csh /home/*
```

```
root@saturno:/# du -s /etc
7028    /etc
root@saturno:/# du -csh /home/*
20K      /home/humberto
16K      /home/iredadmin
16K      /home/iredapd
52K      total
```

Verificando e Corrigindo Sistemas de Arquivos

Computadores eventualmente podem falhar, mesmo por uma parada de energia ou até mesmo um arquivo malicioso

Se uma operação de escrita em disco for abortada antes de se completar, os dados em trânsito poderão se perder e as partes do disco que haviam sido alocadas para eles serão marcadas como utilizadas.

Ambos os cenários levam a inconsistências no sistema de arquivos e precisam ser corrigidos para se garantir uma operação confiável.

Os sistemas de arquivos são verificados com o ***fsck***.

fsck

Sintaxe:

`fsck opções tipo_sistema_arquivo`

O fsck verifica se há erros nos sistemas de arquivos e, opcionalmente, os corrige.

Por padrão, fsck assume que o tipo do sistema é o ext e roda interativamente, pausando para lhe pedir permissão antes de aplicar quaisquer reparos.

Opções:

-A

Roda verificações em todos os sistemas de arquivos especificados em /etc/fstab. Esta opção é para uso no momento do boot, antes de os sistemas de arquivos serem montados.

-N

Não executa, mas mostra o que seria feito.

-t tipo

Especifica o tipo de sistema de arquivos a ser verificado; o padrão é o ext. O valor de tipo determina qual verificador, de qual sistema de arquivos, será chamado.

-c

Verifica se há bad blocks.

-f

Força uma verificação, mesmo que o sistema de arquivos pareça ok.

-p

Repara automaticamente o sistema de arquivos, sem pedir confirmação ao usuário.

-y

Responde “yes” a todos os prompts interativos.

```
root@terceiro:~# fsck -c /dev/sdb1
fsck de util-linux 2.20.1
e2fsck 1.42.5 (29-Jul-2012)
Checking for bad blocks (read-only test): 0.00% done, 0:00 elapsed. (0/0/0 errors)
done
dados: Updating bad block inode.
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information

dados: ***** FILE SYSTEM WAS MODIFIED *****
dados: 11/524288 files (0.0% non-contiguous), 37519/2096896 blocks
```

Forçar uma verificação com o modo verbose ativo:

```
# fsck -fv /dev/sdb1
```

```
Pass 1: Checking inodes, blocks, and sizes
Pass 2: Checking directory structure
Pass 3: Checking directory connectivity
Pass 4: Checking reference counts
Pass 5: Checking group summary information

      11 inodes used (0.00%, out of 655360)
          0 non-contiguous files (0.0%)
          0 non-contiguous directories (0.0%)
          # of inodes with ind/dind/tind blocks: 0/0/0
      46895 blocks used (1.79%, out of 2621184)
          0 bad blocks
          1 large file

          0 regular files
          2 directories
          0 character device files
          0 block device files
          0 fifos
          0 links
          0 symbolic links (0 fast symbolic links)
          0 sockets
-----
          2 files
```

Linux Completo + Servidores

Aula 17: Permissões de Arquivos

Gerenciar a prioridade e as permissões dos arquivos

A segurança do sistema de arquivos é um requerimento fundamental para qualquer sistema operacional multiusuários.

Arquivos de sistema, kernel, arquivos de configuração e os programas precisam ser protegidos contra acidentes e conta a manipulação feita por pessoas não autorizadas.

Os arquivos dos usuários precisam ser protegidos contra modificações feitas por pessoas sem autorização e em alguns casos precisam ser mantidos completamente privados.

Em geral, é preciso implementar alguma forma de controle de acesso para se permitir as operações seguras.

Controle de Acesso Linux

O controle de acesso ao sistema de arquivos do Linux é implementado usando um conjunto de propriedades mantidas separadamente para cada arquivo.

Essas propriedades são chamadas de modo de acesso de um arquivo.

O controle de acesso é dividido em três categorias:

Usuário (User)

O usuário que é o proprietário do arquivo.

Grupo (Group)

O grupo que é o proprietário do arquivo.

Outros (Other)

Todos os outros usuários do sistema.

As definições de propriedade do usuário e do grupo fazem parte do inode e ambas são atribuídas quando um arquivo é criado.

Geralmente, o proprietário é o usuário que criou o arquivo.

O grupo do arquivo normalmente é definido como o grupo padrão do seu criador.

Os “outros” usuários são aqueles que não são membros do grupo do arquivo e também não são o seu proprietário.

Para cada uma dessas três categorias, são definidas três tipos de permissões, que se aplicam diferentemente para arquivos e diretórios.

Permissão	Abreviação	Permissão de arquivo	Permissão do diretório
Leitura	r	Examinar o conteúdo do arquivo	Listar o conteúdo do diretório
Escrita	w	Escrever ou modificar o arquivo	Criar e remover arquivos no diretório
Execução	x	Executar o arquivo como programa	Acessar (cd) diretório

Essas três permissões se aplicam às três classes diferentes:
usuário, grupo e outros.

0	0	0	0	0	0	0	0	0
Ler Usuário	Escreve Usuário	Executa Usário	Ler Grupo	Escreve Grupo	Executa Grupo	Ler Outros	Escreve Outros	Executa Outros

Quando exibidas por comandos como **ls -l**, as permissões usam as abreviaturas.

Para representar apenas a permissão de leitura, por exemplo, seria usado **r--**

Leitura e gravação juntas, seriam indicadas com **rw--**

Essas notações normalmente são apresentadas em conjuntos de três, como por exemplo:



Os bits para permissão

As permissões de arquivos e diretórios podem ser representadas em uma string de 9 bits.

É comum referir-se a esses bits em três conjuntos de três, traduzidos para três dígitos octais (base-8).

Os dígitos octais representam as permissões de leitura, escrita e execução

Se o primeiro bit for 1, acrescente 4 ao número octal (LEITURA)	Se o segundo bit for 1, acrescente 2 ao número octal (ESCRITA)	Se o terceiro bit for 1, acrescente 1 ao número octal (EXECUÇÃO)
1	1	1

A permissão de leitura sozinha é r--, que pode ser entendida como um 100 binário ou 4 octal.

Adicionando-se a permissão de escrita, tem-se rw- ou 110 binário, que equivale a 6 octal.

Valor Octal	Equivalente binário
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Para transformar os bits de modo **111101001** em uma representação octal, primeiramente separe-os em pedaços com três bits cada um:

111, 101 e 001

O primeiro grupo, representando as permissões do usuário, é o 111, ou $4 + 2 + 1 = 7$.

O segundo grupo, representando as permissões do grupo, é o 101, ou $4 + 0 + 1 = 5$.

O último grupo, representando as outras permissões, é o 001, ou $0 + 0 + 1 = 1$.

A string de modo para este exemplo pode, então, ser escrita como o número **octal 751**.

Este formato é usado para se exibir o modo do arquivo na saída do comando **stat**.

```
root@debian:~# stat teste1.txt.gz
  Arquivo: teste1.txt.gz
  Tamanho: 0          Blocos: 0          bloco de E/S: 4096    arquivo comum vazio
Dispositivo: 801h/2049d Inode: 1572877    Links: 1
  Acesso: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
  Acesso: 2020-07-09 08:26:18.000000000 -0300
Modificação: 2020-07-02 08:00:57.000000000 -0300
  Alteração: 2020-07-09 08:31:49.208019933 -0300
  Criação: -
root@debian:~#
```

644 = Usuário dono do arquivo pode ler, escrever, mas não pode executar, o grupo desse usuário só pode ler, e os outros usuários também só podem ler

rw-r--r-- = Usuário dono do arquivo pode ler, escrever, mas não pode executar, o grupo desse usuário só pode ler, e os outros usuários também só podem ler

Modificando modos de acesso

Os modos de acesso podem ser modificados com o comando **chmod**, o qual aceita especificações de modo de acesso octais ou simbólicos.

As especificações de modo simbólico possuem três partes, compostas de caracteres individuais.

Categoria	Modo	Descrição
Classe de usuário	u	Usuário
	g	Grupo
	o	Outros
	a	Todas as Classes
Operação	-	Retira a permissão
	+	Adiciona a permissão
	=	Define a permissão de forma exata
Permissões	r	Permissão de leitura
	w	Permissão de escrita
	x	Permissão de execução

Os caracteres que representam a classe individual do usuário e os que representam as permissões podem ser agrupados para se formarem expressões compostas

Exemplo, ug para usuário e grupo combinados, ou rw para leitura e escrita.

u+x

Adiciona a permissão de execução para o usuário.

go-w

Remove a permissão de escrita das classes grupo e outros.

a=rw

Define as permissões de leitura e escrita, mas não de execução, para todos.

a+x

Concede a todos a permissão de execução para diretórios e para os arquivos que já tenham alguma permissão de execução.

chmod

O comando chmod modifica o modo de acesso para arquivos.

Na primeira forma, usa uma ou mais especificações de modo simbólico, separados por vírgula, para modificar os arquivos.

Na segunda forma, usa um modo octal para modificar os arquivos.

Sintaxe:

chmod opções modo_simbólico arquivos

chmod opções modo_octal arquivos

Opções:

-R

Usa o modo recursivo, repassando as hierarquia de diretórios abaixo dos arquivos e fazendo modificações em todo o percurso.

-v

Usa o comportamento verbose, relatando todas as ações para todos os arquivos.

Exemplo:

Definir o modo de um arquivo como rw-r-r--, usando especificação octal:

`chmod 644 arquivo`

Exemplo:

Definir a mesma permissão, usando-se especificação simbólica, com a opção verbose:

`chmod -v u=rw,go=r arquivo`

Exemplo:

Remover recursivamente todas as permissões para os outros em um diretório:

`chmod -R -v o-rwx diretório`

chown

O comando chown é usado para modificar o proprietário e/ou grupo de arquivos.

Sintaxe:

chown opções usuário-proprietário *arquivos*

chown opções usuário-proprietário.grupo-proprietário *arquivos*

chown opções grupo-proprietário *arquivos*

Na primeira forma, definimos o usuário proprietário.

Na segunda forma, definimos o usuário proprietário e o grupo proprietário.

Na terceira forma, definimos o grupo proprietário.

Opções:

-R

Usa o modo recursivo, descendendo através dos diretórios e fazendo alterações.

-v

Usa o comportamento verbose, relatando ações para todos os arquivos.

Exemplo:

Define o usuário proprietário de um arquivo:

chown –v humberto *arquivo*

Define o usuário e o grupo proprietário de um arquivo:

chown –v humberto.grupo *arquivo*

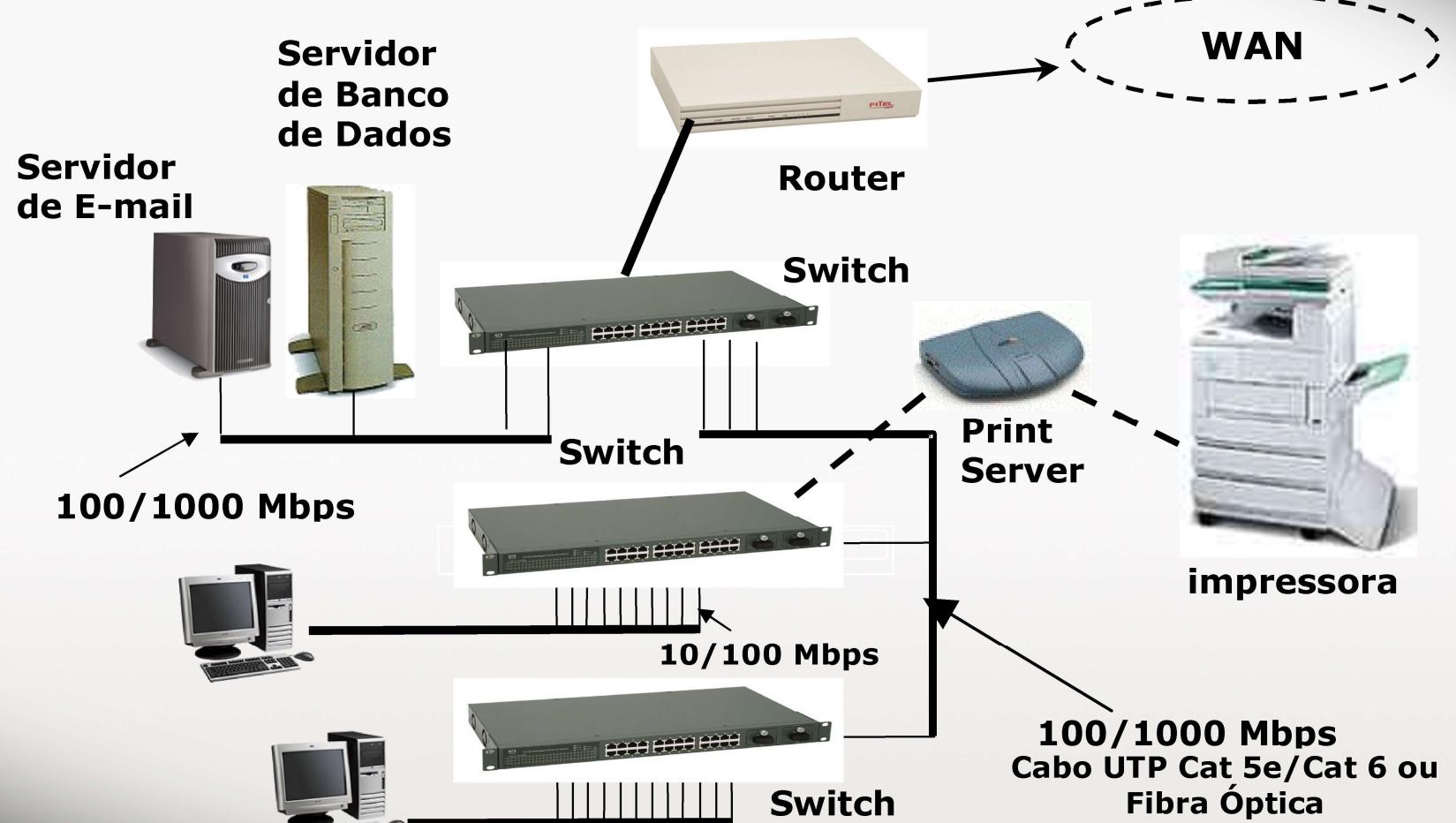
Linux Completo + Servidores

Aula 18: Introdução a Redes de Computadores

O que são Redes de Computadores?

Redes de Computadores são os compartilhamentos de informações e recursos.

O que são Redes de Computadores?



Vantagens

Computadores distribuídos geograficamente são disponíveis e trocam dados entre si.

Compartilhamento de recursos (hardware e software).

Centralização da Informação e Backup.

Requisitos Mínimos

No mínimo duas entidades para se comunicar ou compartilhar algo (DISPOSITIVOS DE COMUNICAÇÃO).

Um método ou caminho entre as duas (CABO DE REDE, WIRELESS).

Regras definidas e padronizadas para que duas ou mais entidades possam se comunicar (PROTOCOLOS).

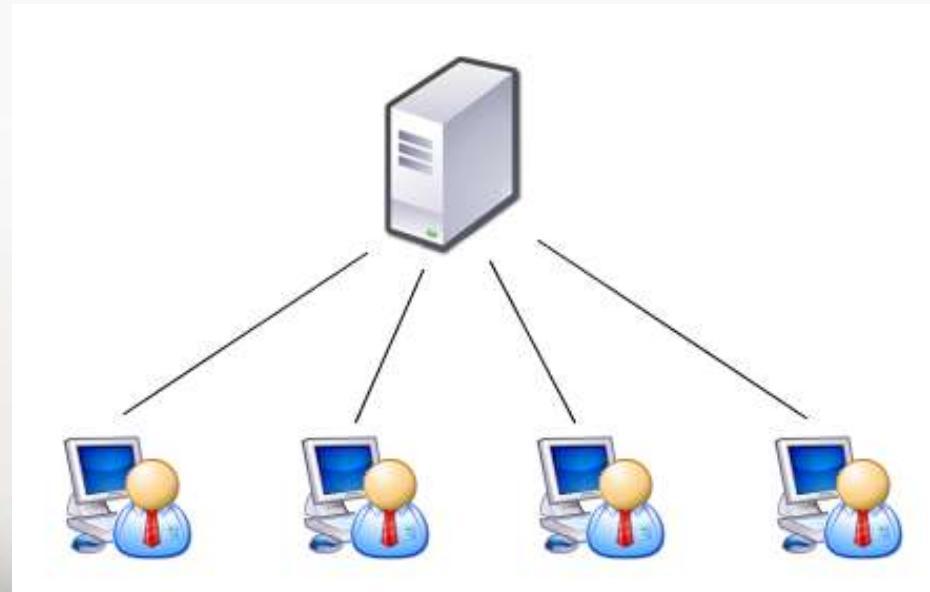
Modelos de Computação

- Computação centralizada;
- Rede distribuída (recursos distribuídos)
- Rede colaborativa (processamento distribuído).

Computação Centralizada

Basicamente, todo o processamento e armazenamento são centralizados em um único servidor.

Trata-se de um único processador de recursos, que é compartilhado por diversos usuários, através do acesso via “terminais” locais ou remotos.



Computação Centralizada



Thin client

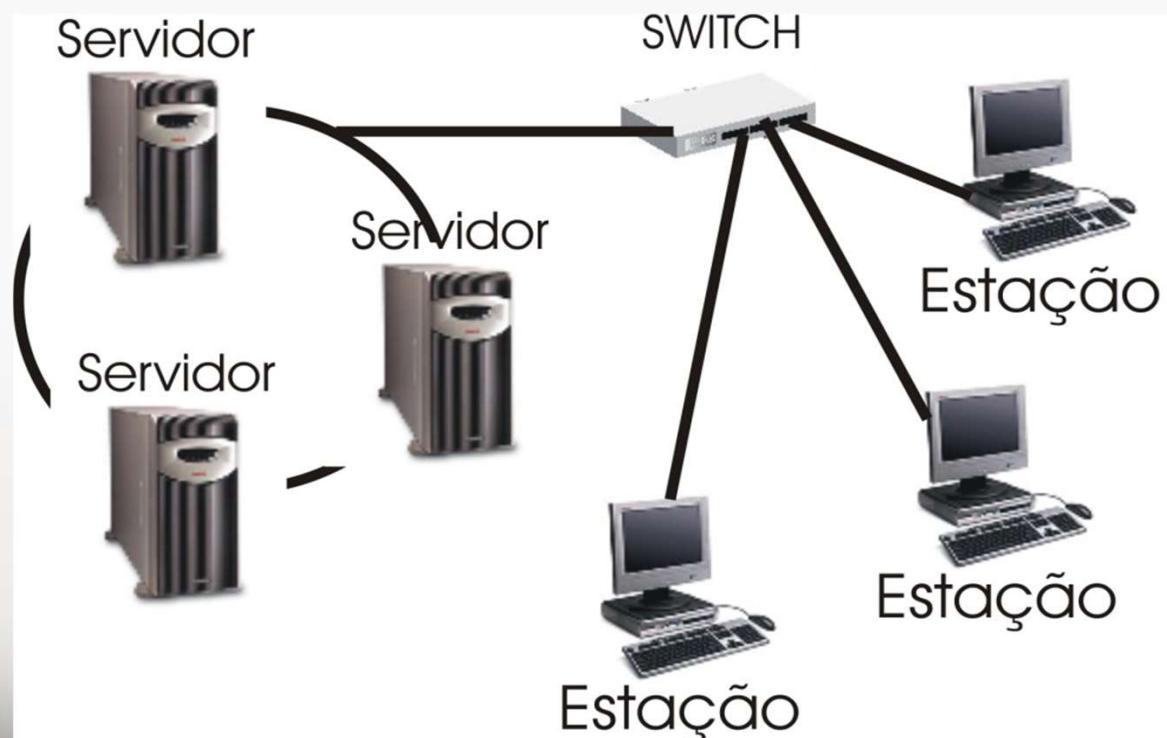
Rede Distribuída

Em vez de centralizar todo o processamento em uma único entidade, a computação distribuída utiliza vários computadores menores para obter os mesmos resultados.



Rede Colaborativa

O modelo de Rede Colaborativa considera o processamento distribuído entre os computadores de toda a rede. Ou seja, ocorre o compartilhamento da capacidade de processamento.



Tipos de Redes (distância entre as estações)

As redes de computadores são classificadas pela distância abrangida.

Tipos de Redes (distância entre as estações)

LAN – Local Area Network	Rede que se limita a se conectar entre si no mesmo ambiente, de uma empresa, instituição ou residência. A LAN podem ser de pequeno ou grande porte.
MAN – Metropolitan Area Network	Rede que abrange uma cidade inteira. Pode se tratar de uma transmissão de internet via rádio ou cabo, podem se ligar a várias LAN que estiverem dentro do seu perímetro.
WAN – Wide Area Network	Redes geograficamente distribuídas, se espalham por um estado, um país ou o mundo todo. São redes de longa distância. A internet é a maior WAN do planeta. São geralmente implementadas e comercializadas pelas empresas de telefonia usando Banda Larga.

Tipos de Redes (distância entre as estações)

LAN (Local Area Network)

As principais características de uma LAN são:

Perímetros bem definidos

Taxas de erros extremamente baixas

Compartilhamento de recursos de hardware e software

Segurança dos Dados

Permite internetwork (interligação de redes distintas)

Os principais equipamentos utilizados em uma rede local são:



Roteadores: Oferece vários serviços, entre eles a interligação entre redes LAN com outros tipos de redes.

Hubs/Switches:
Concentram as conexões da LAN e permitem o uso de meios de cobre de par trançado

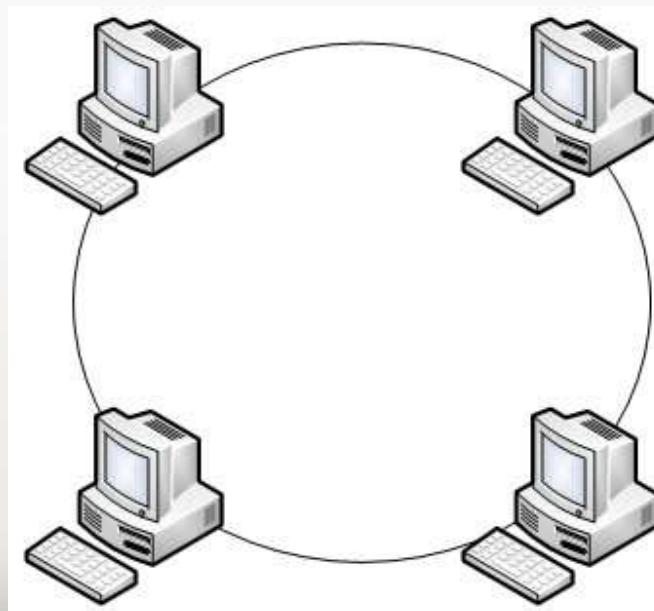


TOPOLOGIAS FÍSICAS DE REDES (tráfego da informação)

A topologia de uma rede descreve como é o layout do meio através do qual há o tráfego de informações e também como os dispositivos estão conectados.

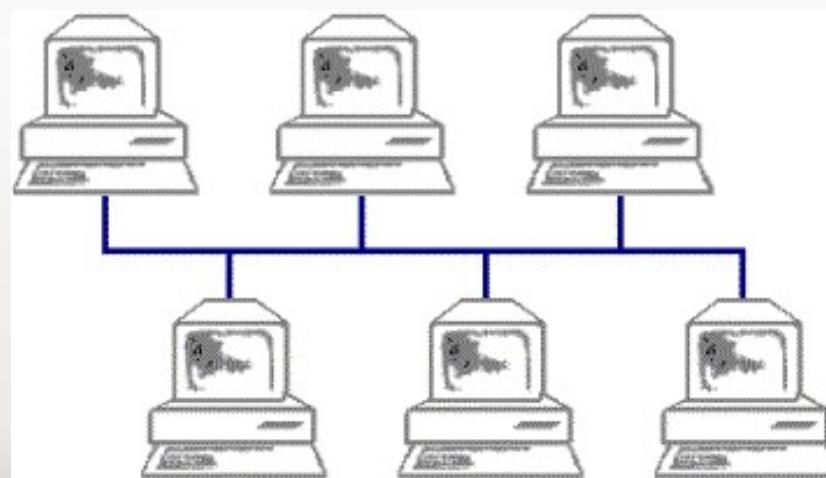
Anel

A rede toma a forma de um anel, com ligações fechadas (anel). A mensagem é repetida de estação para estação até retornar a estação de origem, sendo então retirada do anel. Hoje é um sistema descontinuado.



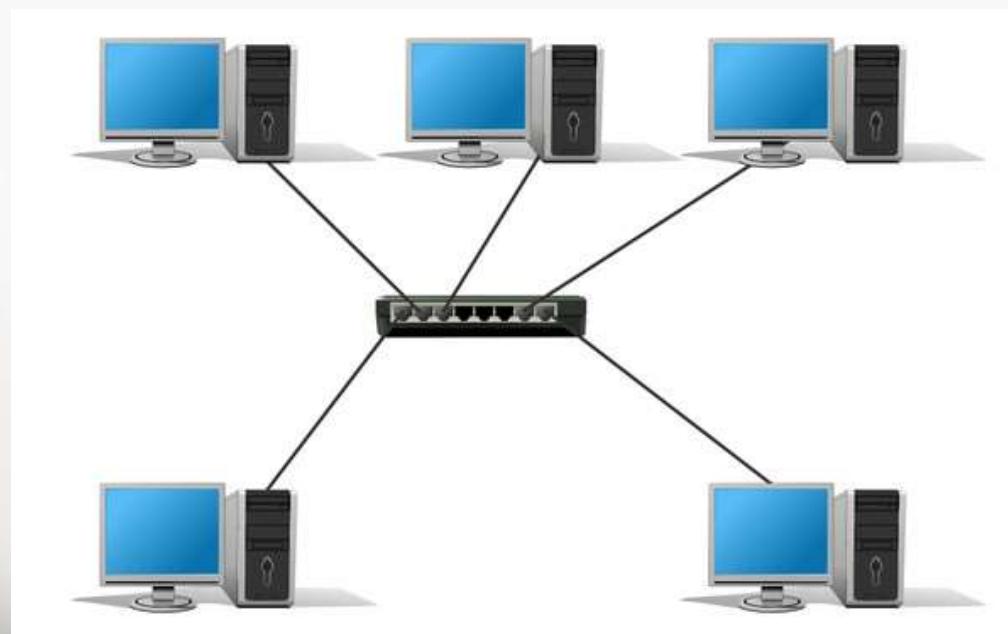
Barramento:

As Estações são conectadas através de um cabo de cobre (coaxial) com difusão da informação para todos os nós. É de fácil expansão, mas de baixa confiabilidade, pois qualquer problema no barramento impossibilita a comunicação em toda a rede. Hoje também é um sistema descontinuado.



Estrela

A Conexão é feita através de um nó central que exerce controle sobre a comunicação, sua confiabilidade é limitada ao seu nó central (Switch). A sua expansão também é limitada ao seu nó central.



Linux Completo + Servidores

Aula 19: Modelo OSI

Modelo OSI (Open System Interconnection)

Nas primeiras redes, computadores de fabricantes diferentes não conseguiam trocar informações

Foi criado então um modelo em camadas para padronizar equipamentos e protocolos de comunicação

O modelo OSI é apenas um modelo de referência mantido pela ISO* criado em 1984

ISO: Organização Internacional para Padronização

Modelo OSI (Open System Interconnection)

Uma rede tipicamente envolve 3 partes:

Dois ou mais dispositivos que se comunicam;

Um canal de comunicação entre os dispositivos
Cabo elétrico (metálico), ótica (fibra ótica) ou wireless;

Protocolos de comunicação

Modelo de referência ISO OSI

O modelo é dividido em 7 camadas e dividido em duas categorias: Superiores e Inferiores

As camadas superiores são relacionadas às aplicações.

As camadas inferiores são relacionadas a transferência de informações



Modelo de referência ISO OSI



Camada 1 – Física: relaciona-se ao hardware da rede, define questões ligadas à voltagem e à velocidade de transmissão, além de tratar da construção dos equipamentos de rede.

Modelo de referência ISO OSI



Camada 2 – de enlace: implanta no meio físico um canal de comunicação.

Quebra as mensagens em quadros de dados, sempre que um receptor recebe um desses quadros, emite de volta uma mensagem de confirmação e o transmissor então envia o próximo.

Além de controlarem a velocidade da transmissão de dados de um dispositivo rápido para outro mais lento.

Padrão Ethernet, 802.11

Modelo de referência ISO OSI



Camada 3 – de rede: controla o direcionamento do fluxo de dados na condução da informação pela rede. Possibilita que os dados passem por vários pontos até serem entregues no destino.

Controla rotas e escolhe os melhores caminhos. Leva em consideração a distância mais curta, congestionamentos ou falhas ocasionadas pelo desaparecimento de um ponto de passagem na rota.

Esta camada possibilita a comunicação entre sub-redes.

Modelo de referência ISO OSI



Camada 4 – de transporte: tem a função de receber dados da camada de rede e fracioná-los em pedaços menores, se isso for necessário.

Organiza os pacotes e os entrega na sequência correta, livres de erros, uma vez que durante a transmissão podem seguir caminhos diferentes, se perderem e ainda chegarem fora de ordem ao destino

Modelo de referência ISO OSI



Camada 5 – de sessão: Administra a sessão, estabelece quando a comunicação se inicia e quando termina. Controla o “diálogo”.

Modelo de referência ISO OSI



Camada 6 – de apresentação: faz a tradução de formato de dados entre máquinas que utilizam formatos diferentes.

Ex: A codificação das letras pode ser diferente, ASCII, ABCDIC da IBM, e daí por diante. São realizadas e convertidas várias interpretações para que a informação recebida seja a idêntica à que foi transmitida.

Modelo de referência ISO OSI



Camada 7 – de aplicação: São protocolos de alto nível que possibilitam que softwares de mesmo tipo troquem informações.

Este nível da rede é responsável pelo formato do conteúdo dos pacotes que estão sendo transmitidos. É constituído de softwares que interagem com o usuário, pois entrega o recurso ao cliente do serviço. Está no fim da rede.

Ex: HTTP, FTP, POP e SMTP

Linux Completo + Servidores

Aula 20: Protocolos de Rede Parte 1

Protocolos

Cada camada possui seus protocolos conhecidos, como o DNS, correios eletrônicos (POP3 e SMTP), FTP na camada de aplicação, o NFS (Network File System), o protocolo TCP na camada de transporte e o IP na camada de rede.

Protocolo TCP

O TCP – Transfer Control Protocol, ou Protocolo de Transferência com Controle, implementa uma solução confiável de envio de dados fim a fim.

Para garantir a confiabilidade, o TCP demanda uma resposta para cada segmento enviado, sinalizando que o pacote chegou ao destino.

Se a resposta da entrega não chegar à origem durante determinado tempo, o segmento é considerado perdido e reenviado até que se obtenha a resposta de confirmação ou que a quantidade máxima de vezes de reenvio do pacote chegue ao limite

Protocolo TCP

A função do protocolo é realizar a comunicação segura e dividir as mensagens vindas de outras camadas em pacotes menores para que a camada de rede possa repassá-los pelos roteadores.

Quando precisa transmitir dados pela internet, uma aplicação de rede tem que abrir uma porta de comunicação, chamada de socket



Missão realizada pela camada de transporte.

Protocolo TCP

Além de segmentar as mensagens, acaba sendo papel do TCP assegurar que estas sejam entregues para a aplicação na ordem correta e sem faltar nenhum pedaço.

A conexão é feita socket a socket, pois podem existir vários sockets dentro da mesma aplicação.



Protocolo TCP

O número de cada porta pode variar de 1 a 65535. Porém, os sistemas operacionais não costumam utilizar portas de número inferior a 1023, por serem consideradas reservadas

Exemplo: **Protocolo FTP** cuja sua **aplicação** solicita por padrão a **porta 21**

Protocolo HTTP cuja sua **aplicação** solicita por padrão a **porta 80**

Protocolo HTTPS cuja sua **aplicação** solicita por padrão a **porta 443**

Protocolo SSH cuja sua **aplicação** solicita por padrão a **porta 22**

Protocolo DNS cuja sua **aplicação** solicita por padrão a **porta 53**

Entrega TCP (3 Way Handshake)

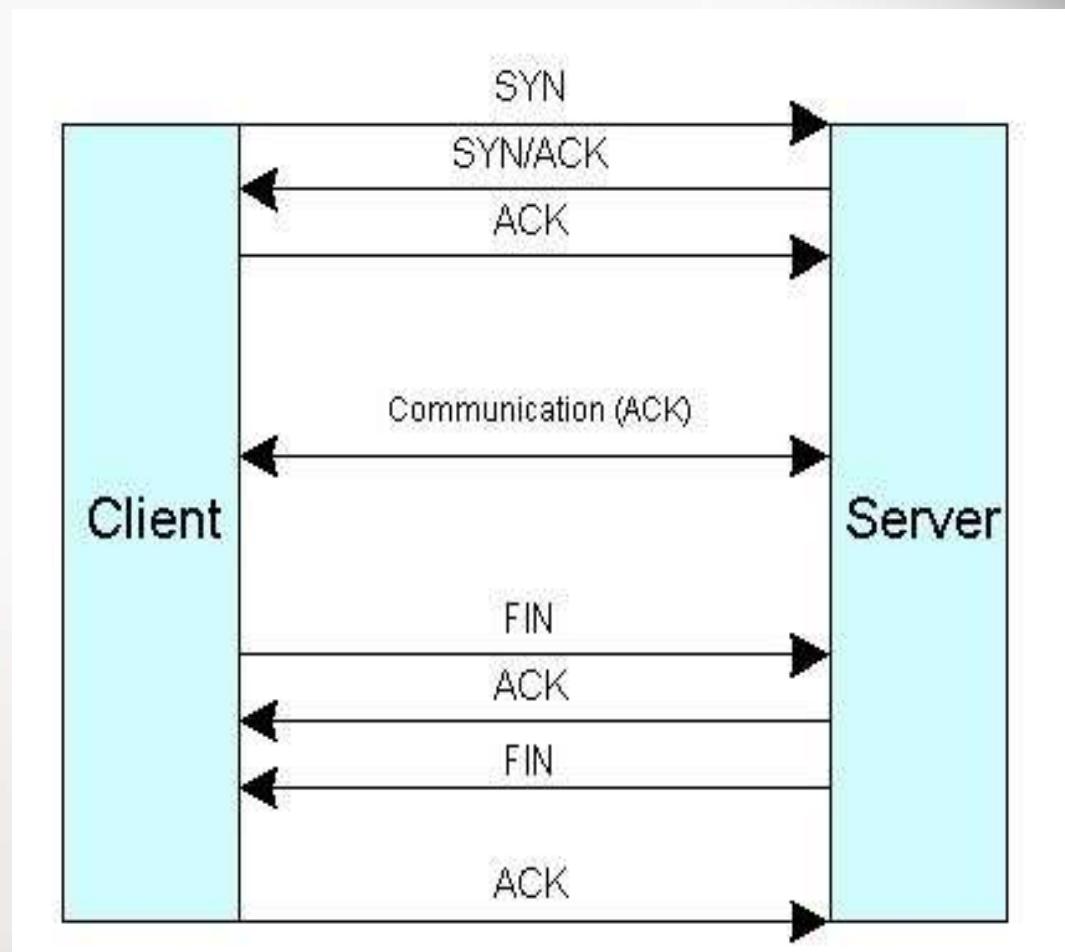
Flags TCP

ACK - Certificação que recebeu o ultimo pacote ou outra resposta.

RST - Reseta a conexão (ocorreu erro ou coisa parecida).

SYN - Inicia conexão.

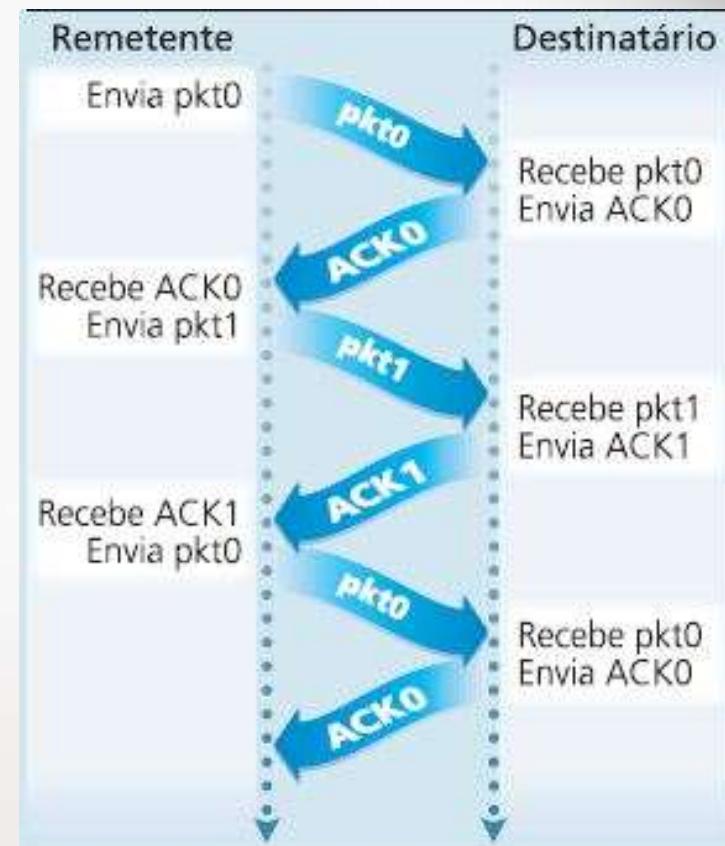
FIN - Termina conexão



Entrega TCP (3 Way Handshake)

A sinalização de entrega é feita por um bit denominado ACK, sigla para a palavra acknowledge (reconhecer), que neste contexto indica que o bit foi aceito no destino.

O TCP também age no controle do sequenciamento dos segmentos, identificando quando um pacote foi enviado duas vezes, ou se falta algum pacote entre os que foram recebidos e encerra a conexão (Handshake).



A internet é uma rede que utiliza o **protocolo IP** como forma de identificar um host e também a origem e o destino dos pacotes.

Protocolo IP (Internet Protocol)

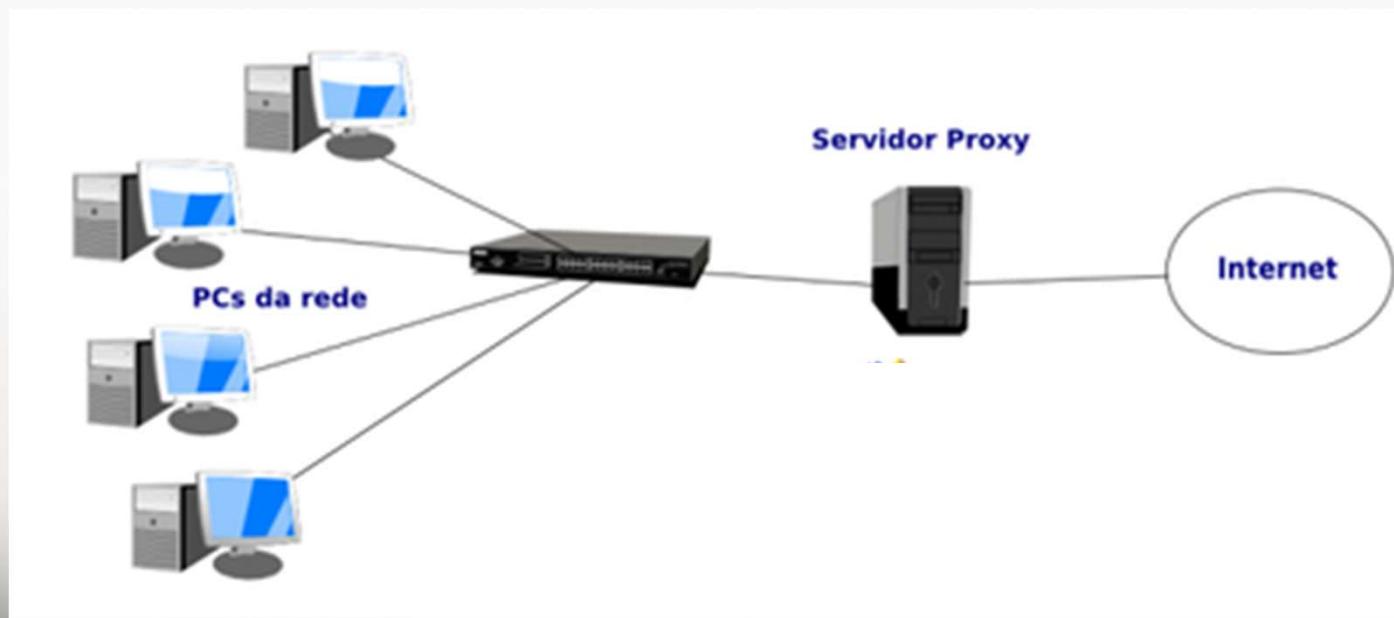
Atualmente, utilizamos a versão 4 do IP, também conhecido por IPv4, essa versão utiliza 32 bits para endereçar até 4.294.967.296 hosts

Por conta dessa “limitação”, poderemos não ter endereços suficientes.

Essa preocupação tem fundamento: há muito mais dispositivos no mundo conectados à internet do que o número de endereços possíveis

Porém, até hoje esse limite não foi alcançado. Isso porque nem todas as máquinas utilizam IP da internet, e sim IP da sua rede interna e compartilham o número IP do servidor ou do roteador.

Isso é possível graças a uma técnica chamada de **NAT** (Natural Address Translation ou Tradução Natural de Endereços).



Endereço IP

Características:

O endereço IP é uma sequência de números composta de 32 bits. Esse valor consiste em um conjunto de quatro grupos de 8 bits. Cada conjunto é separado por um ponto e recebe o nome de octeto ou simplesmente byte.

Exemplo: **192.168.0.1 ou 10.0.0.1**

O endereço IP é dividido em duas partes. A primeira identifica a rede à qual o computador está conectado e a segunda identifica o computador dentro da rede, os primeiros octetos identificarão a rede enquanto os últimos identificarão as máquinas.

Camada de Rede

Originalmente, o espaço do endereço IP foi dividido em estruturas de tamanho fixo chamados de “CLASSES DE ENDEREÇO”.

As principais classes são a **Classe A, Classe B e Classe C**.

Classe A:

1.0.0.1 – 126.255.255.254 suporta 16.777.216 endereços de rede

Classe B:

128.0.0.1 – 191.255.255.254 suporta 1.048.576 endereços de rede

Classe C:

192.168.0.1 – 223.255.255.254 suporta 65.535 endereços de rede

Camada de Rede

Faixas reservadas de endereços para Rede Local

Classe A:

10.x.x.x

Rede

Classe B:

172.16.x.x – 172.31.x.x

Rede

Rede

Classe C:

192.168.0.x – 192.168.255.x

Rede

Rede

8bits . 8bits . 8bits . 8bits
32bits

Convertendo Bits para Decimal

 = 255
1 2 4 8 16 32 64 128

1bits . 0bits . 0bits . 0bits
1 . 0 . 0 . 0

8bits . 8bits . 8bits . 8bits
32bits

Convertendo Bits para Decimal

1 1 1 1 1 1 1 = 255
1 2 4 8 16 32 64 128

8bits . 8bits . 8bits . 8bits
255 . 255 . 255 . 255

Camada de Rede

Na internet, quem controla a distribuição mundial de endereços é Autoridade Atribuidora de Números para Internet

(**IANA** – <http://www.iana.org>), que atribui e repassa o controle regional a entidades chamadas RIRs (Regional Internet Registers).

América Latina e Caribe (LACNIC – <http://www.lacnic.net/pt/>). No Brasil as solicitações devem ser feitas diretamente ao NIC.BR, que é o registro Nacional Internet para o Brasil.

As RIRs vendem faixas de IPs para as provedoras de acesso à internet, que, por sua vez, redistribuem, administram e repassam os custos aos seus clientes.

Linux Completo + Servidores

Aula 21: Protocolos de Rede Parte 2

Máscara de Sub-Rede

As sub-redes são grupos de hosts que têm o mesmo prefixo IP.

Computadores conectados entre si dentro de uma mesma infraestrutura, ligados a switchs ou a um mesmo roteador sem fio formam uma sub-rede.

Camada de Rede

Faixas reservadas de endereços para Rede Local

Classe A:

255.0.0.0

Rede

Classe B:

255.255.0.0

Rede

Classe C:

255.255.255.0

Rede

Faixas reservadas de endereços para Rede Local

Classe A:

255.0.0.0 → 10.x.x.x

Rede Hosts

10.0.0.1
10.255.255.255

\8

Classe A:

255.255.0.0 → 10.x.x.x

Rede Hosts

10.50.0.1
10.50.255.255

\16

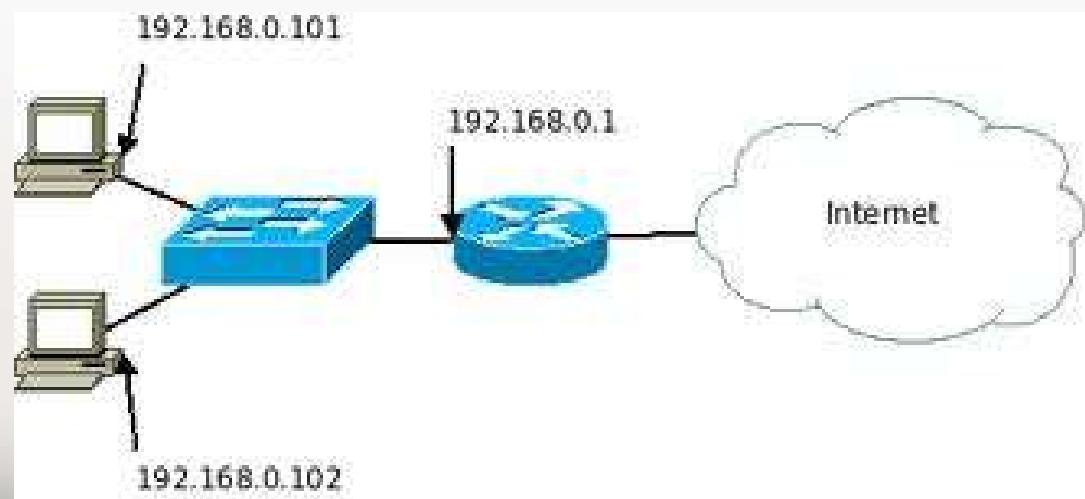
Roteamento

Hosts de uma mesma rede, ou seja, conectada no mesmo barramento, conhecem e repassam as informações entre si

Mas quando um pacote é destinado a um host na internet, esse pacote é encaminhado para o gateway dessa rede.

Podemos dizer que gateway, (gate = portão e way = caminho, caminho do portão), indica que essa máquina tem acesso à saída da LAN, ou seja, a que consegue levar o pacote para fora, ou vice-versa.

Este por sua vez retransmite o pacote a outro gateway seguindo a sua hierarquia.



DNS – Domain Name System

Quando entramos no navegador para acessar uma página qualquer da web digitamos o endereço da homepage como por exemplo, **www.samsec.com.br**. Na barra de endereços a página é carregada.

Para que isso aconteça, a aplicação cliente precisa se conectar com o servidor de páginas na internet que possui o domínio samsec.com.br e está esperando por requisições.

O servidor aceita a requisição e responde pela mesma conexão com o hipertexto solicitado.

Protocolos da Camada de Aplicação

DNS – Domain Name System

Mas como foi possível os roteadores da internet encontrarem esse site?

O que tornou a busca viável foi as aplicações do DNS (Domain Name System, ou Sistema de Nomes de Domínio), um serviço de resolução de nomes.

Sempre que uma conexão é solicitada por meio de um nome, o cliente DNS é acionado. Em seguida, ele se conecta ao seu servidor de nomes requisitando o “**IP**” do domínio informado

O servidor, por sua vez, acessa uma base de dados de nomes e endereços de IP correspondentes e, caso encontre o relativo à solicitação, responde ao cliente.

DNS – Domain Name System

Como a quantidade de domínios cresceu rapidamente, tornou-se impossível a um único servidor de nomes atender a toda a internet

Por isso foi definida uma hierarquia, constituída por 13 servidores, um em Estocolmo, na Suécia, em Londres, Inglaterra, em Tóquio, no Japão. Todos os demais estão nos Estados Unidos.

Esses servidores delegam o controle dos domínios de determinada região a servidores e, em sua maioria, controlam os domínios de um determinado país.

Cada país tem o próprio sufixo, como .jp (Japão), .uk (Inglaterra), .fr (França), .br (Brasil).

Outros Protocolos

UDP (User Datagram Protocol) é um protocolo da camada de transporte para envio de pacotes de informações, **removendo toda a verificação de erros**. O objetivo é acelerar o processo de envio de dados.

Quando o protocolo UDP é acionado, ele simplesmente manda informações a um destinatário, sem se preocupar se elas foram recebidas devidamente — em caso de erros, simplesmente ocorre o envio do próximo pacote programado pelo sistema, e os anteriores não podem ser recuperados.

O **UDP não é confiável**. Caso garantias sejam necessárias, é preciso implementar uma série de estruturas de controle, tais como timeouts, retransmissões, ack, controle de fluxo, etc.

Cada datagrama UDP tem um tamanho e pode ser considerado como um registro indivisível, diferentemente do TCP, que é um protocolo orientado a fluxos de bytes sem início e sem fim.

UDP (User Datagram Protocol)

o UDP é um serviço sem conexão, pois não há necessidade de manter um relacionamento longo entre cliente e o servidor.

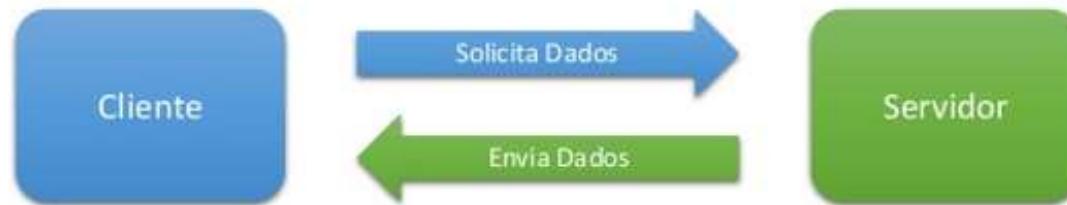
Um cliente UDP pode criar um socket, enviar um datagrama para um servidor e imediatamente enviar outro datagrama com o mesmo socket para um servidor diferente.

Da mesma forma, um servidor poderia ler datagramas vindos de diversos clientes, usando um único socket.

O UDP também fornece os serviços de broadcast e multicast, permitindo que um único cliente envie pacotes para vários outros na rede.

Diferença Protocolo TCP e UDP

Funcionamento do Protocolo UDP



- Funcionamento mais simples
- Mais rápido por ter menos Controles
- Menos Seguro em relação ao recebimento dos Dados (Transporte)
- Não estabelece conexão

Funcionamento do Protocolo TCP



- Funcionamento mais complexo
- Mais Controles
- Mais Seguro em relação ao recebimento dos Dados (Transporte)
- Estabelece conexão antes de transmitir os dados.
- Solicita retransmissão dos dados não recebidos ou corrompidos.

Protocolo HTTP

O Hypertext Transfer Protocol, sigla para **HTTP** é um protocolo de comunicação da camada de aplicação segundo o Modelo OSI

Ele é a base para a comunicação de dados da World Wide Web.

Hipertexto é o texto estruturado que utiliza ligações lógicas (hiperlinks) entre nós contendo texto.

O HTTP é o protocolo para a troca ou transferência de hipertexto normalmente utilizando a porta **80**.

Visão técnica geral

O HTTP funciona como um protocolo de requisição-resposta no modelo computacional **cliente-servidor**.

O cliente submete uma mensagem de requisição HTTP para o servidor. O servidor, que fornece os recursos, como arquivos HTML e outros conteúdos.

O protocolo HTTP define oito métodos (GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS e CONNECT) que indicam a ação a ser realizada no recurso especificado.

OBS: Protocolo com texto em claro.

Ao desenvolver um site dinâmico, existe a necessidade de passar alguns valores de uma página para a outra, para realizar operações como consultas e inserções no banco, autenticação de usuários, etc.

É de extrema importância saber bem a diferença entre os métodos **GET** e **POST**, para que se possa utilizá-los de forma correta e na hora certa.

GET

Com capacidade de 1024 caracteres, este método é utilizado quando se quer passar poucas ou pequenas informações para realizar uma pesquisa ou simplesmente passar uma informação através da URL.

A função do método GET é pura e simplesmente recuperar um recurso existente no servidor.

O resultado de uma requisição GET é “cacheável” pelo cliente, ou seja, fica no histórico do navegador.

Por exemplo:

<http://www.meusite.com.br/index.php?categoria=3&pag=2&tipo=5>

Para entender melhor este exemplo, é preciso olhar para as informações que vem logo após o sinal de interrogação “?”, pois é o símbolo que indica o início dos dados passados através da URL, ou seja, pelo método GET.

POST

Este método utiliza a URI (de Uniform Resource Identifier) para envio de informações ao servidor.

A URI **não é retornável** ao cliente, o que torna o método POST mais seguro, pois não expõe os dados enviados no navegador.

Como não tem limite de capacidade para envio de informações, este método se torna melhor que o GET. No POST, uma conexão paralela é aberta e os dados são passados por ela.

O envio de dados é feito através de formulários (tag <form>), onde são passadas informações para outra página que deverá estar habilitada a recebê-las.

Ao criar formulários de login deve-se utilizar o método POST para troca de informações entre as páginas.

Protocolo HTTPS

HTTPS (Hyper Text Transfer Protocol Secure - protocolo de transferência de hipertexto seguro) é uma implementação do protocolo HTTP sobre uma camada adicional de segurança que utiliza o protocolo **SSL/TLS**.

Essa camada adicional permite que os dados sejam transmitidos por meio de uma **conexão criptografada** e que se verifique a autenticidade do servidor e do cliente por meio de certificados digitais. A porta TCP usada por norma para o protocolo HTTPS é a **443**.

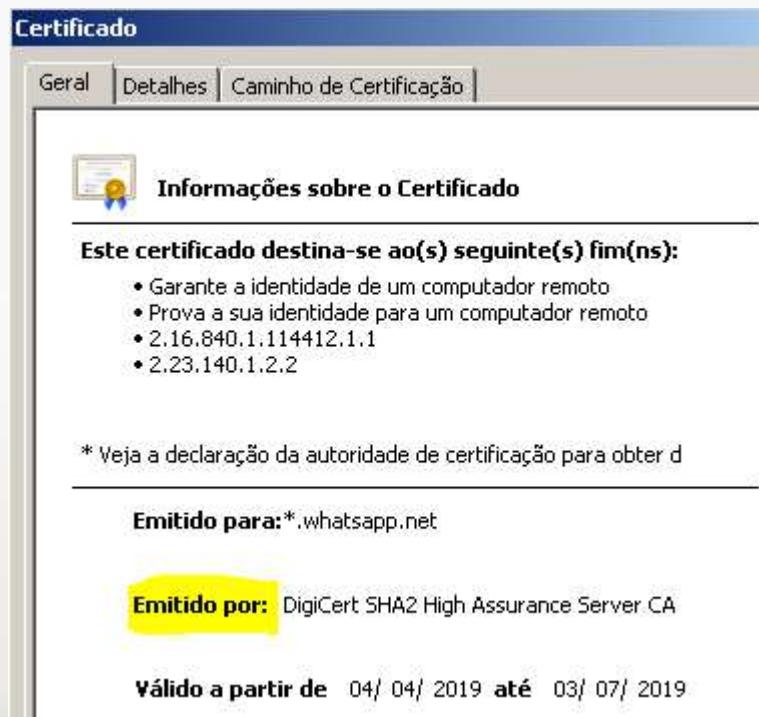
O protocolo HTTPS é utilizado, em regra, quando se deseja evitar que a informação transmitida entre o cliente e o servidor seja visualizada por terceiros, como por exemplo no caso de compras online.

Conexões HTTPS são frequentemente usadas para transações de pagamentos na World Wide Web e para transações sensíveis em sistemas de informação corporativos.

Uma conexão HTTPS pode ser confiável se e somente se todos os itens a seguir são verdade:

- 1- O usuário confia que o navegador implementa corretamente HTTPS com autoridades certificadoras pré-instaladas adequadamente;
- 2- O usuário confia que as autoridades verificadoras só irão confiar em páginas legítimas, que não possuem nomes enganosos;
- 3- A página acessada fornece um certificado válido, o que significa que ele foi assinado por uma autoridade de certificação confiável;
- 4- O certificado identifica corretamente a página (por exemplo, quando o navegador acessa "<https://exemplo.com>", o certificado recebido é realmente de "Exemplo Inc." e não de alguma outra entidade);
- 5- Ou o tráfego na internet é confiável, ou o usuário crê que a camada de encriptação do protocolo SSL/TLS é suficientemente segura contra escutas ilegais.

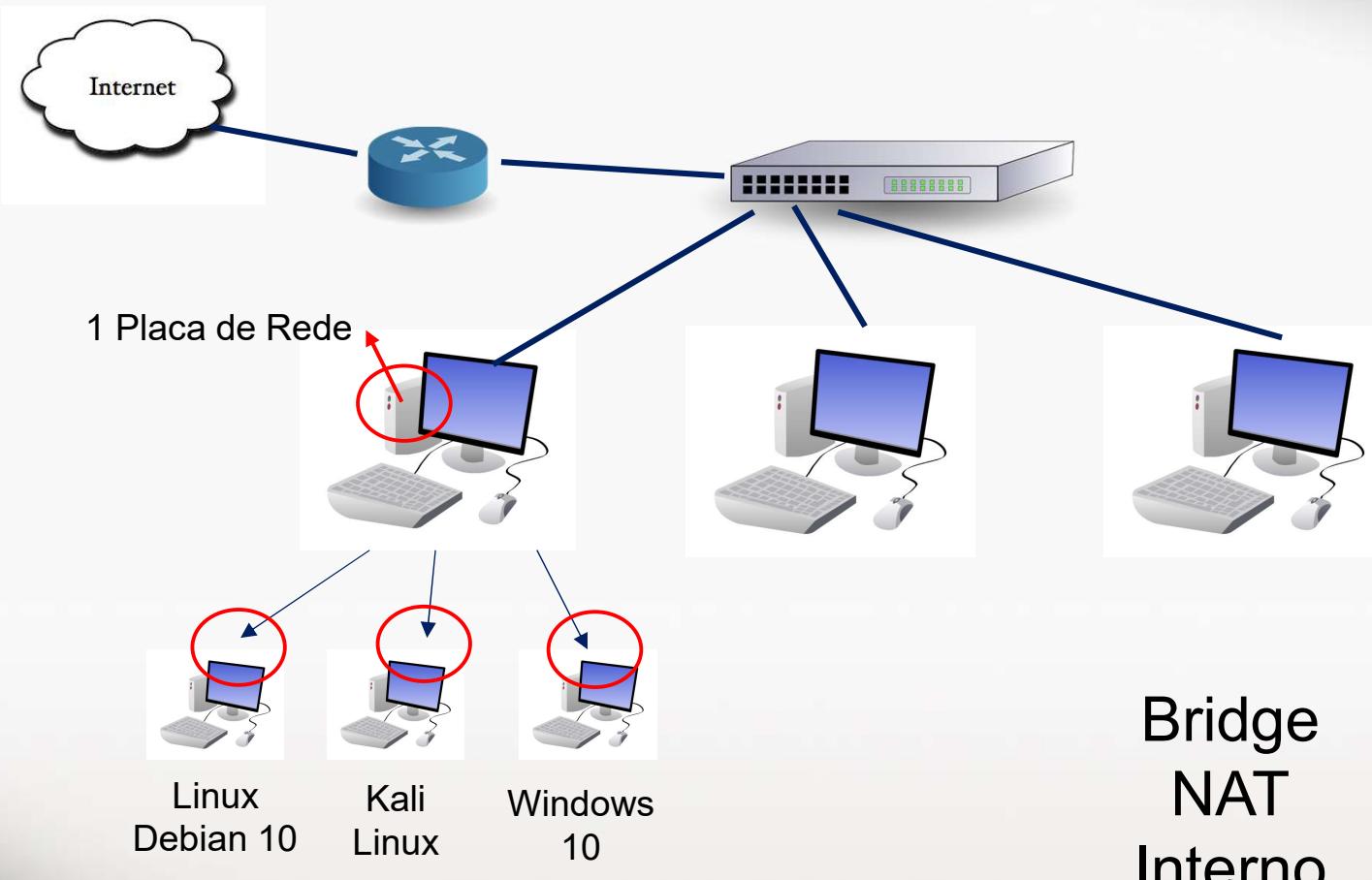
A confiança fornecida pelo **HTTPS** é baseada em autoridades de certificação que vêm pré-instaladas no navegador (isto é equivalente a dizer "Eu confio na autoridade de certificação GoDaddy/Microsoft/etc. para me dizer em quem devo confiar").



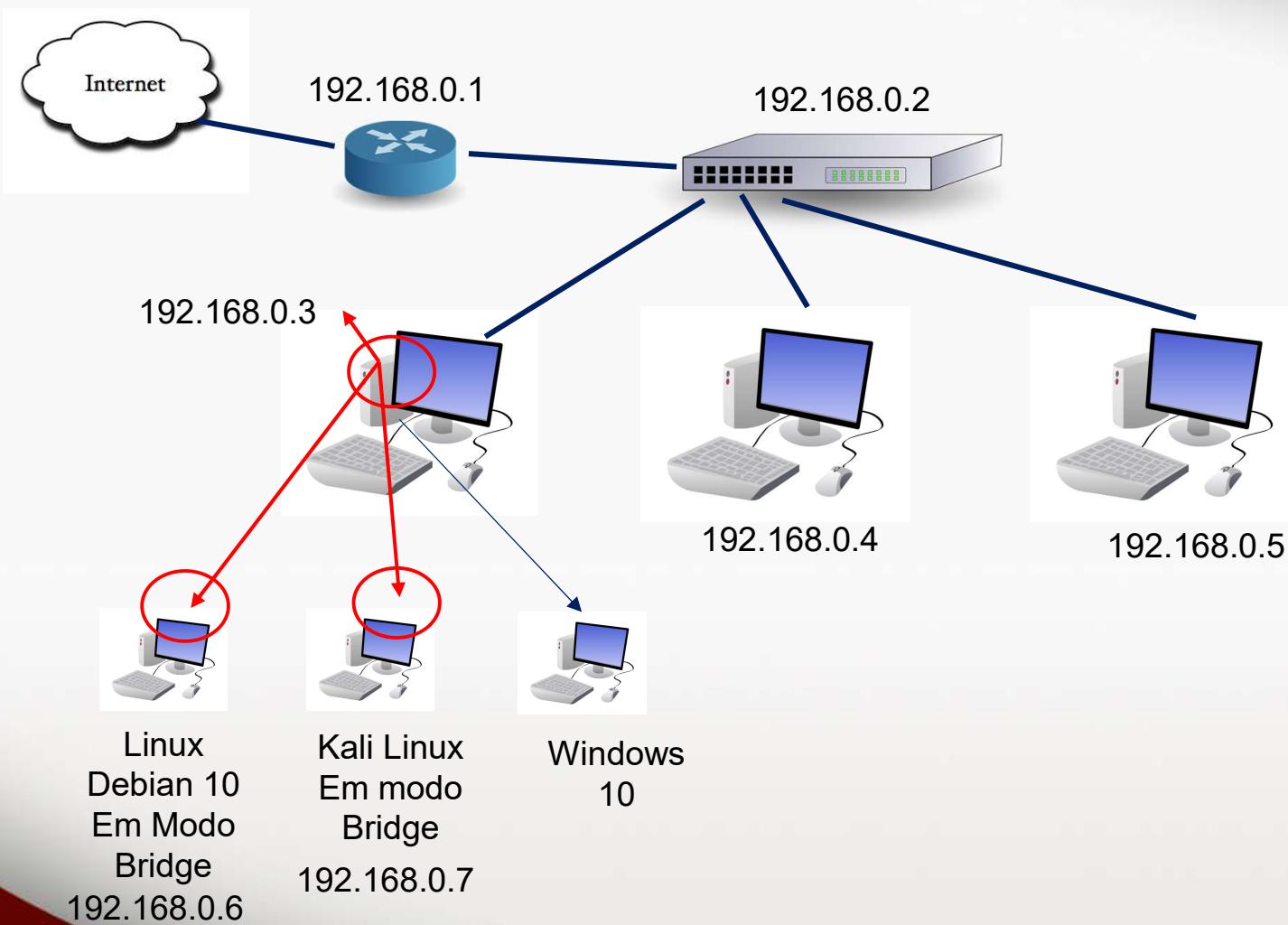
Linux Completo + Servidores

Aula 22: Redes Linux parte 1

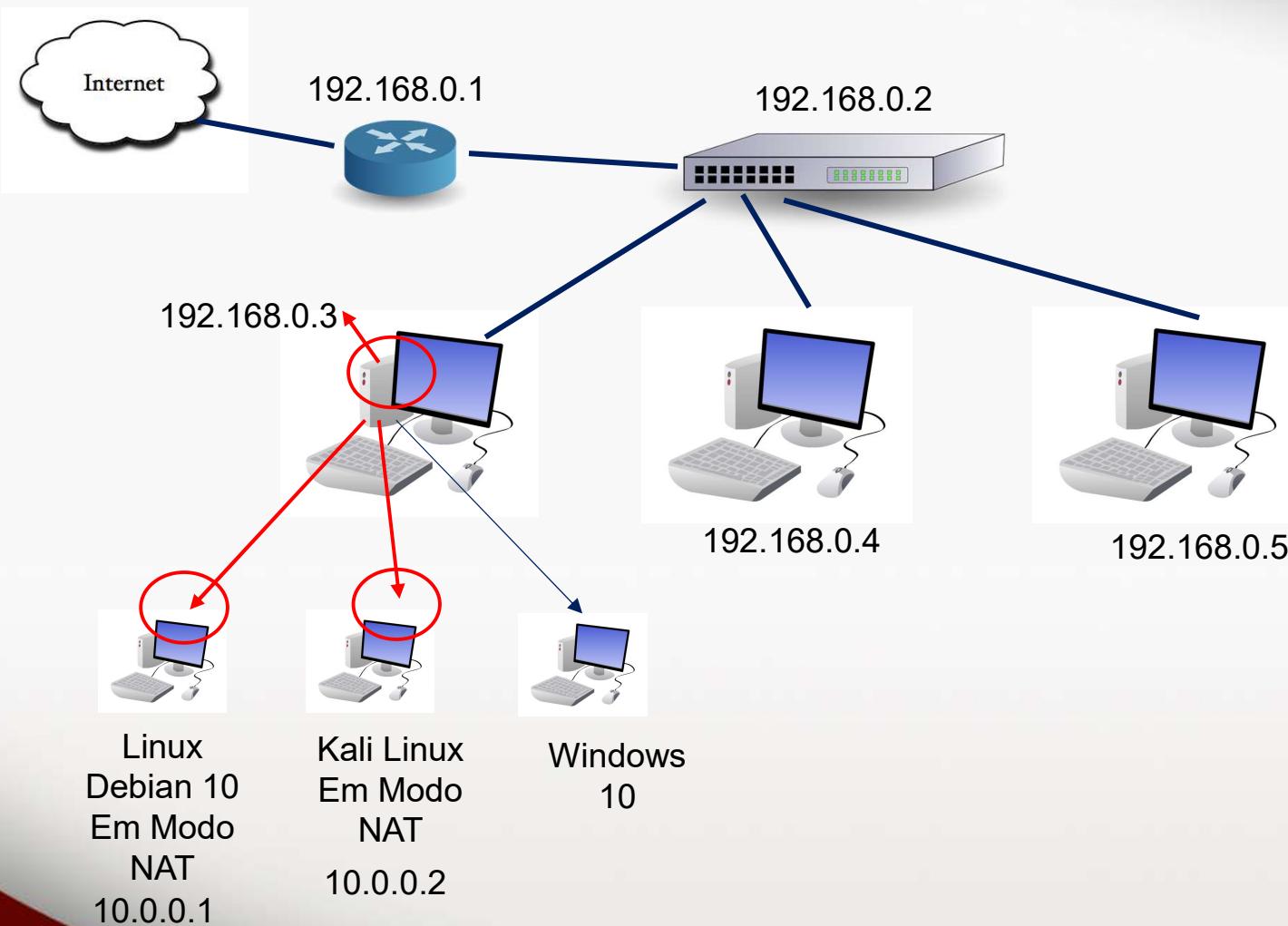
Entendendo a Placa de Rede Virtualizada



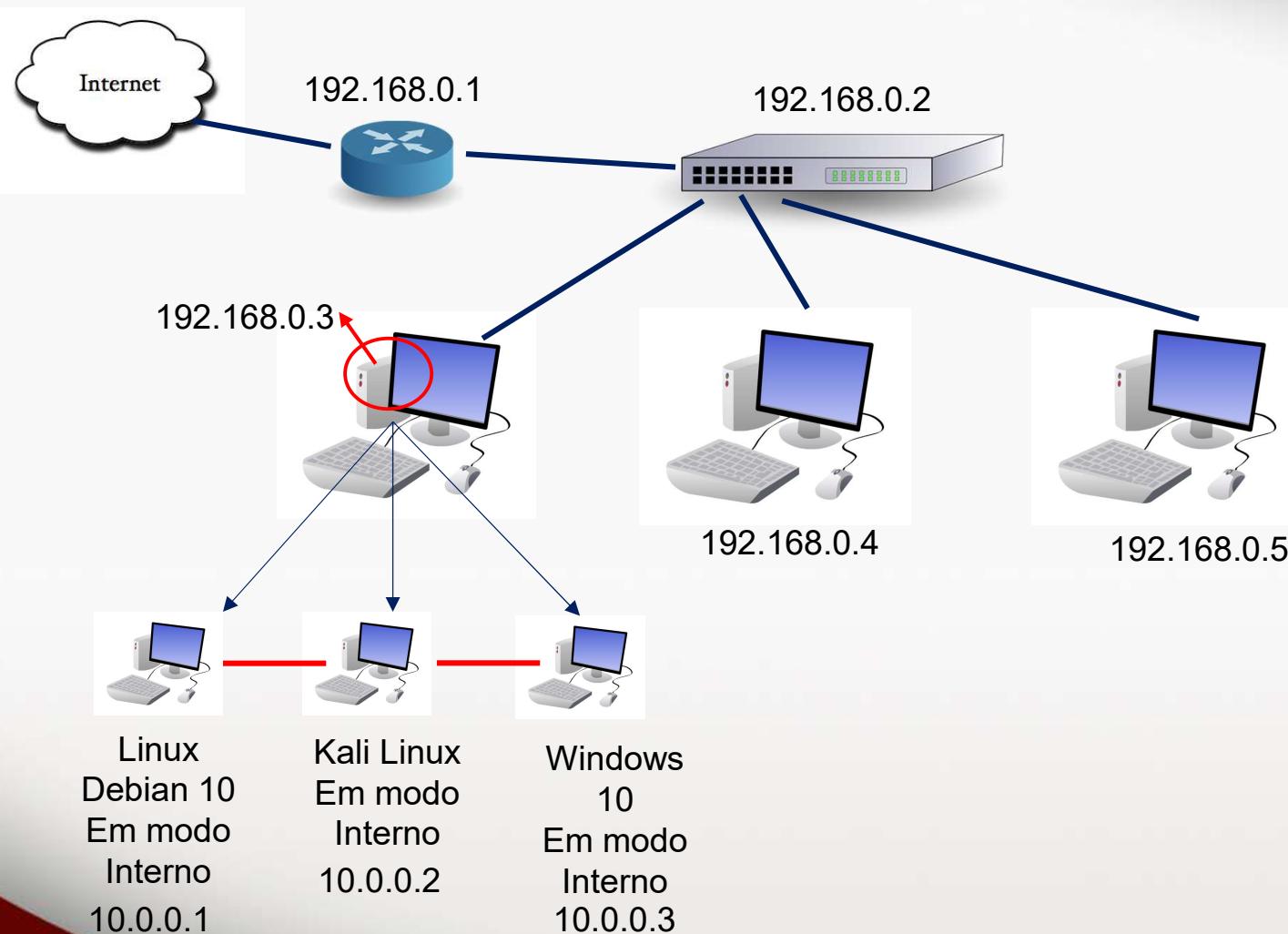
Modo Bridge



Modo NAT - network address translation



Modo Interno



Redes Linux

Quando se trata de ambientes de servidores Linux, independente da distribuição escolhida, normalmente você vai se deparar apenas com a **interface modo texto**, o que nos faz realizar as configurações de rede manualmente, escrevendo as configurações em um arquivo.

No Linux, nas maioria das distribuições, o arquivo de configuração de redes é o arquivo **interfaces**. Localizado dentro de **/etc/network**.

Antes de começar a explorar esse arquivo, também é importante compreender como o Linux chama suas **interfaces de rede**.

Para sistemas que possuam a interface gráfica instalada, utilizamos o **Network Manager**.

Redes Linux

Antigamente se tratando da interface de rede cabeada, o Linux chamava suas interfaces de **eth0, eth1, eth2**.

Se tratando da interface de rede wireless, o Linux chamava suas interfaces pelo nome de **wlan0** e as próximas seguem o mesmo padrão.

É importante salientar que esse padrão não é REGRA, pois esse padrão pode ser alterado em algumas distribuições Linux.

Nova Nomenclatura de Interfaces no Linux

As principais distribuições Linux estão adotando o padrão **systemd**, aonde ocorre algumas padronizações em relação as configurações do sistema, uma delas é justamente a padronização dos comandos e interfaces de rede.

A partir da versão Debian 8 (Jessie) o Debian passou a utilizar o padrão, portanto a não ser que você instale o aplicativo **net-tools**, seus padrões de rede serão os padrões novos.

A partir da versão **v197 do systemd**, o Linux passou a utilizar um novo mecanismo para nomenclatura das interfaces de redes, denominado **Predictable Network Interface Names**. O objetivo da nova nomenclatura foi solucionar problemas reais decorrentes da generalização dos nomes tradicionais que utilizavam o formato ethX (ethernet), wlanX (wireless), etc.

Nova Nomenclatura de Interfaces no Linux

O problema da nomenclatura tradicional é que as interfaces de mesma natureza recebem seus nomes do kernel de maneira sequencial (no formato eth0, eth1, eth2, etc...) assim que elas são consultadas pelo driver.

Ocorre que o mecanismo de comunicação entre o driver e a interface não é previsível, o que implica na possibilidade de alteração nos nomes das interfaces durante o processo de boot de máquinas que tenham múltiplas interfaces de rede em caso de atualização de hardware.

Nova Nomenclatura de Interfaces no Linux

Essa situação traz riscos de segurança em ambientes que tenham configurações e scripts de firewall que foram baseados nos nomes tradicionais.

O novo mecanismo de nomenclatura traz suporte nativo a diferentes políticas para nomeação das interfaces de rede, a destacar:

- Nomes Indexados via Firmware/BIOS On-Board
- Nomes Indexados via Firmware/BIOS PCI Express
- Nomes Indexados via Localização Física do Hardware
- Nomes Indexados via Endereço Físico (MAC)
- Nomes Clássicos Nativos do Kernel (Imprevisíveis)

Nova Nomenclatura de Interfaces no Linux

Todas essas políticas são utilizadas em conjunto, de forma que a primeira política será adotada caso as informações do firmware on-board estejam disponíveis, seguida pela segunda política caso as informações do firmware PCI estejam disponíveis, seguida pela terceira política e assim por diante.

Por exemplo, possíveis nomes de interfaces baseados na primeira, segunda, terceira, quarta e quinta políticas, respectivamente, seriam: **eno1, ens1, enp2s0, enx78e7d1ea46da e eth0**.

Apesar das políticas padrões, as configurações realizadas pelo administrador sempre têm precedência.

Comandos de Redes

Os primeiros comandos de redes, são os comandos para verificação e controle da interface.

ip a

```
root@debian-seg:/home/humberto# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:91:24:82 brd ff:ff:ff:ff:ff:ff
        inet 10.1.137.38/24 brd 10.1.137.255 scope global enp0s3
            valid_lft forever preferred_lft forever
        inet6 fe80::a00:27ff:fe91:2482/64 scope link
            valid_lft forever preferred_lft forever
```

Note o comando irá trazer todas as interfaces de rede configuradas como também os endereços IPv4 e IPv6, os endereços MAC, entre outras opções.

Comandos de Redes

Caso você queira ainda uma visão mais limpa, você pode selecionar apenas os endereços IPv4 ou o IPv6, com os comandos: **ip -4 a** e **ip -6 a**

```
root@debian-seg:/home/humberto# ip -4 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    inet 10.1.137.38/24 brd 10.1.137.255 scope global enp0s3
        valid_lft forever preferred_lft forever
```

```
root@debian-seg:/home/humberto# ip -6 a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 state UNKNOWN qlen 1
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 state UP qlen 1000
    inet6 fe80::a00:27ff:fe91:2482/64 scope link
        valid_lft forever preferred_lft forever
```

Comandos de Redes

Também existe o comando **ip r** que vai lhe mostrar o Gateway padrão.

```
root@debian-seg:/home/humberto# ip r
default via 10.1.137.254 dev enp0s3
10.1.137.0/24 dev enp0s3 proto kernel scope link src 10.1.137.38
```

Comandos de Redes

Podemos também checar o tráfego da placa de rede utilizando a opção **ip -s link**.

```
humberto@debian-seg:~$ ip -s link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    RX: bytes   packets   errors   dropped overrun mcast
        1596      28       0       0       0       0
    TX: bytes   packets   errors   dropped carrier collsns
        1596      28       0       0       0       0
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:91:24:82 brd ff:ff:ff:ff:ff:ff
    RX: bytes   packets   errors   dropped overrun mcast
        5088156    70193     0      33       0       7
    TX: bytes   packets   errors   dropped carrier collsns
        225831     1181     0       0       0       0
```

Comandos de Redes

Continuando com as opções de controle das interfaces, também podemos ativar ou desativar uma determinada interface de rede, utilizando os comandos **ifup** e **ifdown**

Parar placa de rede: **ifdown enp0s3**

Ativa placa de rede: **ifup enp0s3**

```
root@debian-seg:/home/humberto# ifdown enp0s3
Killed old client process
```

Linux Completo + Servidores

Aula 23: Redes Linux parte 2

Configuração da Interface de Rede

Existem duas maneiras da interface de rede adquirir um endereço IP, ou você tem na sua rede um serviço habilitado de **DHCP (Dynamic Host Configuration Protocol)** ou então você irá ter que **configurar manualmente** a sua interface de rede.

O arquivo de configuração de rede se localiza dentro do diretório **/etc/network**. O arquivo se chama **interfaces**.

Configuração da Interface de Rede

Fazendo a leitura do arquivo interfaces, observamos a seguinte configuração por default:

```
# and how to activate them. For more information, see interfaces(5).  
  
source /etc/network/interfaces.d/*  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
allow-hotplug enp0s3  
iface enp0s3 inet dhcp
```

Configuração padrão do arquivo interfaces em modo DHCP

Configuração da Interface de Rede

Note que no nosso exemplo são apresentadas duas interfaces, a interface de **lo** e a interface de rede **enp0s3**.

OBS: A interface de lo ou também chamada de Loopback refere-se ao roteamento de sinais eletrônicos, fluxos de dados digitais ou fluxos de itens que retornam para suas origens sem processamento ou modificação intencional.

O loopback pode ser um canal de comunicação com apenas um ponto final de comunicação, de forma que qualquer mensagem transmitida por meio de tal canal é imediatamente recebida pelo mesmo canal.

Em telecomunicações, dispositivos de loopback realizam testes de transmissão.

Configuração da Interface de Rede

No arquivo de configuração a respeito da interface enp0s3, encontramos as seguintes linhas:

```
allow-hotplug enp0s3  
iface enp0s3 inet dhcp
```

E isto nos diz muitas coisas, como por exemplo:

allow-hotplug – Ativa a placa de rede na inicialização.

enp0s3 – Nome da Interface de rede adicionado automaticamente utilizando o sistema de nomenclatura.

iface – Interface de rede

inet dhcp – Está especificando que o endereço (inet) será atribuído via DHCP.

Em resumo com essas configurações dizem que a interface será iniciada junto com o sistema e terá a sua configuração através do **protocolo DHCP**.

Configuração da Interface de Rede

Agora, vamos então configurar a interface manualmente. Devemos abrir o arquivo interface e adicionar os seguintes itens:

```
auto enp0s3
iface enp0s3 inet static
address 192.168.1.100
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
#allow-hotplug enp0s3
#iface enp0s3 inet dhcp

# Configuração Manual
auto enp0s3
iface enp0s3 inet static
address 192.168.1.100
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Configuração da Interface de Rede

Com essas configurações estamos indicando os parâmetros:

auto enp0s3	– Iniciar a placa de rede junto ao sistema.
iface enp0s3 inet static	– Especificando que o endereço para enp0s3 será manual
address 192.168.1.100	– Endereço IP
netmask 255.255.255.0	– Máscara de Sub Rede
network 192.168.1.0	– Endereço de Rede
broadcast 192.168.1.255	– Endereço de Broadcast
gateway 192.168.1.1	– Endereço do Gateway

Ao término para carregar as novas configurações, entre com o comando para reiniciar o serviço de rede:

service networking restart

Comandos de Redes

Outro comando muito importante é o ping, que serve para verificar se um dispositivo na rede responde a uma solicitação, isso mostra que o dispositivo está ativo na rede.

Sintaxe: **ping *endereço_ip***

```
root@debian:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=1036 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=5.19 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=1.71 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=2.07 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=1.69 ms
64 bytes from 192.168.0.1: icmp_seq=6 ttl=64 time=1.61 ms
^C
--- 192.168.0.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 82ms
rtt min/avg/max/mdev = 1.610/174.675/1035.771/385.095 ms, pipe 2
root@debian:~#
```

Comandos de Redes

Também podemos verificar o **DNS** consultando o arquivo **resolv.conf** localizado dentro do **/etc**

```
root@debian-seg:/etc# cat resolv.conf
nameserver 8.8.8.8
nameserver 192.168.1.1
```

Você pode alterar ou acrescentar novos servidores DNS inserindo a linha “**nameserver**” mais o endereço IP.

Aproveitando o DNS, vamos falar agora sobre o arquivo **hostname**, esse que serve para consultar ou definir o nome do equipamento.

```
root@debian-seg:/etc# hostname
debian-seg
```

O arquivo **hostname** fica localizado dentro do diretório **/etc**, você pode editar o arquivo afim de trocar o nome da estação.

Comandos de Redes

Podemos também consultar o IP de determinados sites consultando o nosso DNS

Utilizando **nslookup**.

```
root@debian-seg:~# nslookup www.globo.com
Server:          172.20.9.6
Address:        172.20.9.6#53

Non-authoritative answer:
Name:    www.globo.com
Address: 186.192.81.5
```

Obs: O NSLOOKUP faz parte do pacote do **dnsutils**, que dever ser instalado no sistema

Comandos de Redes

traceroute ip ou domínio

Com traceroute podemos ver em tempo real todo o caminho que um pacote percorre até chegar ao seu destino.

```
root@debian:~# traceroute samsec.com.br
traceroute to samsec.com.br (191.252.51.11), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  1.404 ms  2.540 ms  2.523 ms
 2  10.72.64.1 (10.72.64.1)  13.134 ms  13.168 ms  13.129 ms
 3  c937e801.virtua.com.br (201.55.232.1)  13.658 ms  13.828 ms  13.880 ms
 4  187.28.225.17 (187.28.225.17)  18.212 ms  18.110 ms  18.079 ms
 5  200.230.235.97 (200.230.235.97)  20.105 ms  20.090 ms  19.968 ms
 6  ebt-B12-tcore01.cas.embratel.net.br (200.244.214.1)  25.761 ms  21.534 ms  25.924 ms
 7  ebt-B1191-tcore01.spo.embratel.net.br (200.230.252.130)  27.020 ms  26.522 ms  26.897 ms
 8  ebt-H0-12-0-1-agg03.spo.embratel.net.br (200.230.242.40)  22.738 ms  22.399 ms  22.048 ms
 9  peer-B59-agg03.spo.embratel.net.br (189.43.57.34)  22.010 ms  21.435 ms  21.898 ms
10  siteprotect.security.neustar (69.164.45.193)  22.737 ms  22.372 ms  22.336 ms
11  10.14.225.224 (10.14.225.224)  21.937 ms  20.091 ms  19.975 ms
12  172.16.50.165 (172.16.50.165)  20.188 ms  20.091 ms  19.340 ms
13  156.154.254.17 (156.154.254.17)  20.529 ms  20.483 ms  156.154.254.15 (156.154.254.15)  20.463 ms
14  ib1-2.r02.ita.br.as27715.net (177.153.201.38)  20.012 ms  19.941 ms  iv1500.g1b.ita.br.as27715.net (179.188.31.4)  25.593 ms
15  iv1500.g1a.ita.br.as27715.net (179.188.31.3)  24.964 ms  dist-fvbg2ita005.locaweb.com.br (179.188.36.172)  23.652 ms  23.201 ms
16  186.202.158.125 (186.202.158.125)  26.719 ms  dist-fvbg2ita005.locaweb.com.br (179.188.36.172)  19.763 ms  186.202.158.125 (186.202.158.125)  41.305 ms
17  186.202.158.125 (186.202.158.125)  43.908 ms  43.767 ms *
18  * * *
19  * * *
```

Comandos de Redes

ss

O comando ss serve para você verificar quais portas de rede estão abertas em seu Linux.

Opções:

- r resolve nomes dos hosts
- t mostrar portas tcp
- u mostrar portas udp
- l mostrar portas que estão em escuta
- p mostrar os processos que estão usando as portas
- n não resolve os nomes dos serviços (apresenta o serviço Linux e o ID)
- 4 somente ipv4
- 6 somente ipv6

Exemplo: ss -tulpn

Comandos de Redes

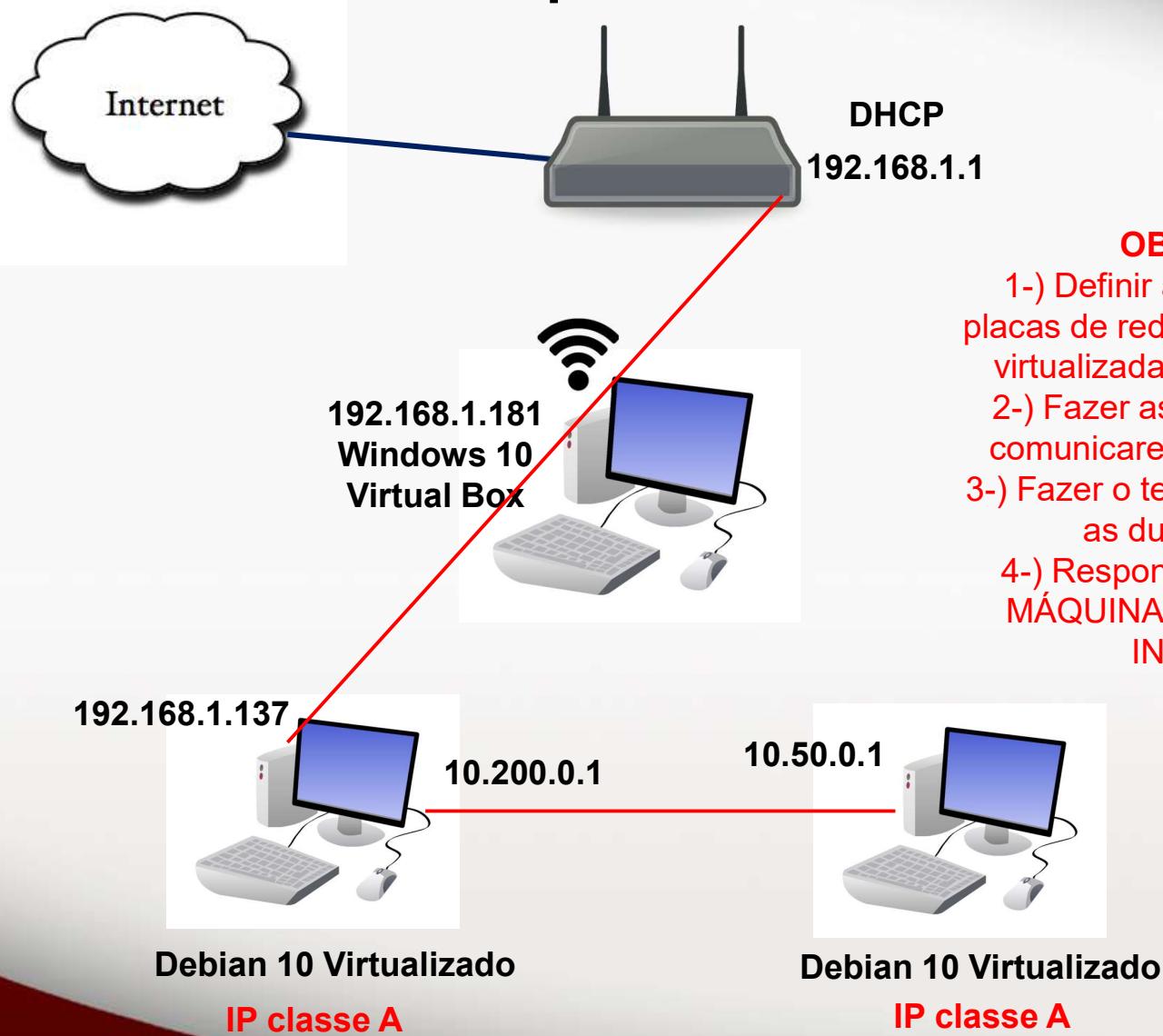
ss

```
root@debian:~# ss -tulpn
Netid State  Recv-Q Send-Q Local Address:Port  Peer Address:Port
udp  UNCONN 0        0          0.0.0.0:68      0.0.0.0:*      users:(("dhclient",pid=388,fd=7))
udp  UNCONN 0        0        192.168.0.255:137  0.0.0.0:*      users:(("nmbd",pid=376,fd=17))
udp  UNCONN 0        0        192.168.0.118:137  0.0.0.0:*      users:(("nmbd",pid=376,fd=16))
udp  UNCONN 0        0          0.0.0.0:137     0.0.0.0:*      users:(("nmbd",pid=376,fd=14))
udp  UNCONN 0        0        192.168.0.255:138  0.0.0.0:*      users:(("nmbd",pid=376,fd=19))
udp  UNCONN 0        0        192.168.0.118:138  0.0.0.0:*      users:(("nmbd",pid=376,fd=18))
udp  UNCONN 0        0          0.0.0.0:138     0.0.0.0:*      users:(("nmbd",pid=376,fd=15))
tcp  LISTEN 0       50         0.0.0.0:445     0.0.0.0:*      users:(("smbd",pid=447,fd=34))
tcp  LISTEN 0       50         0.0.0.0:139     0.0.0.0:*      users:(("smbd",pid=447,fd=35))
tcp  LISTEN 0      128        0.0.0.0:22      0.0.0.0:*      users:(("sshd",pid=402,fd=3))
tcp  LISTEN 0       50         [::]:445       [::]:*       users:(("smbd",pid=447,fd=32))
tcp  LISTEN 0       50         [::]:139       [::]:*       users:(("smbd",pid=447,fd=33))
tcp  LISTEN 0      128        [::]:22        [::]:*       users:(("sshd",pid=402,fd=4))
root@debian:~#
```

Linux Completo + Servidores

Aula 24: Prática Redes Linux

Arquitetura LAN



OBJETIVO 1:

- 1-) Definir a configuração das placas de rede das duas máquinas virtualizadas em modo Interno.
- 2-) Fazer as duas máquinas se comunicarem na rede classe A.
- 3-) Fazer o teste de conexão entre as duas máquinas.
- 4-) Responder a pergunta: AS MÁQUINAS TEM ACESSO A INTERNET?

Linux Completo + Servidores

Aula 25: Servidor de Arquivos (SAMBA)

Servidores de Arquivos

Um **servidor de arquivos** é um computador conectado a uma rede que tem o objetivo principal de proporcionar um local para o armazenamento compartilhado de arquivos de computadores (como documentos, arquivos de som, fotografias, filmes, imagens, bases de dados, etc)

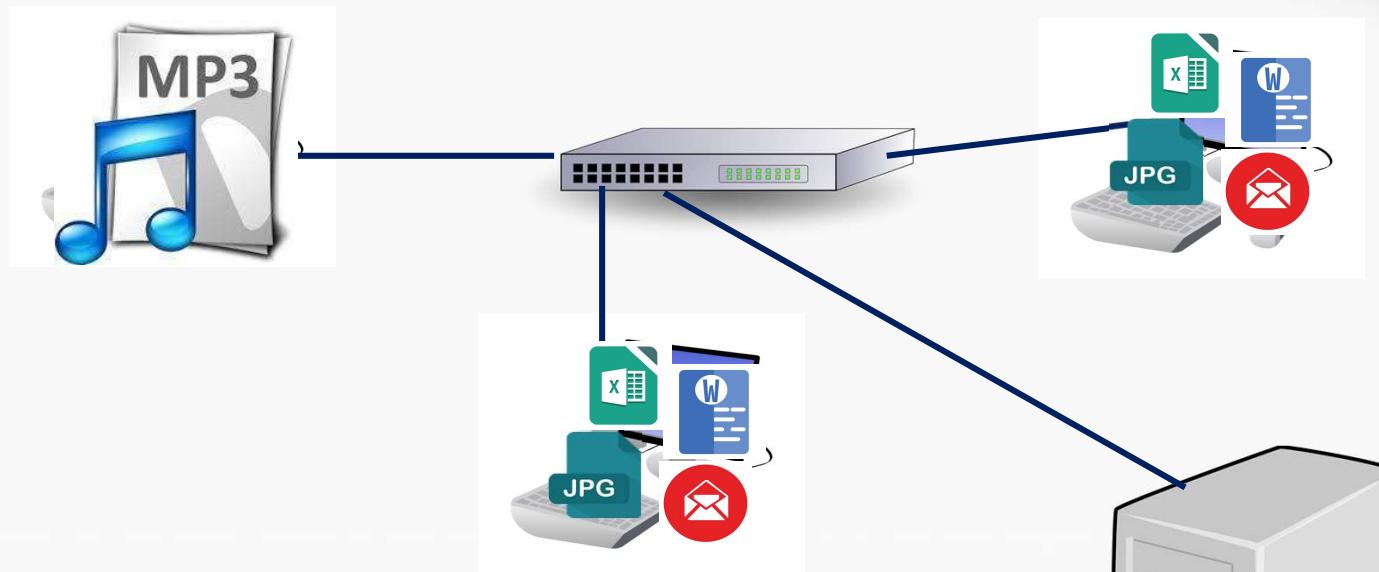
No Linux, o servidor de arquivos é o Samba, um conjunto de programas de interoperabilidade padrão do Windows para Linux e Unix

O Samba é um Software Livre licenciado sob a GNU General Public License , o projeto Samba é um membro da Software Freedom Conservancy .

Desde 1992 , o Samba fornece serviços de arquivo para todos os clientes que usam o protocolo **SMB (Server Message Block) /CIFS (Common Internet File System)**, como todas as versões do DOS e Windows, OS / 2, Linux e muitos outros.

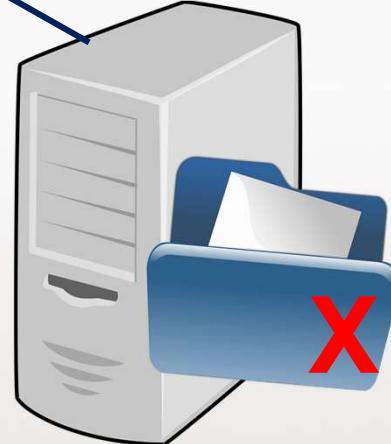
O Samba é um componente importante para integrar perfeitamente servidores e desktops Linux/Unix em ambientes do **Active Directory**. Ele pode funcionar como um controlador de domínio ou como um membro regular do domínio.

SAMBA – Servidor de Arquivos



Quais as vantagens de se ter um Servidor de Arquivos?

- 1- Backup
- 2- Centralização da Informação e Disponibilidade
- 3- Confidencialidade e Integridade da informação



**Servidor de
Arquivos
SAMBA**

Servidor de Arquivos

O Linux tem a capacidade de agir como um servidor de arquivos

Para essa tarefa vamos utilizar os serviços do SAMBA que é um conjunto de serviços que permite que máquinas Linux e Windows se comuniquem, compartilhando serviços de arquivos

Características:

- Compartilhamento de arquivos entre máquinas Linux e Windows.
- Controle de acesso leitura/gravação por compartilhamento ou por usuário autenticado.
- Possibilidade de definir compartilhamento público.
- Permite ocultar o conteúdo de determinados diretórios que não quer que sejam exibidos na rede.
- Permite montar unidades mapeadas de sistemas Windows ou outros servidores Linux como um diretório.
- Permite a configuração de recursos simples através de programas de configuração gráficos via web.

Servidor de Arquivos

Instalação

A instalação pode ser feita através do gerenciador de pacotes [apt-get](#). Entre com o comando:

```
apt-get install samba smbclient cifs-utils
```

O pacote samba é o servidor samba e os pacotes smbclient e cifs-utils fazem parte dos aplicativos cliente.

Servidor de Arquivos

Após a instalação, execute o comando:

service --status-all

```
root@debian-seg:/etc/systemd# service --status-all
[ - ]  console-setup.sh
[ + ]  cron
[ + ]  dbus
[ - ]  hwclock.sh
[ - ]  isc-dhcp-server
[ - ]  keyboard-setup.sh
[ + ]  kmod
[ + ]  networking
[ + ]  nmbd
[ + ]  procps
[ + ]  rsyslog
[ + ]  samba
[ - ]  samba-ad-dc
[ - ]  selinux-autorelabel
[ + ]  smbd
[ + ]  ssh
[ + ]  udev
[ + ]  winbind
```

Observe que o serviço do Samba estará aparecendo e com o sinal de + na frente, indicando que está ativo.

Servidor de Arquivos

Pode se controlar o serviço usando os comandos:

service smbd status

service smbd start

service smbd stop

service smbd restart

Servidor de Arquivos

Toda a configuração do Samba, incluindo as configurações gerais do servidor, impressoras e todos os compartilhamentos, é feita em um único arquivo de configuração, o **/etc/samba/smb.conf**

Por padrão, o arquivo **smb.conf** já vem com informações escritas e é possível ser personalizado, afim de estudos, renomeie o arquivo **smb.conf** para **smb.conf.original** dessa forma se você precisar para consulta de alguma informação do arquivo original ele ainda estará disponível

Crie um novo arquivo chamado **smb.conf** dentro do diretório **/etc/samba**.

Servidor de Arquivos

Com o arquivo **smb.conf** aberto, vamos adicionar as seguintes linhas, esse exemplo básico, cria um compartilhamento básico e público (sem autenticação nenhuma).

```
[global]
workgroup = WORKGROUP
log file = /var/log/samba/log.%m
syslog = 0
server role = standalone server
map to guest = bad user

[dados]
path = /dados
available = yes
browseable = yes
writable = yes
guest ok = yes
```

Servidor de Arquivos

O parâmetro **map to guest** mapeia usuários mal autenticados para a conta de convidado, portanto, basta adicionar o parâmetro **guest ok = yes** na sessão de compartilhamento.

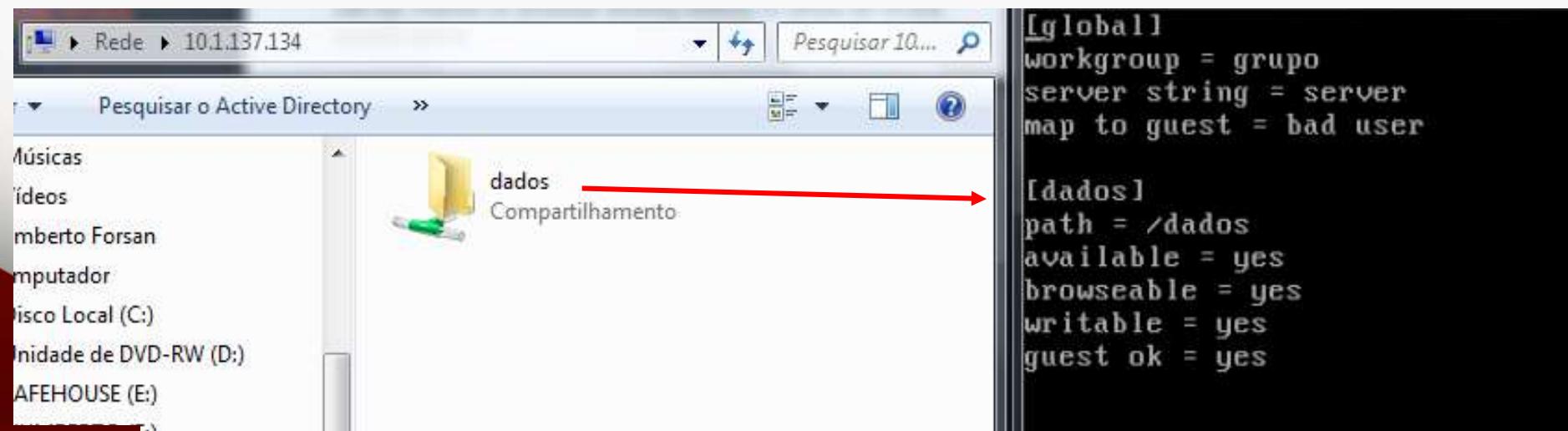
No nosso exemplo **[dados]**. Essa situação, cria um compartilhamento público chamado dados, sem a necessidade de autenticação.

Os outros parâmetros no compartilhamento são:

- **Path**, é o parâmetro que indica o caminho do diretório a ser compartilhado.
- **Available**, é o parâmetro que indica se o compartilhamento está habilitado ou não.

Servidor de Arquivos

- **Writable**, é o parâmetro que indica se o compartilhamento está com permissão de escrita. Aqui cabe uma observação, pois indicando **YES** o compartilhamento aceita gravação, colocando **NO** ele passa ser somente leitura, no caso de somente leitura, pode se substituir pela opção **read only = yes**.
- **Browsable**, é o parâmetro que indica se o compartilhamento vai estar visível ou oculto para a sua rede. (OBS: Não use como quesito de segurança a ocultação de compartilhamentos de rede, segurança por obscuridade não é totalmente eficaz.)



Servidor de Arquivos

Esses parâmetros configurados dentro do **smb.conf** permitem que um compartilhamento seja criado.

Mas para que o diretório possa ser acessado, ele tem q existir na HD do servidor Linux e também tem que ter a permissão local configurada. Segue os passos:

```
root@debian-seg:/# mkdir dados
root@debian-seg:/# ls
bin    dev  initrd.img   lost+found  opt    run    sys  var
boot   etc  initrd.img.old media      proc   sbin   tmp  vmlinuz
dados  home lib           mnt      root   srv    usr  vmlinuz.old
```

```
root@debian-seg:/# chmod 777 dados
```

Servidor de Arquivos

Vamos agora criar mais um compartilhamento que solicite autenticação de usuário e senha. Vamos criar o compartilhamento chamado TI.

Para isso, crie o diretório em sua HD chamado TI e de a permissão de CHMOD, para os testes vamos definir 777. Logo após abra o arquivo **smb.conf** e adicione os itens:

```
[global]
workgroup = grupo
server string = server
map to guest = bad user

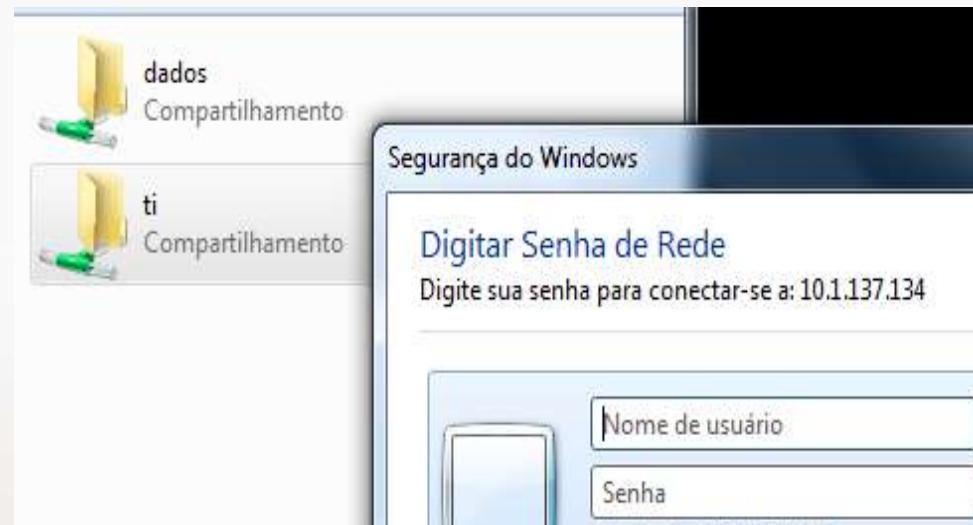
[dados]
path = /dados
available = yes
browseable = yes
writable = yes
guest ok = yes

[ti]
path = /ti
available = yes
browseable = yes
writable = yes
valid users = humberto, joao
```

Servidor de Arquivos

Aqui, você pode observar que o compartilhamento **[ti]** foi criado e também foi apresentado o parâmetro **valid users**.

Com isso ao tentar acessar o compartilhamento **ti** será solicitado um usuário e senha.



Servidor de Arquivos

O usuário solicitado é o descrito na frente da linha **valid users**, que em nosso exemplo são os usuários **humberto** e **joao**.

Esses usuários do nosso exemplo são usuários locais, portanto deve ser criados no Linux e configurado a devida permissão de acesso ao Samba.

Para criar os usuários Humberto e João, vamos executar o comando **adduser** e depois usar o **smbpasswd** para configurar permitir o acesso ao Samba.

Servidor de Arquivos

```
root@debian-seg:/# adduser joao
Adicionando usuário 'joao' ...
Adicionando novo grupo 'joao' (1001) ...
Adicionando novo usuário 'joao' (1001) com grupo 'joao' ...
Criando diretório pessoal '/home/joao' ...
Copiando arquivos de '/etc/skel' ...
Digite a nova senha UNIX:
Redigite a nova senha UNIX:
passwd: senha atualizada com sucesso
Modificando as informações de usuário para joao
Informe o novo valor ou pressione ENTER para aceitar o padrão
  Nome Completo []:
  Número da Sala []:
  Fone de Trabalho []:
  Fone Residencial []:
  Outro []:
A informação está correta? [S/n] s
```

```
root@debian-seg:/# smbpasswd -a joao
New SMB password:
Retype new SMB password:
Added user joao.
```

Segurança do Windows

Digite as credenciais de rede

Digite suas credenciais para conectar-se a:



joao

.....

Domínio:

Servidor de Arquivos

Dentro do seu compartilhamento, também pode ser adicionado o acesso a usuários que somente podem ler os arquivos, usando a opção:

```
[ti]
path = /ti
#available = yes
#browseable = yes
read only = yes
valid users = maria, humberto, joao
write list = humberto, joao
```

Servidor de Arquivos

Lixeira no Samba

Em qualquer servidor de arquivos, a principal prioridade é assegurar a integridade e a segurança dos dados.

Entretanto, por mais estável que seja a rede e por mais robusto que seja o servidor, o elo mais fraco da cadeia acaba sendo sempre o usuário.

E às vezes por acidente seu usuário pode então apagar um arquivo acidentalmente.

Para isso podemos habilitar o recurso de lixeira dentro do seu compartilhamento, permitindo um restore mais rápido em caso de acidentes. Para isso adicione na guia **[global]** a sessão da lixeira.

```
vfs object = recycle
recycle:repository = lixeira
recycle:keeptree = yes
recycle:versions = yes
recycle:repository = /lixeira
```

Servidor de Arquivos

Exemplo:

```
[global]
workgroup = grupo
server string = server
map to guest = bad user
vfs object = recycle
recycle:repository = lixeira
recycle:keeptree = yes
recycle:version = yes
recycle:repository = /lixeira
```

Lembre-se de **criar** o diretório **/lixeira** e dar a permissão de escrita com o comando **chmod 776**.

Será aqui que os arquivos apagados irão parar quando forem deletados

Também lembre-se que após qualquer alteração no arquivo **smb.conf**, o serviço do samba deve ser reinicializado utilizando o comando **service smbd restart**.

Servidor de Arquivos

Veto Files

Também é possível restringir os tipos de arquivos que podem ser salvos em um compartilhamento.

Por exemplo, pode se bloquear a gravação de arquivos .exe, .mp3, .mp4 entre outros.

Para realizar o bloqueio basta adicionar a opção **veto files** em seu compartilhamento.

veto files = /*.extensão 1/*.extensão 2

```
[dados]
path = /dados
available = yes
browseable = yes
writable = yes
quest ok = yes
veto files = /*.mp3/*.jpg
```

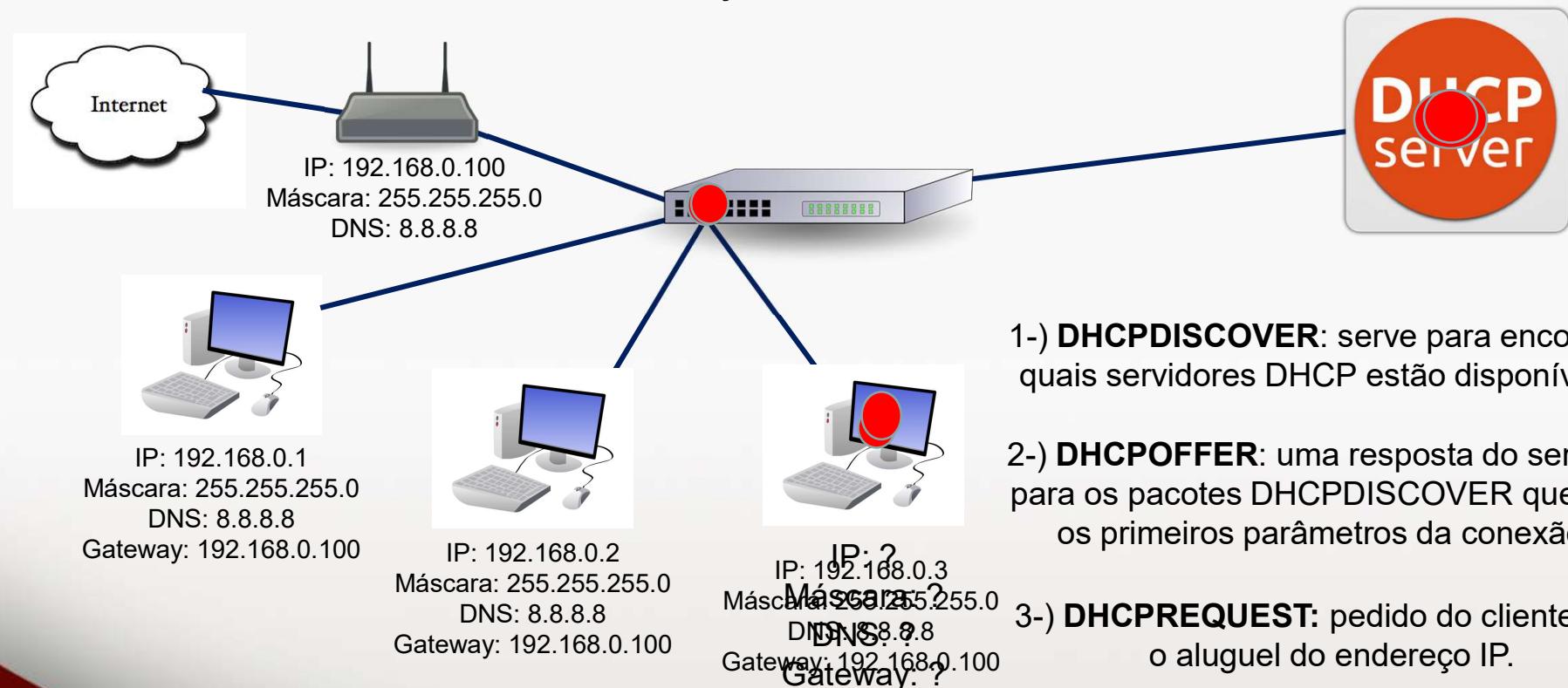
Linux Completo + Servidores

Aula 26: Servidor DHCP

Servidor DHCP

O **DHCP, Dynamic Host Configuration Protocol**, é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede.

O DHCP usa um modelo cliente-servidor, no qual o servidor DHCP mantém o **gerenciamento centralizado** dos endereços IP usados na rede.



1-) **DHCPDISCOVER**: serve para encontrar quais servidores DHCP estão disponíveis.

2-) **DHCPOFFER**: uma resposta do servidor para os pacotes DHCPDISCOVER que têm os primeiros parâmetros da conexão.

3-) **DHCPREQUEST**: pedido do cliente para o aluguel do endereço IP.

4-) **DHCPACK**: uma resposta do servidor com os parâmetros e o IP do computador do cliente.

Servidor DHCP

A instalação é feita com o pacote **isc-dhcp-server**

```
apt-get install isc-dhcp-server
```

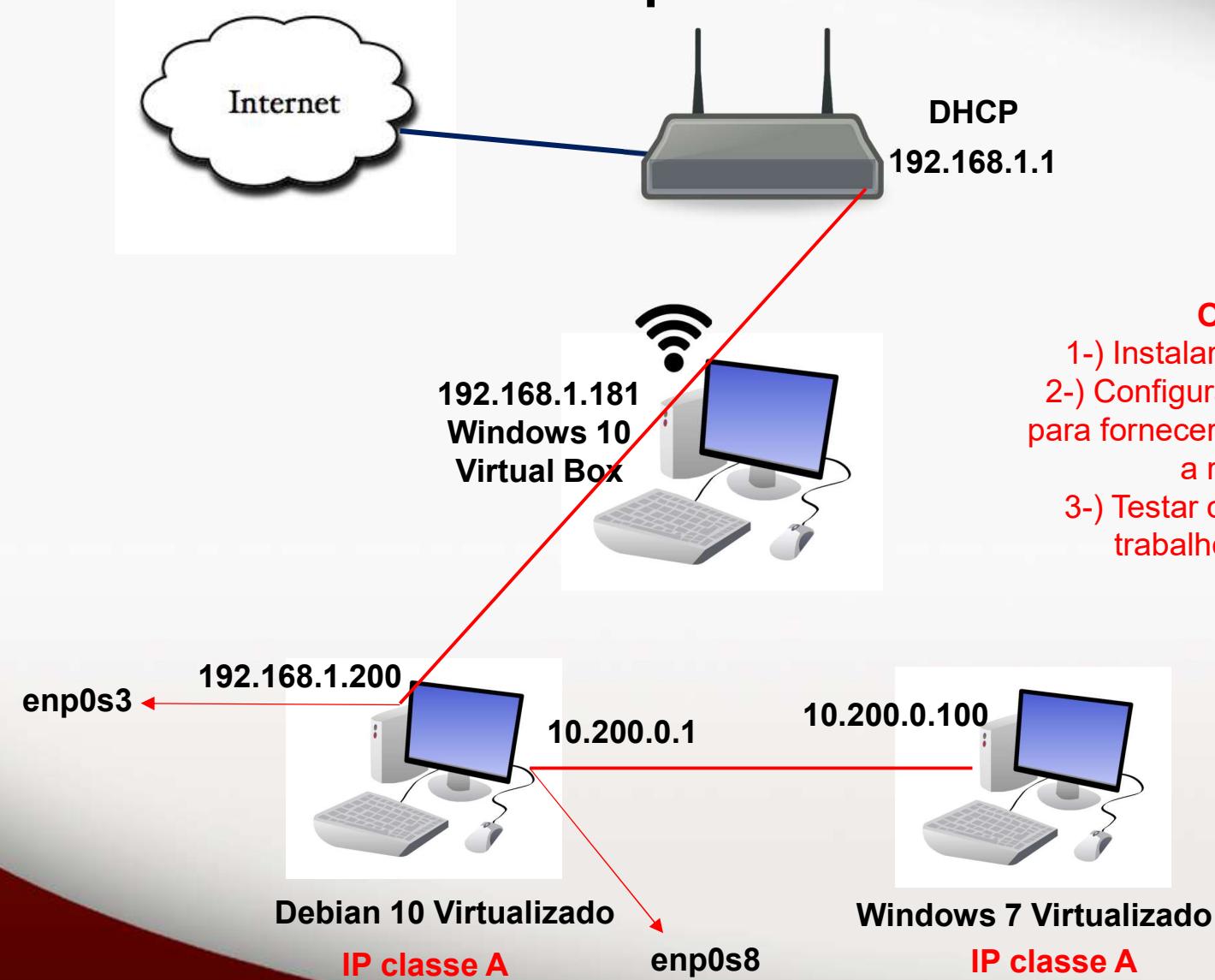
Como todo serviço, o DHCP pode ser iniciado, parado ou então reiniciado, para isso use os comandos:

```
service isc-dhcp-server start  
stop  
restart  
status
```

Arquivo de Configuração:

```
# /etc/dhcp/dhcpd.conf
```

Arquitetura LAN



OBJETIVO:

- 1-) Instalar o serviço de DHCP.
- 2-) Configurar o serviço de DHCP para fornecer as configurações para a rede interna.
- 3-) Testar com uma estação de trabalho na rede interna

Servidor DHCP

Primeiro vamos configurar qual placa de rede vai servir como DHCP

O arquivo que define as configurações é o **isc-dhcp-server** dentro do diretório **/etc/default**.

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpcd.conf).
#DHCPDV4_CONF=/etc/dhcp/dhcpcd.conf
#DHCPDV6_CONF=/etc/dhcp/dhcpcd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDV4_PID=/var/run/dhcpcd.pid
#DHCPDV6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESV4="enp0s8"
INTERFACESV6=""
```

Servidor DHCP

Configuração

A configuração do DHCP está dentro do **dhcpd.conf**.

/etc/dhcp/dhcpd.conf

```
ddns-update-style none;
option domain-name "samsec.com.br";
option domain-name-servers 10.200.0.1, 8.8.8.8;
default-lease-time 600;
max-lease-time 7200;
authoritative;

subnet 10.200.0.0 netmask 255.255.255.0 {
range 10.200.0.2 10.200.0.20;
option routers 10.200.0.1;
option broadcast-address 10.200.0.255;
}
```

Servidor DHCP

Você também pode consultar os equipamentos conectados em seu servidor DHCP consultando o arquivo **dhcpd.leases** localizado dentro de **/var/lib/dhcp**.

```
root@ad:/etc/dhcp# cat /var/lib/dhcp/dhcpd.leases
# The format of this file is documented in the dhcpd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.3.5

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

server-uid "\000\001\000\001!~k*\010\000'\227\0031";

lease 10.200.0.2 {
    starts 6 2017/10/21 20:50:35;
    ends 6 2017/10/21 21:00:35;
    cltt 6 2017/10/21 20:50:35;
    binding state active;
    next binding state free;
    rewind binding state free;
    hardware ethernet 08:00:27:56:40:61;
    uid "\001\010\000'v@a";
    set vendor-class-identifier = "MSFT 5.0";
    client-hostname "cp-ara-01";
}
```

Servidor DHCP

Também podemos criar reservas para equipamentos que precisem sempre manter o mesmo IP. Para isso devemos acrescentar no arquivo **dhcpd.conf** os itens abaixo:

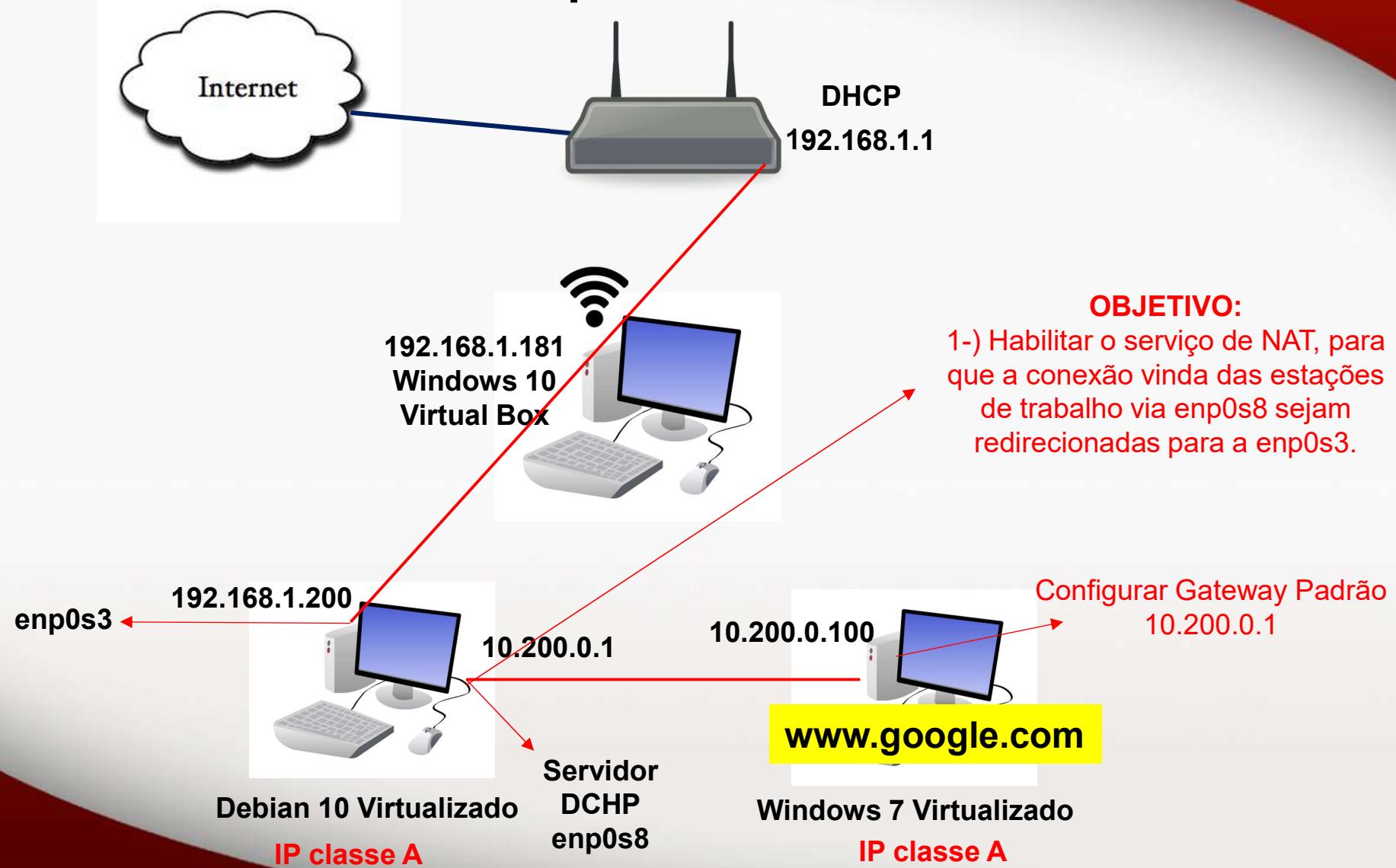
Exemplo Reserva DHCP

```
host m5 {  
hardware ethernet 00:0F:B0:55:EA:13;  
fixed-address 192.168.1.211;  
}  
  
ddns-update-style none;  
option domain-name "samsec.com.br";  
option domain-name-servers 10.200.0.1, 8.8.8.8;  
default-lease-time 600;  
max-lease-time 7200;  
authoritative;  
  
subnet 10.200.0.0 netmask 255.255.255.0 {  
range 10.200.0.2 10.200.0.20;  
option routers 10.200.0.1;  
option broadcast-address 10.200.0.255;  
}  
  
host cp_ara_01 {  
hardware ethernet 08:00:27:56:40:61;  
fixed-address 10.200.0.101;  
}
```

Linux Completo + Servidores

Aula 27: Compartilhando a Internet

Arquitetura LAN



Compartilhando a Internet

A próxima configuração, fará que possa ser compartilhado a internet para suas estações de trabalho. Transformando seu servidor Linux em um servidor de Internet.

Para compartilhar a internet, seguimos os seguintes comandos:

```
modprobe iptable_nat  
echo 1 > /proc/sys/net/ipv4/ip_forward  
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Compartilhando a Internet

Onde:

```
modprobe iptable_nat
```

modprobe – carrega os módulos necessários
iptable_nat – Carrega os módulos de roteamento

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

echo 1> - Inicia um script

/proc/sys/net/ipv4/ip_forward - ativa o "ip_forward", o módulo responsável pelo encaminhamento dos pacotes

```
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Cria uma regra de roteamento, que orienta o servidor a direcionar para a internet todos os pacotes (recebidos dos clientes) que se destinarem a endereços que não façam parte da rede local. A partir daí o servidor passa a ser o gateway da rede.

Compartilhando a Internet

O problema é que esses são comandos de terminal, ao executar, todo o tráfego da interface enp0s3 está fazendo um NAT para a interface enp0s8, mas ao reiniciar o equipamento, será perdido as configurações.

Para isso podemos criar um script e coloca-lo na inicialização de seu Linux, vamos criar o script chamado internet dentro do diretório **/etc/init.d**.

O script deve conter as informações abaixo:

```
#!/bin/sh

modprobe iptables_nat

echo 1 > /proc/sys/net/ipv4/ip_forward

# Limpando as tabelas iptables
iptables -F
iptables -t nat -F
iptables -t mangle -F

# Compartilhando a internet
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
```

Linux Completo + Servidores

Aula 28: Servidor WEB (Apache2 + Php)

Servidor WEB

Servidor web é um software responsável por aceitar pedidos em HTTP de clientes, geralmente os navegadores, e servi-los com respostas em HTTP

Isso inclui dados, que geralmente são páginas web, tais como documentos em HTML com objetos embutidos (imagens, etc.)

O mais popular, e mais utilizado no mundo, é o servidor **Apache** (software livre). A Microsoft possui a sua própria solução denominada **IIS** (Internet Information Services).

O servidor de web, é responsável por hospedar e publicar os recursos de HTTP e Banco de Dados, existem vários serviços e maneiras de realizara a publicação, normalmente se usa a combinação entre **APACHE, MYSQL e PHP**.



APACHE

O Servidor Apache, é o servidor web livre criado em 1995 por *Rob McCool*. É a principal tecnologia da Apache Software Foundation, responsável por mais de uma dezena de projetos envolvendo tecnologias de transmissão via web, processamento de dados e execução de aplicativos distribuídos.

É um servidor de protocolo HTTP e disponibilizado em versões para os sistemas operacionais Windows, Novell, OS/2 e outros do padrão POSIX IEEE 1003 (Unix, Linux, FreeBSD, etc.).

Instalação

```
apt-get install apache2
```

Durante a instalação do apache2 é criado um ficheiro de configuração localizado em:
/etc/apache2/sites-available/000-default.conf.

Reiniciar o servidor Apache2:
service apache 2 restart

APACHE

O Apache vem com um arquivo host virtual padrão chamado **000-default.conf** que você pode usar como default.

Caso seu servidor apache tenha apenas um site, basta deixar o arquivo padrão e adicionar o seu site dentro do diretório **/var/www/html**.

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
```

Porta de rede
configurada
para o
APACHE

Contato e
diretório de
armazenamento
padrão dos sites

Opções de LOG
*O diretório dos
arquivos de log do
Apache, são
armazenados dentro
de **/var/log/apache2**

APACHE

access.log

```
./var/log/apache2/access.log
root@humberto:/# cat /var/log/apache2/access.log
192.168.1.181 - - [30/Jul/2020:06:42:42 -0300] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36"
192.168.1.181 - - [30/Jul/2020:06:42:43 -0300] "GET /icons/openlogo-75.png HTTP/1.1" 200 6040 "http://192.168.1.200/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36"
192.168.1.181 - - [30/Jul/2020:06:42:43 -0300] "GET /favicon.ico HTTP/1.1" 404 491 "http://192.168.1.200/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36"
192.168.1.181 - - [30/Jul/2020:06:44:36 -0300] "GET / HTTP/1.1" 200 3380 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/84.0.4147.105 Safari/537.36"
root@humberto:/# _
```

error.log

```
root@humberto:/var/log/apache2# cat error.log
[Thu Jul 30 06:41:40.994261 2020] [mpm_event:notice] [pid 1035:tid 139850853274752] AH00489: Apache/2.4.38 (Debian) configured -- resuming normal operations
[Thu Jul 30 06:41:40.994394 2020] [core:notice] [pid 1035:tid 139850853274752] AH00094: Command line
: '/usr/sbin/apache2'
root@humberto:/var/log/apache2#
```

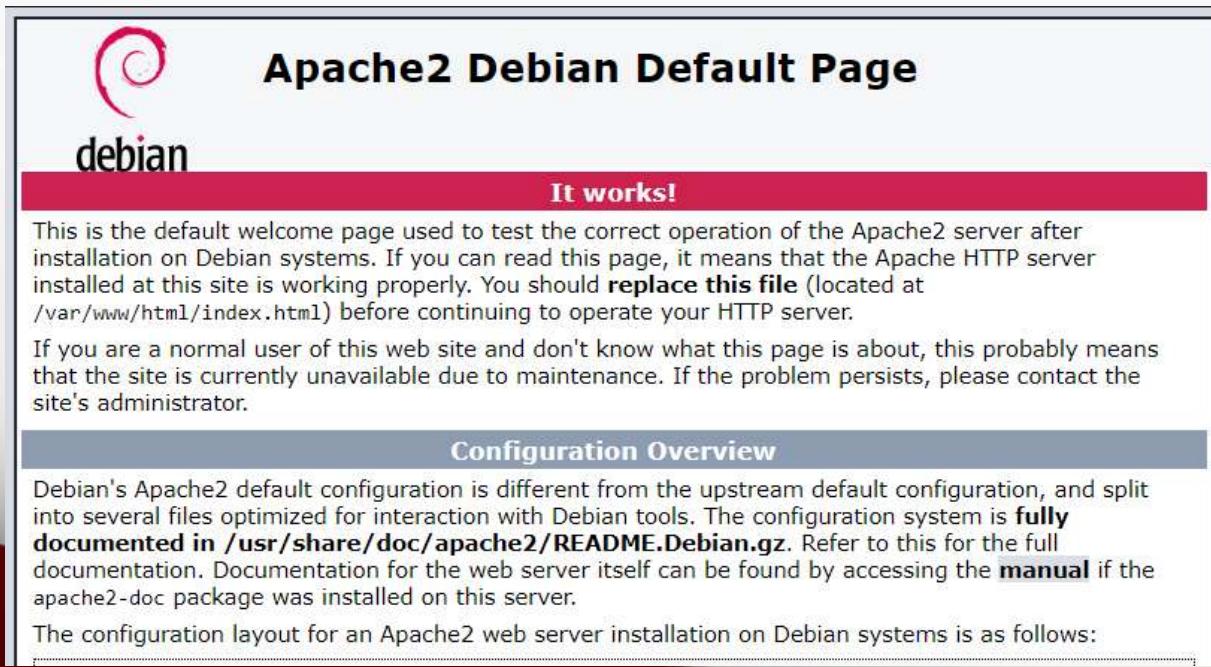
APACHE

index.html default

```
root@humberto:/var/www/html# ls  
index.html  
root@humberto:/var/www/html#
```

O index.html é a página padrão dentro dos diretórios nos servidores de websites que é carregada sempre que uma pasta seja solicitada e não seja especificado o nome de um arquivo específico, neste caso o próprio servidor se encarrega de procurar pelo arquivo index.html e entregar para o visitante.

A palavra index vem do Inglês, que quer dizer Índice. Traduzindo para a Internet, o arquivo index, seria a página principal, que guarda o índice (links) de todo o site.



The screenshot shows a web browser displaying the Apache2 Debian Default Page. The page features the Debian logo (a red spiral icon) and the word "debian" below it. The main title is "Apache2 Debian Default Page". A red banner across the middle contains the text "It works!". Below the banner, a paragraph explains that this is the default welcome page for testing the Apache2 server on Debian systems. It mentions that if the page is visible, the server is working correctly and suggests replacing the file at /var/www/html/index.html before continuing. Another section, "Configuration Overview", provides information about the Debian-specific configuration files, mentioning /usr/share/doc/apache2/README.Debian.gz for full documentation and the apache2-doc package for the manual. At the bottom, it notes the configuration layout for an Apache2 web server installation on Debian systems.

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

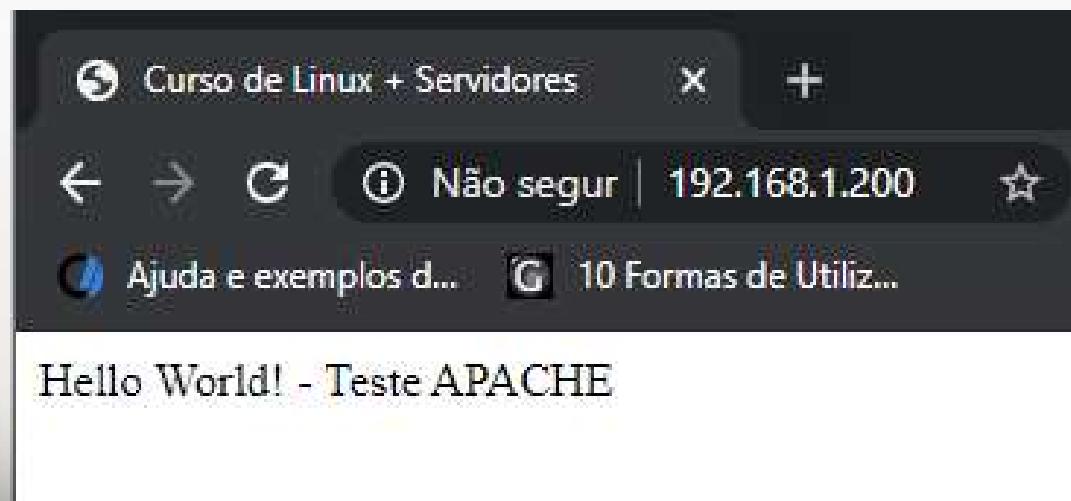
Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

APACHE

Teste Hello World

```
<!DOCTYPE html>
<html>
<head>
<title>Curso de Linux + Servidores</title>
</head>
<body>
Hello World! - Teste APACHE
</body>
</html>
~
```



APACHE

Mas se seu servidor for hospedar mais páginas, será necessário trabalhar com arquivos de host virtual.

Os arquivos do host virtual especificam a configuração real de nossos hosts virtuais e editam como o servidor da web Apache responderá a várias solicitações de domínio.

Crie o diretório para o seu novo site:

Exemplos:

```
mkdir -p /var/www/teste.com.br/public_html  
mkdir -p /var/www/zezinho.com.br/public_html
```

Crie um novo **index.html**, exemplo de conteúdo:

```
<html>  
  <head>  
    <title>Bem vindo!</title>  
  </head>  
  <body>  
    <h1>Teste do Servidor Apache</h1>  
  </body>  
</html>
```

Servidor Internet

Criar o arquivo de configuração dos sites:

O Apache vem com um arquivo host virtual padrão chamado **000-default.conf** que você pode usar como ponto de partida. Copie este arquivo para o primeiro domínio:

```
cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/teste.com.br.conf
```

Após a cópia do arquivo, realizar as seguintes alterações:

```
<VirtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port th
at
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin contato@teste.com.br
    ServerName teste.com.br
    ServerAlias www.teste.com.br
    DocumentRoot /var/www/teste.com.br/public_html

    # Available loglevels: trace0, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn
```

Servidor Internet

Ativar o site:
a2ensite teste.com.br.conf

Após a execução será retornada a seguinte mensagem:

Enabling site example.com.

To activate the new configuration, you need to run:
service apache2 reload

Lembre-se de desativar o site padrão 000-default.conf:
a2dissite 000-default.conf

Reinicie o apache
service apache2 restart

Extras

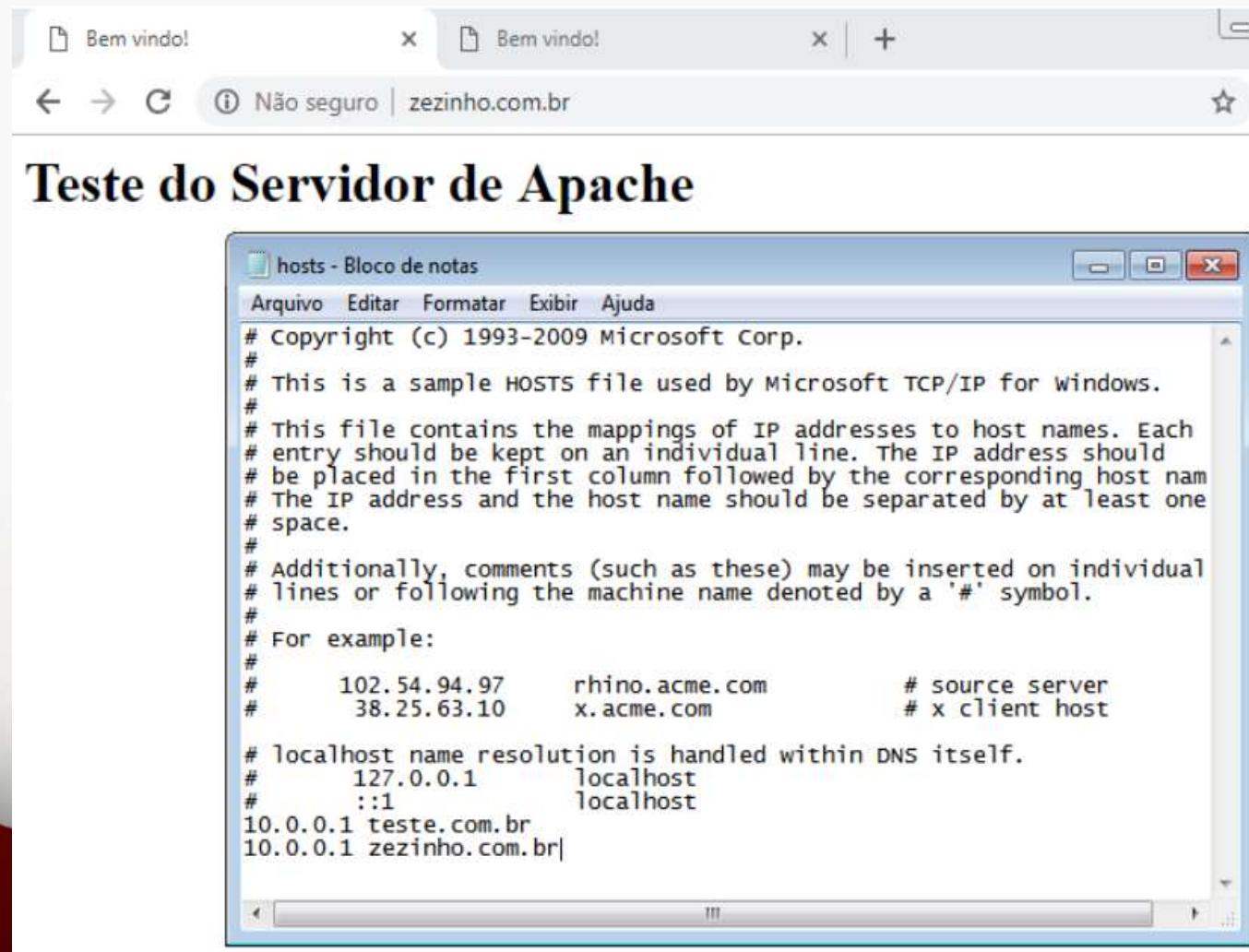
Verificar que a sintaxe do ficheiro de configuração está correta:
apachectl -t

Verificar versão Apache:
apache2 -v

Servidor Internet

Teste no Windows

```
c:\> notepad %windir%\system32\drivers\etc\hosts
```





O PHP (um acrônimo recursivo para PHP: Hypertext Preprocessor) é uma linguagem de script open source de uso geral, muito utilizada, e especialmente adequada para o desenvolvimento web e que pode ser embutida dentro do HTML.

Instalar PHP

```
# apt-get install php7.3 libapache2-mod-php7.3 php7.3-mysql php-common  
php7.3-cli php7.3-common php7.3-json php7.3-opcache php7.3-readline
```

OBS: a última verão é a 7.3

Ativar o módulo do PHP

```
# a2enmod php7.3
```

Consultar a versão do PHP

```
# php --version
```

Linux Completo + Servidores

Aula 29: MariaDB

Banco de Dados: São conjuntos de arquivos armazenados e relacionados através de tabelas. São coleções organizadas de dados que se relacionam de forma a criar algum sentido e dar mais eficiência durante uma pesquisa.

SGBD: Sistema Gerenciador de Banco de Dados são os softwares responsáveis pela criação, administração e armazenamento de um banco de dados.

Tabelas: São os locais lógicos onde os dados ficam armazenados de uma maneira organizada, uma tabela é formada por campos e registros. Os campos são os valores fixos de uma tabela, como nome, telefone, email... Já os registros são as informações adicionadas dentro da tabela.



O MySQL original foi criado por uma empresa finlandesa/sueca, a MySQL AB, fundada por David Axmark, Allan Larsson e Michael "Monty" Widenius.

A primeira versão do MySQL apareceu em 1995 . Foi criado inicialmente para uso pessoal, mas em poucos anos evoluiu para um banco de dados de nível empresarial e se tornou o software de banco de dados relacional de código aberto mais popular do mundo.

Em janeiro de 2008, a Sun Microsystems comprou o MySQL por US \$ 1 bilhão. Logo depois, a Oracle adquiriu toda a Sun Microsystems após obter aprovação da Comissão Europeia no final de 2009

Por desconfiar da administração do MySQL pela Oracle, os desenvolvedores originais do MySQL criaram o **MariaDB** em 2009 . Com o passar do tempo, o MariaDB substituiu o MySQL.

MariaDB

Instalar MySQL (Maria DB)

apt-get install mariadb-server

Após a instalação, executar a configuração de segurança

mysql_secure_installation

```
root@debian:/# mysql_secure_installation
```

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!
```

```
In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.
```

```
Enter current password for root (enter for none):
OK, successfully used password, moving on...
```

```
Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorisation.
```

```
You already have a root password set, so you can safely answer 'n'.
```

Para conectar no banco de dados

mariadb -u root

MariaDB

1) Criar um Banco de Dados:

create database teste;

```
mysql> create database teste;
Query OK, 1 row affected (0.00 sec)
```

2) Criar uma tabela cadastro com os campos codigo, nome, email, endereço, nascimento, nacionalidade:

```
create table cadastro
(
codigo int,
nome varchar(40),
email varchar(40),
endereco varchar(50),
nascimento char(8),
nacionalidade varchar(40)
);
```

```
mysql> create table cadastro
-> (
-> codigo int,
-> nome varchar(40),
-> email varchar(40),
-> endereco varchar(50),
-> nascimento char(8),
-> nacionalidade varchar(40)
-> )
-> ;
Query OK, 0 rows affected (0.11 sec)
```

* Visualizar uma tabela:

```
select *
from cadastro;
```

MariaDB

3) Apagar uma tabela:

drop table cadastro;

```
mysql> drop table cadastro;
Query OK, 0 rows affected (0.02 sec)
```

4) Apagar um banco de dados:

drop database teste;

```
mysql> drop database teste;
Query OK, 0 rows affected (0.00 sec)
```

5) Mostrar as tabelas:

show tables;

```
mysql> show tables;
+-----+
| Tables_in_teste |
+-----+
| cadastro         |
+-----+
1 row in set (0.00 sec)
```

6) Mostrar os bancos de dados:

show databases;

```
mysql> show databases;
+-----+
| Database      |
+-----+
| information_schema |
| mysql          |
| performance_schema |
| snort          |
| teste          |
+-----+
5 rows in set (0.00 sec)
```

MariaDB

7) Inserir dados em uma tabela:

```
insert into cadastro ( codigo, nome, email, endereco, nascimento, nacionalidade)
values ( 1, 'Humberto Forsan', 'hforsan@gmail.com', 'Rua X', '20091984', 'Brasileiro');
```

```
mysql> insert into cadastro (codigo, nome, email, endereco, nascimento, nacionalidade)
values (1, 'Humberto Forsan', 'hforsan@gmail.com', 'Rua X', '20091984', 'Brasileiro');
Query OK, 1 row affected (0.06 sec)
```

8) Recuperando e visualizando os dados armazenados em uma tabela:

```
select *
```

```
from cadastro;
```

```
mysql> select * from cadastro;
+-----+-----+-----+-----+-----+
| codigo | nome           | email          | endereco | nascimento | nacionalidade |
+-----+-----+-----+-----+-----+
|       1 | Humberto Forsan | hforsan@gmail.com | Rua X    | 20091984   | Brasileiro    |
+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)
```

9) Apagando os dados armazenados em uma tabela:

```
delete from cadastro
```

```
where nome='Humberto Forsan';
```

```
mysql> delete from cadastro
      -> where nome = 'Humberto Forsan';
Query OK, 1 row affected (0.10 sec)
```

Linux Completo + Servidores

Aula 30: WordPress



WordPress é um sistema livre e aberto de gestão de conteúdo para internet (do inglês: Content Management System - CMS), baseado em PHP com banco de dados MySQL

Executado em um servidor interpretador, voltado principalmente para a criação de páginas eletrônicas (sites) e blogs online.

É uma das ferramentas mais utilizadas para conteúdo na web

É possível desenvolver sites de tipo comércio eletrônico, revistas, portfólio, gerenciador de projeto, agregador de eventos e, outros conteúdos devido a sua capacidade de extensão através de ***plugins, API's (Application Programming Interface) temas e programação.***

WordPress

Instalação

Pré Requisitos:

O WordPress precisará de um **servidor web (APACHE)**, um **banco de dados (MARIADB)** e o **PHP** para funcionar corretamente. A configuração de uma pilha LAMP (Linux, Apache, MariaDB e PHP) atende a todos esses requisitos.

- 1-) Criando um Banco de Dados MariaDB e um Usuário para o WordPress

CREATE DATABASE wordpress DEFAULT CHARACTER SET utf8 COLLATE utf8_unicode_ci;

```
root@humberto:~# mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 10.3.23-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

[ MariaDB [(none)]> create database wordpress default character set utf8 collate utf8_unicode_ci;
Query OK, 1 row affected (0.003 sec)
|
```

WordPress

Crie uma conta de usuário MySQL que usaremos exclusivamente para operar em nosso novo banco de dados.

GRANT ALL ON wordpress.* TO 'wordpress_user'@'localhost' IDENTIFIED BY 'senha';

```
MariaDB [(none)]> grant all on wordpress.* to 'wordpress_user'@'localhost' identified by 'teste';
Query OK, 0 rows affected (0.002 sec)
```

Agora você tem um banco de dados e uma conta de usuário, cada um feito especificamente para o WordPress. Execute o seguinte comando para recarregar as permissões:

FLUSH PRIVILEGES;

```
MariaDB [(none)]> flush privileges;
Query OK, 0 rows affected (0.000 sec)
```

WordPress

2-) Instalando Extensões Adicionais do PHP

apt-get install php-curl php-gd php-mbstring php-xml php-xmlrpc php-soap php-intl php-zip

```
root@humberto:~# apt-get install php-curl php-gd php-mbstring php-xml php-xmlrpc php-soap php-intl php-zip
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
The following additional packages will be installed:
 libgd3 libxmlrpc-epi0 libxpm4 libxs1t1.1 libzip4 php7.3-curl php7.3-gd php7.3-intl
 php7.3-mbstring php7.3-soap php7.3-xml php7.3-xmlrpc php7.3-zip
Pacotes sugeridos:
 libgd-tools
Os NOVOS pacotes a seguir serão instalados:
 libgd3 libxmlrpc-epi0 libxpm4 libxs1t1.1 libzip4 php-curl php-gd php-intl php-mbstring php-soap
 php-xml php-xmlrpc php-zip php7.3-curl php7.3-gd php7.3-intl php7.3-mbstring php7.3-soap
 php7.3-xml php7.3-xmlrpc php7.3-zip
0 pacotes atualizados, 21 pacotes novos instalados, 0 a serem removidos e 1 não atualizados.
É preciso baixar 1.518 kB de arquivos.
Depois desta operação, 4.838 kB adicionais de espaço em disco serão usados.
Você quer continuar? [S/n] s_
```

Reinicie o serviço do Apache

service apache2 restart

WordPress

3-) Ajustando a Configuração do Apache para Permitir Sobreposições e Reescritas no .htaccess

Com base nos tutoriais de pré-requisito, você deve ter um arquivo de configuração para o seu site no diretório **/etc/apache2/sites-available/**. Usaremos **/etc/apache2/sites-available/wordpress.conf** como exemplo aqui.

Além disso, usaremos **/var/www/wordpress** como o diretório raiz da nossa instalação do WordPress.

Crie o arquivo **wordpress.conf**

```
root@humberto:~# vi /etc/apache2/sites-available/wordpress.conf_
```

WordPress

E adicione o seguinte conteúdo:

OBS: Lembre-se de copiar o arquivo 000-default.conf para o wordpress.conf e faça as alterações

```
<virtualHost *:80>
    # The ServerName directive sets the request scheme, hostname and port that
    # the server uses to identify itself. This is used when creating
    # redirection URLs. In the context of virtual hosts, the ServerName
    # specifies what hostname must appear in the request's Host: header to
    # match this virtual host. For the default virtual host (this file) this
    # value is not decisive as it is used as a last resort host regardless.
    # However, you must set it for any further virtual host explicitly.
    #ServerName www.example.com

    ServerAdmin contato@wordpress.com.br
    ServerName wordpress.com.br
    ServerAlias www.wordpress.com.br
    DocumentRoot /var/www/wordpress

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf
</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
~
```

WordPress

Em seguida, ative o módulo rewrite para utilizar o recurso de link permanente ou permalink do WordPress:

a2enmod rewrite

Depois teste os arquivos de configuração com o comando:

apache2ctl configtest

E reinicie novamente o serviço do Apache

```
root@humberto:~# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@humberto:~# apache2ctl configtest
AH00557: apache2: apr_sockaddr_info_get() failed for humberto
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0
.0.1. Set the 'ServerName' directive globally to suppress this message
Syntax OK
root@humberto:~# service apache2 restart
root@humberto:~# _
```

WordPress

4-) Baixando o WordPress

wget https://wordpress.org/latest.tar.gz

```
root@humberto:~# wget https://wordpress.org/latest.tar.gz
--2020-08-05 17:05:48-- https://wordpress.org/latest.tar.gz
Resolvendo wordpress.org (wordpress.org)... 198.143.164.252
Conectando-se a wordpress.org (wordpress.org)|198.143.164.252|:443... conectado.
A requisição HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 12238031 (12M) [application/octet-stream]
Salvando em: "latest.tar.gz"

latest.tar.gz          100%[=====] 11,67M 713KB/s   em 55s

2020-08-05 17:06:43 (217 KB/s) - "latest.tar.gz" salvo [12238031/12238031]

root@humberto:~# ls
compactado.tar  grep      latest.tar.gz  teste      teste2.doc  teste5.txt
dados.tar       humberto.tar tar        teste1.txt  teste3.jpg  w
root@humberto:~# _
```

Descompacte o arquivo:
tar xzvf latest.tar.gz

E você terá um diretório chamado **wordpress**

WordPress

Vamos mover esses arquivos para o nosso **document root**. Antes, porém, adicionamos um arquivo vazio **.htaccess** para que este fique disponível para uso posterior do WordPress.

```
touch /root/wordpress/.htaccess
```

Em seguida, copie o arquivo de configuração de amostra para o nome de arquivo que o WordPress realmente lê:

```
cp /root/wordpress/wp-config-sample.php /root/wordpress/wp-config.php
```

Além disso, crie o diretório upgrade para que o WordPress não tenha problemas de permissão ao tentar fazer isso sozinho após uma atualização do software:

```
mkdir /root/wordpress/wp-content/upgrade
```

Em seguida, copie todo o conteúdo do diretório para seu document root. Observe que o comando a seguir inclui um ponto no final do diretório de origem para indicar que tudo dentro do diretório deve ser copiado:

```
cp -a /root/wordpress/. /var/www/wordpress
```

WordPress

5-) Configurando o Diretório do WordPress

Antes de iniciarmos o processo de configuração baseado em web do WordPress, precisamos ajustar alguns itens em nosso diretório do WordPress.

Vamos alterar as permissões de todos os arquivos ao usuário e grupo **www-data**. Este é o usuário com o qual o servidor web Apache é executado, e o Apache precisará ler e gravar arquivos do WordPress para servir o site e executar atualizações automáticas.

```
chown -R www-data.www-data /var/www/wordpress
```

Vamos ajustar um pouco mais as permissões corretas nos diretórios e arquivos do WordPress:

```
find /var/www/wordpress/ -type d -exec chmod 750 {} +
find /var/www/wordpress/ -type f -exec chmod 640 {} +
```

```
root@humberto:~# find /var/www/wordpress/ -type d -exec chmod 750 {} +
root@humberto:~# find /var/www/wordpress/ -type f -exec chmod 640 {} +
root@humberto:~#
```

WordPress

6-) Configurando o arquivo wp-config.php

Agora vamos modificar as configurações de conexão do banco de dados na parte superior do arquivo. Você precisa ajustar o nome do banco de dados, o usuário do banco de dados e a senha associada que você configurou no MariaDB.

```
// ** MySQL settings - You can get this info from your web host ** //^M
//** The name of the database for WordPress **/^M
define( 'DB_NAME', 'wordpress' );^M
^M
//** MySQL database username **/^M
define( 'DB_USER', 'wordpress_user' );^M
^M
//** MySQL database password **/^M
define( 'DB_PASSWORD', 'teste' );^M
^M
//** MySQL hostname **/^M
define( 'DB_HOST', 'localhost' );^M
^M
//** Database Charset to use in creating database tables. **/^M
define( 'DB_CHARSET', 'utf8' );^M
^M
//** The Database Collate type. Don't change this if in doubt. **/^M
define( 'DB_COLLATE', '' );^M
^M
/**#@+^M
```

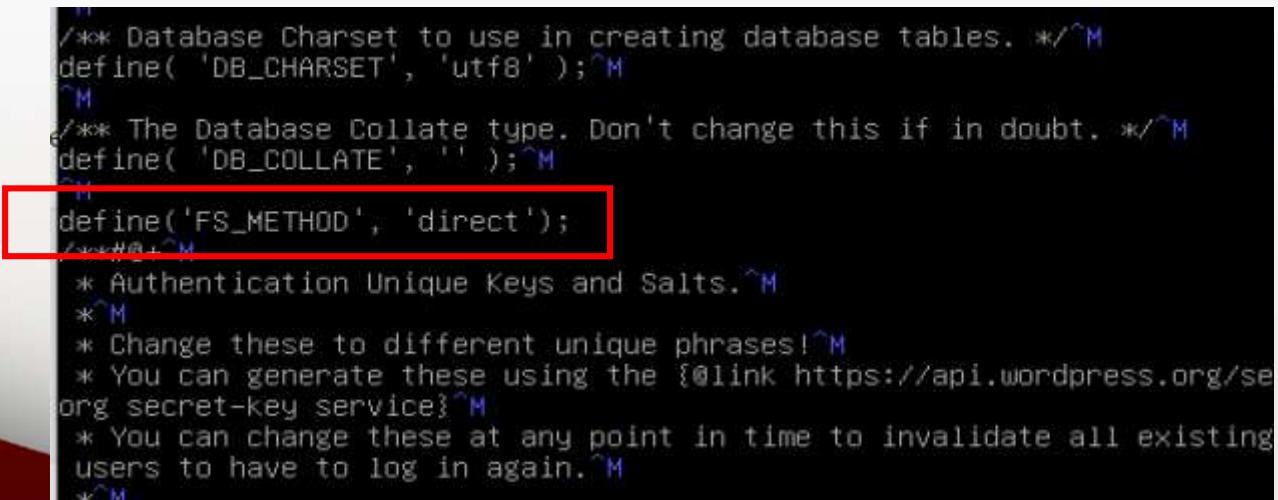
WordPress

A outra alteração que você deve fazer é definir o método que o WordPress deve usar para gravar no sistema de arquivos. Como concedemos ao servidor web permissão para gravar onde ele precisar, podemos definir explicitamente o método do sistema de arquivos como “**direct**”.

Se você não definir isso com nossas configurações atuais, o WordPress solicitará credenciais de FTP quando você executar determinadas ações.

Essa configuração pode ser adicionada abaixo das configurações de conexão com o banco de dados ou em qualquer outro local do arquivo:

```
define('FS_METHOD', 'direct');
```



```
/* Database Charset to use in creating database tables. */^M
define( 'DB_CHARSET', 'utf8' );^M
^M
/* The Database Collate type. Don't change this if in doubt. */^M
define( 'DB_COLLATE', '' );^M
^M
define('FS_METHOD', 'direct');
^M#^M
 * Authentication Unique Keys and Salts.^M
 *^M
 * Change these to different unique phrases!^M
 * You can generate these using the {@link https://api.wordpress.org/se
org secret-key service}^M
 * You can change these at any point in time to invalidate all existing
users to have to log in again.^M
 *^M
```

WordPress

7-) Caso você esteja usando a mesma máquina das aulas sobre o Apache, MariaDB, vamos desativar os sites criados anteriormente e ativar o site wordpress. Siga os comandos abaixo:

```
root@humberto:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf  teste.com.br.conf  wordpress.conf  zezinho.com.br.conf
root@humberto:/etc/apache2/sites-available# a2dissite teste.com.br.conf
Site teste.com.br disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@humberto:/etc/apache2/sites-available# a2dissite zezinho.com.br.conf
Site zezinho.com.br disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@humberto:/etc/apache2/sites-available# service apache2 restart
root@humberto:/etc/apache2/sites-available# a2ensite wordpress.conf
Enabling site wordpress.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@humberto:/etc/apache2/sites-available# service apache2 restart
[1] + 17777 Stopped                  nginx
```

WordPress

8-) Completando a Instalação Através da Interface Web

Agora que a configuração do servidor está concluída, podemos concluir a instalação através da interface web.

No seu navegador, entre com o IP do seu servidor:

192.168.1.200/wp-admin/install.php

Welcome

Welcome to the famous five-minute WordPress installation process! Just fill in the information below and you'll be on your way to using the most extendable and powerful personal publishing platform in the world.

Information needed

Please provide the following information. Don't worry, you can always change these settings later.

Site Title

Username
Usernames can have only alphanumeric characters, spaces, underscores, hyphens, periods, and the @ symbol.

Password Hide
Strong

Important: You will need this password to log in. Please store it in a secure location.

Your Email
Double-check your email address before continuing.

Search Engine Visibility Discourage search engines from indexing this site
It is up to search engines to honor this request.

Install WordPress

WordPress

Após a instalação, você terá o ambiente de login acessando o endereço:
http://ip_do_seu_servidor/wp-login.php

192.168.1.200/wp-login.php



Username or Email Address

Password

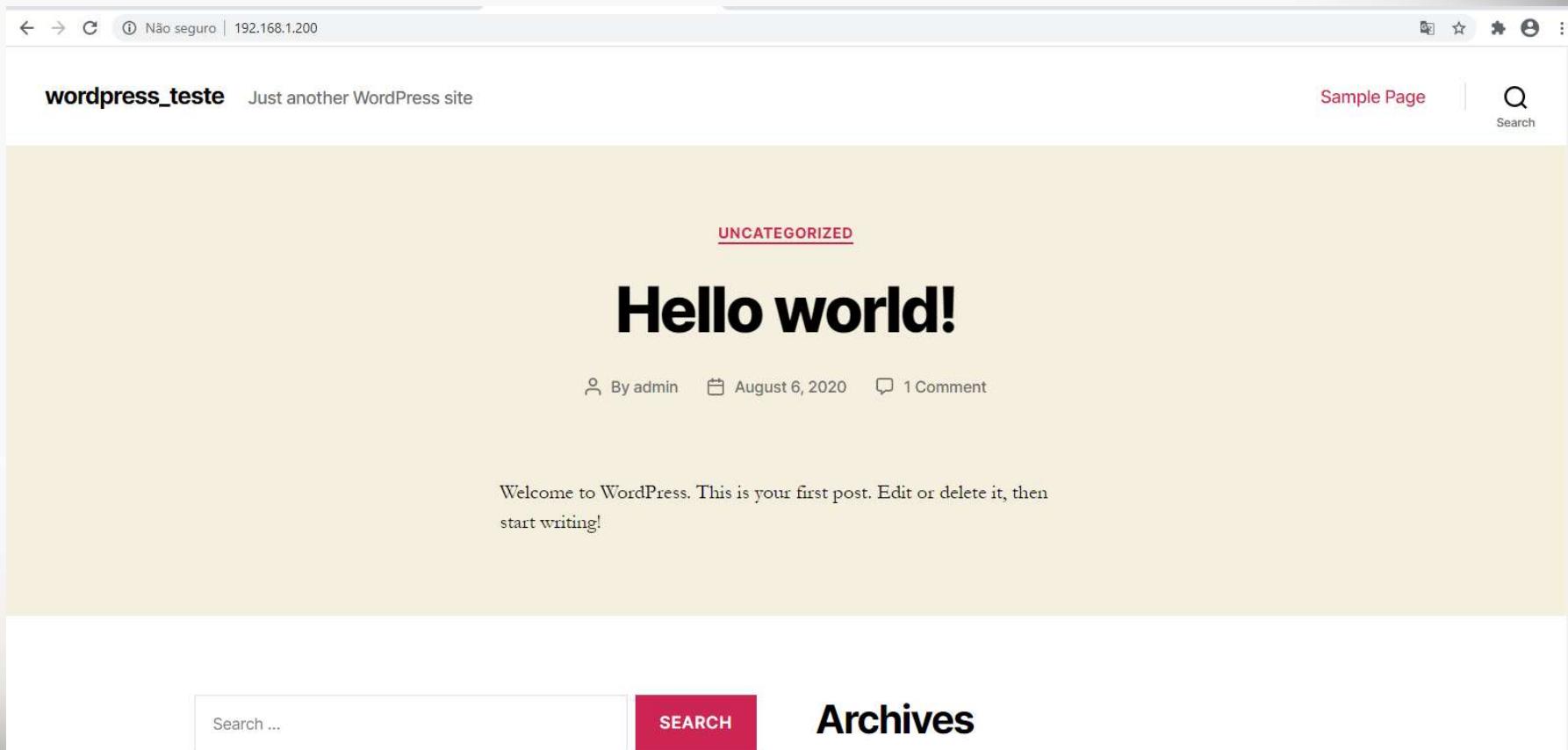
A small blue eye icon is located at the far right end of the password input field.

Remember Me

Log In

WordPress

E seu Wordpress está funcional:



Linux Completo + Servidores

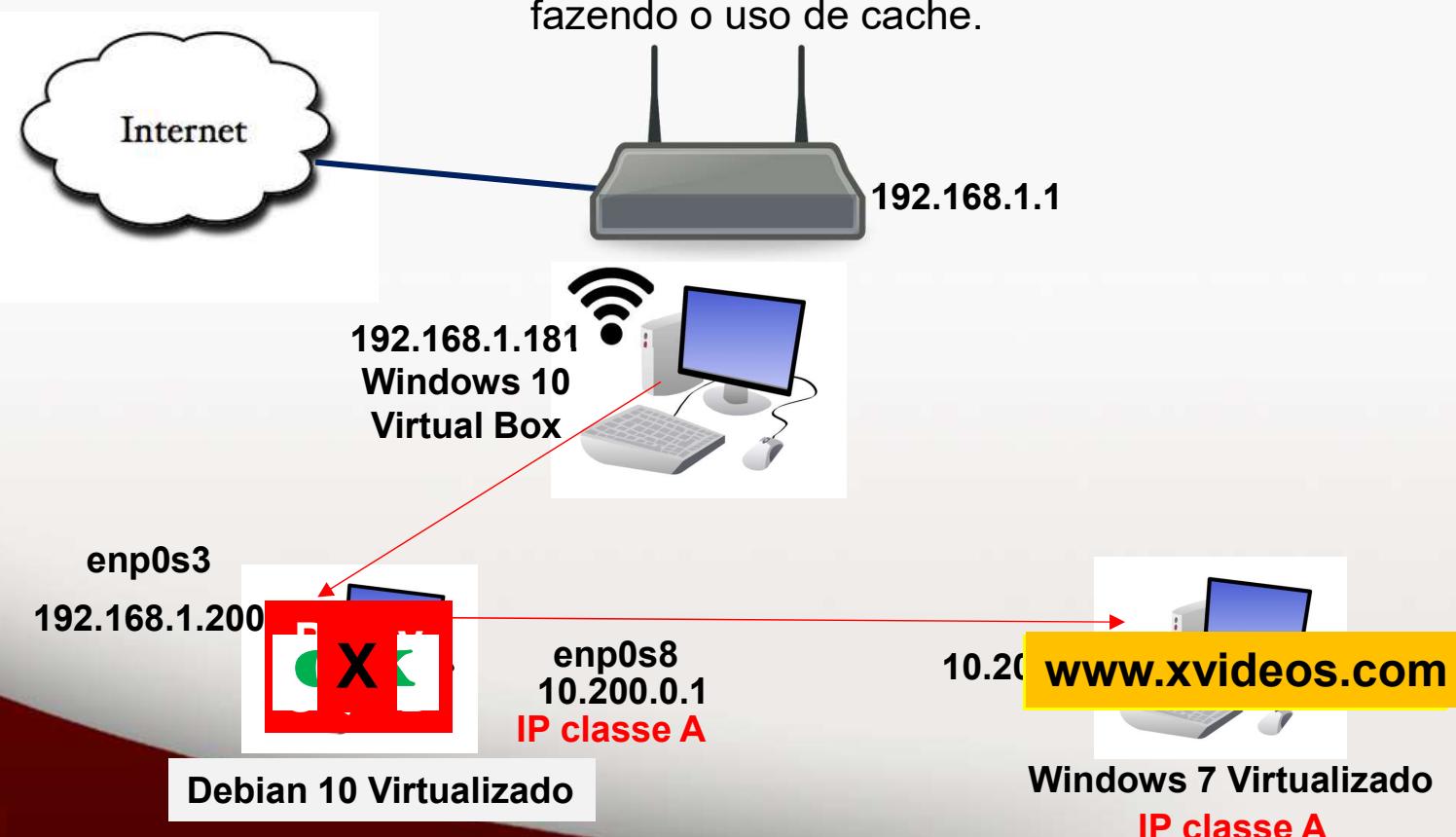
Aula 31: Proxy Squid

Proxy

Em redes de computadores, um proxy é um servidor que age como um intermediário para requisições de clientes.

Um cliente conecta-se ao servidor proxy, solicitando algum serviço, como um arquivo, conexão, página web ou outros recursos disponíveis de um servidor diferente, e o proxy avalia a solicitação

Um servidor proxy pode, opcionalmente, alterar a requisição do cliente ou a resposta do servidor e, algumas vezes, pode disponibilizar este recurso mesmo sem se conectar ao servidor especificado, fazendo o uso de cache.





**Squid
Proxy**

Squid

O Squid permite compartilhar a conexão entre vários micros, servindo como um intermediário entre eles e a internet.

Usar um proxy é diferente de simplesmente compartilhar a conexão diretamente, via NAT.

Instalar Squid:
apt-get install squid

Arquivo de configuração:
/etc/squid/squid.conf

Squid

Arquivo de configuração básico 1:
/etc/squid/squid.conf

```
#Porta Squid
http_port 3128

#Cache
cache_mem 1000 MB
maximum_object_size 100 MB
minimum_object_size 10 KB
cache_dir ufs /var/spool/squid 2048 16 256
cache_access_log /var/log/squid/access.log

#Máquinas Liberadas no Proxy
acl liberados src 10.200.0.101
http_access allow liberados

#Bloqueio de domínios e palavras
acl bloqueados url_regex -i "/etc/squid/bloqueados"
http_access deny bloqueados

#Bloqueio Download
acl bloqueio_downloads url_regex -i "/etc/squid/bloqueio_downloads"
http_access deny bloqueio_downloads

acl home.lan src 10.200.0.0/8
http_access allow localhost
http_access allow home.lan
http_access deny all
```

Squid com autenticação

Arquivo de configuração: /etc/squid/squid.conf

```
#Porta Squid
http_port 3128

#Autenticação
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid/passwd
auth_param basic realm Squid
auth_param basic credentialsttl 30 minutes

#Cache
cache_mem 1000 MB
maximum_object_size 100 MB
minimum_object_size 10 KB
cache_dir ufs /var/spool/squid 2048 16 256
cache_access_log /var/log/squid/access.log

#Máquinas Liberadas no Proxy
#acl liberados src 10.200.0.101
#http_access allow liberados

#Bloqueio de domínios e palavras
acl bloqueados url_regex -i "/etc/squid/bloqueados"
http_access deny bloqueados

#Bloqueio Download
acl bloqueio_downloads url_regex -i "/etc/squid/bloqueio_downloads"
http_access deny bloqueio_downloads

acl home.lan src 10.200.0.0/8
http_access allow localhost
acl password proxy_auth REQUIRED
http_access allow password
http_access allow home.lan
http_access deny all
```

Squid com autenticação

Para cadastrar o usuário:

Crie o arquivo **passwd** dentro de /etc/squid

Configure a permissão de escrita com o comando **chmod 754 /etc/squid/passwd**

Crie o usuário com o comando **htpasswd /etc/squid/passwd humberto**

Para remover o usuário utilize o comando **htpasswd -D /etc/squid/passwd humberto**

```
root@samsec:/etc/squid# htpasswd /etc/squid/passwd humberto
New password:
Re-type new password:
Adding password for user humberto
root@samsec:/etc/squid#
```

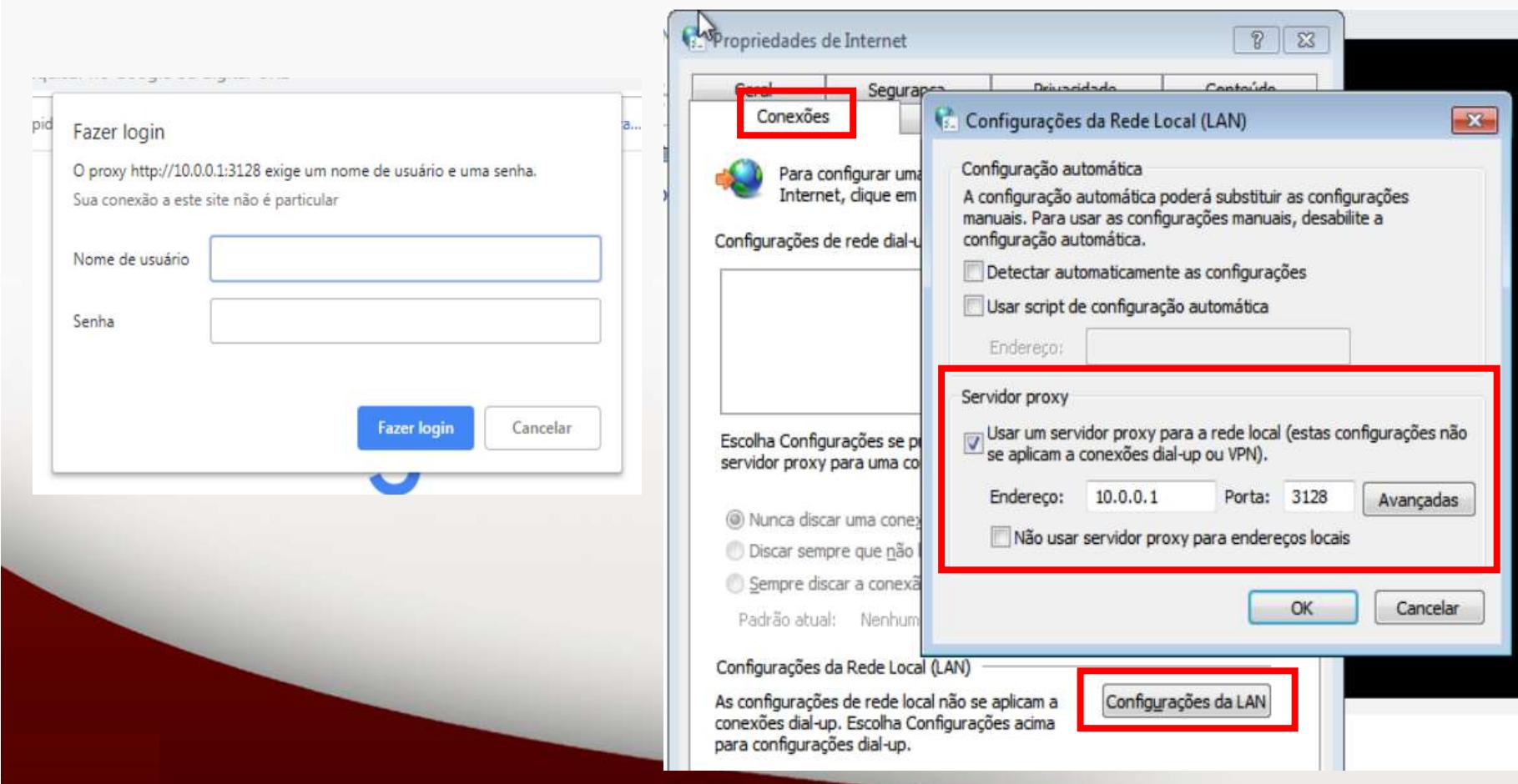
```
user1:$apr1$NGZ1RKbr$2npj2TW8s1I5pyufUMoWc/
humberto:$apr1$luypdEiQ$NXL3UEwi1UUUsyVdmr0Qjh.
```

Squid com autenticação

CRIAÇÃO DE USUÁRIOS

```
# htpasswd /etc/squid/passwd humberto
```

Ele pedirá a senha, digite e confirme, depois disso o usuário será criado.



Linux Completo + Servidores

Aula 32: Acesso Remoto

SSH

O SSH , para Secure Shell , é um protocolo de rede usado para operar logins remotos em máquinas distantes dentro de uma rede local ou pela Internet. As arquiteturas SSH normalmente incluem um servidor SSH usado pelos clientes SSH para conectar-se à máquina remota

O SSH é um protocolo Criptografado.

No Debian, o pacote de instalação é o **openssh-server**

```
root@samsec:/etc/bind# apt-get install openssh-server
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
The following additional packages will be installed:
  openssh-sftp-server
Pacotes sugeridos:
  molly-guard monkeysphere rssh ssh-askpass ufw
Os NOVOS pacotes a seguir serão instalados:
  openssh-server openssh-sftp-server
0 pacotes atualizados, 2 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso baixar 397 kB de arquivos.
Depois desta operação, 1.609 kB adicionais de espaço em disco serão usados.
Você quer continuar? [S/n]
```

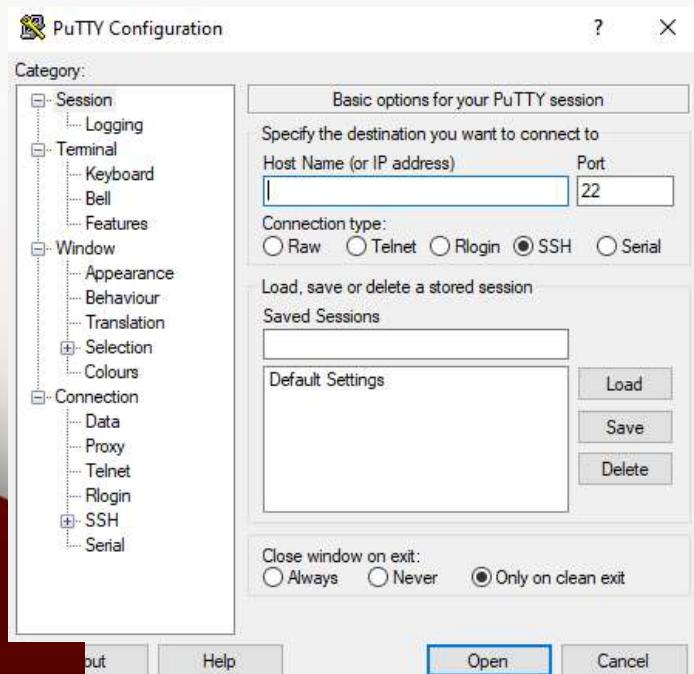
SSH

Com o comando **ss -tlpn | grep 22** você irá ver a porta de conexão com o serviço de SSH

```
root@humberto:~# ss -tlpn | grep 22
LISTEN      0      80          127.0.0.1:3306          0.0.0.0:*      users:(("mysqld",pid=484,fd=22))
LISTEN      0      10          127.0.0.1:53          0.0.0.0:*      users:(("named",pid=433,fd=22))
LISTEN      0      128         0.0.0.0:22          0.0.0.0:*      users:(("sshd",pid=925,fd=3))
LISTEN      0      128         [:]:22              [:]:*:        users:(("sshd",pid=925,fd=4))
root@humberto:~#
```

O arquivo de configuração é o `/etc/ssh/sshd_config`

Lembrando que o usuário root é desativado por padrão



Para o acesso ao seu servidor, podemos utilizar ferramentas como o PuTTY:

<https://www.putty.org>

Linux Completo + Servidores

Aula 33: DNS – Bind Recursivo e Autoritativo

DNS

Sempre que é utilizado um nome para designar um servidor, como www.debian.org, este deve ser traduzido para o endereço IP único desse servidor.

A este processo chama-se resolução e é efetuado graças ao Sistema de Nomes de Domínios ou **DNS (Domain Name System)**.

Quando falamos em DNS, estamos falando do servidor **Autoritativo** e **Recursivo**

DNS AUTORITIVO

É o serviço DNS que possui autoridade sob um domínio. Assim como servidor ns1.teste.com.br é o DNS autoritativo do domínio teste.com.br, dessa forma é ele que é responsável por responder qualquer subdomínio do domínio teste.com.br, como por exemplo ftp.teste.com.br, intranet.teste.com.br.

É um servidor Autoritativo que quando um domínio é adquirido é especificado junto ao *registro.br*



DNS

DNS RECURSIVO

O DNS recursivo é responsável pela resolução de nomes de consultas vindas dos **resolvers** (não é um servidor de DNS. É um cliente (ex.: o navegador)) nos servidores raízes.

DNS recursivo também realiza o cache DNS. Armazenando os resultados de consultas para aumentar o desempenho dos equipamentos conectados em sua rede.

Bind

BIND (Berkeley Internet Name Domain) é um serviço de servidor DNS para sistemas operacionais Linux e Unix.

Ele pode ser configurado como servidor **Autoritativo** ou **Recursivo**

Instalação Bind
apt-get install bind9 dnsutils

DNS Recursivo

Após a instalação, seu servidor DNS já estará pronto e realizando consultas, para o teste podemos utilizar o comando **dig**

```
; <>> DiG 9.11.5-P4-5.1+deb10u1-Debian <>> google.com.br
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8035
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 4096
;; COOKIE: cf65720fce9fbd477403a8b5f311f00742eee3e2417f3b4 (good)
;; QUESTION SECTION:
;google.com.br.          IN      A

;; ANSWER SECTION:
google.com.br.        300     IN      A      172.217.30.67

;; AUTHORITY SECTION:
google.com.br.        3419    IN      NS     ns3.google.com.
google.com.br.        3419    IN      NS     ns2.google.com.
google.com.br.        3419    IN      NS     ns4.google.com.
google.com.br.        3419    IN      NS     ns1.google.com.

;; ADDITIONAL SECTION:
ns1.google.com.       172613  IN      A      216.239.32.10
ns2.google.com.       172613  IN      A      216.239.34.10
ns3.google.com.       172613  IN      A      216.239.36.10
ns4.google.com.       172613  IN      A      216.239.38.10
ns1.google.com.       172613  IN      AAAA   2001:4860:4802:32::a
ns2.google.com.       172613  IN      AAAA   2001:4860:4802:34::a
ns3.google.com.       172613  IN      AAAA   2001:4860:4802:36::a
ns4.google.com.       172613  IN      AAAA   2001:4860:4802:38::a

;; Query time: 66 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: seg ago 10 07:18:40 -03 2020
;; MSG SIZE  rcvd: 344
```

DNS Recursivo

Arquivo de Configuração Cache DNS
/etc/bind/named.conf.options

```
options {
    directory "/var/cache/bind";

    // forwarders {
    //     0.0.0.0;
    // };

    dnssec-validation auto;
    auth-nxdomain no;

    listen-on {
        127.0.0.1;
    };

    allow-query {
        127.0.0.1;
        10.0.0.0/8;
    };

};
```

DNS Autoritativo

nigmasec.com

registro.br



Registro de domínio .com.br

Registro de domínio .com



Apache

```
<VirtualHost *:80>
    # The ServerName directive sets the
    # the server uses to identify itself
    # redirection URLs. In the context
    # specifies what hostname must appear
    # match this virtual host. For the
    # value is not decisive as it is used
    # However, you must set it for any
    #ServerName www.example.com

    ServerAdmin contato@nigmasec.com
    ServerName www.nigmasec.com
    ServerAlias nigmasec.com
    DocumentRoot /var/www/html

    # Available loglevels: trace8, ...,
```

DNS
AUTORITATIVO
DO SITE
nigmasec.com



DNS
Recursivo



nigmasec.com

DNS Autoritativo

1- Alterar o arquivo:
/etc/hostname

```
root@nsl:~# hostname  
nsl.nigmasec.com  
root@nsl:~# vi /etc/hostname
```

2- Edite o arquivo **named.conf.local** e adicione a zona para o seu site:

```
//  
// Do any local configuration here  
//  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
zone "nigmasec.com" IN {  
    type master;  
    file "/etc/bind/db.nigmasec";  
};
```

- O “**zone**” indica o domínio que estamos configurando no caso de exemplo **nigmasec.com**;
- O “**type master**” indica que o servidor é o **MASTER** (principal);
- O “**file**” indica o arquivo que contém as configurações desse domínio.

Também poderíamos inserir o **allow-transfer {IP};** para adicionar o servidor DNS secundário

DNS Autoritativo

Lembrando que na configuração do servidor secundário

```
//  
// Do any local configuration here  
//  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
zone "nigmasec.com" IN {  
    type slave;  
    file "/etc/bind/db.nigmasec";  
};
```

Também teríamos de inserir o **masters {IP};** para adicionar o servidor DNS secundário

DNS Autoritativo

2- Agora vamos criar o arquivo **db.nigmasec** apontado no arquivo **named.conf.local**

```
$TTL 300
@ IN SOA ns1.nigmasec.com. contato@nigmasec.com. (
                  2020081020      3H      15M      1W      1D )
@ IN NS   nigmasec.com.
@ IN A    155.138.205.22
www IN CNAME nigmasec.com.
```

Para este arquivo de configuração do domínio a formatação é importante, você pode utilizar espaços ou tabs, mas os campos tem que ficar alinhados.

O campo **\$TTL 300** indica o tempo de atualização do seu DNS com o servidor de registro, no caso está configurado com 300 segundos, ou 5 minutos, qualquer alteração no seu DNS demoraria esse tempo para a atualização do registro.

O **@** indica a origem do domínio, o **IN** é abreviação de internet, o **SOA** é a abreviação de Start of authority que indica o inicio de uma zona de autoridade

O número **2020081020** é o valor de sincronismo com o servidor DNS secundário que normalmente é a data da ultima configuração acrescido de dois números aleatórios. Na frente os 4 campos significam o tempo que o servidor aguarda entre as atualizações (3H), o segundo campo é o tempo que o servidor secundário espera antes de voltar o uso para o servidor master, o terceiro significa o tempo máximo que ele pode responder pelo domínio e o quarto é o tempo mínimo que o secundário espera para devolver as configurações para o master.

DNS Autoritativo

```
$TTL 300
@ IN SOA ns1.nigmasec.com. contato@nigmasec.com. (
    2020081020 3H 15M 1W 1D )
@ IN NS nigmasec.com.
@ IN A 155.138.205.22
www IN CNAME nigmasec.com.
```

A chave de registro **NS** (nameserver) indica o nome da autoridade do domínio.

A chave **A** indica o endereço de host.

A chave **CNAME** é o nome canônico.

Após salvar e reiniciar o serviço, podemos testar com o comando **dig**

```
root@ns1:~# dig nigmasec.com @155.138.205.22

; <>> DiG 9.11.5-P4-5.1+deb10u1-Debian <>> nigmasec.com @155.138.205.22
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6843
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:: udp: 4096
;. COOKIE: 2faaca983d60d2a8672e4df55f3267ecc20071ffe5ded4e4 (good)

;; QUESTION SECTION:
;nigmasec.com.           IN      A

;; ANSWER SECTION:
nigmasec.com.        300     IN      A      155.138.205.22

;; AUTHORITY SECTION:
nigmasec.com.        300     IN      NS     nigmasec.com.

;; Query time: 0 msec
;; SERVER: 155.138.205.22#53(155.138.205.22)
;; WHEN: Tue Aug 11 09:42:06 UTC 2020
;; MSG SIZE  rcvd: 99
```

DNS Autoritativo

O DNS reverso é o recurso que permite outros servidores verificarem a autenticidade do seu servidor, verificando se o endereço ip atual bate com o endereço ip informado na zona DNS do seu servidor.

3- Adicionar a zona reversa dentro do **/etc/bind/named.conf.local**.

```
//  
// Do any local configuration here  
  
// Consider adding the 1918 zones here, if they are not used in your  
// organization  
//include "/etc/bind/zones.rfc1918";  
zone "nigmasec.com" IN {  
    type master;  
    file "/etc/bind/db.nigmasec";  
};  
  
zone "205.138.155.in-addr.arpa" {  
    type master;  
    file "/etc/bind/db.nigmasec.rev";  
};
```

DNS Autoritativo

4- Criar o arquivo **/etc/bind/db.nigmasec.rev**

```
$TTL      300
@       IN      SOA     ns1.nigmasec.com.      contato@nigmasec.com. (
                           2020081020      3H      15M      1W      1D )
@       IN      NS      nigmasec.com.
22      IN      PTR     nigmasec.com.
```

Para testar a zona reversa utilize o comando **dig -x ip_servidor_DNS**

DNS Autoritativo

5- Configurar o seu register domain para ler o seu servidor DNS

The screenshot shows the nigmasec.com domain management interface. The top navigation bar includes a home icon, the domain name 'nigmasec.com', and links for 'Domain', 'Products', 'Sharing & Transfer', and 'Advanced DNS'. The 'Advanced DNS' tab is selected, indicated by a teal background and white text. Below the tabs, there are sections for 'DNS TEMPLATES' and 'HOST RECORDS'. The 'HOST RECORDS' section contains a table with columns: 'Type', 'Host', 'Value', and 'TTL'. Two entries are visible: one for '@' with Value '155.138.205.22' and TTL '5 min', and another for 'www' with Value '155.138.205.22' and TTL '5 min'. Both entries have a small trash can icon in the 'Actions' column. A red box highlights the entire table area.

Type	Host	Value	TTL	Actions
A Record	@	155.138.205.22	5 min	
A Record	www	155.138.205.22	5 min	

Linux Completo + Servidores

Aula 34: Firewall

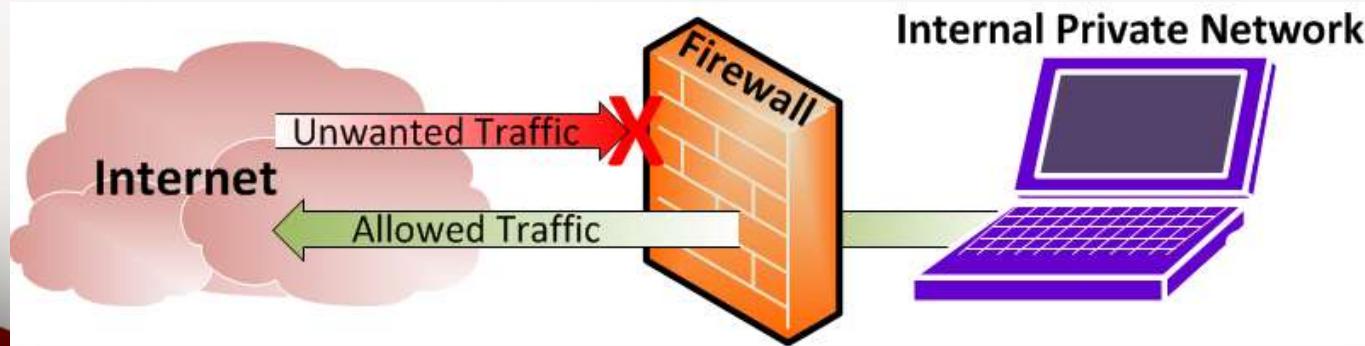
FIREWALL

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

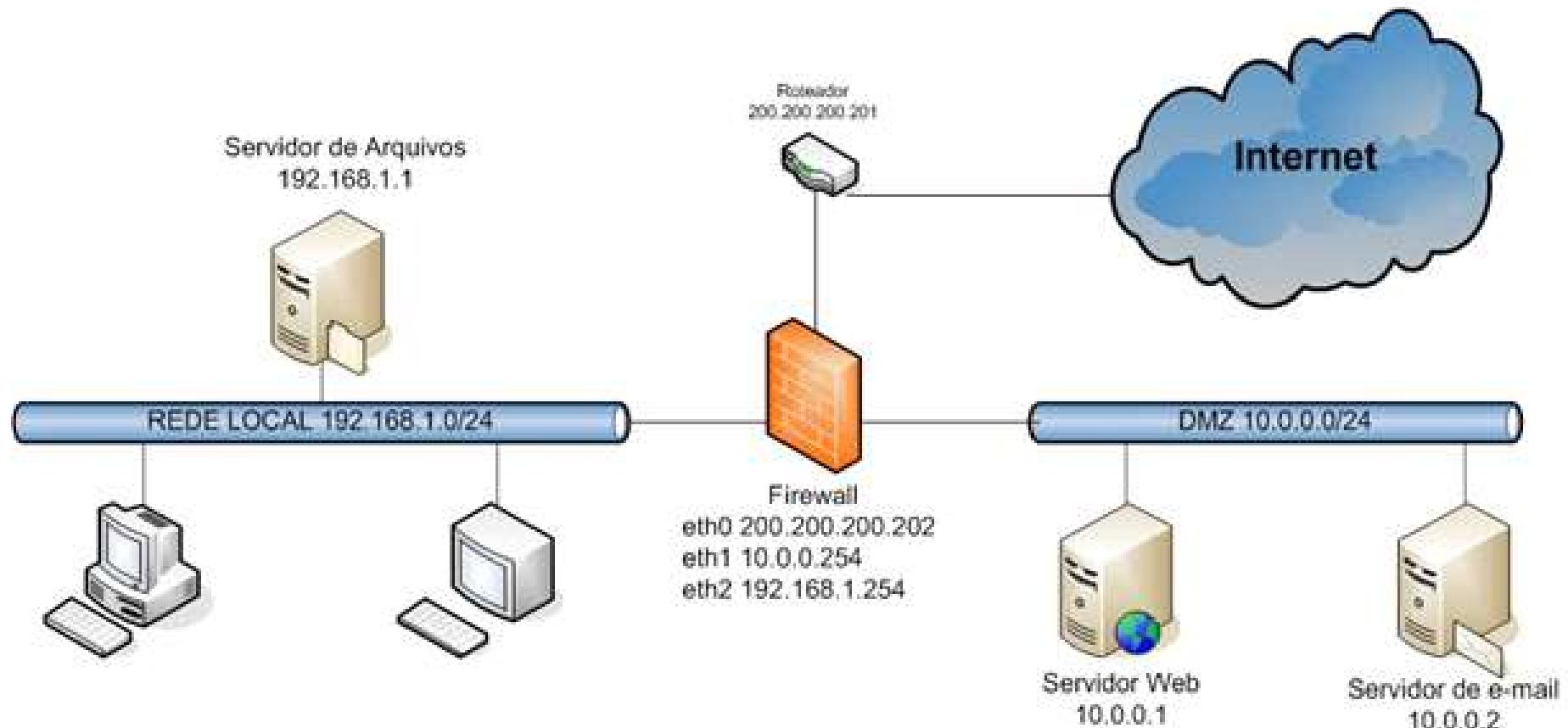
Os firewalls têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos.

Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet.

Um firewall pode ser um hardware, software ou ambos.



FIREWALL



DMZ: Demilitarized Zone

IPTABLES

A função do Firewall é tomar conta das portas, verificar quem as está acessando e conforme as regras do usuário deixar ou não o acesso dos programas através das referidas portas.

Para usuários Linux temos o **iptables**, configurado via scripts.

As regras do iptables são compostas de uma Tabela, Opção, Chain, Dados e Ação.

`iptables [-t tabela] [opção] [chain] [dados] -j [ação]`

IPTABLES

`iptables -t tabela opção chain dados -j ação`

Tabelas:

São os locais usados para armazenar os chains.

As tabelas são referenciadas em uma regra iptables com a opção “-t tabela”.

Existem 3 tabelas disponíveis:

filter – As regras contidas na tabela filter determinam a aceitação (ou não) de um pacote. Dentro dessa tabela existem três cadeias: INPUT, OUTPUT, FORWARD.

nat – usada quando há ocorrência de NAT (geração de outra conexão);

mangle – raramente usada, utilizada para alterações especiais de pacotes.

Se você deixar em branco [-t tabela], a tabela usada será a filter.

IPTABLES

`iptables -t tabela opção chain dados -j ação`

Opções:

Representada por uma letra sempre escrita em maiúscula.

-A = acrescenta uma nova regra às existentes;

-L = lista as regras existentes;

-F = apaga todas as regras;

-I = insere uma nova regra;

-D = zera uma regra específica;

IPTABLES

`iptables -t tabela opção chain dados -j ação`

Chains:

Com eles podemos especificar a situação do tratamento dos pacotes, seja qual tabela for,
exemplo: para tabelas **filter** temos as seguintes tipos de chains:

INPUT – consultado para dados que chegam ao computador;

OUTPUT – consultado para dados que saem do computador;

FORWARD – consultado para dados que são redirecionados para outra interface de rede ou outra máquina.

Já para as tabelas **nat** os chains possíveis são:

PREROUTING – consultado para os dados que precisam ser modificados logo que chegam (DNAT e redirecionamento de portas);

POSTROUTING – consultado para dados que precisam ser modificados após o tratamento de roteamento (IP Masquerading);

OUTPUT – consultado quando os dados gerados localmente precisam ser modificados antes de serem roteados (IPs locais).

IPTABLES

iptables -t tabela opção chain **dados** -j ação

Dados:

As opções de dados possíveis de inserção em uma regra iptables são:

-s

Especifica a origem do pacote. Origem que pode ser informada como:

- * endereço IP completo (-s 192.168.1.1);
- * hostname (-s ubuntu);
- * endereço fqdn (-s www.ubuntu.com);
- * par rede/máscara (-s 200.200.200.0/255.255.255.0 ou -s 200.200.200.0/24).

-d

Especifica um destino para o pacote, com a mesma sintaxe descrita acima por -s.

IPTABLES

`iptables -t tabela opção chain dados -j ação`

-i

Identifica a interface de entrada do pacote, podendo ser placa de rede, modem ou interface de conexão:

`-i eth0`

`-i enp0s3`

`-i wlan0`

-o

Identifica a interface de saída do pacote, com a mesma sintaxe descrita acima em `-i`.

-p

Especifica o protocolo usado na regra, podendo ser:

`-p tcp`

`-p udp`

`-p icmp`

IPTABLES

iptables -t tabela opção chain **dados** -j ação

--sport ou --source-port

Especifica uma porta ou faixa de portas de origem. Deve sempre ser acompanhado por -p tcp e -p udp.

--dport ou --destination-port

Especifica uma porta ou faixa de portas de destino. Deve sempre ser acompanhado por -p tcp e -p udp.

!

Exclui determinado argumento (exceção).

IPTABLES

iptables -t tabela opção chain dados **-j ação**

Ações:

Sempre vem após o parâmetro **-j** e os mais usados são:

ACCEPT – O pacote é aceito e o processamento das regras daquele chains é concluído;

DROP – Rejeita o pacote sem nenhum aviso;

REJECT – Rejeita o pacote, mas envia um aviso;

IPTABLES

Exemplos:

```
root@debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Bloquear todo tráfego de entrada na porta 80 proveniente de um IP.

iptables -A INPUT -s 192.168.0.198 -p tcp --dport 80 -j DROP

```
root@debian:~# iptables -A INPUT -s 192.168.0.198 -p tcp --dport 80 -j DROP
root@debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP      tcp   --  192.168.0.198      anywhere            tcp  dpt:http
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

IPTABLES

Resultado:

```
C:\Users\Humberto>telnet 192.168.0.198 80
Conectando-se a 192.168.0.198...Nao foi possível abrir conexão com host, na porta 80: conexão falhou

C:\Users\Humberto>
```

Facebook | WhatsApp | 192.168.0.142

← → ⌂ ⓘ 192.168.0.142

ERR_CONNECTION_TIMED_OUT

Não é possível acessar esse site

192.168.0.142 demorou muito para responder.

Tente:

- Verificar a conexão
- Verificar o proxy e o firewall
- Executar o Diagnóstico de Rede do Windows

IPTABLES

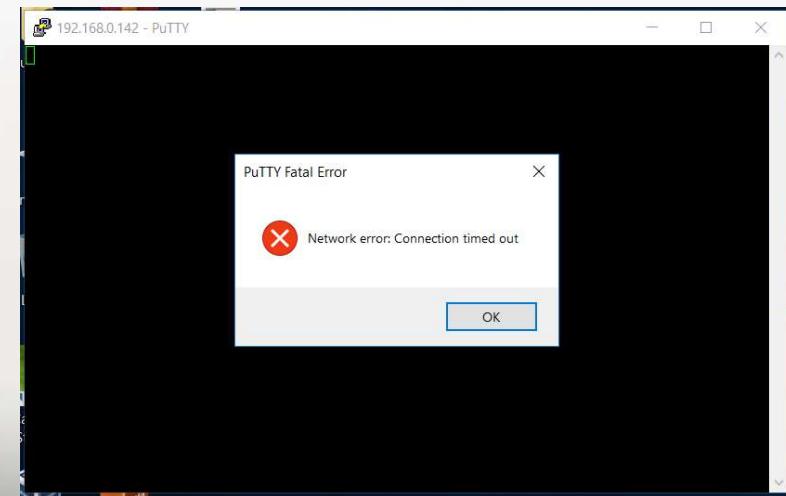
Bloquear todo tráfego de entrada no serviço de ssh proveniente de um IP.

```
# iptables -A INPUT -p tcp --dport ssh -j DROP
```

```
root@debian:~# iptables -A INPUT -p tcp --dport ssh -j DROP
root@debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  192.168.0.198        anywhere             tcp dpt:http
DROP       tcp  --  anywhere            anywhere            tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```



IPTABLES

Apagar determinada regra
iptables -D INPUT 2

```
root@debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP      tcp   --  192.168.0.198        anywhere             tcp dpt:http
2 DROP      tcp   --  anywhere          anywhere             tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

```
root@debian:~# iptables -D INPUT 2
root@debian:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP      tcp   --  192.168.0.198        anywhere             tcp dpt:http

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
```

IPTABLES

Bloquear Ping

```
# iptables -A INPUT -p icmp -j DROP
```

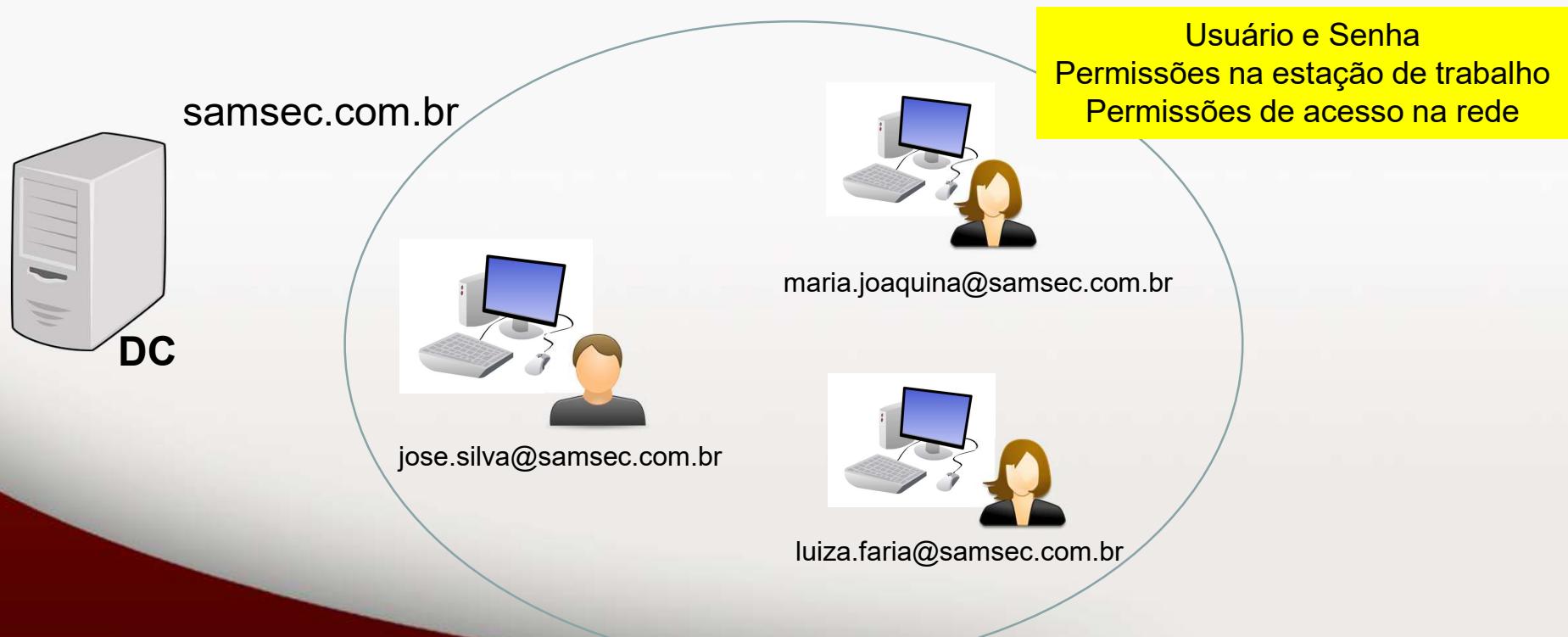
Linux Completo + Servidores

Aula 35: Controlador de Domínio (SAMBA) parte 1

Controlador de Domínio

Um controlador de domínio, do inglês domain controller (DC), é um servidor que responde à requisições seguras de autenticação (login, verificação de permissões etc.) dentro de uma rede de computadores

Um domínio é um conceito introduzido no Windows NT em que um usuário pode ter acesso a uma série de recursos de computador com o uso de uma única combinação de nome de usuário e senha.



Controlador de Domínio

Uma das funções do Samba também é atuar como controlador de domínio, esse recurso serve para controlar os usuários que podem acessar seus computadores e também definir permissões de uso.

O Linux conta com o Samba que além de compartilhar arquivos também pode ser do Domain Controller de uma rede.

Para a configuração, será necessário a instalação dos pacotes de serviços:

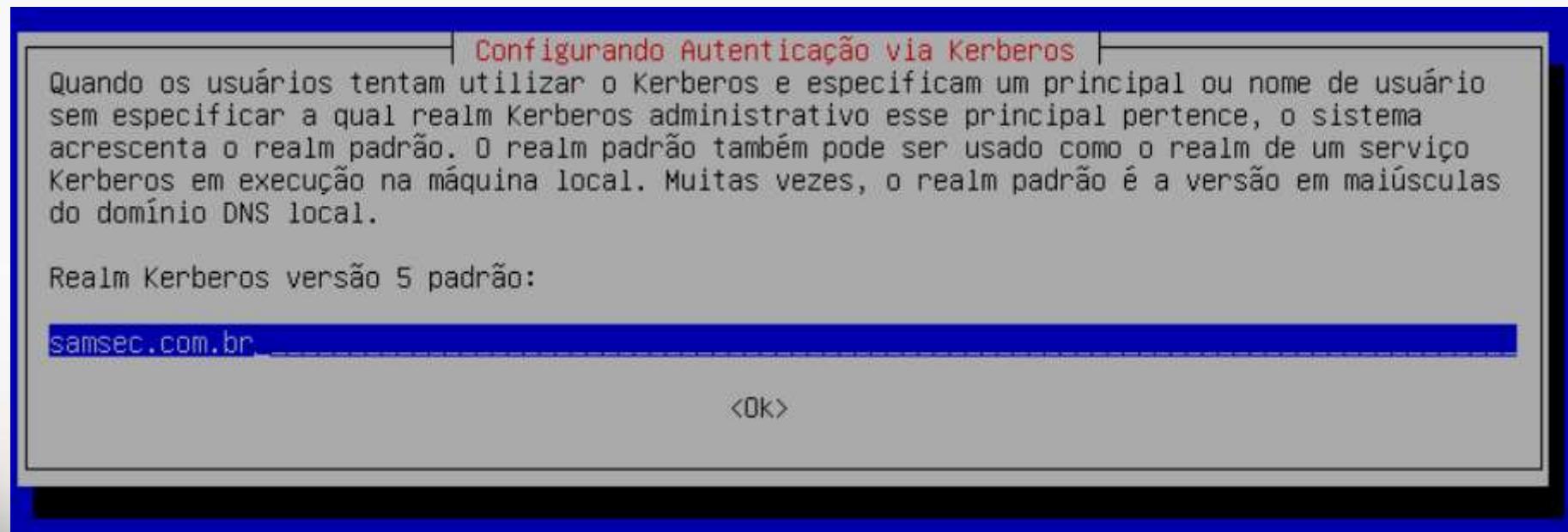
Samba, krb5-config, winbind e smbclient

```
root@samsec:/etc/squid# apt-get install krb5-config winbind smbclient
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
The following additional packages will be installed:
  libarchive13 libsmbclient
Pacotes sugeridos:
  lzzip cifs-utils heimdal-clients libnss-winbind libpam-winbind
Os NOVOS pacotes a seguir serão instalados:
  krb5-config libarchive13 libsmbclient smbclient winbind
0 pacotes atualizados, 5 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso baixar 1.525 kB de arquivos.
Depois desta operação, 5.047 kB adicionais de espaço em disco serão usados.
Você quer continuar? [S/n]
```

Controlador de Domínio

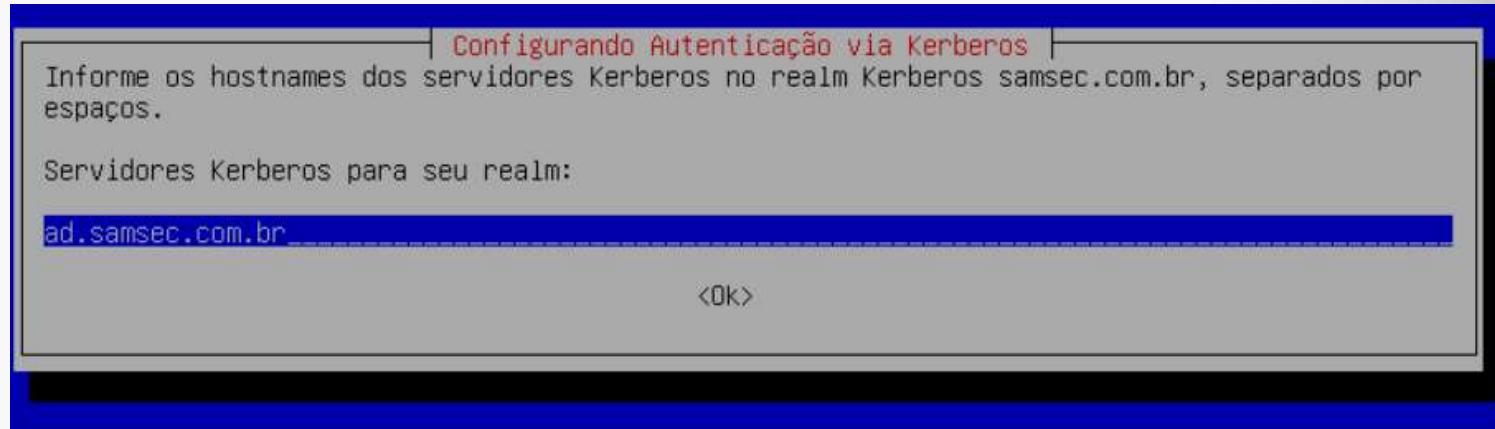
Durante a instalação dos pacotes será solicitado o nome do domínio no Kerberos.

Digite o domínio, exemplo **SAMSEC.COM.BR**

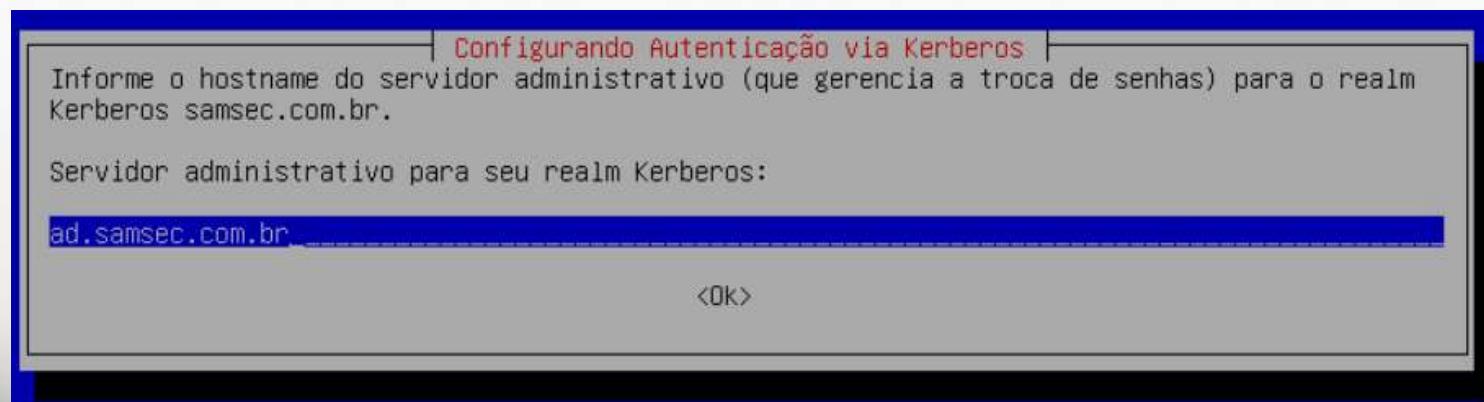


Controlador de Domínio

Logo em seguida, entre com o nome do servidor.



E finalmente entre com o servidor que vai gerenciar a troca de senha.



Controlador de Domínio

Apague ou renomeie o arquivo *smb.conf* original, pois será criado um novo arquivo.

Agora execute o comando de configuração de domínio:

samba-tool domain provision

```
root@samsec:/etc/squid# samba-tool domain provision
Realm: samsec.com.br
Domain [samsec]:
Server Role (dc, member, standalone) [dc]:
DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
DNS forwarder IP address (write 'none' to disable forwarding) [8.8.8.8]: 10.200.0.1
Administrator password:
Retype password:
```

Aqui será solicitado novamente o nome do domínio, se o servidor é o controlador de domínio, um membro, qual servidor DNS será utilizado e a senha de administrador.

Controlador de Domínio

Agora faça a cópia do arquivo **krb5.conf** que está em **/var/lib** para a pasta **/etc**:

```
cp /var/lib/samba/private/krb5.conf /etc/
```

Siga com os comandos para gerenciar serviços:

```
systemctl stop smbd nmbd winbind
```

```
systemctl disable smbd nmbd winbind
```

```
systemctl unmask samba-ad-dc
```

```
systemctl start samba-ad-dc
```

```
systemctl enable samba-ad-dc
```

Controlador de Domínio

Agora consulte o status do sistema:

smbclient -L localhost -U%

```
root@ad:~# smbclient -L localhost -U%  
  
      Sharename          Type        Comment  
-----  
    netlogon            Disk  
    sysvol              Disk  
    IPC$                IPC         IPC Service (Samba 4.9.5-Debian)  
Reconnecting with SMB1 for workgroup listing.  
  
      Server          Comment  
-----  
    Workgroup          Master  
-----  
    WORKGROUP          AD  
root@ad:~#
```

Controlador de Domínio

Também confirme o nível do sistema:

samba-tool domain level show

```
root@ad:~# samba-tool domain level show
Domain and forest function level for domain 'DC=samsec,DC=com,DC=br'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
root@ad:~#
```

Controlador de Domínio

Para obter informações detalhadas sobre o seu domínio:

samba-tool domain info 10.200.0.1

```
root@ad:~# samba-tool domain info 10.200.0.1
Forest          : samsec.com.br
Domain          : samsec.com.br
Netbios domain  : SAMSEC
DC name         : ad.samsec.com.br
DC netbios name: AD
Server site     : Default-First-Site-Name
Client site    : Default-First-Site-Name
```

Controlador de Domínio

E crie um usuário para autenticar na sua estação de trabalho:

samba-tool user create zezinho

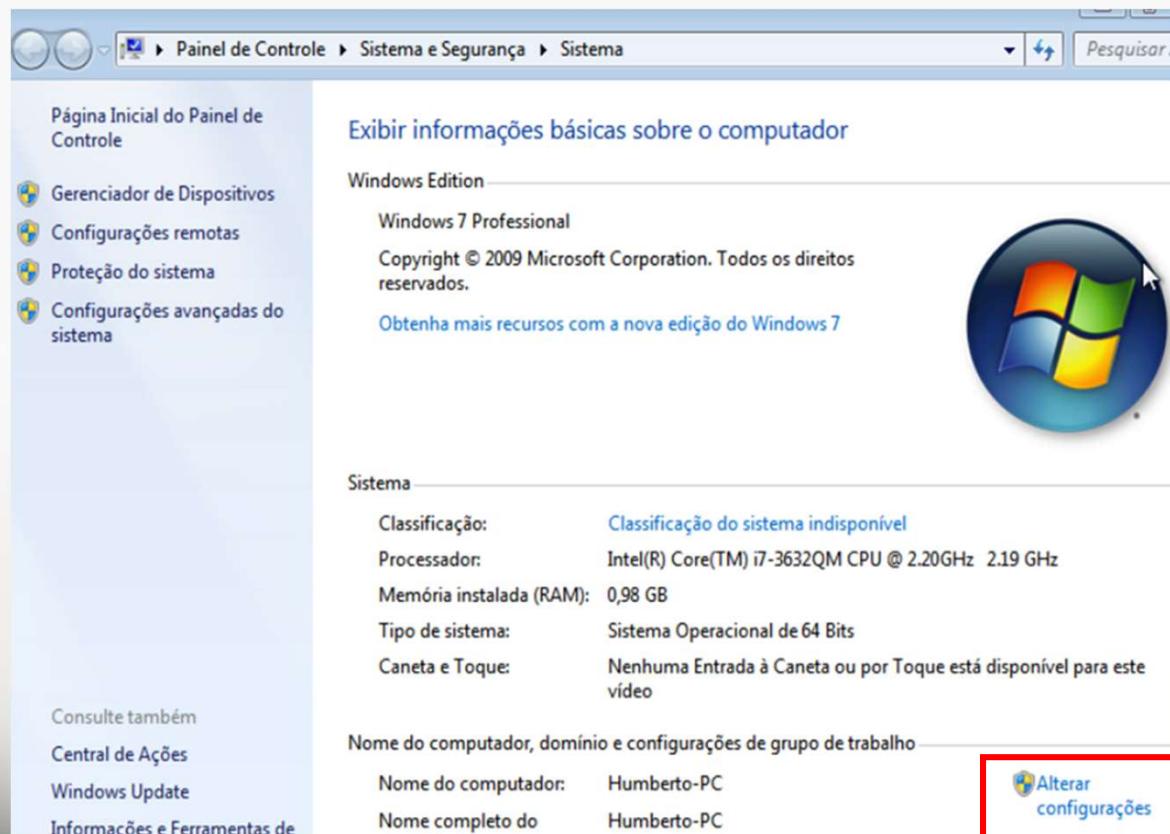
```
root@ad:~# samba-tool user create zezinho
New Password:
Retype Password:
User 'zezinho' created successfully
```

Controlador de Domínio

Agora podemos adicionar nossa estação Windows no domínio SAMSEC.COM.BR.

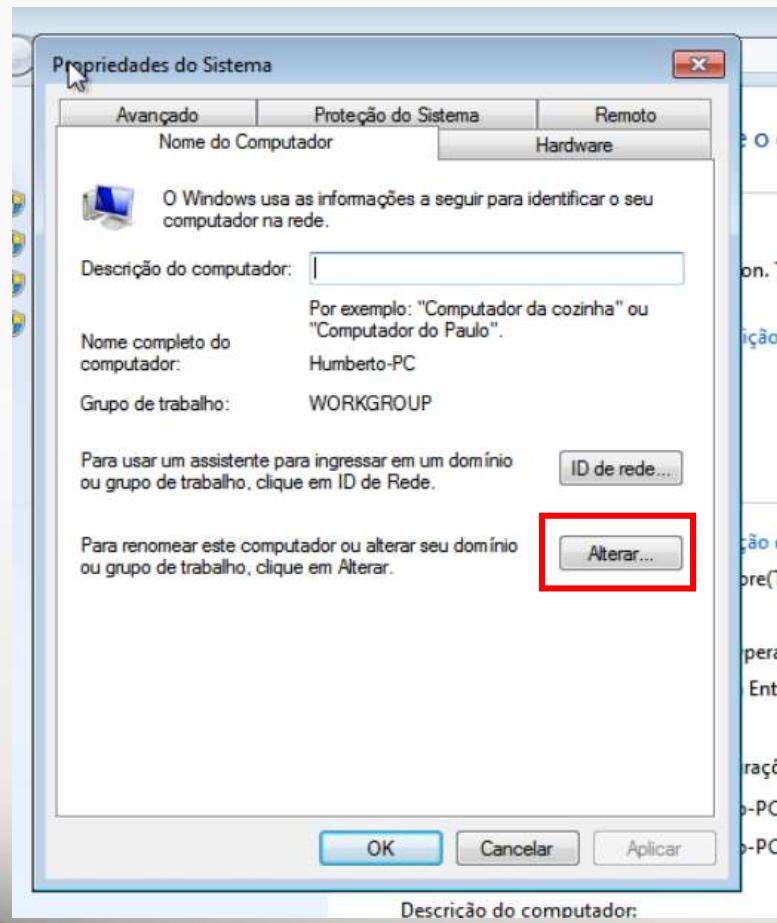
Primeiro clique com o botão direito em Meu Computador e abra as Propriedades.

Agora clique no Botão Alterar as Configurações



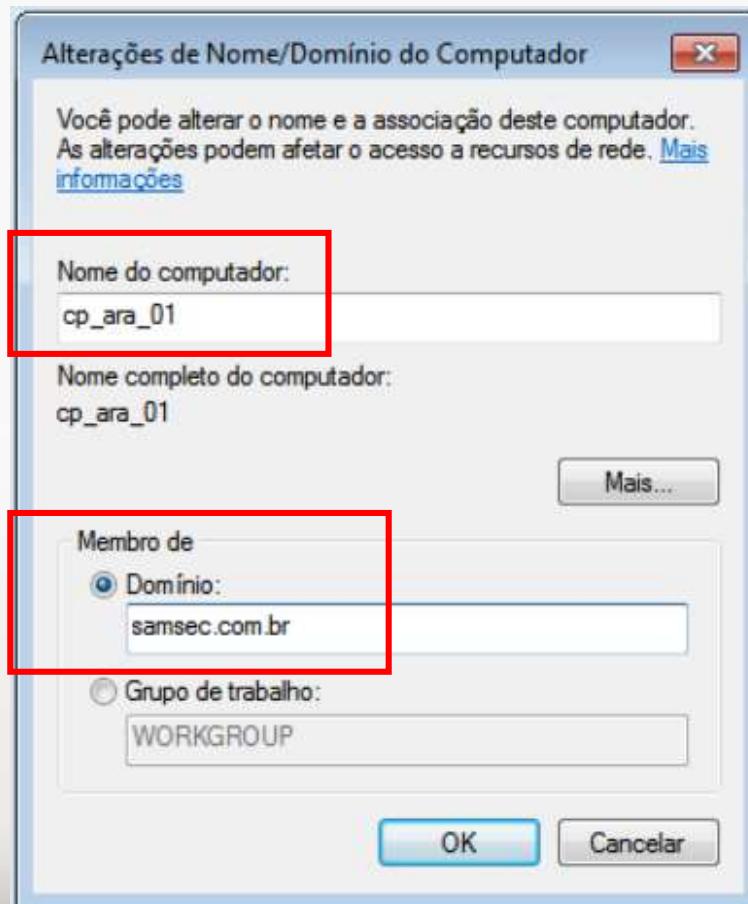
Controlador de Domínio

Na nova janela aberta, clique no botão Alterar, aqui nós podemos entrar com o nome da máquina e o nome do domínio.



Controlador de Domínio

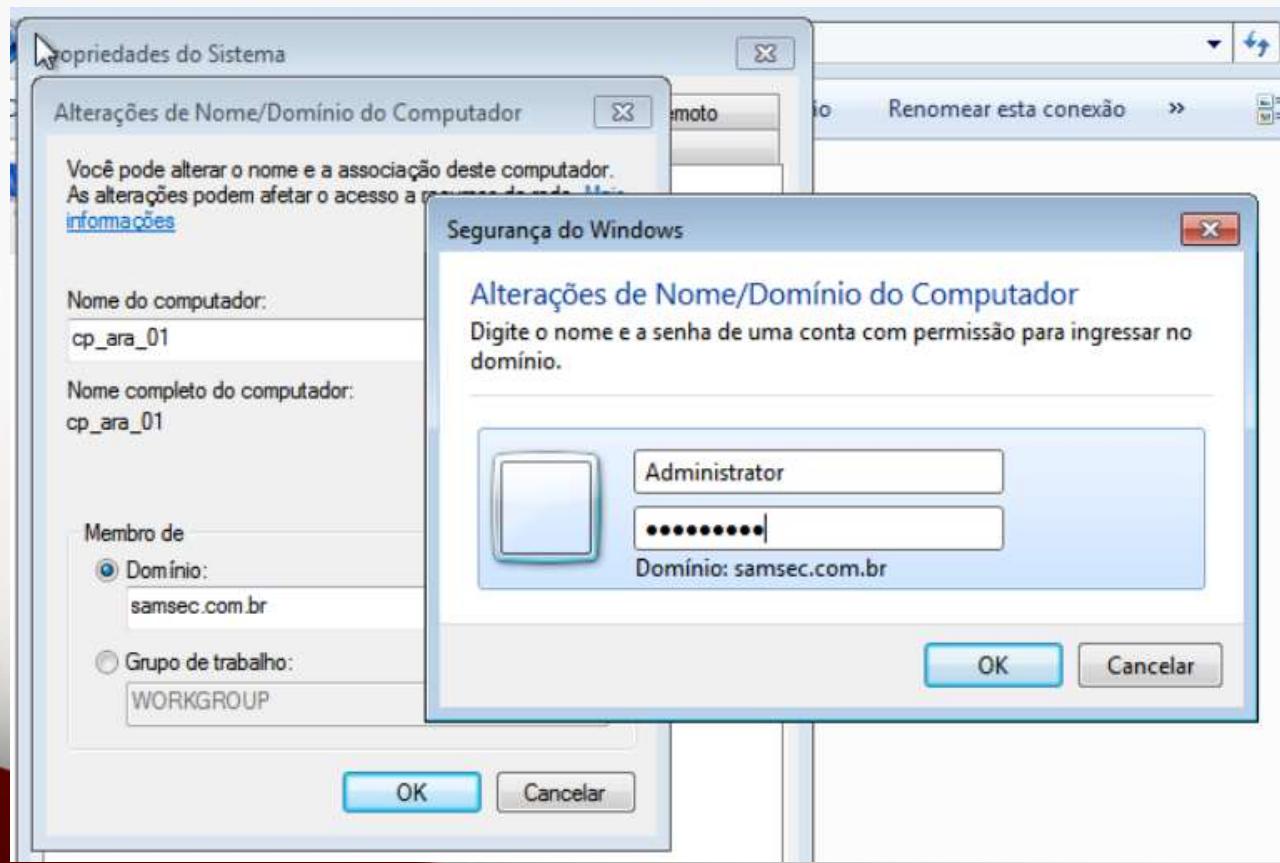
Entre com os seus dados como no exemplo:



Controlador de Domínio

Clicando em OK, será solicitado o usuário administrador do domínio e sua senha. (O usuário é Administrator e a senha você especificou durante a configuração do Samba.

Logo após será necessário reiniciar o computador, confirme para aplicar as configurações.



Controlador de Domínio

Após a reinicialização será solicitado o login já no domínio:



Linux Completo + Servidores

Aula 36: Controlador de Domínio (SAMBA) parte 2

Controlador de Domínio

Vamos agora verificar alguns comandos de gerenciamento.

Primeiro vamos verificar os usuários existentes no seu domínio:

samba-tool user list

```
root@ad:~# samba-tool user list
Administrator
zezinho
krbtgt
Guest
root@ad:~#
```

Controlador de Domínio

Também podemos criar novos usuários

samba-tool user create joaozinho

```
root@ad:~# samba-tool user create joaozinho
New Password:
Retype Password:
User 'joaozinho' created successfully
root@ad:~#
```

Controlador de Domínio

Também temos o comando para deletar usuários.

samba-tool user delete joaozinho

```
root@ad:~# samba-tool user delete joaozinho
Deleted user joaozinho
root@ad:~# samba-tool user list
```

Controlador de Domínio

Podemos resetar a senha de um usuário.

samba-tool user setpassword zezinho

```
root@ad:~# samba-tool user setpassword zezinho
New Password:
Retype Password:
Changed password OK
root@ad:~#
```

Controlador de Domínio

O próximo comando define o tempo para que o usuário expire em seu domínio.

samba-tool user setexpiry joaozinho --days=7

```
root@ad:~# samba-tool user setexpiry joaozinho --days=1
Expiry for user 'Joaozinho' set to 1 days.
root@ad:~#
```

Também é possível ativar ou desativar o usuário

samba-tool user disable joaozinho

samba-tool user enable joaozinho

Controlador de Domínio

Criando e Gerenciando Grupos

Para criar ou deletar um grupo, segue os comandos:

samba-tool group add Administrativo

ou

samba-tool group delete Administrativo

```
root@ad:~# samba-tool group add Administrativo
Added group Administrativo
root@ad:~# samba-tool group add RH
Added group RH
root@ad:~# samba-tool group delete RH
Deleted group RH
root@ad:~#
```

Controlador de Domínio

Depois de criado o grupo, precisamos adicionar os usuários neste grupo.

samba-tool group addmembers Administrativo zezinho,joaozinho,humberto

```
root@ad:~# samba-tool group addmembers Administrativo joaozinho,zezinho
Added members to group Administrativo
root@ad:~# samba-tool group listmembers Administrativo
zezinho
joaozinho
root@ad:~#
```

Para remover um usuário:

samba-tool group removemembers Administrativo zezinho

```
root@ad:~# samba-tool group removemembers Administrativo zezinho
Removed members from group Administrativo
root@ad:~#
```

Para checar quais grupos existem e os membros dentro de um determinado grupo:

samba-tool group list

samba-tool group listmembers "Administrativo"

Controlador de Domínio

Alterando requisitos de senha:

Para consultar seus parâmetros de senha:

samba-tool domain passwordsettings show

```
root@ad:~# samba-tool domain passwordsettings show
Password informations for domain 'DC=samsec,DC=com,DC=br'

Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
root@ad:~#
```

Controlador de Domínio

Para modificar as configurações:

EXEMPLO: samba-tool domain passwordsettings set --min-pwd-length=5

O comando acima obriga o usuário criar uma senha por pelo menos cinco caracteres.

```
root@ad:~# samba-tool domain passwordsettings set --min-pwd-length=5
Minimum password length changed!
All changes applied successfully!
root@ad:~# samba-tool domain passwordsettings show
Password informations for domain 'DC=samsec,DC=com,DC=br'

Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 5
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
root@ad:~#
```

Controlador de Domínio

Para consultar todas as opções:

samba-tool domain passwordsettings -h

```
--complexity=COMPLEXITY
    The password complexity (on | off | default). Default
    is 'on'
--store-plaintext=STORE_PLAINTEXT
    Store plaintext passwords where account have 'store
    passwords with reversible encryption' set (on | off | |
    default). Default is 'off'
--history-length=HISTORY_LENGTH
    The password history length (<integer> | default).
    Default is 24.
--min-pwd-length=MIN_PWD_LENGTH
    The minimum password length (<integer> | default).
    Default is 7.
--min-pwd-age=MIN_PWD_AGE
    The minimum password age (<integer in days> |
    default). Default is 1.
--max-pwd-age=MAX_PWD_AGE
    The maximum password age (<integer in days> |
    default). Default is 43.
--account-lockout-duration=ACCOUNT_LOCKOUT_DURATION
    The the length of time an account is locked out after
    exceeding the limit on bad password attempts (<integer
    in mins> | default). Default is 30 mins.
--account-lockout-threshold=ACCOUNT_LOCKOUT_THRESHOLD
    The number of bad password attempts allowed before
    locking out the account (<integer> | default).
    Default is 0 (never lock out).
--reset-account-lockout-after=RESET_ACCOUNT_LOCKOUT_AFTER
    After this time is elapsed, the recorded number of
    attempts restarts from zero (<integer> | default).
    Default is 30.
```

Controlador de Domínio

A Unidade Organizacional (**OU**) é um contêiner no domínio que pode conter objetos como grupos, contas de usuário e computador.

A OU é uma unidade administrativa no qual um administrador pode vincular objetos de Diretiva de Grupo e atribuir permissões a outro usuário.

Portanto, podemos distinguir duas tarefas principais ao usar a OU, exceto para armazenar objetos do domínio:

- Delegação de tarefas administrativas e de gerenciamento no domínio a outros administradores e usuários sem conceder a eles as permissões de administrador do domínio;
- Vinculando diretivas de grupo (GPO) a todos os objetos (usuários e computadores) nesta OU.

Controlador de Domínio

Para criar uma OU:

samba-tool ou create ‘OU=Araras’

```
root@ad:~# samba-tool ou create 'OU=Araras'  
Created ou "OU=Araras,DC=samsec,DC=com,DC=br"  
root@ad:~#
```

Para listar as OU's criadas:

samba-tool ou list

```
root@ad:~# samba-tool ou list  
OU=Araras  
OU=Domain Controllers  
root@ad:~#
```

Para verificar os objetos dentro de uma OU:

samba-tool ou listobjects ‘OU=Araras’

```
root@ad:~# samba-tool ou listobjects 'OU=Araras'  
ou "OU=Araras" is empty  
root@ad:~#
```

Controlador de Domínio

Para mover um grupo para dentro de uma OU:

samba-tool group move Administrativo 'OU=Araras'

```
root@ad:~# samba-tool group move Administrativo 'OU=Araras'  
Moved group "Administrativo" into "OU=Araras,DC=samsec,DC=com,DC=br"  
root@ad:~#
```

Para confirmar list os objetos dentro da OU Araras:

```
root@ad:~# samba-tool ou listobjects 'OU=Araras'  
CN=Administrativo,OU=Araras  
root@ad:~#
```

Também podemos confirmar mostrando as informações do grupo para consultar se ele faz parte de alguma OU:

```
root@ad:~# samba-tool group show Administrativo  
dn: CN=Administrativo,OU=Araras,DC=samsec,DC=com,DC=br  
objectClass: top  
objectClass: group  
cn: Administrativo  
instanceType: 4  
whenCreated: 20200504182840.02  
uSNCreated: 4651  
name: Administrativo  
objectGUID: beab3dcc-2a79-4dce-9df0-b74f855bf133  
objectSid: S-1-5-21-3316795626-2069486437-2947886286-1106  
sAMAccountName: Administrativo  
sAMAccountType: 268435456  
groupType: -2147483646  
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=samsec,DC=com,DC=br  
member: CN=joaozinho,CN=Users,DC=samsec,DC=com,DC=br  
whenChanged: 20200504205033.02  
usNChanged: 5130  
distinguishedName: CN=Administrativo,OU=Araras,DC=samsec,DC=com,DC=br
```

Controlador de Domínio

Password Settings Objects (PSO)

Dentro de um domínio é possível criar padrões de senhas diferentes para determinados objetos como Grupos.

Essas permissões especiais, são chamadas de pso (Password Settings Objects)

Quando chamamos o comando de ajuda: **samba-tool domain passwordsettings -h** podemos então consultar as opções do pso:

```
root@ad:~# samba-tool domain passwordsettings -h
Usage: samba-tool domain passwordsettings <subcommand>

Manage password policy settings.

Options:
  -h, --help  show this help message and exit

Available subcommands:
  pso    - Manage fine-grained Password Settings Objects (PSOs).
  set    - Set password settings.
  show   - Display current password settings for the domain.
For more help on a specific subcommand, please type: samba-tool domain passwordsettings <subcommand>
  (-h|--help)
```

Controlador de Domínio

Password Settings Objects (PSO)

Quando chamamos o comando de ajuda da opção pso:

samba-tool domain passwordsettings pso -h

Podemos observar as opções para criar, aplicar, deletar, mostrar e etc.

```
root@ad:~# samba-tool domain passwordsettings pso -h
Usage: samba-tool domain passwordsettings pso <subcommand>

Manage fine-grained Password Settings Objects (PSOs).

Options:
-h, --help  show this help message and exit

Available subcommands:
apply      - Applies a PSO's password policy to a user or group.
create     - Creates a new Password Settings Object (PSO).
delete     - Deletes a Password Settings Object (PSO).
list       - Lists all Password Settings Objects (PSOs).
set        - Modifies a Password Settings Object (PSO).
show       - Display a Password Settings Object's details.
show-user   - Displays the Password Settings that apply to a user.
unapply    - Updates a PSO to no longer apply to a user or group.
```

Controlador de Domínio

Password Settings Objects (PSO)

Para criar um pso:

```
samba-tool domain passwordsettings pso create senhas_administrativo 1 --complexity=on
```

```
root@ad:~# samba-tool domain passwordsettings pso create senhas_administrativo 1 --complexity=on
Not all password policy options have been specified.
For unspecified options, the current domain password settings will be used as the default values.
PSO successfully created: CN=senhas_administrativo,CN=Password Settings Container,CN=System,DC=samse
c,DC=com,DC=br
Password information for PSO 'senhas_administrativo'

Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 5
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Controlador de Domínio

Password Settings Objects (PSO)

Para alterar o pso criada utilizamos a função **set**:

samba-tool domain passwordsettings pso set senhas_administrativo --min-pwd-length=8

```
root@ad:~# samba-tool domain passwordsettings pso set senhas_administrativo --min-pwd-length=8
Successfully updated PSO: CN=senhas_administrativo,CN=Password Settings Container,CN=System,DC=samse
c,DC=com,DC=br
Password information for PSO 'senhas_administrativo'

Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 8
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Controlador de Domínio

Password Settings Objects (PSO)

Para alterar o pso criada utilizamos a função **set**.

Outro exemplo para definir o tempo máximo de uma senha:

samba-tool domain passwordsettings pso set senhas_administrativo --max-pwd-age=90

```
root@ad:~# samba-tool domain passwordsettings pso set senhas_administrativo --max-pwd-age=90
Successfully updated PSO: CN=senhas_administrativo,CN=Password Settings Container,CN=System,DC=samse
c,DC=com,DC=br
Password information for PSO 'senhas_administrativo'

Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 8
Minimum password age (days): 1
Maximum password age (days): 90
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
```

Controlador de Domínio

Para aplicar um pso a um determinado grupo:

samba-tool domain passwordsettings pso apply 'senhas_administrativo' 'RH'

```
root@ad:~# samba-tool domain passwordsettings pso apply 'senhas_administrativo' 'RH'  
PSO 'senhas_administrativo' applied to 'RH'  
[100%]
```

Controlador de Domínio

Password Settings Objects (PSO)

Para consultar as opções configuradas de um pso:

samba-tool domain passwordsettings pso show senhas_administrativo

```
root@ad:~# samba-tool domain passwordsettings pso show senhas_administrativo
Password information for PSO 'senhas_administrativo'

Precedence (lowest is best): 1
Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 8
Minimum password age (days): 1
Maximum password age (days): 90
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30

PSO applies directly to 2 groups/users:
  CN=RH,OU=Araras,DC=samsec,DC=com,DC=br
  CN=Administrativo,OU=Araras,DC=samsec,DC=com,DC=br
```

Controlador de Domínio

Password Settings Objects (PSO)

Para consultar se um determinado grupo tem o pso associado:

samba-tool group show Administrativo

```
root@ad:~# samba-tool group show Administrativo
dn: CN=Administrativo,OU=Araras,DC=samsec,DC=com,DC=br
objectClass: top
objectClass: group
cn: Administrativo
instanceType: 4
whenCreated: 20200504182840.02
uSNCreated: 4651
name: Administrativo
objectGUID: beab3dcc-2a79-4dce-9df0-b74f855bf133
objectSid: S-1-5-21-3316795626-2069486437-2947886286-1106
sAMAccountName: Administrativo
sAMAccountType: 268435456
groupType: -2147483646
objectCategory: CN=Group,CN=Schema,CN=Configuration,DC=samsec,DC=com,DC=br
member: CN=pedrinho,CN=Users,DC=samsec,DC=com,DC=br
member: CN=joaozinho,CN=Users,DC=samsec,DC=com,DC=br
whenChanged: 20200505133507.02
uSNChanged: 5176
msDS-PSOApplied: CN=senhas_administrativo,CN=Password Settings Container,CN=System,DC=samsec,DC=com,DC=br
distinguishedName: CN=Administrativo,OU=Araras,DC=samsec,DC=com,DC=br
```

Controlador de Domínio

Password Settings Objects (PSO)

Para consultar todos os pso's criados:

samba-tool domain passwordsettings pso list

```
root@ad:~# samba-tool domain passwordsettings pso list
Precedence | PSO name
-----
1          | senhas_administrativo
root@ad:~#
```

Linux Completo + Servidores

Aula 37: Controlador de Domínio (SAMBA) parte 3

Controlador de Domínio

Diretiva de Grupo, ou Group Policy (GPO), é uma funcionalidade da família de sistemas operacionais Microsoft Windows NT.

É um conjunto de regras que controlam o ambiente de trabalho de contas de usuário e contas de computador.

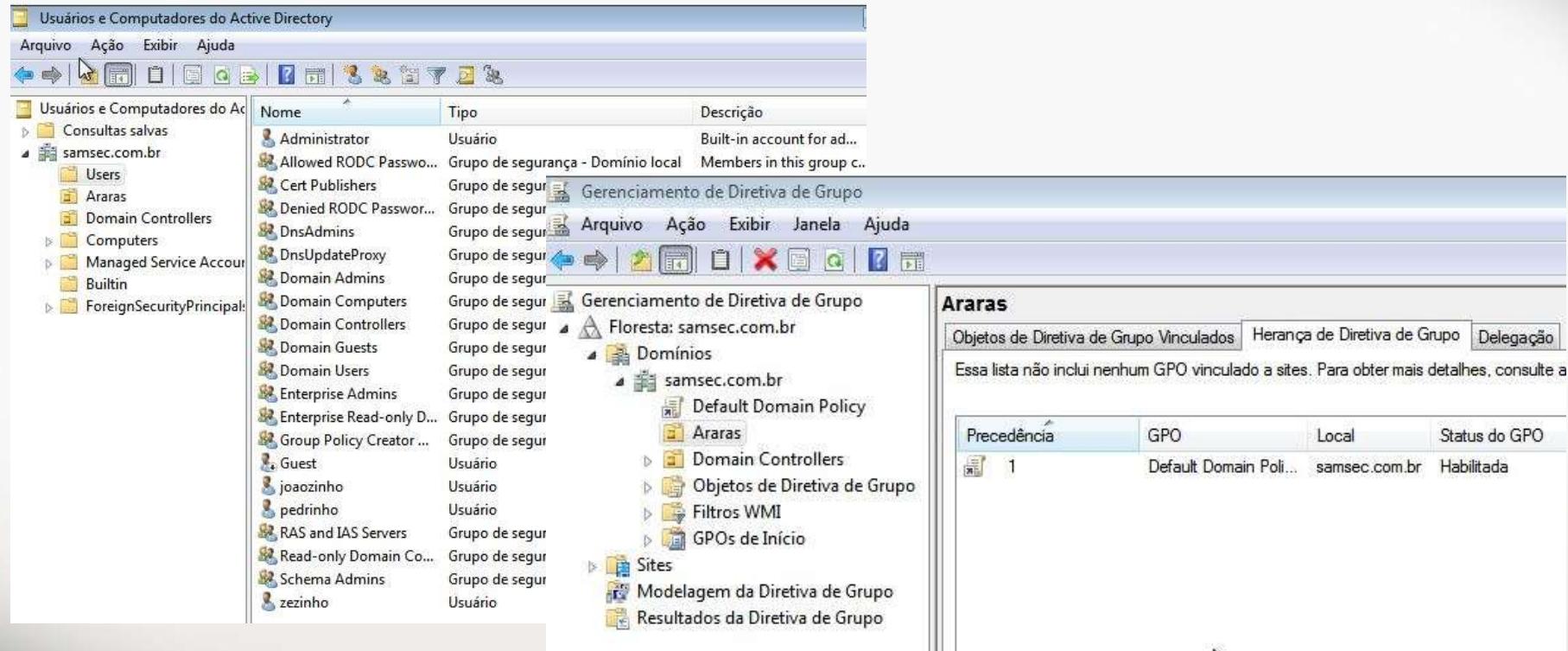
Ela fornece o gerenciamento e configuração centralizados de sistemas operacionais, aplicativos e configurações dos usuários em um ambiente Active Directory\SAMBA.

Em outras palavras, a Diretiva de Grupo controla em parte o que os usuários podem ou não fazer em um sistema de computador.

Controlador de Domínio

O SAMBA tem suporte ao RSAT (Remote Server Administration Tools).

Isso permite que todo o domínio, inclusive a criação de GPO's possam ser executadas remotamente.



Download Windows 10

<https://www.microsoft.com/en-us/download/details.aspx?id=45520>

Download Windows 7

<https://www.microsoft.com/pt-br/download/details.aspx?id=7887>

Controlador de Domínio

Group Policy (GPO)

Bloquear o acesso ao painel de controle

1-) Crie uma nova GPO



2-) Defina um nome para a GPO



Controlador de Domínio

Group Policy (GPO)

Bloquear o acesso ao painel de controle

3-) Selecione a nova GPO

The screenshot shows the 'Gerenciamento de Diretiva de Grupo' (Group Policy Management) console. On the left, under 'Floresta: samsec.com.br', the 'Domínios' node is expanded, showing 'samsec.com.br' with its subfolders: 'Bloqueio Painel de Controle' (highlighted with a red box), 'Default Domain Policy', 'Araras', 'Domain Controllers', 'Leme', 'Objetos de Diretiva de Grupo', 'Filtros WMI', and 'GPOs de Início'. Under 'Sites', there are 'Modelagem da Diretiva de Grupo' and 'Resultados da Diretiva de Grupo'. On the right, the 'Default Domain Policy' properties are displayed. The 'Links' tab is selected, showing 'samsec.com.br' as the local link. The 'Filtros de Segurança' section indicates that the policy can only apply to groups, users, and computers, and lists 'Administrativo (SAMSEC\Administrativo)' in the 'Nome' column. A red arrow points from the text 'Adicione os grupos que farão parte dessa GPO' to the 'Nome' column in the security filter table.

Gerenciamento de Diretiva de Grupo

Floresta: samsec.com.br

Domínios

samsec.com.br

- Bloqueio Painel de Controle
- Default Domain Policy
- Araras
- Domain Controllers
- Leme
- Objetos de Diretiva de Grupo
- Filtros WMI
- GPOs de Início

Sites

- Modelagem da Diretiva de Grupo
- Resultados da Diretiva de Grupo

Default Domain Policy

Escopo Detalhes Opções Delegação

Links

Exibir links neste local: samsec.com.br

Os sites, domínios e UOs a seguir estão vinculados a este GPO:

Local	Imposto	Vínculo Habilida
samsec.com.br	Não	Sim

Filtros de Segurança

As configurações deste GPO só podem se aplicar aos grupos, usuários e computadores

Nome
Administrativo (SAMSEC\Administrativo)

Adicionar... Remover Propriedades

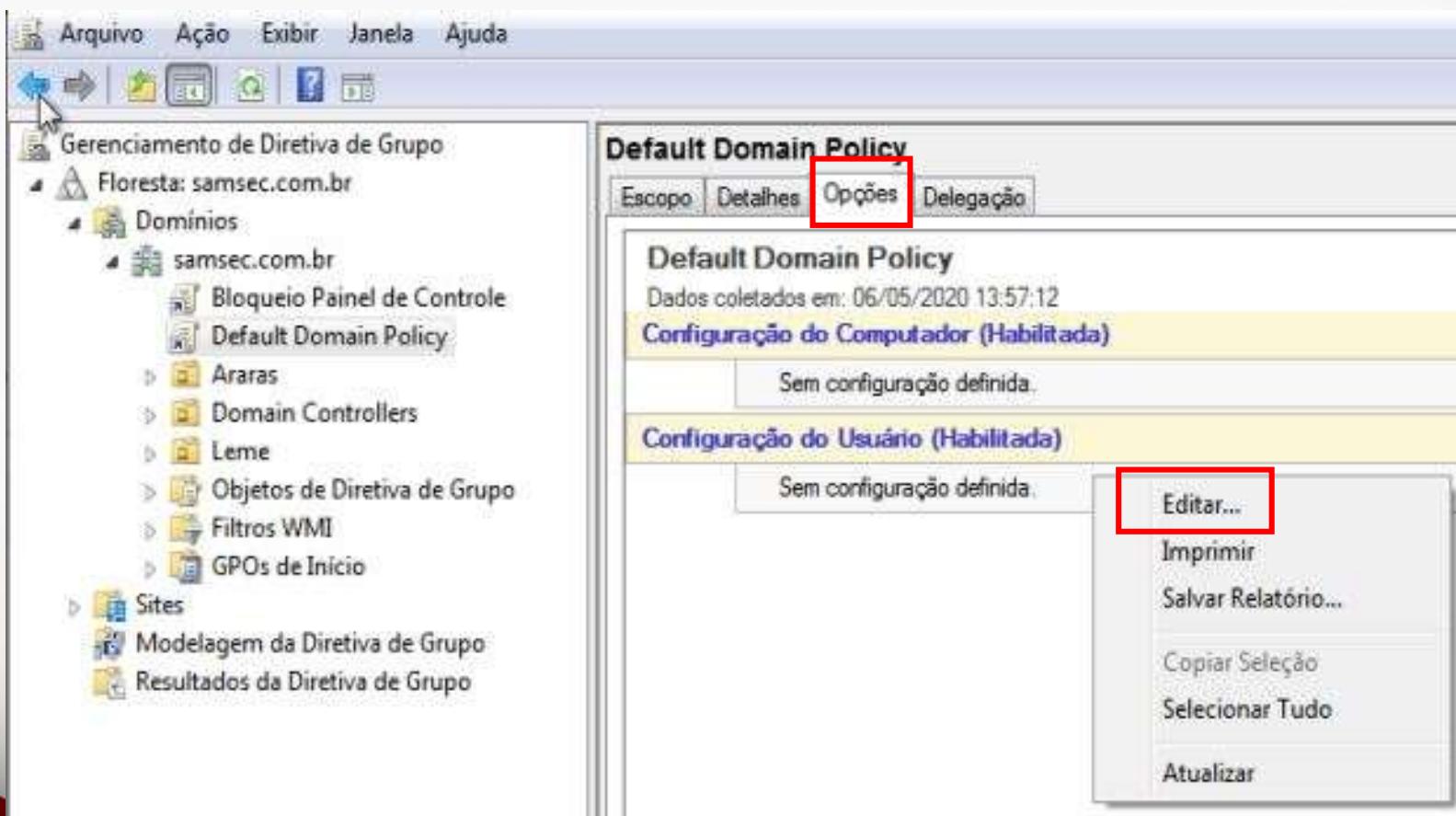
Adicione os grupos que farão parte dessa GPO

Controlador de Domínio

Group Policy (GPO)

Bloquear o acesso ao painel de controle

4-) Em Opções, edite a GPO

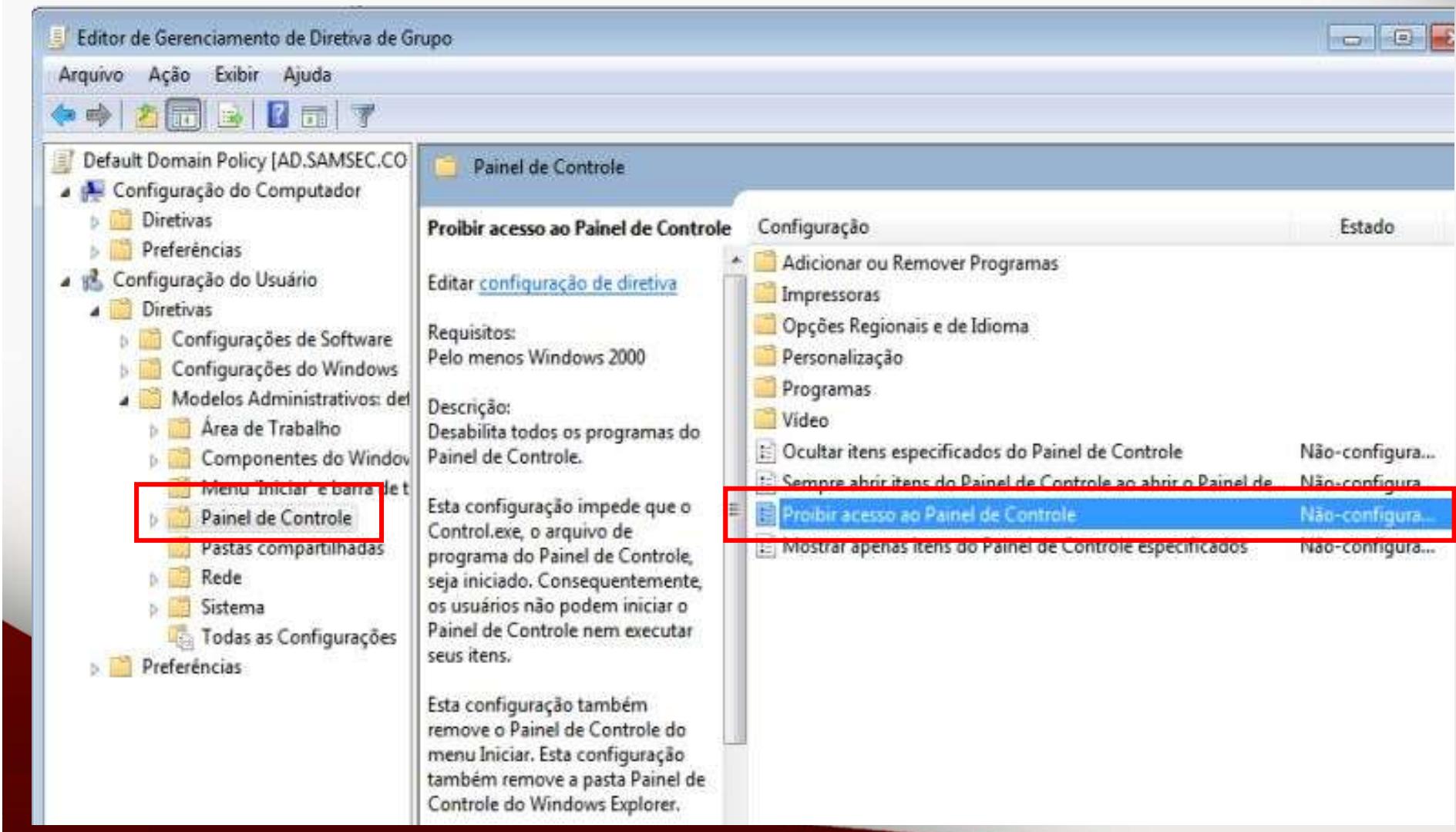


Controlador de Domínio

Group Policy (GPO)

Bloquear o acesso ao painel de controle

5-) Selecione Configurações do Usuário\Diretivas\Modelos Administrativos\Painel de Controle



Controlador de Domínio

Group Policy (GPO)

Bloquear o acesso ao painel de controle
6-) Por fim Habilite a configuração:

The screenshot shows two windows related to Group Policy Management.

Proibir acesso ao Painel de Controle (Configure a GPO):

- Opções:** A radio button labeled "Habilitado" is selected and highlighted with a red box.
- Aceito em:** "Pelo menos Windows 2000"
- Ajuda:** Desabilita todos os programas do Painel de Controle. This configuration prevents the Control.exe file from running, which stops the Control Panel from starting. Consequently, users cannot open the Control Panel or run its items.

Default Domain Policy (View GPO details):

- Configuração do Computador (Habilitada):** No "Modelos Administrativos" section, the "Painel de Controle" policy is listed with the following details:

Diretiva	Configuração	comentário
Proibir acesso ao Painel de Controle	Ativada	