

Sistemas operacionais II

Trabalho 1 - Cluster de máquinas

Akira Kotsugai
Felipe Menino Carlos
Weslei Luiz

18 de abril de 2018

SUMÁRIO

	Sumário	2
	Lista de ilustrações	3
	Lista de tabelas	5
1	CONTEXTUALIZAÇÃO	6
2	CRIAÇÃO DO CLUSTER	8
2.1	Arquitetura	8
2.2	Instalação do sistema operacional	8
2.3	Configuração das interfaces de rede	11
2.3.1	Configuração do gateway	11
2.3.2	Configuração do host	11
2.4	Gerenciamento dos usuários e grupos	12
2.4.1	Adicionar usuários ao sistema	13
2.4.2	Configuração usuário admin	13
2.4.3	Criação e configuração dos diretórios	14
2.4.4	Configuração dos grupos	15
2.5	Configuração do quota	16
2.6	Configuração dos serviços de rede	18
2.6.1	Configuração do SSH no Gateway	18
2.6.2	Configuração do SSH no Host	19
2.6.3	Configuração do compartilhamento de rede	20
2.7	Testes	21
2.7.1	Partições	21
2.7.2	Configuração de redes das máquinas	23
2.7.3	Conexões SSH	24
2.7.4	Poderes de root para o Administrador	28
2.7.5	Quotas	30
2.7.6	Grupos	31
3	CONCLUSÃO	32

LISTA DE ILUSTRAÇÕES

Figura 1 – Topologia do projeto	8
Figura 2 – Tela inicial de instalação	9
Figura 3 – Configuração das partições	9
Figura 4 – Definições dos serviços/ <i>softwares</i> padrão	10
Figura 5 – Confirmação da separação das partições	10
Figura 6 – Configuração de rede - Gateway	11
Figura 7 – Configuração de rede - Host 1	12
Figura 8 – Configuração de rede - Host 2	12
Figura 9 – Adicionando usuários com <i>adduser</i>	13
Figura 10 – Instalação do pacote <i>sudo</i>	13
Figura 11 – Configuração do arquivo <i>sudoers</i>	14
Figura 12 – Grupos e Diretórios para os agendadores e arquivadores	14
Figura 13 – Alteração de grupo dos diretórios agendadores - arquivadores	15
Figura 14 – Permissões - diretórios agendadores e arquivadores	15
Figura 15 – Incluindo usuários a seus grupos	15
Figura 16 – Definição de usuários administradores	16
Figura 17 – Arquivo de configuração de quota	16
Figura 18 – Configuração de quota para usuário	17
Figura 19 – Configuração de SSH - Gateway	19
Figura 20 – Configuração de SSH - Host	19
Figura 21 – Bloqueio de acesso externo ao cluster	20
Figura 22 – Gateway particionado.	21
Figura 23 – Host 1 particionado.	22
Figura 24 – Host 2 particionado.	22
Figura 25 – Rede externa e interna do Gateway.	23
Figura 26 – Rede interna do Host 1.	23
Figura 27 – Rede interna do Host 2.	24
Figura 28 – Host 1 dando SSH no Gateway com sucesso.	24
Figura 29 – Host 1 dando SSH no Host 2 diretamente.	25
Figura 30 – Host 1 dando SSH no Host 2 pelo Gateway	25
Figura 31 – SSH de outra máquina não pertencente ao cluster, no Gateway.	26
Figura 32 – SSH de outra máquina não pertencente ao cluster no Host 1, através do Gateway	26
Figura 33 – Host 2 tentando dar SSH em máquina fora do cluster sem sucesso.	27
Figura 34 – Root tentando dar SSH sem sucesso.	27

Figura 35 – Admin conseguindo apagar arquivo de outro usuário. 28

Figura 36 – Outro usuário tentando ter poder de root sem sucesso. 28

Figura 37 – Admin não consegue se tornar root. 29

Figura 38 – Admin não consegue mudar senha do root. 29

Figura 39 – Usuário conseguindo baixar arquivo de 7mb. 30

Figura 40 – Usuário não conseguindo baixar arquivo de 50mb. 30

Figura 41 – Pastas com acesso restrito para os grupos. 31

Figura 42 – Agendador tentando acessar pasta de arquivador sem sucesso. 31

LISTA DE TABELAS

Tabela 1 – Permissões	15
---------------------------------	----

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.

O objetivo deste trabalho é realizar 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 rede, uma para comunicação interna e outra para comunicação externa.
- Deverá existir uma máquina gateway, 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. 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:

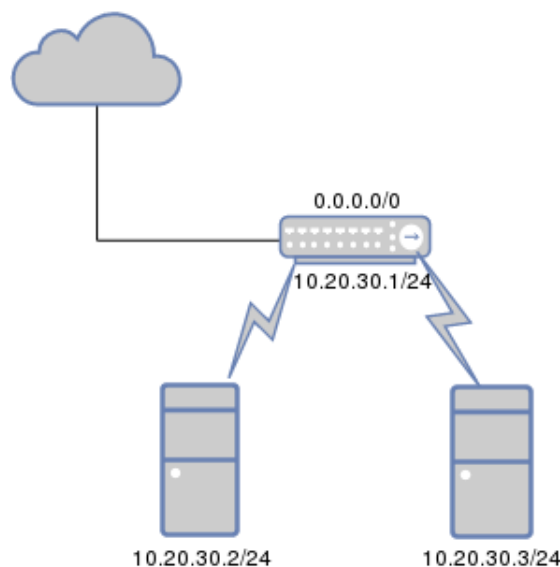


Figura 1 – Topologia do projeto

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.

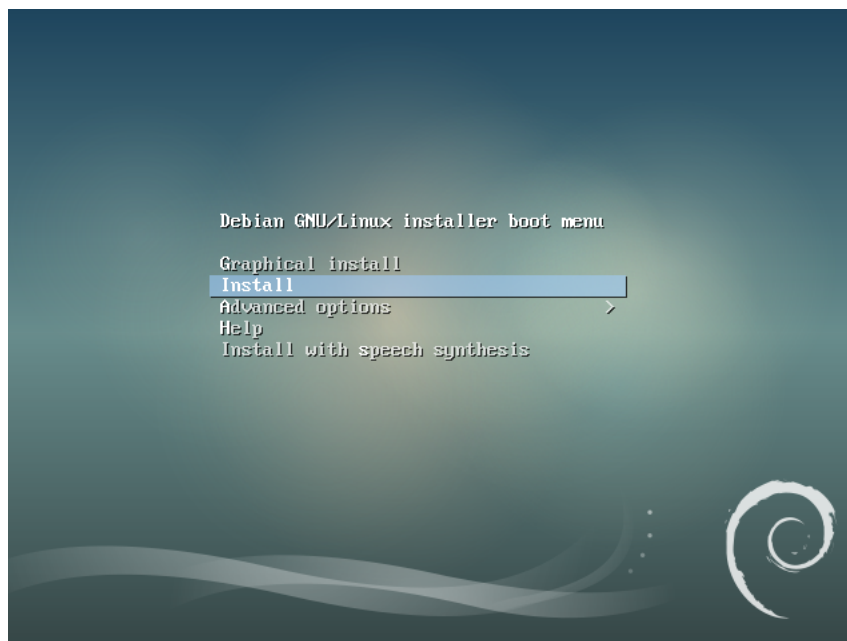


Figura 2 – Tela inicial de instalação

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.

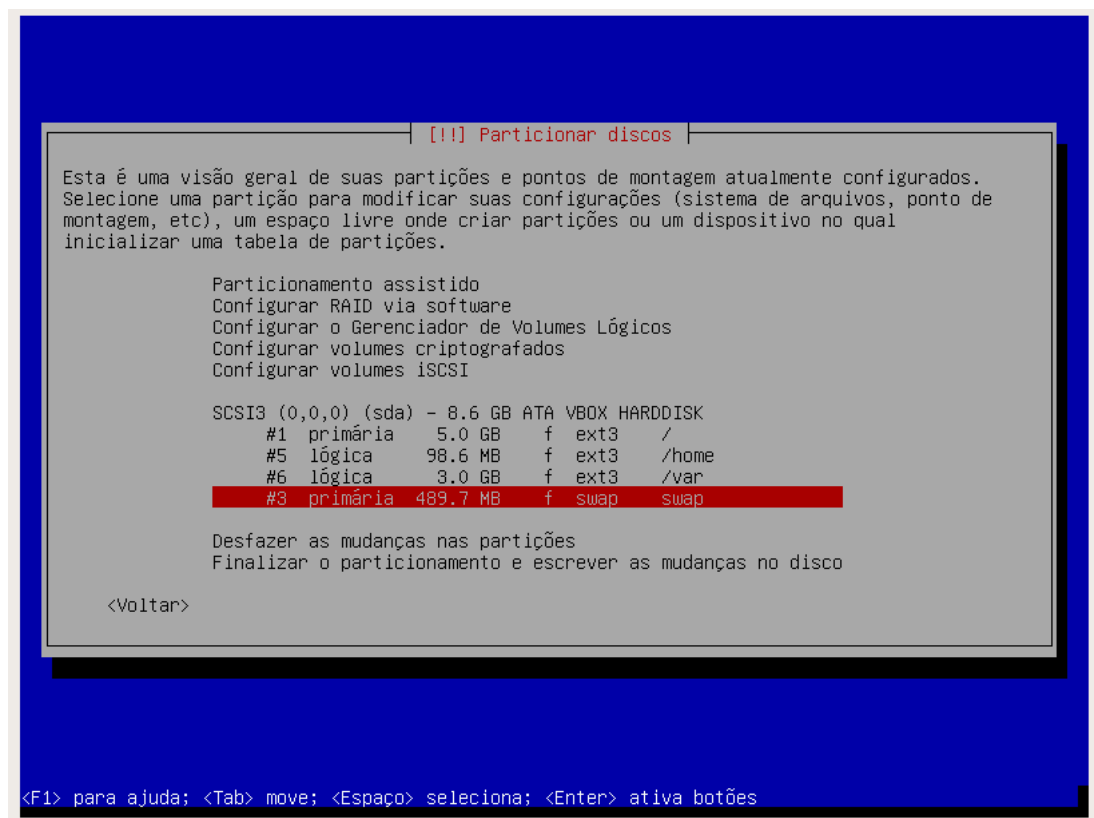


Figura 3 – Configuração das partições

O sistema instalado tem apenas os serviços básicos

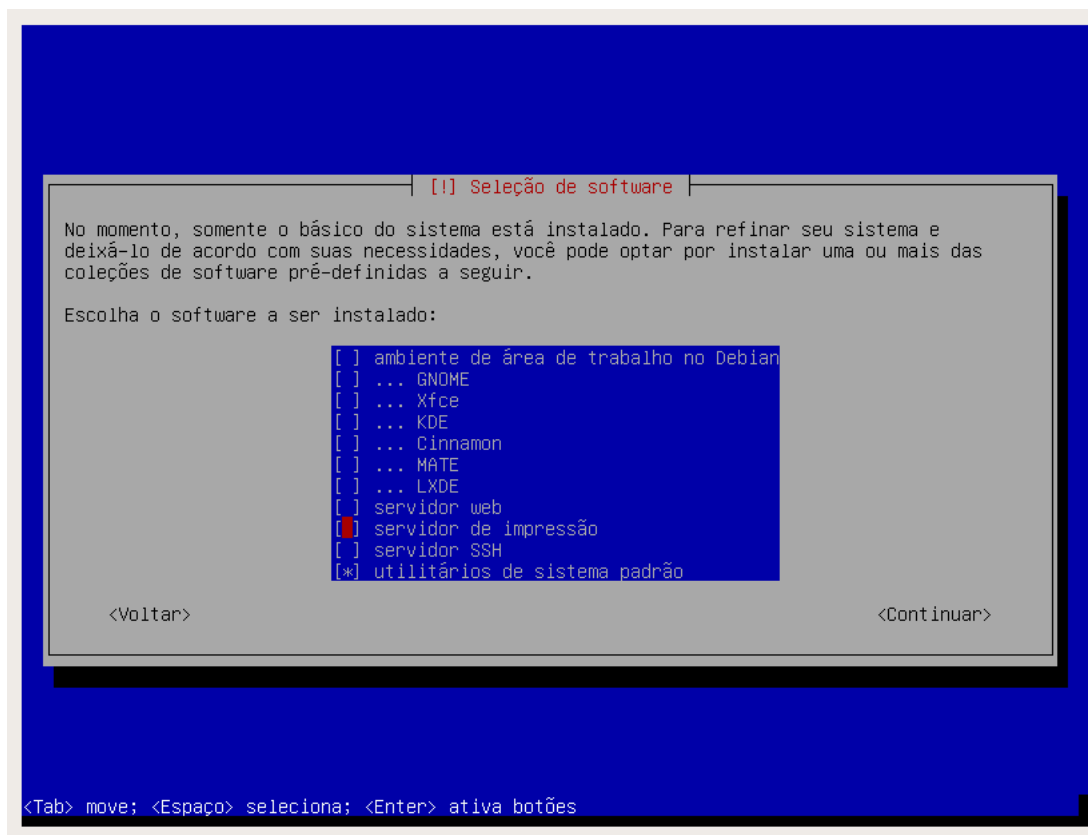


Figura 4 – Definições dos serviços/*softwares* padrão

A etapa abaixo, demonstra as partições criadas anteriormente.

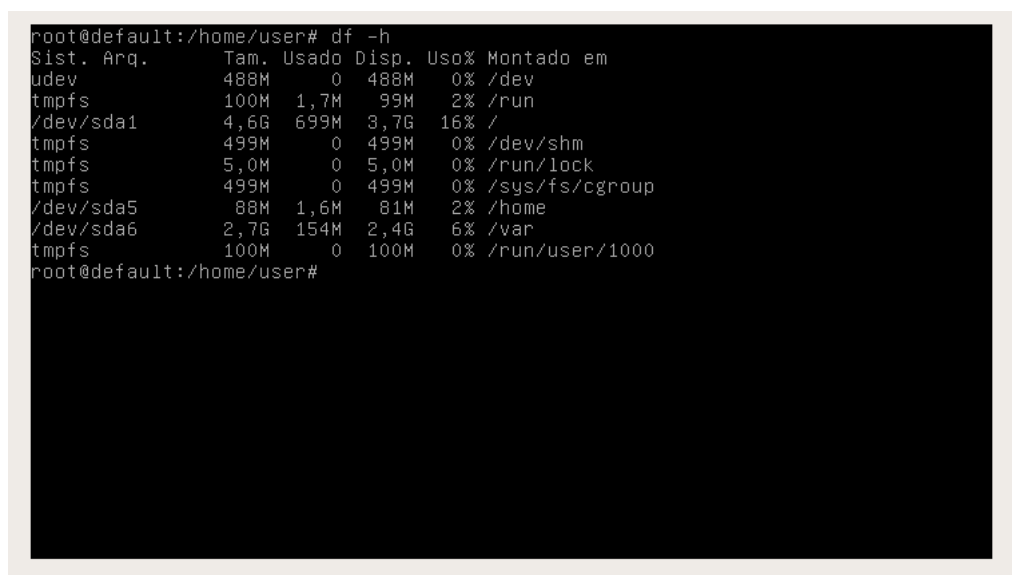


Figura 5 – Confirmação da separação das partições

Após realizar os passos demonstrados acima, a 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*.

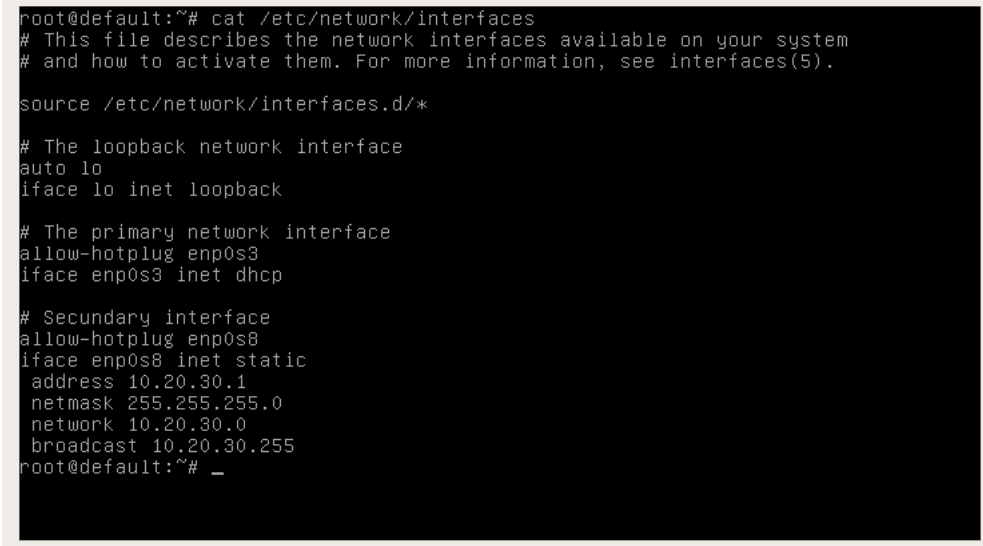
2.3.1 Configuração do gateway

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 interface, 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 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, sem possuir a senha do root;
- Administrador para o grupo Arquivadores;
- Administrador para o grupo Agendadores;

2.4.1 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 9 – Adicionando usuários com adduser

2.4.2 Configuração usuário admin

Para conceder privilégios de **root** ao usuário **admin** 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 use:

```
# apt-get install sudo
```

```
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.
É 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 10 – 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 ou não 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,!/bin/su,!/usr/bin/passwd
# 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 11 – Configuração do arquivo sudoers

Após esta configuração o usuário admin conseguirá executar comandos com elevação root, o ponto de exclamação seguido do último ALL, significa que o comando a seguir não poderá ser executado, no caso o **su** e o **passwd**. Se estes comandos estivessem habilitados, seria possível obter acesso root ou alterar a senha do root e conseguir acesso.

2.4.3 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) ...
Concluido.
root@default:/var# addgroup agendadores
Adicionando grupo 'agendadores' (GID 1008) ...
Concluido.
root@default:/var# ls
agendadores  arquivadores  backups  cache  lib  local  lock  log  lost+found  mail  opt  run  spool  tmp
root@default:/var#
```

Figura 12 – 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 13 – 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 14 – Permissões - diretórios agendadores e arquivadores

Tabela 1 – Permissões

Usuário	0	- - -
Grupo	7	rwX
Outros	0	- - -

2.4.4 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 15 – 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 16 – Definição de usuários administradores

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

2.5 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 seria criado utilizando o **EXT3**, isto 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.

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 o quote será aplicado em todas as partições, para que o usuário seja limitado ao máximo no uso do disco.

```
# /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 usrquota,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,usrquota 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 17 – Arquivo de configuração de quota

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

Após realizar as configurações acima, será necessário reinicializar o sistema. Antes de continuar as configurações do **quotas**, veja a explicação de alguns parâmetros que serão utilizados:

- **-a** - Checar todos os sistemas de arquivos em **/etc/fstab** que estão habilitados como 'automount';
- **-u** - Checa **quotas** de usuários (Esta é uma opção padrão, ou seja, mesmo quando não especificada, será utilizada);
- **-g** - Checa **quotas** de grupos;
- **-v** - Mostra mais detalhes na saída do comando.

Com o conhecimento sobre cada um dos parâmetros utilizados no **quotas**, será agora realizado a continuação da configuração

Para a continuação, será necessário parar os serviços de **quotas**, isto porque no momento da inicialização ele é iniciado.

```
# quotaoff -augv
```

Com o serviço parado faça a verificação das **quotas** de disco, em todos os sistemas de arquivos que estão em **/etc/fstab**.

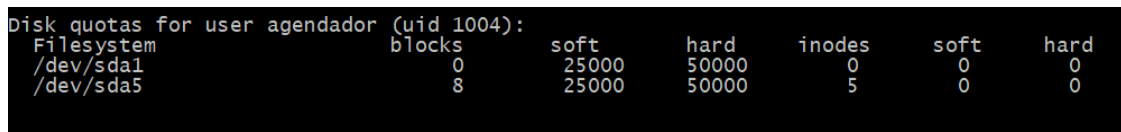
```
# quotacheck -augv
```

Neste momento o serviço já está configurado, porém há um passo a ser realizado, adicionar os usuários que terão limites de uso, neste caso, será os usuários comuns, criados na seção de gerenciamento de usuários.

A edição será inicialmente feita apenas para um usuário, neste caso o **agendador**.

```
# edquota agendador
```

Dentro deste arquivo insira os parâmetros como demonstrado abaixo.



Disk quotas for user agendador (uid 1004):						
Filesystem	blocks	soft	hard	inodes	soft	hard
/dev/sda1	0	25000	50000	0	0	0
/dev/sda5	8	25000	50000	5	0	0

Figura 18 – Configuração de **quota** para usuário

Na figura apresentada anteriormente, há alguns parâmetros que devem ser levados em consideração

- **Filesystem** - Partição que terá a quota do usuário editada. No exemplo **/dev/sda1** e **/dev/sda5**

- **blocks** - Número máximo de blocos (especificado em Kbytes) que o usuário possui atualmente;
- **soft** - Restrição mínima de espaço em disco usado. No exemplo 25000 Kbytes (25 MB);
- **hard** - Limite máximo aceitável de uso em disco para o usuário. O sistema de **quotas** nunca deixará este limite ser ultrapassado. No exemplo 50000 Kbytes (50 MB);
- **inodes** - Número máximo de arquivos (inodes) que o usuário possui atualmente na partição especificada;
- **soft** - Restrição mínima de número de arquivos que o usuário possui no disco;
- **hard** - Restrição máxima de número de arquivos que o usuário.

Após inserir a regra para este usuário, será realizada uma cópia dessas configurações para os demais usuário, veja:

```
# edquota -p agendador arquivador
```

As regras foram copiadas, agora será necessário fazer as verificações e ativar o serviço

```
# quotacheck -augv
```

O comando acima, além de fazer a verificação, cria os arquivos **aquota.user** e **aquota.group**, que serão utilizados para criar as regras para usuários e grupos respectivamente.

```
# quotaon -augv
```

Com isso as regras de **quotes** já estarão habilitadas e funcionando.

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 serão alterados 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 19 – 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 nos hosts.

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 20 – 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 de rede **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 21 – Bloqueio de acesso externo ao cluster

É importante lembrar que todas estas 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** para 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 MASQUERADE
```

Abaixo, é exibido, uma pequena descrição de cada um dos comandos:

- **sysctl -w** - Utilizado para escrever uma regra no sysctl;
- **sysctl -p** - Carrega o arquivo onde a regra será salva (Por padrão `/etc/sysctl.conf`);
- **iptables -X** - Exclui todas as chain non-builtin existentes, que estejam vazias;
- **iptables -F** - Deleta todas as regras definidas na chain;

- `iptables -t nat -X` - Exclui todas as chain non-builtin existentes, que estejam vazias, da tabela nat;
- `iptables -t nat -F` - Deleta todas as regras definidas na chain, desta tabela;
- `iptables -I INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT`
 - RELATED: Significa que o pacote está começando uma nova conexão, mas está associado a uma conexão existente, como uma transferência de dados, por exemplo;
 - ESTABLISHED: Significa que o pacote está associado a uma conexão com pacotes em ambas direções.
- `iptables -t nat -I POSTROUTING -o enp0s3 -j MASQUERADE` - Este é o comando que faz o roteamento funcionar, é aqui onde uma mascara é aplicada sobre o pacote recebido, e faz com que ele saia para a *internet* com o endereço do gateway.

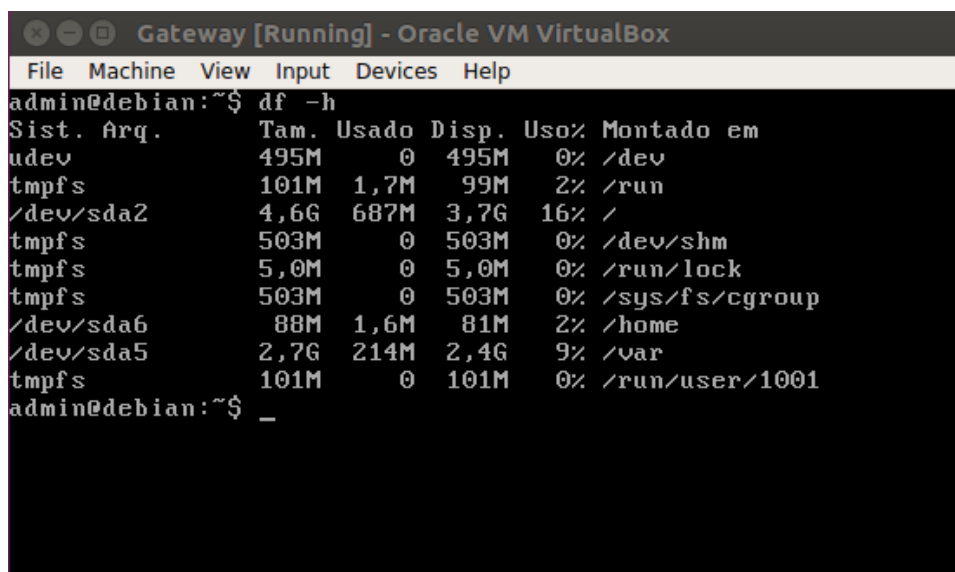
Ao final da execução das linhas demonstradas acima, os **hosts** terão acesso aos serviços de *internet* fornecidos pelo **gateway**.

2.7 TESTES

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

2.7.1 Partições

Todas as máquinas particionadas:



```

Gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ df -h
Sist. Arq.      Tam. Usado Disp. Uso% Montado em
udev          495M      0 495M   0% /dev
tmpfs         101M    1,7M   99M    2% /run
/dev/sda2      4,6G   687M   3,7G   16% /
tmpfs         503M      0 503M   0% /dev/shm
tmpfs         5,0M      0 5,0M   0% /run/lock
tmpfs         503M      0 503M   0% /sys/fs/cgroup
/dev/sda6       88M    1,6M    81M    2% /home
/dev/sda5      2,7G   214M   2,4G    9% /var
tmpfs         101M      0  101M   0% /run/user/1001
admin@debian:~$ _

```

Figura 22 – Gateway particionado.

```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ df -h
Sist. Arq.      Tam. Usado Disp. Uso% Montado em
udev           495M    0  495M   0% /dev
tmpfs          101M  1,7M   99M   2% /run
/dev/sda2      4,6G  687M  3,7G  16% /
tmpfs          503M    0  503M   0% /dev/shm
tmpfs          5,0M    0   5,0M   0% /run/lock
tmpfs          503M    0  503M   0% /sys/fs/cgroup
/dev/sda5      2,7G  210M  2,4G   9% /var
/dev/sda6       88M   1,6M   81M   2% /home
tmpfs          101M    0  101M   0% /run/user/1001
admin@debian:~$ _
```

Figura 23 – Host 1 particionado.

```
Host 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ df -h
Sist. Arq.      Tam. Usado Disp. Uso% Montado em
udev           494M    0  494M   0% /dev
tmpfs          101M  1,7M   99M   2% /run
/dev/sda2      4,6G  687M  3,7G  16% /
tmpfs          503M    0  503M   0% /dev/shm
tmpfs          5,0M    0   5,0M   0% /run/lock
tmpfs          503M    0  503M   0% /sys/fs/cgroup
/dev/sda6       88M   1,6M   81M   2% /home
/dev/sda5      2,7G  210M  2,4G   9% /var
tmpfs          101M    0  101M   0% /run/user/1001
admin@debian:~$ _
```

Figura 24 – Host 2 particionado.

2.7.2 Configuração de redes das máquinas

```
Gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
root@debian:/home/admin# 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@debian:/home/admin#
```

Figura 25 – Rede externa e interna do Gateway.

```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ 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 static
    address 10.20.30.2
    netmask 255.255.255.0
    network 10.20.30.0
    gateway 10.20.30.1
admin@debian:~$
```

Figura 26 – Rede interna do Host 1.

```
Host 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ 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 static
    address 10.20.30.3
    netmask 255.255.255.0
    network 10.20.30.0
    gateway 10.20.30.1
admin@debian:~$ _
```

Figura 27 – Rede interna do Host 2.

2.7.3 Conexões SSH

```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
agendador@debian:~$ ssh agendador@10.20.30.1
The authenticity of host '10.20.30.1 (10.20.30.1)' can't be established.
ECDSA key fingerprint is SHA256:5zibuQPOY3d3zwN/1h2htrMrS3jlk1wmxC1Z+M6iL10.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.20.30.1' (ECDSA) to the list of known hosts.
agendador@10.20.30.1's password:
Linux debian 4.9.0-6-686 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 16 15:59:35 2018 from 10.20.30.2
agendador@debian:~$
```

Figura 28 – Host 1 dando SSH no Gateway com sucesso.


```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
arquivador@debian:~$ ssh arquivador@10.20.30.3 -p 5678
arquivador@10.20.30.3's password:
Linux debian 4.9.0-6-686 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Apr 17 11:16:14 2018 from 10.20.30.2
arquivador@debian:~$ _
```

Figura 29 – Host 1 dando SSH no Host 2 diretamente.

```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ ssh admin@10.20.30.1
admin@10.20.30.1's password:
Linux debian 4.9.0-6-686 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 16 17:57:39 2018 from 10.20.30.2
admin@debian:~$ ssh admin@10.20.30.3
admin@10.20.30.3's password:
Linux debian 4.9.0-6-686 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 16 17:58:06 2018 from 10.20.30.1
admin@debian:~$ _
```


Figura 30 – Host 1 dando SSH no Host 2 pelo Gateway

```
admin@debian: ~  
akiraaaaaa@AKIRAAAAAA:~$ ssh admin@192.168.15.19  
admin@192.168.15.19's password:  
Linux debian 4.9.0-6-686 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) i686  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Mon Apr 16 18:14:33 2018 from 192.168.15.15  
admin@debian:~$
```

Figura 31 – SSH de outra máquina não pertencente ao cluster, no Gateway.

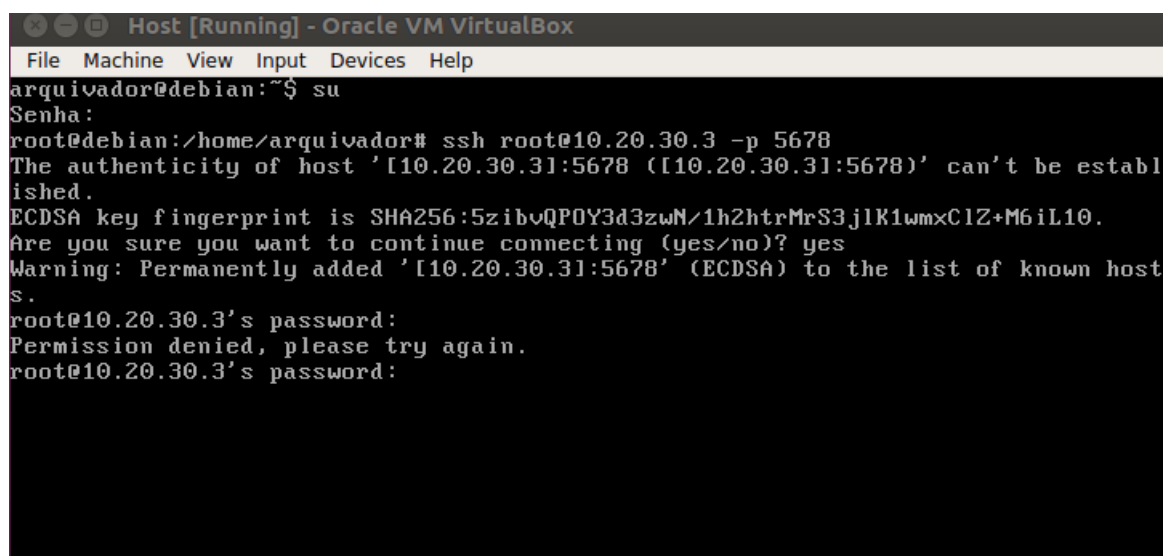
```
admin@debian: ~  
akiraaaaaa@AKIRAAAAAA:~$ ssh admin@192.168.15.19  
admin@192.168.15.19's password:  
Linux debian 4.9.0-6-686 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) i686  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Mon Apr 16 18:15:05 2018 from 192.168.15.15  
admin@debian:~$ ssh admin@10.20.30.2  
admin@10.20.30.2's password:  
Linux debian 4.9.0-6-686 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) i686  
  
The programs included with the Debian GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Mon Apr 16 18:16:58 2018 from 10.20.30.1  
admin@debian:~$
```

Figura 32 – SSH de outra máquina não pertencente ao cluster no Host 1, através do Gateway



```
Host 2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ ssh akiraaaaaaa@192.168.15.15
ssh: connect to host 192.168.15.15 port 22: Connection timed out
admin@debian:~$
```

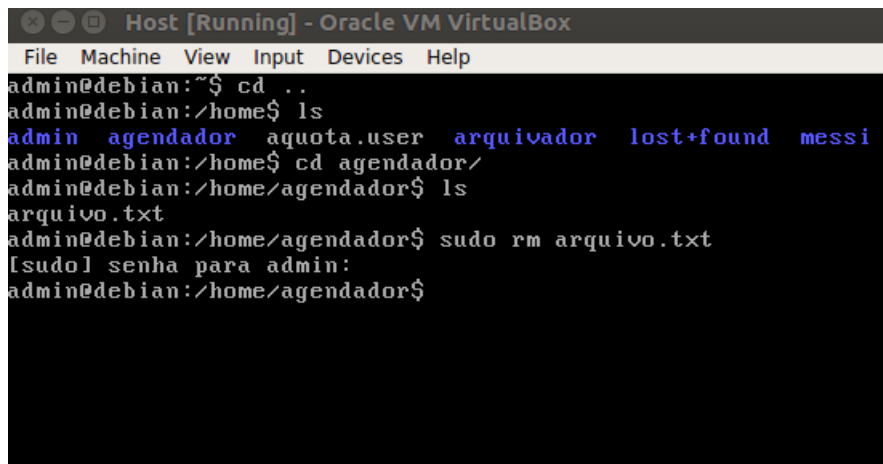
Figura 33 – Host 2 tentando dar SSH em máquina fora do cluster sem sucesso.



```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
arquivador@debian:~$ su
Senha:
root@debian:/home/arquivador# ssh root@10.20.30.3 -p 5678
The authenticity of host '[10.20.30.3]:5678 ([10.20.30.3]:5678)' can't be established.
ECDSA key fingerprint is SHA256:5zibuQPOY3d3zwN/1h2htrMrS3jlk1wmxC1Z+M6iL10.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[10.20.30.3]:5678' (ECDSA) to the list of known hosts.
root@10.20.30.3's password:
Permission denied, please try again.
root@10.20.30.3's password:
```

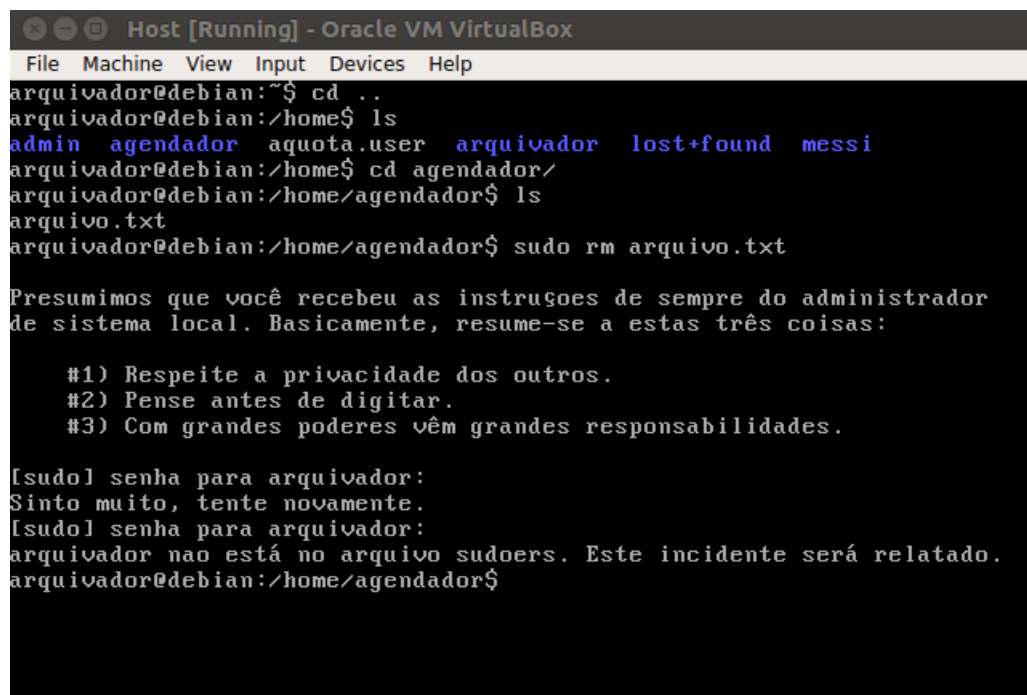
Figura 34 – Root tentando dar SSH sem sucesso.

2.7.4 Poderes de root para o Administrador



```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ cd ..
admin@debian:/home$ ls
admin  agendador  aquota.user  arquivador  lost+found  messi
admin@debian:/home$ cd agendador/
admin@debian:/home/agendador$ ls
arquivo.txt
admin@debian:/home/agendador$ sudo rm arquivo.txt
[sudo] senha para admin:
admin@debian:/home/agendador$
```

Figura 35 – Admin conseguindo apagar arquivo de outro usuário.



```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
arquivador@debian:~$ cd ..
arquivador@debian:/home$ ls
admin  agendador  aquota.user  arquivador  lost+found  messi
arquivador@debian:/home$ cd agendador/
arquivador@debian:/home/agendador$ ls
arquivo.txt
arquivador@debian:/home/agendador$ sudo rm arquivo.txt

Presumimos que você recebeu as instruções de sempre do administrador
de sistema local. Basicamente, resume-se a estas três coisas:

#1) Respeite a privacidade dos outros.
#2) Pense antes de digitar.
#3) Com grandes poderes vêm grandes responsabilidades.

[sudo] senha para arquivador:
Sinto muito, tente novamente.
[sudo] senha para arquivador:
arquivador nao está no arquivo sudoers. Este incidente será relatado.
arquivador@debian:/home/agendador$
```

Figura 36 – Outro usuário tentando ter poder de root sem sucesso.

```
Gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ sudo su
[sudo] senha para admin:
Sinto muito, usuário admin nao tem permissao para executar "/bin/su" como root e
m debian.
admin@debian:~$ _
```

Figura 37 – Admin não consegue se tornar root.

```
Gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:~$ sudo passwd root
[sudo] senha para admin:
Sinto muito, usuário admin nao tem permissao para executar "/usr/bin/passwd root
" como root em debian.
admin@debian:~$
```

Figura 38 – Admin não consegue mudar senha do root.

2.7.5 Quotas

```
Gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
agendador@debian:~$ wget https://landsat-pds.s3.amazonaws.com/L8/139/045/LC81390452014295LGN00/LC81390452014295LGN00_B3.TIF.ovr
--2018-04-16 21:49:40-- https://landsat-pds.s3.amazonaws.com/L8/139/045/LC81390452014295LGN00/LC81390452014295LGN00_B3.TIF.ovr
Resolvendo landsat-pds.s3.amazonaws.com (landsat-pds.s3.amazonaws.com)... 52.218.209.154
Conectando-se a landsat-pds.s3.amazonaws.com (landsat-pds.s3.amazonaws.com) [52.218.209.154]:443... conectado.
A requisicao HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 7327730 (7,0M) [application/octet-stream]
Salvando em: ■LC81390452014295LGN00_B3.TIF.ovr■

LC81390452014295LGN 100%[=====>] 6,99M 1,72MB/s in 4,1s

2018-04-16 21:49:45 (1,72 MB/s) - ■LC81390452014295LGN00_B3.TIF.ovr■ salvo [7327730/7327730]

agendador@debian:~$ _
```

Figura 39 – Usuário conseguindo baixar arquivo de 7mb.

```
Gateway [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
agendador@debian:~$ wget https://landsat-pds.s3.amazonaws.com/L8/139/045/LC81390452014295LGN00/LC81390452014295LGN00_B1.TIF
--2018-04-16 21:51:35-- https://landsat-pds.s3.amazonaws.com/L8/139/045/LC81390452014295LGN00/LC81390452014295LGN00_B1.TIF
Resolvendo landsat-pds.s3.amazonaws.com (landsat-pds.s3.amazonaws.com)... 52.218.208.242
Conectando-se a landsat-pds.s3.amazonaws.com (landsat-pds.s3.amazonaws.com) [52.218.208.242]:443... conectado.
A requisicao HTTP foi enviada, aguardando resposta... 200 OK
Tamanho: 51099231 (49M) [image/tiff]
Salvando em: ■LC81390452014295LGN00_B1.TIF■

1.TIF 35%[=====>] 1 17,31M 2,78MB/s eta 14s s
da6: warning, user block quota exceeded.
00_B1.TIF 83%[=====>] 1 40,71M 4,01MB/s eta 4s s
da6: write failed, user block limit reached.
sda6: write failed, user block limit reached.
LC81390452014295LGN 85%[=====>] 1 41,63M 4,11MB/s in 16s

Nao foi possível escrever em ■LC81390452014295LGN00_B1.TIF■ (Disk quota exceeded).
agendador@debian:~$ _
```

Figura 40 – Usuário não conseguindo baixar arquivo de 50mb.

2.7.6 Grupos

```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
admin@debian:/home$ cd /var
admin@debian:/var$ ls
agendadores  arquivos  cache  local  log  mail  run  tmp
aquota.user  backups  lib  lock  lost+found  opt  spool
admin@debian:/var$ ls -l
total 68
d---rwx--- 2 root agendadores 4096 abr 14 18:23 agendadores
-rw----- 1 root root 7168 abr 15 22:09 aquota.user
d---rwx--- 2 root arquivos 4096 abr 14 18:23 arquivos
drwxr-xr-x 2 root root 4096 abr 16 15:30 backups
drwxr-xr-x 7 root root 4096 abr 14 15:38 cache
drwxr-xr-x 26 root root 4096 abr 14 18:46 lib
drwxrwsr-x 2 root staff 4096 fev 23 20:23 local
lrwxrwxrwx 1 root root 9 abr 14 15:22 lock -> run/lock
drwxr-xr-x 4 root root 4096 abr 16 15:30 log
drwx----- 2 root root 16384 abr 14 15:21 lost+found
drwxrwsr-x 2 root mail 4096 abr 14 15:22 mail
drwxr-xr-x 2 root root 4096 abr 14 15:22 opt
lrwxrwxrwx 1 root root 4 abr 14 15:22 run -> /run
drwxr-xr-x 5 root root 4096 abr 14 15:38 spool
drwxrwxrwt 4 root root 4096 abr 16 18:57 tmp
admin@debian:/var$
```

Figura 41 – Pastas com acesso restrito para os grupos.

```
Host [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
agendador@debian:~$ cd /var
agendador@debian:/var$ ls
agendadores  arquivos  cache  local  log  mail  run  tmp
aquota.user  backups  lib  lock  lost+found  opt  spool
agendador@debian:/var$ cd agendadores/
agendador@debian:/var/agendadores$ > arquivo.mp3
agendador@debian:/var/agendadores$ cd ..
agendador@debian:/var$ cd arquivos/
-bash: cd: arquivos/: Permissao negada
agendador@debian:/var$
```

Figura 42 – Agendador tentando acessar pasta de arquivador sem sucesso.

3 CONCLUSÃO

Com o desenvolvimento do projeto, conclui-se que, o sistema operacional Debian, oferece formas simples e robustas para o gerenciamento e controle de máquinas, grupos e usuários. O que permite a administradores de sistemas criar formas de garantir a integridade e disponibilidade dos servidores e seus serviços.