

Sistemas operacionais II
Trabalho 1 - Cluster de máquinas

Akira Kotsugai
Felipe Menino Carlos
Weslei Luiz

13 de abril de 2018

1 CONTEXTUALIZAÇÃO

Linux é um termo utilizado para se referir a sistemas operacionais que utilizem o núcleo Linux. O núcleo ou kernel Linux foi desenvolvido pelo programador finlandês Linus Torvalds, inspirado no sistema Minix. O seu código fonte está disponível sob a licença GPL (versão 2) para que qualquer pessoa o possa utilizar, estudar, modificar e distribuir livremente de acordo com os termos da licença. Atualmente este sistema operacional é muito usado em servidores (Web, e-mail, Banco de Dados...), e também como ferramenta administrativa para segurança em redes de computadores. Saber instalar e configurar este sistema operacional é importante e uma falha pode causar um resultado catastrófico.

Seu objetivo neste trabalho é entregar uma configuração de cluster, com duas máquinas no mínimo, instaladas e configuradas de acordo com os seguintes requisitos:

- Sistema operacional: Debian
 - Sem interface gráfica;
 - Partições separadas para o /home e /var. /home com no máximo 100mb e /var com 3gb. O formato das partições será o EXT3
- As máquinas deverão estar na mesma rede. Mesma máscara de rede e faixa de IP.
- A comunicação entre elas deverá ser habilitada por ssh e não deve ser permitido a uma máquina realizar conexão remota com outra que não pertença ao cluster, exceto o gateway. O acesso ao cluster por máquinas externas deverá ser habilitado, e por isso o gateway deverá ter duas interfaces de redes, uma para comunicação interna e outra para comunicação externa.
- Deverá existir uma máquina gateway e ela irá fornecer acesso, as outras máquinas, à Internet e a conexão remota externa, ou seja, alguém poderá realizar ssh para o gateway e a partir daí acessar as máquinas do cluster.
- Não será permitido ssh como root direto. E o usuário administrador não deverá ter acesso a senha do usuário root.
- Os usuários do cluster deverão ter contas em cada máquina e serão pelo menos 3 usuários. Sendo que deve existir um usuário administrador responsável por gerenciar os demais. Este administrador será o único com acesso a poderes de root em todas as máquinas. Cada usuário deverá ter uma quota em disco de no máximo 50mb, para isso será necessário estudar o funcionamento do pacote quota.
- Os sistemas deverão ter os seguintes grupos:

- Arquivadores: Usuários responsáveis pelo gerenciamento de arquivos
 - Agendadores: Usuários responsáveis pelo agendamento de tarefas
- O usuário administrador deverá distribuir os demais nos grupos.
- Para cada grupo deverá ser criado uma pasta no /var. O acesso deverá ser restrito ao grupo, ou seja, usuários que não sejam dos grupos supracitados não poderão acessar o conteúdo das pastas.

2 CRIAÇÃO DO CLUSTER

Neste capítulo será descrito as etapas tomadas para a criação do cluster.

2.1 ARQUITETURA

A arquitetura adotada para a solução dos problemas apresentados, seguirá o modelo cliente/servidor, e pode ser visualizada abaixo:

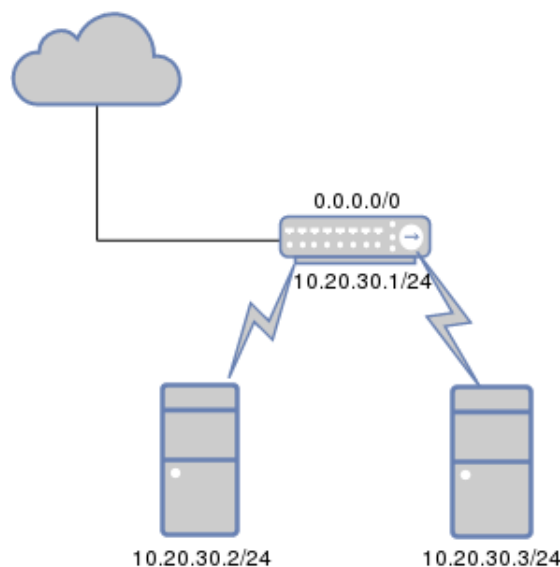


Figura 1 – Topologia do projeto

Nas próximas seções serão apresentados os passos para a configuração desta arquitetura. É importante lembrar que, os passos estão na mesma sequência em que as configurações foram realizadas.

2.2 INSTALAÇÃO DO SISTEMA OPERACIONAL

O primeiro passo para a configuração do **cluster** será a instalação do sistema operacional. Nesta etapa foi realizada a divisão das partições para a utilização separada dos diretórios **/home**, com até 100 MB de espaço e o **/var** com até 3GB de espaço livre.

Veja abaixo os passos da instalação.

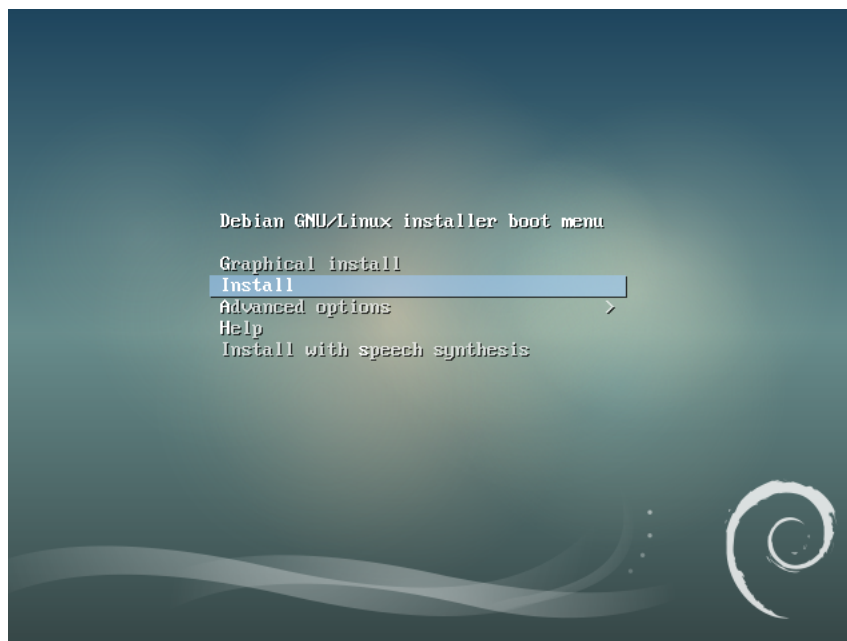


Figura 2 – Tela inicial de instalação

Na imagem que segue, é realizada a configuração das partições, essas foram configuradas utilizando o **EXT3**, para que em um passo futuro a configuração do pacote **quotes**, seja realizada sem problemas.

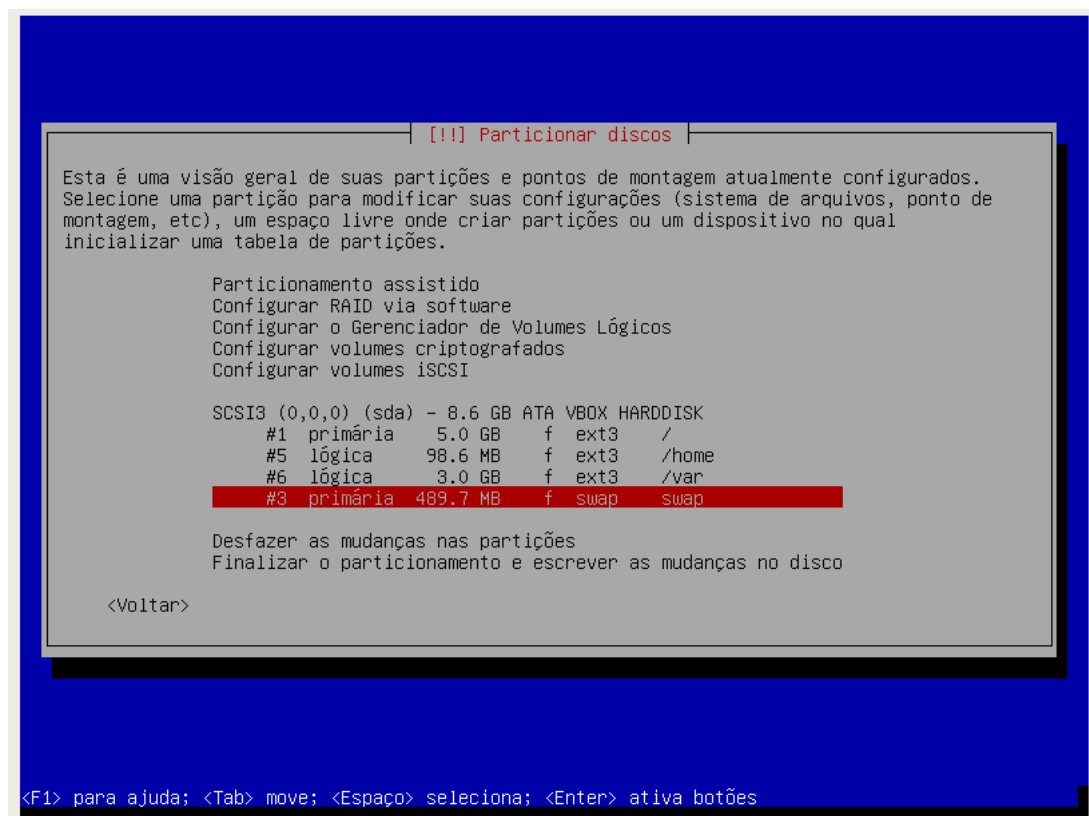


Figura 3 – Configuração das partições

O sistema instalado tem apenas os serviços básicos

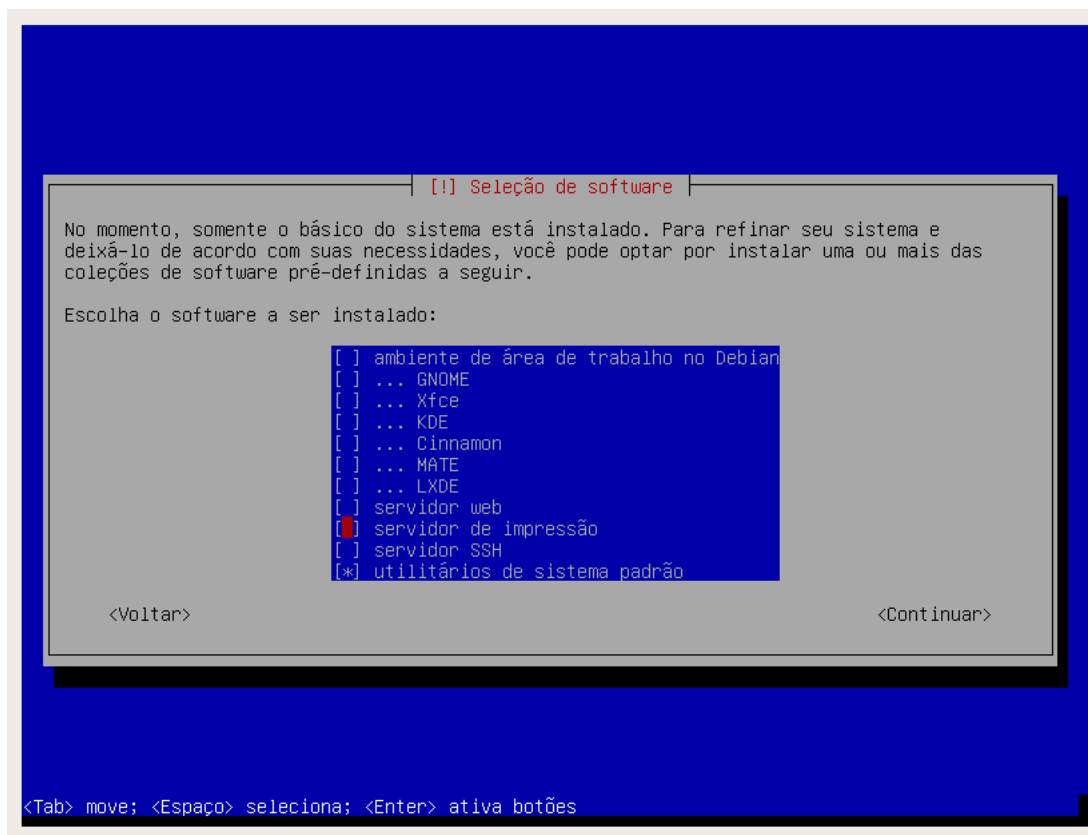


Figura 4 – Definições dos serviços/*softwares* padrão

A etapa abaixo, demonstra as partições criadas anteriormente.

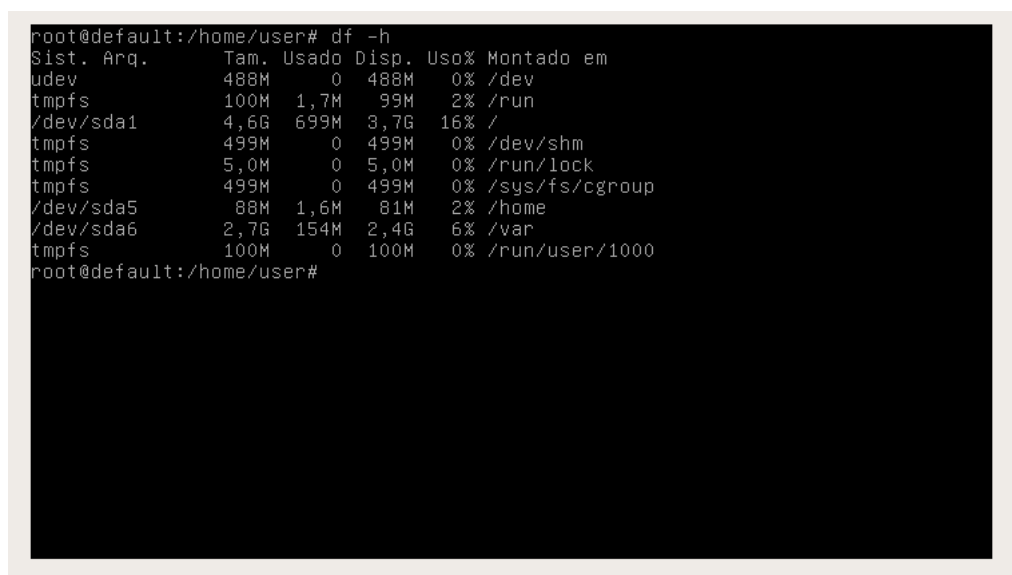


Figura 5 – Confirmação da separação das partições

Após realizar os passos demonstrados acima, a parte de instalação do sistema operacional foi realizada.

2.3 CONFIGURAÇÃO DAS INTERFACES DE REDE

Nesta etapa será realizado as interfaces de rede, no *gateway* e no *host*.

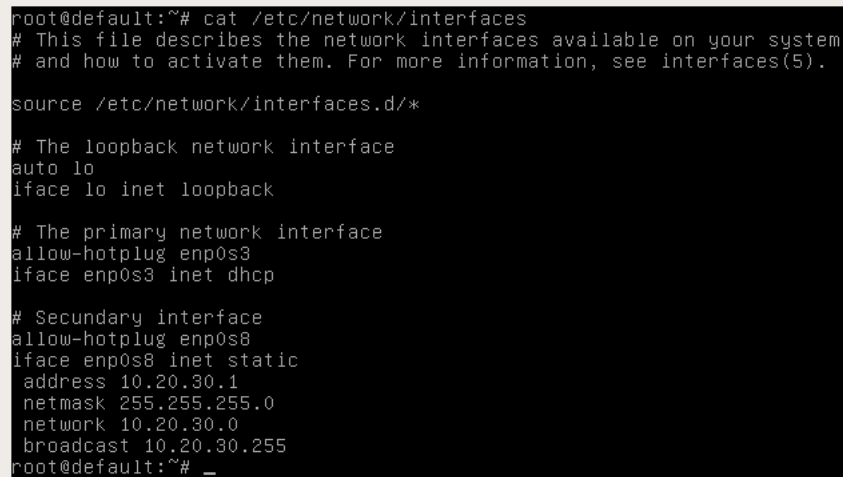
2.3.1 Configuração do gateway

No caso do *gateway*, ele terá duas interfaces de rede, uma para realizar a comunicação com a rede externa (*internet*) e outra para a comunicação interna, entre as máquinas do cluster.

As interfaces do gateway são:

- **enp0s3** - Rede externa
 - IP: Dinâmico
- **enp0s8** - Rede interna
 - IP: 10.20.30.1
 - Rede: 255.255.255.0 (/24)

Abaixo é demonstrado o arquivo de configuração da interface de rede.



```
root@default:~# cat /etc/network/interfaces
# 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

# Secondary interface
allow-hotplug enp0s8
iface enp0s8 inet static
    address 10.20.30.1
    netmask 255.255.255.0
    network 10.20.30.0
    broadcast 10.20.30.255
root@default:~# _
```

Figura 6 – Configuração de rede - Gateway

O arquivo representado na imagem é o **/etc/network/interfaces**

2.3.2 Configuração do host

Diferente do *gateway*, os *hosts* terão apenas uma única interface, essa que será conectada com o *gateway*.

A configuração seguida na interface dos hosts foi a seguinte

- Host 1
 - IP: 10.20.30.2
 - Rede: 255.255.255.0 (/24)
- Host 2
 - IP: 10.20.30.3
 - Rede: 255.255.255.0 (/24)

```
# 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 static
    address 10.20.30.2
    netmask 255.255.255.0
    network 10.20.30.0
    gateway 10.20.30.1
```

Figura 7 – Configuração de rede - Host 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 static
    address 10.20.30.3
    netmask 255.255.255.0
    network 10.20.30.0
    gateway 10.20.30.1
```

Figura 8 – Configuração de rede - Host 2

2.4 CONFIGURAÇÃO DO QUOTA

A **quota** é uma ferramenta que facilita o gerenciamento de espaços e limite para grupos e usuários. No tópico de instalação do sistema, foi mencionado que o particionamento será criado utilizando o **EXT3** foi feito por conta do quota, é importante citar este tópico pois, este é um pré-requisito para a utilização do pacote. Veja abaixo os passos utilizados na configuração do quota.

1° - Instalação do pacote

```
apt install quota
```


Após realizar a instalação, será necessário definir quais partições farão a utilização do **quota**, para isso é feito o acesso a `/etc/fstab`, dentro deste arquivo, é inserido nas opções da partição escolhida a opção **usrquota**, isso porque neste caso será feito o controle através de usuários. Aqui a partição escolhida foi a `/home`.

```
# /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=e5aa58d8-626f-473c-8c81-5e21ff578974 / ext3 errors=remount-ro 0 1
# /home was on /dev/sda5 during installation
UUID=6f23edfd-6330-4c25-ad08-f1dba68d5bbb /home ext3 defaults,usrquota 0 2
# /var was on /dev/sda6 during installation
UUID=c569d992-a350-47c4-8e2c-d134c72ee249 /var ext3 defaults 0 2
# swap was on /dev/sda3 during installation
UUID=3461bcde-702d-4c53-87d5-209b028b2969 none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
```

Figura 9 – Arquivo de configuração de quota

As configurações de **quota** demonstradas acima, estão replicadas em todas as máquinas *host* do cluster.

2.5 GERENCIAMENTO DOS USUÁRIOS E GRUPOS

Neste capítulo todo o gerenciamento de grupos e usuários é abordado. Três usuários foram adicionados para atender os requisitos citados na contextualização:

- Usuário administrador com privilégios de root para gerenciar todos os usuários
- Administrador para o grupo Arquivadores
- Administrador para o grupo Agendadores

2.5.1 Adicionar usuários ao sistema

O comando utilizado para adicionar os usuários "admin", "agendador" e "arquivador", foi o `# adduser` conforme exemplo abaixo:

```

root@default:~# adduser exemplo
Adicionando usuário 'exemplo' ...
Adicionando novo grupo 'exemplo' (1009) ...
Adicionando novo usuário 'exemplo' (1007) com grupo 'exemplo' ...
Criando diretório pessoal '/home/exemplo' ...
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 exemplo
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@default:~#

```

Figura 10 – Adicionando usuários com `#adduser`

2.5.2 Configuração usuário admin

Para conceder privilégios de root ao usuário **adimin** foi utilizado o pacote **sudo**, este pacote eleva a permissão de usuários comuns, para que possam executar tarefas de administradores quando necessário, digitando **sudo**, antes de comandos que são autorizados apenas para o root. Para realizar a instalação do pacote sudo o comando `# apt-get install sudo` foi executado:

```

root@default:~# apt-get install sudo
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Os NOVOS pacotes a seguir serão instalados:
 sudo
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
E preciso baixar 0 B/1.055 kB de arquivos.
Depois desta operação, 3.108 kB adicionais de espaço em disco serão usados.
A seleccionar pacote anteriormente não seleccionado sudo.
(Lendo banco de dados ... 28870 ficheiros e directórios actualmente instalados.)
A preparar para desempacotar .../sudo_1.8.19p1-2.1_amd64.deb ...
A descompactar sudo (1.8.19p1-2.1) ...
Configurando sudo (1.8.19p1-2.1) ...
A processar 'triggers' para systemd (232-25+deb9u3) ...
A processar 'triggers' para man-db (2.7.6.1-2) ...
root@default:~#

```

Figura 11 – Instalação do pacote sudo

As permissões de administrador para usuários comuns, são configuradas no arquivo `sudoers` localizado em `/etc/sudoers`, preferencialmente utilizando o comando **visudo**, os parâmetros definidos são:

- Máquinas em que os comandos poderão ser executados
- Usuários que poderão executar os comandos
- Comandos permitidos

Na imagem abaixo as permissões do usuário admin são configuradas:

```

# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"
# Host alias specification
# User alias specification
# Cmnd alias specification
# User privilege specification
root    ALL=(ALL:ALL) ALL
admin   ALL=(ALL:ALL) ALL
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
# See sudoers(5) for more information on "#include" directives:
#include_dir /etc/sudoers.d

```

Figura 12 – Configuração do arquivo sudoers

Após esta configuração o usuário admin conseguirá executar comandos root.

2.5.3 Criação e configuração dos diretórios

Os diretórios e grupos **arquivadores** e **agendadores** foram criados para atender os dois últimos requisitos deste capítulo:

```

root@default:/var# ls
backups cache lib local lock log lost+found mail opt run spool tmp
root@default:/var# mkdir arquivadores
root@default:/var# mkdir agendadores
root@default:/var# addgroup arquivadores
Adicionando grupo 'arquivadores' (GID 1007) ...
Concluído.
root@default:/var# addgroup agendadores
Adicionando grupo 'agendadores' (GID 1008) ...
Concluído.
root@default:/var# ls
agendadores arquivadores backups cache lib local lock log lost+found mail opt run spool tmp
root@default:/var#

```

Figura 13 – Grupos e Diretórios para os agendadores e arquivadores

Os diretórios arquivadores e agendadores foram alterados de grupo, para seus respectivos administradores com o comando **chgrp agendadores agendadores** e **chgrp arquivadores arquivadores**, seguindo esta sintaxe **chgrp [grupo] [diretório]** conforme imagem abaixo:

```

root@default:/var# ls -l
total 60
drwxr-xr-x  2 root agendadores  4096 abr 11 11:39 agendadores
drwxr-xr-x  2 root arquivadores 4096 abr 11 11:39 arquivadores
drwxr-xr-x  2 root root          4096 abr 9 22:08 backups
drwxr-xr-x  7 root root          4096 abr 8 19:25 cache
drwxr-xr-x 26 root root          4096 abr 11 11:21 lib
drwxrwsr-x  2 root staff        4096 fev 23 20:23 local
lrwxrwxrwx  1 root root          9 abr 8 19:07 lock -> /run/lock
drwxr-xr-x  4 root root          4096 abr 8 19:28 log
drwx----- 2 root root        16384 abr 8 19:07 lost+found
drwxrwsr-x  2 root mail         4096 abr 8 19:07 mail
drwxr-xr-x  2 root root         4096 abr 8 19:07 opt
lrwxrwxrwx  1 root root          4 abr 8 19:07 run -> /run
drwxr-xr-x  4 root root          4096 abr 8 19:08 spool
drwxrwxrwt  4 root root          4096 abr 11 10:56 tmp
root@default:/var# chgrp grupo diretorio

```

Figura 14 – Alteração de grupo dos diretórios agendadores - arquivadores

Todas as permissões de execução, leitura e escrita foram removidas dos outros e do dono utilizando o comando **chmod** para que apenas usuários que pertencerem aos grupos agendadores e/ou arquivadores possam realizar operações nos diretórios:

```

root@default:/var# chmod 070 agendadores/ arquivadores/
root@default:/var# ls -l
total 60
d---rwx---  2 root agendadores  4096 abr 11 11:39 agendadores
d---rwx---  2 root arquivadores 4096 abr 11 11:39 arquivadores
drwxr-xr-x  2 root root          4096 abr 9 22:08 backups
drwxr-xr-x  7 root root          4096 abr 8 19:25 cache
drwxr-xr-x 26 root root          4096 abr 11 11:21 lib
drwxrwsr-x  2 root staff        4096 fev 23 20:23 local
lrwxrwxrwx  1 root root          9 abr 8 19:07 lock -> /run/lock
drwxr-xr-x  4 root root          4096 abr 8 19:28 log
drwx----- 2 root root        16384 abr 8 19:07 lost+found
drwxrwsr-x  2 root mail         4096 abr 8 19:07 mail
drwxr-xr-x  2 root root         4096 abr 8 19:07 opt
lrwxrwxrwx  1 root root          4 abr 8 19:07 run -> /run
drwxr-xr-x  4 root root          4096 abr 8 19:08 spool
drwxrwxrwt  4 root root          4096 abr 11 10:56 tmp
root@default:/var#

```

Figura 15 – Permissões - diretórios agendadores e arquivadores

Tabela 1 – Permissões

Usuário	0	- - -
Grupo	7	rwx
Outros	0	- - -

2.5.4 Configuração dos grupos

Os usuários agendador e arquivador, foram adicionados em seus grupos agendadores e arquivadores, respectivamente:

```

root@default:~# gpasswd -a agendador agendadores
Adicionando usuário agendador ao grupo agendadores
root@default:~# gpasswd -a arquivador arquivadores
Adicionando usuário arquivador ao grupo arquivadores
root@default:~#

```

Figura 16 – Incluindo usuários a seus grupos

Os mesmos foram definidos como administradores de seu grupo para que realizem o gerenciamento de usuários com o comando **gpasswd**:

```
root@default:~# gpasswd -A agendador agendadores
root@default:~# gpasswd -A arquivador arquivadores
root@default:~#
```

Figura 17 – Definição de usuários administradores

Desta forma toda a administração dos grupos pode ser feita por usuários sem elevação de root.

2.6 CONFIGURAÇÃO DOS SERVIÇOS DE REDE

Neste etapa, será demonstrado o processo de configuração dos serviços de rede que irão permitir a comunicação entre as máquinas do cluster. Serão instalados e configurados o **SSH** e o compartilhamento de rede utilizando o **IPTABLES**.

2.6.1 Configuração do SSH no Gateway

A configuração do **ssh** no *gateway* será realizada para que ele aceite conexões na porta **5678**. O primeiro passo será a instalação do pacote **ssh**.

```
apt install ssh
```

Após a instalação do pacote, será necessário realizar o acesso ao arquivo de configuração do **ssh**, este que fica no diretório **/etc/ssh/sshd_config**, dentro deste arquivo será alterado os argumentos **Port** e **PermitRootLogin**, como demonstrado abaixo

```
Port 5678
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin no
```

Figura 18 – Configuração de SSH - Gateway

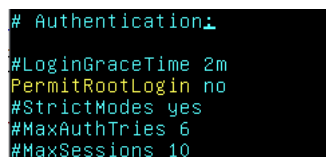
Depois de configurado, o acesso não será permitido para o usuário **root** e a conexão **ssh** para o **gateway** só poderá ser realizada na porta **5678**.

2.6.2 Configuração do SSH no Host

Da mesma forma que demonstrado no tópico anterior, o pacote **ssh** deverá estar instalado.

Com o pacote instalado será necessário acessar o arquivo `/etc/ssh/sshd_config`, e modificar apenas a linha de permissão de acesso do **root**.

Ao realizar a configuração a linha a ser alterada ficará como demonstrado abaixo:

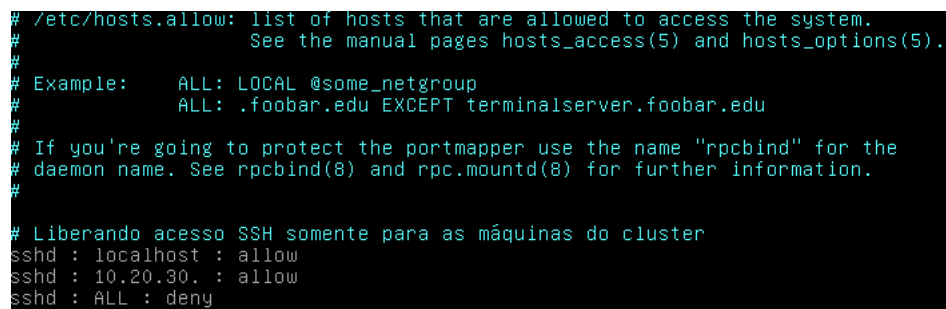


```
# Authentication␣
#LoginGraceTime 2m
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

Figura 19 – Configuração de SSH - Host

As máquinas **host** terão ainda uma opção para negar o acesso de todos os pedidos de conexão **ssh** que não venham de máquinas do cluster. Esta configuração será realizada no arquivo `/etc/hosts.allow`.

Dentro deste arquivo será declarado que qualquer conexão **ssh** que tenha origem diferente do endereço **10.20.30.0**, deverá ser recusada. Abaixo há o arquivo já com as definições feitas.



```
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                               See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#               ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "rpcbind" for the
# daemon name. See rpcbind(8) and rpc.mountd(8) for further information.
#
# Liberando acesso SSH somente para as máquinas do cluster
sshd : localhost : allow
sshd : 10.20.30. : allow
sshd : ALL : deny
```

Figura 20 – Bloqueio de acesso externo ao cluster

É importante lembrar que todas essas configurações foram feitas nas duas máquinas **host** presentes no cluster.

2.6.3 Configuração do compartilhamento de rede

Para finalizar o processo de configuração dos serviços de rede, será realizado o compartilhamento dos serviços de *internet* do **gateway** e os **hosts**.

O processo de configuração do compartilhamento de rede pode ser visualizado abaixo

```

sysctl -w net.ipv4.ip_forward=1
sysctl -p
iptables -X
iptables -F
iptables -t nat -X
iptables -t nat -F
iptables -I INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -I FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -t nat -I POSTROUTING -o enp0s3 -j MA

```

Ao final da execução das linhas demonstradas acima, os **hosts** terão acesso aos serviços de *internet* fornecidos pelo **gateway**.

2.7 TESTES

As configurações realizadas nos capítulos anteriores serão evidenciados neste, para exemplificar como o projeto funciona na prática.

2.7.1 Grupos

Teste de administração de grupo:

```

root@default:/var# chmod 070 agendadores/ arquivadores/
root@default:/var# ls -l
total 60
d---rwx--- 2 root agendadores 4096 abr 11 11:39 agendadores
d---rwx--- 2 root arquivadores 4096 abr 11 11:39 arquivadores
drwxr-xr-x 2 root root 4096 abr 9 22:08 backups
drwxr-xr-x 7 root root 4096 abr 8 19:25 cache
drwxr-xr-x 26 root root 4096 abr 11 11:21 lib
drwxrwsr-x 2 root staff 4096 fev 23 20:23 local
lrwxrwxrwx 1 root root 9 abr 8 19:07 lock -> /run/lock
drwxr-xr-x 4 root root 4096 abr 8 19:28 log
drwx----- 2 root root 16384 abr 8 19:07 lost+found
drwxrwsr-x 2 root mail 4096 abr 8 19:07 mail
drwxr-xr-x 2 root root 4096 abr 8 19:07 opt
lrwxrwxrwx 1 root root 4 abr 8 19:07 run -> /run
drwxr-xr-x 4 root root 4096 abr 8 19:08 spool
drwxrwxrwt 4 root root 4096 abr 11 10:56 tmp
root@default:/var#

```

Figura 21 – Gerenciamento de grupos

Neste exemplo o usuário `user` é adicionado ao grupo `agendadores` pelo usuário `agendador`. Um arquivo é criado por `user` e removido para testes de leitura escrita e execução. Após isso o mesmo é removido do grupo `agendadores` e não consegue mais realizar acesso ao diretório `agendadores`.

3 CONCLUSÃO