hInstituto Federal do Sudeste de Minas Gerais – Campus Barbacena
Curso Superior de Tecnologia em Sistemas para Internet

1ª Avaliação de Gerência e Configuração de Serviços de Internet – ERE 172/86

Nome:Lucas Cristovam Henriques Fonseca **Data:** _____

AVISOS:

1 – avaliação individual com consulta permitida a livros impressos e materiais na Internet;
2 – não serão consideradas as respostas que por ventura sejam cópias (plágios), sejam de livros, artigos de Internet, colegas e outros meios;
3 – havendo cópia (plágio), mesmo que seja de uma questão apenas, toda a prova será anulada sem direito à segunda chance;
4 – as respostas escritas deverão ser preenchidas neste mesmo arquivo dentro das caixas de texto correspondentes, com fonte arial 12, espaçamento simples e mesmo tamanho de margem deste arquivo original;
5 – o arquivo final, em formato ODT, deverá ser postado no Sigaa em local a ser definido pelo professor até às 23:59 hs do dia 07/12/2021. Se o Sigaa estiver com problemas no momento de envio, o aluno poderá enviar o arquivo como anexo para o e-mail herlon.camargo@ifsudestemg.edu.br respeitando o prazo definido acima;
6 – o nome do arquivo texto final deverá ser: SERVIÇOS-121-ERE-SEUNOME.odt, onde "SEUNOME" deverá ser alterado para o primeiro nome do aluno em maiúsculas;
7 – a máquina virtual servidora, e somente ela, deverá ser enviada em formato .OVA (Appliance), com todas as configurações de rede, vídeo e armazenamento realizadas no VirtualBox, de forma que o professor possa executá-la sem a necessidade de realizar nenhuma configuração no VirtualBox (se houver a necessidade do professor realizar alguma configuração no VirtualBox para executar a máquina virtual haverá uma penalidade de 50% na nota final desta avaliação);
8 – o nome do arquivo .OVA deverá ser SERVIDOR-121-ERE-SEUNOME.ova, onde "SEUNOME" deverá ser alterado para o primeiro nome do aluno em maiúsculas;
9 – após o fechamento da Appliance, calcular o hash MD5 do arquivo .OVA e informá-lo no campo apropriado abaixo;
10 – fazer upload do arquivo .OVA para o Google Drive, compartilhar de forma privada entre o aluno e o professor, e disponibilizar o link para download em campo apropriado abaixo;
11 – é de inteira responsabilidade do aluno deixar o arquivo .OVA íntegro no Google Drive (integridade será conferida através do hash MD5 após o professor fazer o download – hashes diferentes indicam adulteração na máquina virtual e, portanto, será atribuída nota zero nesta avaliação, sem direito à segunda chance);
12 – o envio de link errado que não corresponda ao arquivo .OVA desta avaliação implicará em nota zero sem direito à segunda chance;
12 – havendo indícios de compartilhamento do arquivo .OVA com alguma outra pessoa, além do professor e do próprio aluno, a prova será anulada sem direito à segunda chance;
13 – qualquer outra orientação que se julgar pertinente e necessária será informada através do grupo da disciplina no Telegram;
13 – Valor desta avaliação: 200 / 2 = 100 pts.

Hash MD5: 7f8de4e942a92bc0db63da6f6aabbd59

Link do arquivo .OVA: https://drive.google.com/file/d/1GlETU8DGnI3E6v_vAkEW3oGW07jeioI5/view?usp=sharing

Instruções para a realização das questões:

1 – instalar uma VM Servidora baseada no sistema operacional Rocky Linux 8.5 com armazenamento de 8GB, memória RAM de 768 MB a 1024 MB, duas interfaces de rede: adaptador 1 em modo bridge e adaptador 2 em modo rede interna de nome “switch-1” e senha do root igual a “prova”;

2 – instalar uma VM Cliente baseada no Windows 10 com interface de rede em modo rede interna de nome “switch-1” (pode-se usar a VM Windows 10 disponibilizada pelo professor durante as aulas). Configurar o endereço MAC dessa interface de rede como sendo 08:00:27:63:F6:F3;

3 – valores de IP para a VM Servidora: externa → ip fixo a sua escolha configurado manualmente no arquivo de configuração da placa de rede; interna → 10.3.1.81/28;

4 – valor de IP para a VM Cliente: 10.3.1.82/28 recebido por DHCP;

5 – qualquer configuração que tenha sido feita na VM Servidora deverá ficar ativa após a sua inicialização. O professor não irá executar comando algum para ativar qualquer configuração ou serviço;

6 – as questões deverão atender a “condições necessárias para correção” - CNC descritas em cada questão para que possam ser corrigidas;

1 – (20 pts) – Instalar e configurar o servidor ISC DHCP, na VM Servidora, para atender a sua rede interna de acordo com as seguintes características:

- **(04 pts) -** configurar o servidor DHCP para fornecer dados apenas para a rede interna;
- **(02 pts) -** configurar como sendo 3 minutos o intervalo de tempo em que o servidor usa para verificar se há hosts inativos e liberar o IP atribuído;
- **(02 pts) -** configurar com sendo 15 minutos o tempo máximo em que um cliente poderá ficar com as configurações fornecidas pelo servidor;
- **(04 pts) -** permitir uma faixa automática de IP's para a sua rede interna virtual utilizando apenas os dez últimos IPs válidos;
- **(04 pts) -** fornecer automaticamente as configurações de rede: nome do domínio (tsi.com.br), IP, máscara, gateway e DNS primário (8.8.8.8) e secundário (8.8.4.4);
- **(04 pts) -** definir que a VM Cliente terá endereço IP fixo 10.3.1.82/28.

CNC: o servidor ISC DHCP deverá ser capaz de fornecer um IP ao ser solicitado.

2 – (30 pts) – Configurar um servidor OpenSSH na VM Servidora atendendo às seguintes exigências:

- criar os usuários “seunome” e “seuultimosobrenome”, ambos com senha “abacaxi”, onde “seunome” deverá ser alterado para o primeiro nome do aluno em minúsculas e “seuultimosobrenome” deverá ser alterado para o último sobrenome do aluno em minúsculas;

- **(07 pts) –** criar uma chave para realizar acesso remoto **com chave e sem senha** com o usuário “seunome”;
- **(08 pts) –** criar uma chave para realizar acesso remoto **com chave e com senha** (senha da chave “banana”) com o usuário “seuultimosobrenome”;
- **(15 pts) -** no quadro abaixo, fazer um mini-relatório (tutorial) **citando e explicando** todos os passos envolvidos para a resolução desta questão além de explicar como é feita a importação de chaves para uma outra máquina e sua utilização.

Obs: deixar os arquivos das chaves dentro do diretório /root com nomes de “chave-seunome” e “chave-seuultimosobrenome”, em formato que elas possam ser copiadas e importadas para outra máquina que use o serviço SSH.

CNC: o servidor SSH deverá ser acessado por pelo menos uma das formas solicitadas nesta questão.

Usuario1: lucas
Usuário2: fonseca

Adicionando os usuários:

```
[root@servidor ~]# adduser lucas_
[root@servidor ~]# adduser fonseca_
```

```
[root@servidor ~]# passwd lucas
Changing password for user lucas.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@servidor ~]# passwd fonseca
Changing password for user fonseca.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

Para a criação das chaves para o usuário ***lucas***, foi realizado o acesso ssh atraves de uma vm Linux mint, através, foi executado o comando *ssh-keygen -t rsa* que realiza a geração do par de chaves de acesso:

```
lucas@lucasc-VirtualBox:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/lucas/.ssh/id_rsa): /home/lucas/.ssh/
chave-lucas
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/lucas/.ssh/chave-lucas
Your public key has been saved in /home/lucas/.ssh/chave-lucas.pub
The key fingerprint is:
SHA256:ZyQzCtXlbpYqhQ7iwGjzfOzilE82aOuNs9NEqmsXRBM lucas@lucasc-VirtualBox
The key's randomart image is:
+---[RSA 3072]----+
|   E. .. ..      |
|   o .  ..       |
|  . o   + o      |
|o  . o o * .     |
|o+o + o S B      |
|.o++++ . *       |
|  oB+*o .        |
| oo=X...         |
|..=*=+           |
+----[SHA256]-----+
```

Após a geração das chaves, foi usado o *ssh-copy* para realizar a cópia da chave pública para o servidor:

```
lucas@lucasc-VirtualBox:~$ ssh-copy-id -i ~/.ssh/chave-lucas lucas@10.3.1.81
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/lucas/.ssh/
chave-lucas.pub"
The authenticity of host '10.3.1.81 (10.3.1.81)' can't be established.
ECDSA key fingerprint is SHA256:dZLaMJN2O8xyiOlU/PMkKQaC57uwbrAPD2LU+U8N/sk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
lucas@10.3.1.81's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'lucas@10.3.1.81'"
and check to make sure that only the key(s) you wanted were added.
```

Feito isso, o acesso pôde ser realizado sem senha:

```
lucas@lucasc-VirtualBox:~$ ssh -i ~/.ssh/chave-lucas lucas@10.3.1.81
Last login: Mon Dec  6 14:31:17 2021 from 10.3.1.89
[lucas@servidor ~]$
```

Para a criação da chave do usuário *fonseca* o processo foi o mesmo, exceto que agora a *passphrase* foi informada.

```
lucas@lucasc-VirtualBox:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/lucas/.ssh/id_rsa): /home/lucas/.ssh/
chave-fonseca
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/lucas/.ssh/chave-fonseca
Your public key has been saved in /home/lucas/.ssh/chave-fonseca.pub
The key fingerprint is:
SHA256:tYrJqlQ7QkeVvIt4ZCC6u9Aq7HtHeuk1VBg+ZB3t9C0 lucas@lucasc-VirtualBox
The key's randomart image is:
+---[RSA 3072]----+
|      ..=..o     |
|. .  .* o. o     |
|.. ..  = .+ . .  |
|.  .o . o. o E . |
| ..+o. oS .   .  |
|.o.oo+oo .       |
|o.+.= =o.        |
|++ + *. .        |
|=++.=.           |
+----[SHA256]-----+
```

Feito isso, foi realizada a cópia da chave para o servidor:

```
lucas@lucasc-VirtualBox:~$ ssh-copy-id -i ~/.ssh/chave-fonseca fonseca@10.3.1.81
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/lucas/.ssh/
chave-fonseca.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
fonseca@10.3.1.81's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'fonseca@10.3.1.81'"
and check to make sure that only the key(s) you wanted were added.
```

Feita a cópia, o acesso pôde ser realizado através da chave:

```
lucas@lucasc-VirtualBox:~$ ssh -i ~/.ssh/chave-fonseca fonseca@10.3.1.81
Enter passphrase for key '/home/lucas/.ssh/chave-fonseca':
Last login: Mon Dec  6 14:19:04 2021 from 10.3.1.89
[fonseca@servidor ~]$
```

Foi realizada a cópia de chaves para o diretório */root* do servidor através do comando *scp*:

```
lucas@lucasc-VirtualBox:~$ scp /home/lucas/.ssh/chave-* root@10.3.1.81:/root
root@10.3.1.81's password:
chave-fonseca                                 100% 2655     3.5MB/s   00:00
chave-fonseca.pub                             100%  577     1.3MB/s   00:00
chave-lucas                                   100% 2610     5.7MB/s   00:00
chave-lucas.pub                               100%  577     1.4MB/s   00:00
```

```
[root@servidor ~]# ls /root/
anaconda-ks.cfg  chave-fonseca  chave-fonseca.pub  chave-lucas  chave-lucas.pub
```

A fim de confirmar que as chaves estão funcionando, foi realizada a cópia para uma terceira VM:

```
lucas@slave:~$ scp root@10.3.1.81:/root/chave* /home/lucas/.ssh
root@10.3.1.81's password:
chave-fonseca                                 100% 2655     4.1MB/s   00:00
chave-fonseca.pub                             100%  577     1.0MB/s   00:00
chave-lucas                                   100% 2610     6.4MB/s   00:00
chave-lucas.pub                               100%  577     1.9MB/s   00:00
```

E realizado o acesso com ambas as chaves:

```
lucas@slave:~$ ssh -i /home/lucas/.ssh/chave-lucas lucas@10.3.1.81
Last login: Mon Dec  6 14:31:37 2021 from 10.3.1.89
[lucas@servidor ~]$
```

```
lucas@slave:~$ ssh -i /home/lucas/.ssh/chave-fonseca fonseca@10.3.1.81
Enter passphrase for key '/home/lucas/.ssh/chave-fonseca':
Last login: Mon Dec  6 14:36:02 2021 from 10.3.1.89
[fonseca@servidor ~]$
```

3 – 62 pts (70 pts) – Instalar e configurar o servidor proxy e web cache Squid, atendendo às seguintes características:

- **(05 pts) –** usar autenticação obrigatória de usuários (usar os usuários “tom”, “lau”, “zeca” e “boi”, e todos com senha iguais ao próprio login);
- **(08 pts) –** fazer proxy e realizar web cache para todas as máquinas da sua rede interna com exceção do usuário “tom” que poderá utilizar o proxy de dentro e de fora da rede interna sem nenhuma restrição;
- **(01 pts) –** tamanho máximo do cache em memória igual a 16 MB;
- **(01 pts) –** tamanho máximo do cache em disco igual a 128 MB;
- **(01 pts) –** tamanho máximo de um objeto em cache na memória igual a 8 KB;
- **(01 pts) –** tamanho máximo de um objeto em cache no disco igual a 512 KB;
- **(07 pts) –** criar um contexto (história 1) para implantar um controle de acesso composto de 03 ACLs de tipos diferentes (url, tempo e origem) invocadas na mesma linha http_access;
- **(07 pts) –** criar um contexto (história 2) para implantar um controle de acesso composto de 04 ACLs invocadas em duas linhas http_access;
- **00 pts (04 pts) –** não permitir que as máquinas da rede interna acessem a Internet diretamente pelas portas 20, 21, 80 e 443 implementando um firewall controlado pelo systemd;
- **31 pts (35 pts) –** no quadro abaixo, fazer um mini-relatório (tutorial) **citando** e **explicando** todos os passos envolvidos para a resolução desta questão.

Obs: as ACLs e linhas http_access deverão estar funcionais simultaneamente para serem pontuadas.

CNC: o servidor proxy deverá responder a solicitações vindas de um browser.

Para a realização dessa questão, foi necessária a instalação da ferramenta squid. Com o squid instalado na máquina, foi realizada uma cópia do arquivo de configurações de exemplo do squid e só então, foram inicializadas as configurações.

Para instalar o squid:

```
[root@servidor ~]# yum install squid
```

Para realizar a cópia do arquivo de configuração de exemplo e sobrescrita do arquivo de configurações:

```
[root@servidor ~]# cp /usr/share/doc/squid/squid.conf.documented /etc/squid/squid.conf
```

Autenticação obrigatória.

Para o uso de autenticação, foi necessária a instalação do pacote httpd-tools.

```
[root@servidor ~]# yum install httpd-tools_
```

Uma vez instalado o pacote httpd-tools, foi criado o arquivo /etc/squid/senhas.txt para o gerenciamento de usuários do squid:

```
[root@servidor ~]# touch /etc/squid/senhas.txt
```

Os usuários foram criados através do comando htpasswd.

```
[root@servidor ~]# htpasswd /etc/squid/senhas.txt tom
New password:
Re-type new password:
Adding password for user tom
[root@servidor ~]# htpasswd /etc/squid/senhas.txt lau
New password:
Re-type new password:
Adding password for user lau
[root@servidor ~]# htpasswd /etc/squid/senhas.txt zeca
New password:
Re-type new password:
Adding password for user zeca
[root@servidor ~]# htpasswd /etc/squid/senhas.txt boi
New password:
Re-type new password:
Adding password for user boi
```

Uma vez registrados os usuários, foi realizada a checagem de suas senhas através da ferramenta basic_ncsa_auth (essa ferramenta é utilizada pelo squid na autenticação). Para isso foi usado o seguinte comando:

```
[root@servidor ~]# /usr/lib64/squid/basic_ncsa_auth /etc/squid/senhas.txt
tom tom
OK
lau lau
OK
zeca zeca
OK
boi boi
OK
```

No arquivo de configuração do squid, foi configurado o programa usado para autenticação (no caso o basic_ncsa_auth) e a mensagem de autenticação:

```
...
auth_param basic program /usr/lib64/squid/basic_ncsa_auth /etc/squid/senhas.txt
##auth_param basic children 5 startup=5 idle=1
auth_param basic realm Acesso restrito
```

Então, foram criadas as seguintes ACLs:

autenticados - indica a necessidade de autenticação no proxy.

```
acl autenticados proxy_auth REQUIRED
```

redelocal - para gerenciamento da rede interna:

```
acl redelocal src 10.3.1.80/28
```

user_tom - já que o usuário "tom" tem acesso sem restrições.

```
acl user_tom proxy_auth tom
```

Essas regras foram aplicadas na seguinte ordem:

```
http_access allow user_tom
```

Permitindo acesso total a rede externa e interna ao usuário tom

```
http_access allow redelocal autenticados
```

Permitindo acesso à rede interna somente usuários autenticados

Cache

Para definir o tamanho máximo do cache em memória, aproximadamente na linha 3435, foi removido o comentário e alterado o valor para o valor solicitado:

```
cache_mem 16 MB
```

O tamanho máximo de um objeto em memória foi definido através da alteração da linha ***maximum_object_size_in_memory*** (aproximadamente 3463)

```
maximum_object_size_in_memory 8 KB
```

Para o tamanho máximo do cache em disco, foi alterada a linha ***cache_dir*** (aproximadamente linha 3725)

```
cache_dir ufs /var/spool/squid 128 16 256
```

O tamanho máximo de um objeto em disco foi definido através da alteração da linha ***maximum_object_size*** (aproximadamente 3568)

```
maximum_object_size 512 KB
```

Contexto 1:

Neste contexto, o acesso aos sites de notícias g1, r7 e cnn durante o horário de trabalho somente pode ser realizado através da máquina da recepção. Para isso foram criadas as ACLs:

```
acl maquina_recepcao src 10.3.1.82
acl horas_uteis time 07:00-20:29
acl sites_noticias url_regex "/etc/squid/sites_noticias.txt"
```

O conteúdo do arquivo */etc/squid/sites_noticias.txt:*

```
g1.globo.com
r7.com
cnn.com
```

Então foi aplicada a seguinte regra:

```
http_access deny sites_noticias horas_uteis !maquina_recepcao
```

Contexto 2:

Neste contexto, existem duas restrições:

1-O acesso ao youtube, facebook e Instagram só pode ser realizado durante o intervalo compreendido entre 20:30 e 22:00;
2- O usuário Zeca, durante o horário de trabalho, só tem acesso através da máquina da recepção.

Para gerenciar isso foram criadas as seguintes ACLs:

```
acl user_zeca proxy_auth zeca
acl intervalo_noite time 20:30-22:00
acl redes_sociais url_regex "/etc/squid/redes_sociais.txt"
```

O conteúdo do arquivo */etc/squid/redes_sociais.txt:*

```
facebook.com
instagram.com
youtube.com
```

Então, foram aplicadas as seguintes regras:

```
http_access deny user_zeca horas_uteis !maquina_recepcao
http_access deny redes_sociais !intervalo_noite
```

Para bloqueio do acesso direto à internet foi adicionada as seguintes regras através do iptables:

```
[root@servidor ~]# iptables -A FORWARD -o enp0s3 -p tcp --dport 80 -j REJECT
[root@servidor ~]# iptables -A FORWARD -o enp0s3 -p tcp --dport 443 -j REJECT
[root@servidor ~]# iptables -A FORWARD -o enp0s3 -p tcp --dport 20 -j REJECT
[root@servidor ~]# iptables -A FORWARD -o enp0s3 -p tcp --dport 21 -j REJECT
```

Após aplicar essas regras, foi usado o comando iptables-save para que estas regras fossem persistidas:

```
[root@servidor ~]# iptables-save > /etc/iptables//iptables.conf
```

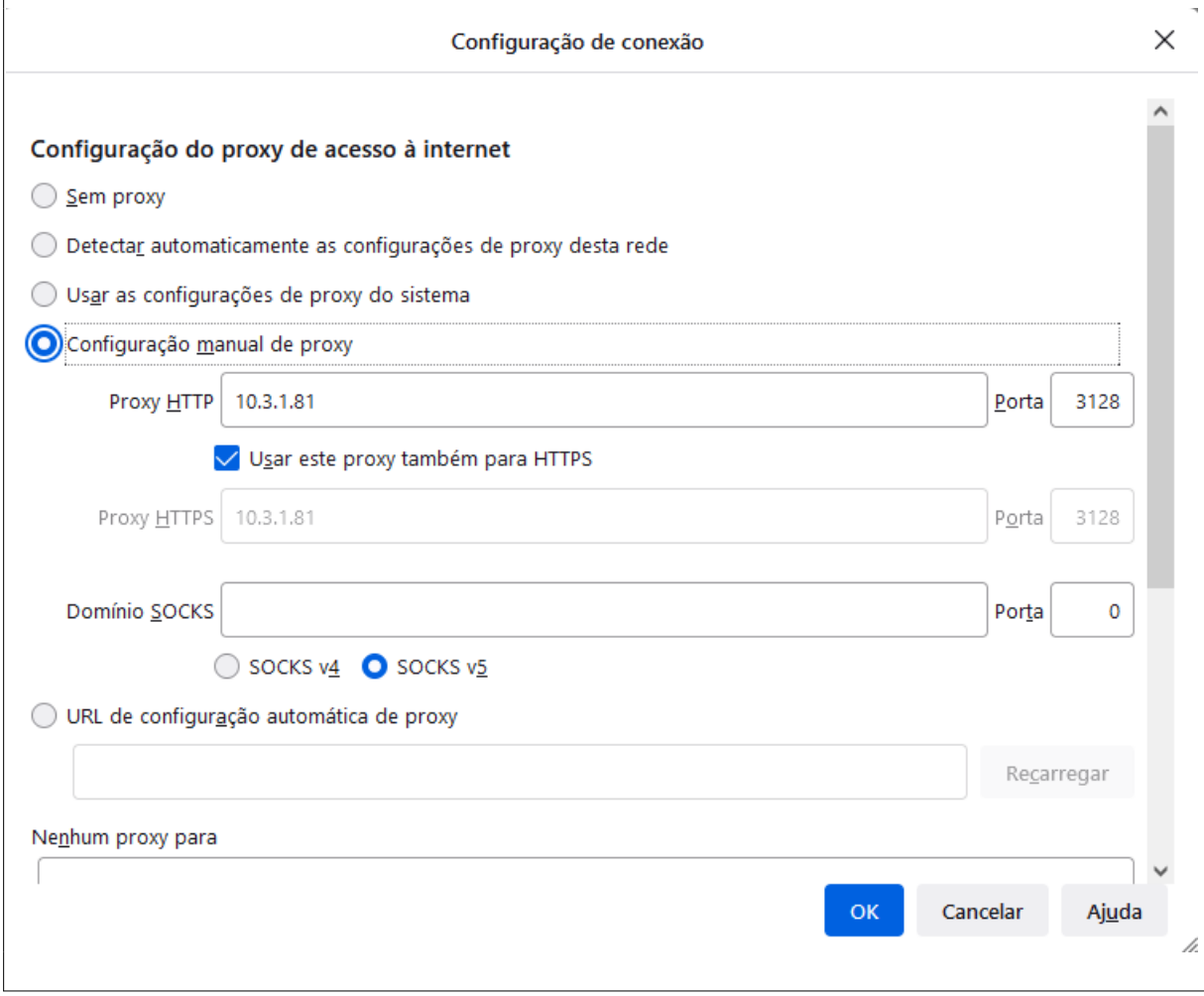
Para que essas regras sejam carregadas ao inicializar o sistema, foi adicionada a seguinte linha ao arquivo */etc/rc.local*:

```
iptables-restore < /etc/iptables/iptables.conf
```

após todas as configurações, foi usado o comando systemctl para iniciar o squid e para habilitá-lo durante a inicialização do sistema.

```
[root@servidor ~]# systemctl start squid
[root@servidor ~]# systemctl enable squid
```

No cliente, foi necessária apenas a configuração para uso do proxy no navegador.



4 – 60 pts (80 pts) – Instalar e configurar o servidor de arquivos e autenticação Samba, atendendo às seguintes características:

- alterar todas as variáveis de configurações necessárias do servidor Samba para que ele se comporte como um PDC;
- **(01 pts) –** criar um domínio de nome “SEUNOME”, onde “SEUNOME” deverá ser alterado para o primeiro nome do aluno em maiúsculas;
- **(01 pts) –** o nome Netbios da VM cliente é “seusobrenome”, onde “seusobrenome” deverá ser alterado para o último nome do aluno em minúsculas (a utilização de outro nome para a VM Cliente implicará numa penalidade de 30% do valor desta questão);
- **(01 pts) –** desabilitar o uso de perfis móveis;
- **00 pts (02 pts) –** tornar o servidor Samba um servidor WINS

- **00 pts (02 pts) –** configurar a VM Cliente para usar o Samba como servidor WINS;
- **(03 pts) –** permitir que somente máquinas da rede interna possam acessar o servidor Samba;
- **(03 pts) –** permitir que o servidor Samba “apareça” espontaneamente em “Rede”;
- **(03 pts) –** mapear o diretório pessoal dos usuários para a unidade “H:”;
- **(01 pts) –** permitir acesso remoto e pleno aos respectivos diretórios pessoais;
- **(03 pts) –** cadastrar os usuários “safira”, “hebe” e “vanessa” no Linux e no Samba, todos com senha “123456”. Os usuários “safira” e “vanessa” devem pertencer ao grupo “siameses”;
- **07 pts (08 pts) –** criar o diretório “/home/samba/imagens” e permitir que ele seja compartilhado com o nome “fotos” e mapeado com a letra “F:” **(04 pts)**, com permissões de leitura e escrita para todo o grupo “siameses” exceto o usuário “vanessa” que terá permissão apenas de leitura **(02 pts)**, e os demais usuários, que já existem ou poderão existir futuramente, não poderão acessá-lo de forma alguma **01 pts (02 pts)**;
- **00 pts (03 pts) –** configurar no serviço Samba para que arquivos criados no compartilhamento “fotos”, via cliente Windows, nasçam com permissão de leitura e escrita apenas para o dono, leitura para os outros membros do grupo, e nenhuma permissão para o restante;
- **00 pts (03 pts) –** configurar no serviço Samba para que diretórios criados no compartilhamento “arquivos”, via cliente Windows, nasçam com permissão de leitura, escrita e acesso apenas para o dono e grupo e nenhuma permissão para os outros;
- **(06 pts) –** configurar o arquivo /etc/fstab da VM Servidora de forma que a pasta “Documents” do usuário “aluno” na VM Cliente possa ser compartilhada e montada sobre o diretório “/home/samba/windows” simplesmente digitando o comando “mount.cifs /home/samba/windows” na VM Servidora;
- **31 pts (40 pts) –** no quadro abaixo, fazer um mini-relatório (tutorial) **citando** e **explicando** todos os passos envolvidos para a resolução desta questão, citando, inclusive, os nomes adotados para o domínio e para o netbios-name.

CNC: a máquina VM Cliente deverá ingressar no domínio criado pelo servidor Samba.

Netbios cliente: fonseca
Dominio: LUCAS

Para a realização dessa questão, foi necessária a instalação da ferramenta samba. Com o samba instalado na máquina, foi realizada uma cópia do arquivo de configurações de exemplo do samba e só então, foram inicializadas as configurações.

Para a instalação do samba foi usado o comando

```
root@servidor ~]# yum install samba samba-client
```

Foi também instalado o pacote *epel-release*. Esse pacote e necessário para a instalação da ferramenta *wsdd* que permite a descoberta das máquinas da rede.

```
[root@servidor ~]# yum install epel-release_
```

Após a instalação do pacote *epel*, e realizada a atualização dos repositórios e então a ferramenta *wsdd* e instalada através do comando yum.

```
[root@servidor ~]# yum update
```

```
root@servidor ~]# yum install wsdd
```

Feitas as instalações desses pacotes, é realizada a cópia do arquivo de exemplo de configuração do samba substituindo o arquivo de configuração dele. A partir daí, e que se inicia as configurações.

```
[root@servidor ~]# cp /etc/samba/smb.conf.example /etc/samba/smb.conf
```

Criação do PDC

Para a criação do domínio PDC, o primeiro passo foi a alteração do nome de domínio, a string do servidor e a configuração de restrição à rede interna:

```
        workgroup = LUCAS
        server string = Servidor Samba - Prova
        wins support = yes
        netbios name = MYSERVER

        interfaces = lo enp0s8
```

A fim de tornar o servidor, um servidor wins, foi adicionada a diretiva ***wins support = yes***

Feito isso foram alteradas as configurações do script de *logon* e *logon path*. O *logon path* vazio, indica que o uso de perfis móveis está desabilitado.

```
logon script = smblogon.bat
logon path = \\%L\Profiles\%u
# use an empty path to disable profile support:
logon path =
```

Para o controle de domínio, as seguintes linhas foram habilitadas

```
    domain master = yes
    domain logons = yes
```

O samba foi definido como servidor local preferido com o nível mais elevado. Assim caso haja mais candidatos, sua escolha é mais garantida.

```
    local master = yes
    os level = 255
    preferred master = yes
```

Para o mapeamento do diretório pessoal dos usuários, foi adicionada a seguinte linha nas opções do sistema de arquivo:

```
logon drive = H:
```

A fim de ocultar o home de outros usuários, a sessão homes sofreu uma alteração passando a ter permissão apenas o usuário da sessão através da restrição *valid users*.

```
[homes]
        comment = Home Directories
        browseable = no
        writable = yes
        valid users = %S
```

Agora a configuração do *netlogon*. Foram removidos os comentários da sessão *netlogon*. A sessão foi alterada de forma a ser não navegável e ter o caminho em */home/samba/netlogon*

```
[netlogon]
        comment = Network Logon Service
        path = /home/samba/netlogon
        guest ok = yes
        writable = no
        browseable = no
```

Uma vez que o caminho definido para o *netlogon* ainda não existia, foi necessária sua criação

```
[root@servidor ~]# mkdir /home/samba/ /home/samba/Snetlogon
```

Em seguida, foi criado o script de *logon*:

```
[root@servidor ~]# vim /home/samba/netlogon/smblogon.bat
```

Neste arquivo foi inserida uma linha indicando o mapeamento do diretório home:

```
net use H: /HOME
```

Como a codificação do Windows se difere da codificação do Linux, é necessária a conversão da codificação deste arquivo de script. Para tal, é necessária a instalação da ferramenta *dos2unix*

```
[root@servidor ~]# yum install dos2unix
```

Feita a instalação, o seguinte comando foi executado para a alteração da codificação:

```
[root@servidor ~]# unix2dos /home/samba/netlogon/smblogon.bat
unix2dos: converting file /home/samba/netlogon/smblogon.bat to DOS format...
```

Realizada a conversão, foi dada a permissão de execução para este arquivo:

```
[root@servidor ~]# chmod 755 /home/samba/netlogon/smblogon.bat
```

Registro de usuários

Para o cadastro dos usuários no samba, foi necessário o cadastro prévio no Linux através do comando *adduser* e criadas as senhas para cada um:

```
[root@servidor ~]# adduser safira
[root@servidor ~]# adduser vanessa
[root@servidor ~]# adduser hebe
[root@servidor ~]# passwd safira
Changing password for user safira.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@servidor ~]# passwd vanessa
Changing password for user vanessa.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
[root@servidor ~]# passwd hebe
Changing password for user hebe.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

Foi criado o grupo *siameses* e os usuários *safira* e *vanessa* foram inseridos nele:

```
[root@servidor ~]# groupadd siameses
[root@servidor ~]# usermod -G siameses vanessa
[root@servidor ~]# usermod -G siameses safira
```

Em seguida, os usuários foram cadastrados no samba:

```
[root@servidor ~]# smbpasswd -a safira
New SMB password:
Retype new SMB password:
Added user safira.
[root@servidor ~]# smbpasswd -a vanessa
New SMB password:
Retype new SMB password:
Added user vanessa.
[root@servidor ~]# smbpasswd -a hebe
New SMB password:
Retype new SMB password:
Added user hebe.
```

De modo a limitar o acesso a somente máquinas registradas, foi criado também um usuário para a máquina cliente

```
[root@servidor ~]# useradd -d /dev/null -s /bin/false fonseca$
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.
```

Em seguida foi bloqueada sua senha

```
[root@servidor ~]# passwd -l fonseca$
Locking password for user fonseca$.
passwd: Success
```

E o usuário adicionado ao samba

```
[root@servidor ~]# smbpasswd -a -m fonseca$
Added user fonseca$.
```

Como o *shell /bin/false* não existe, foi preciso registrá-lo no arquivo */etc/shells*. Para isso foi adicionada a seguinte linha no final do arquivo

```
/bin/false
```

Compartilhamento do diretório imagens

Como o diretório */home/samba/imagens* ainda não existia, ele foi criado:

```
[root@servidor ~]# mkdir /home/samba/imagens
```

Como foi definido que o compartilhamento fosse realizado exclusivamente com o grupo de usuários *siameses*, o grupo deste diretório foi alterado para *siameses*:

```
[root@servidor ~]# chgrp siameses /home/samba/imagens/
```

As permissões do diretório foram alteradas para 775

```
[root@servidor ~]# chmod 775 /home/samba/imagens/
```

Então, no arquivo de configuração do samba, foi criada uma sessão para o compartilhamento:

```
[fotos]
        comment = imagens gerais
        path = /home/samba/imagens
        browseable = no
        guest ok = yes
        writable = yes
        valid users = +siameses
        read list = vanessa
        create mask = 0755
        directory mask = 0755
```

Como foi definido que o compartilhamento fosse realizado para o grupo *siameses*, foi aplicada a restrição para somente este grupo através da diretiva ***valid users = +siameses***.

Foi definido também que qualquer usuário do grupo *siameses* possui a permissão de escrita com exceção do usuário *vanessa*. Então, foram aplicadas as diretivas:

writable = yes que permite que qualquer um com acesso a esse diretório, tem permissão de escrita;
read list = vanessa indicando que o usuário *vanessa* está restrito a somente leitura do conteúdo deste diretório.

Foi definido também que este compartilhamento não ficará visível na rede através da diretiva ***browseable = no***

A diretiva ***create mask = 0755*** indica que os usuários terão pleno acesso aos seus próprios ficheiros. todos os outros apenas terão acesso de leitura e execução, mas não de escrita.

A diretiva ***directory mask = 0755*** tem a mesma idéia da diretiva *create mask,* porém aplicada para diretórios.

Como houve algumas falhas relacionadas às permissões, as permissões do diretório **/home/samba/imagens** foram alteradas:

```
[root@servidor ~]# chmod +t /home/samba/imagens/
```

Nota: Para os testes de permissão, foi adicionado um usuário que também faz parte do grupo *siameses*:

Usuário: joao
Senha: 123456

A configuração do arquivo */etc/fstab* para a montagem da pasta compartilhada documentos foi realizada adicionando a seguinte linha no final do arquivo */etc/fstab*

```
//10.3.1.82/Documents   /home/samba/windows     cifs    username=aluno,password=123456    0 0
```

Essa linha especifica o endereço remoto da pasta compartilhada, o ponto de montagem, o tipo do sistema de arquivos, informações do usuário Windows, se tem ou não dump e se tem fsk. No caso as opções jump e fsk não foram habilitadas.

Foi instalada a ferramenta cifs através do comando:

```
[root@servidor ~]# yum install cifs-utils
```

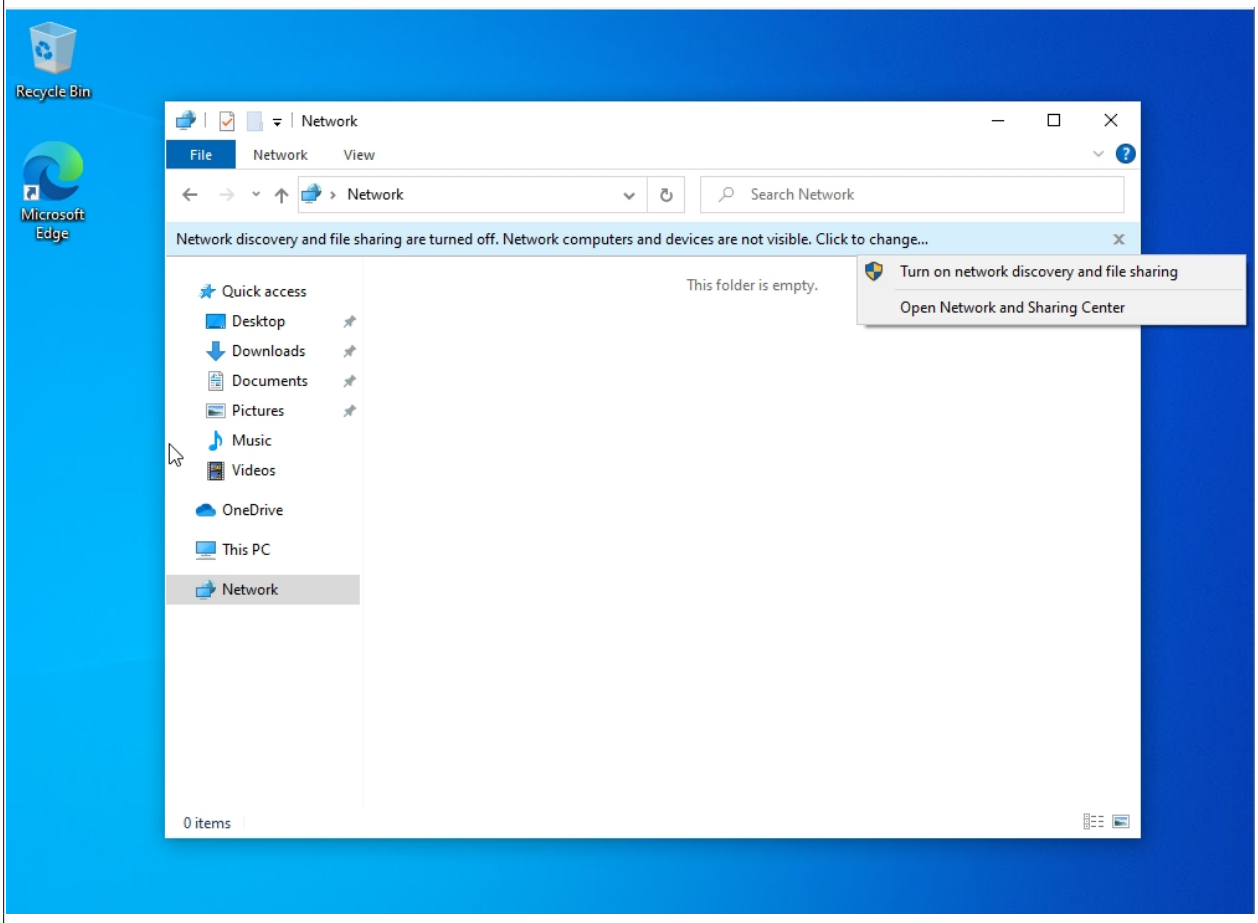
NOTA: Para a realização dessa montagem, usa-se o comando abaixo (não foi possível realizar a montagem usando o comando *mount.cifs /home/samba/Windows*)

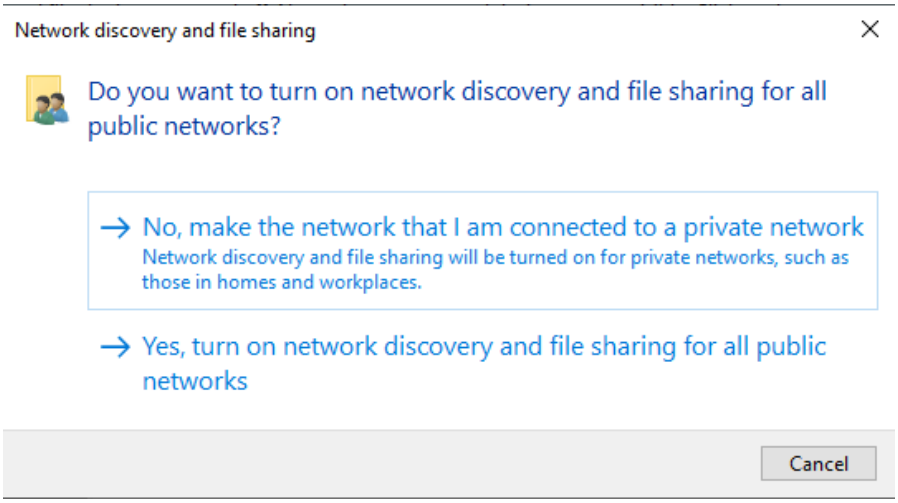
```
[root@servidor ~]# mount /home/samba/windows/
```

Samba cliente

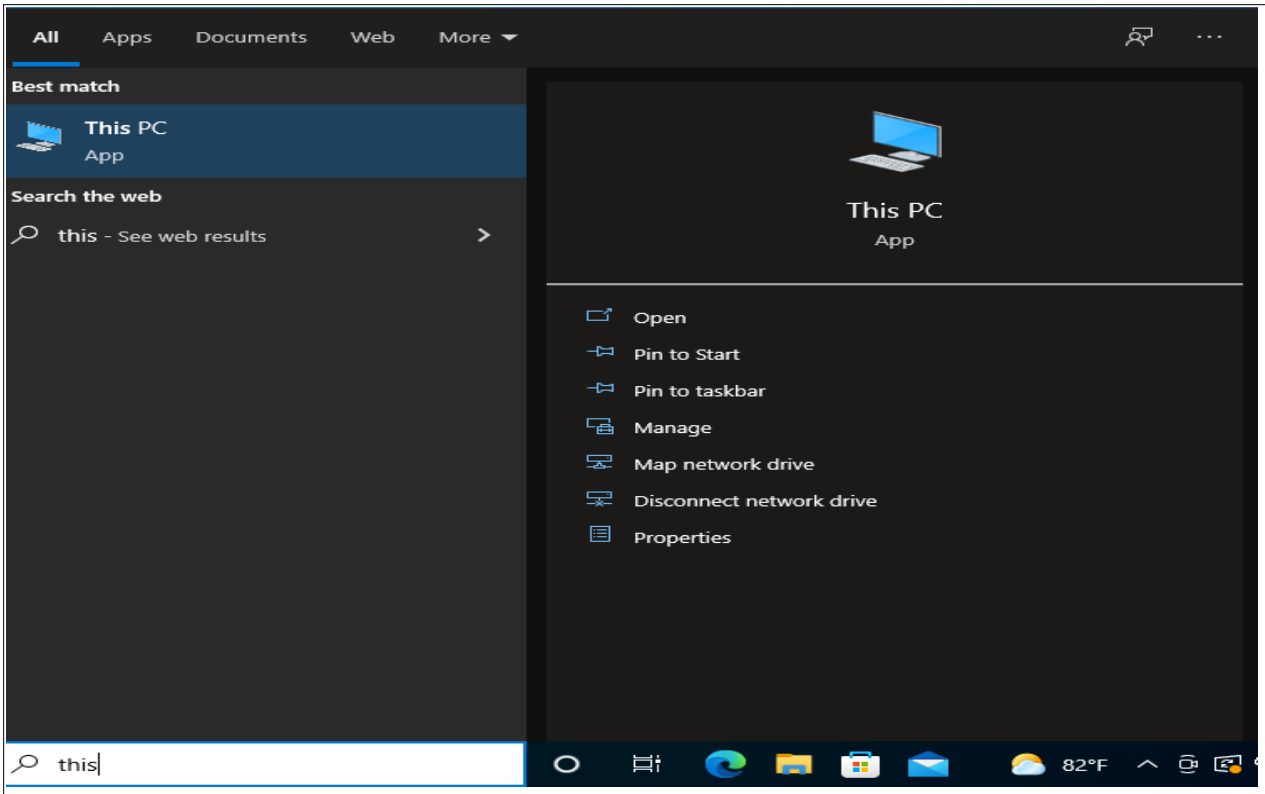
Os passos de configuração do samba no Windows são bem simples. Dessa forma, vou só dar uma passada rápida no que foi feito.

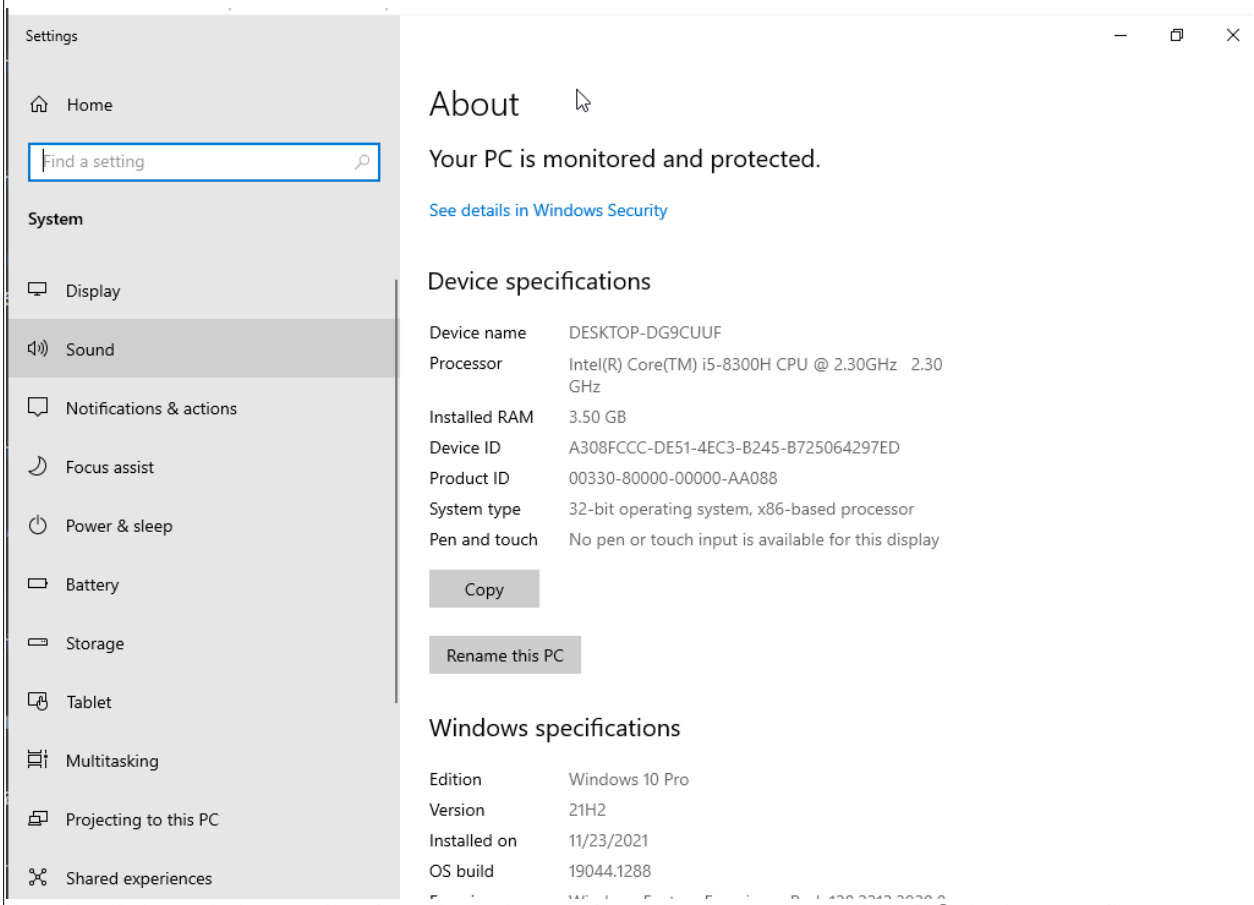
Foi configurado a descoberta do computador em rede:



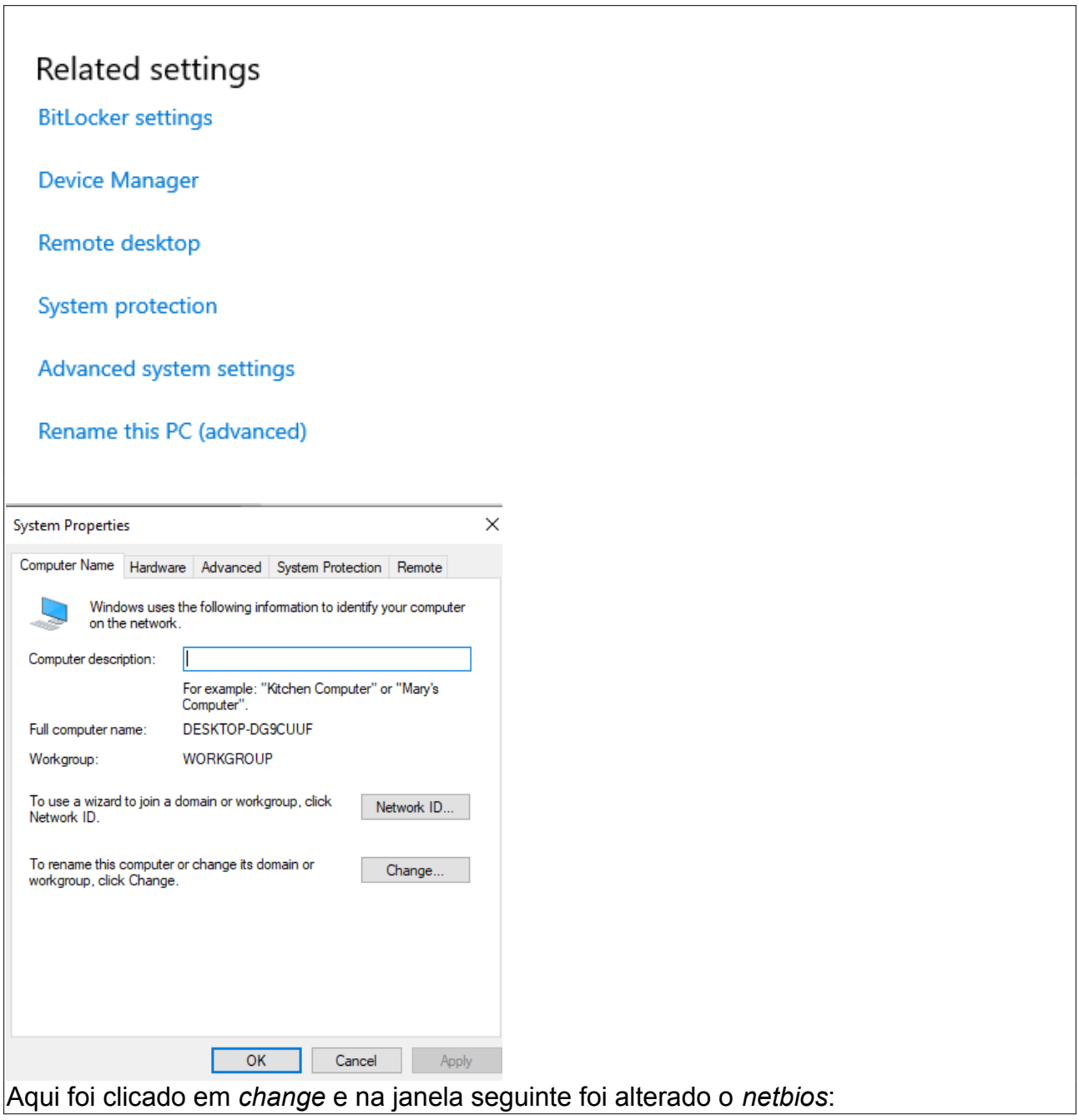


Em seguida, a máquina cliente foi adicionada ao domínio:

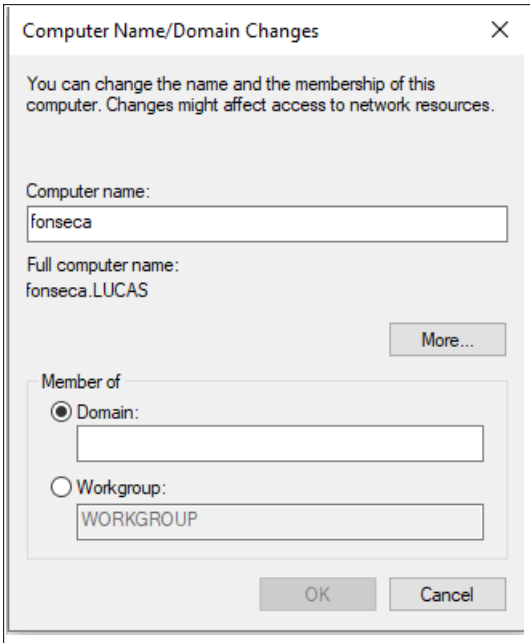




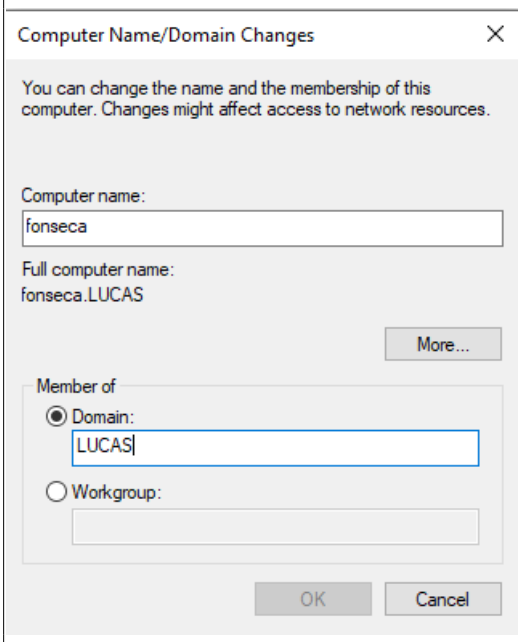
Aqui, rolei a página até *related settings*, cliquei em *rename this PC (advanced)*



Aqui foi clicado em *change* e na janela seguinte foi alterado o *netbios*:



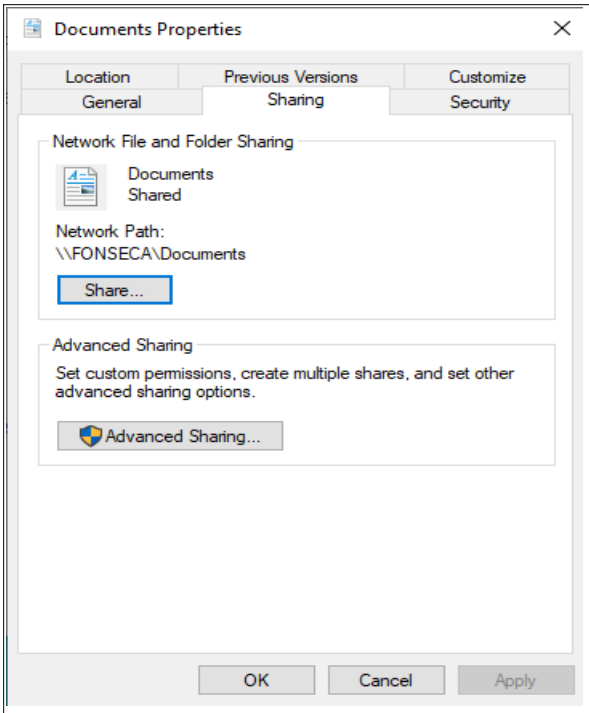
Após a alteração do netbios, a máquina foi reinicializada e repetindo os passos acima foi alterado o domínio:



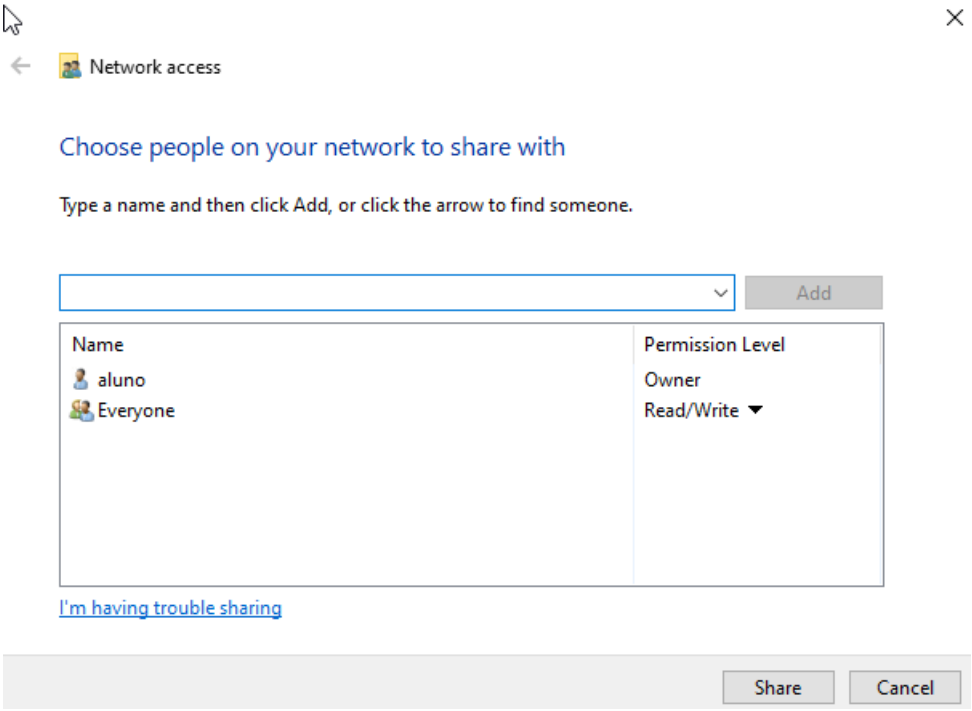
Em seguida, a máquina foi reiniciada e após a reinicialização, foi executado o arquivo de registro do Windows disponibilizado em aula: https://github.com/lucaschf/Internet-Service-Management-and-Configuration/blob/main/client/Win10-netlogon.reg

Compartilhamento da pasta documentos

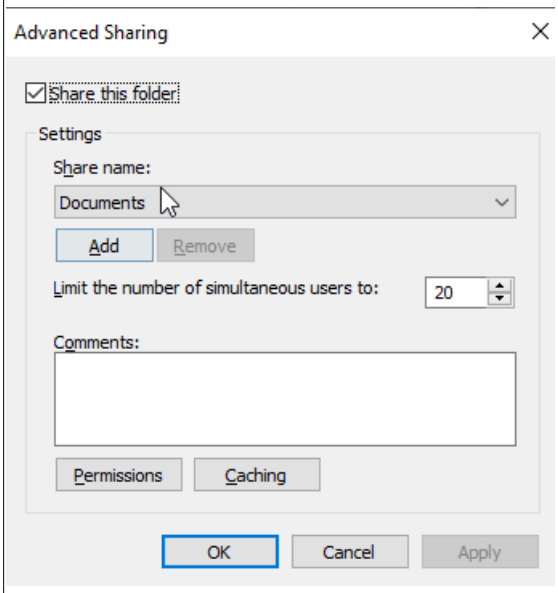
Para o compartilhamento da pasta documentos, foram realizados os seguintes passos:
Acesso às propriedades do diretório *documentos->sharing*:



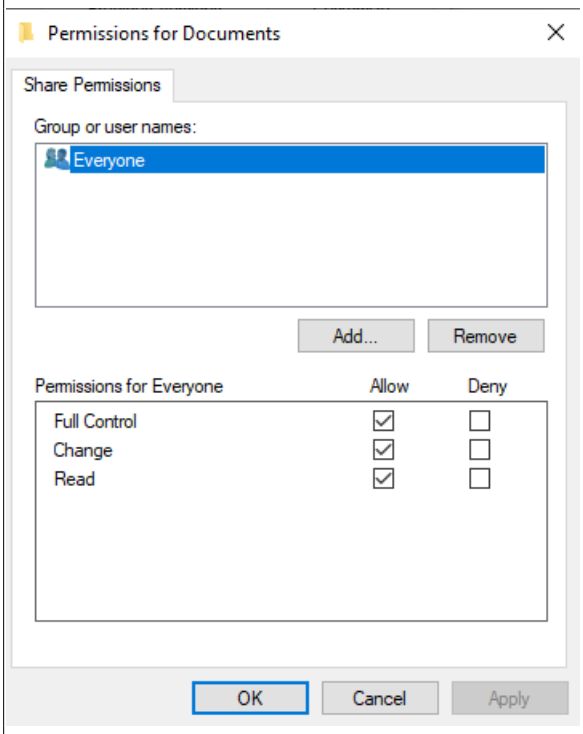
Foi clicado em compartilhar e adicionado o compartilhamento para todos com permissão de leitura e escrita:



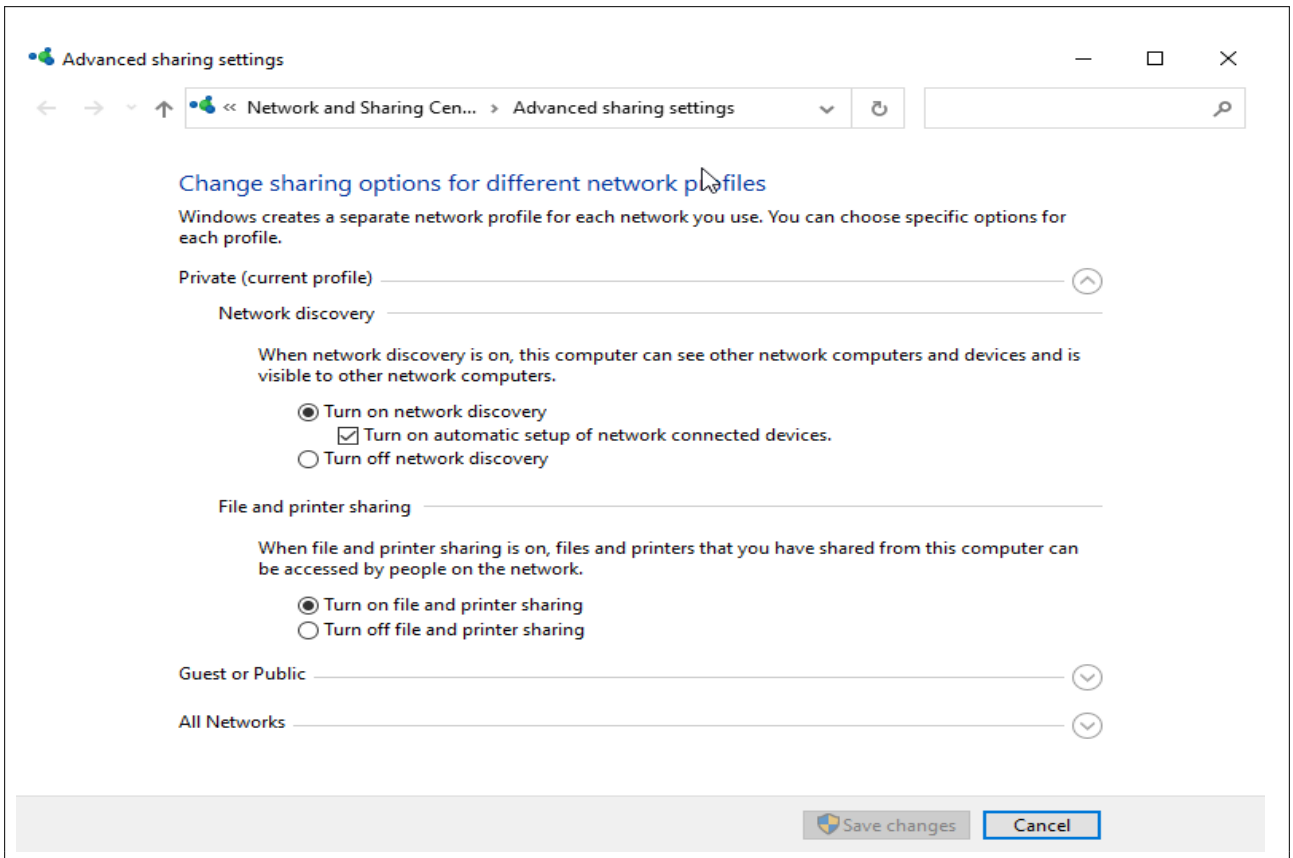
Após a confirmação de compartilhamento, de volta a tela de propriedades (sharing), foi clicado em *compartilhamento avancado*. Na tela seguinte foi marcada a opção *compartilhar esta pasta*:

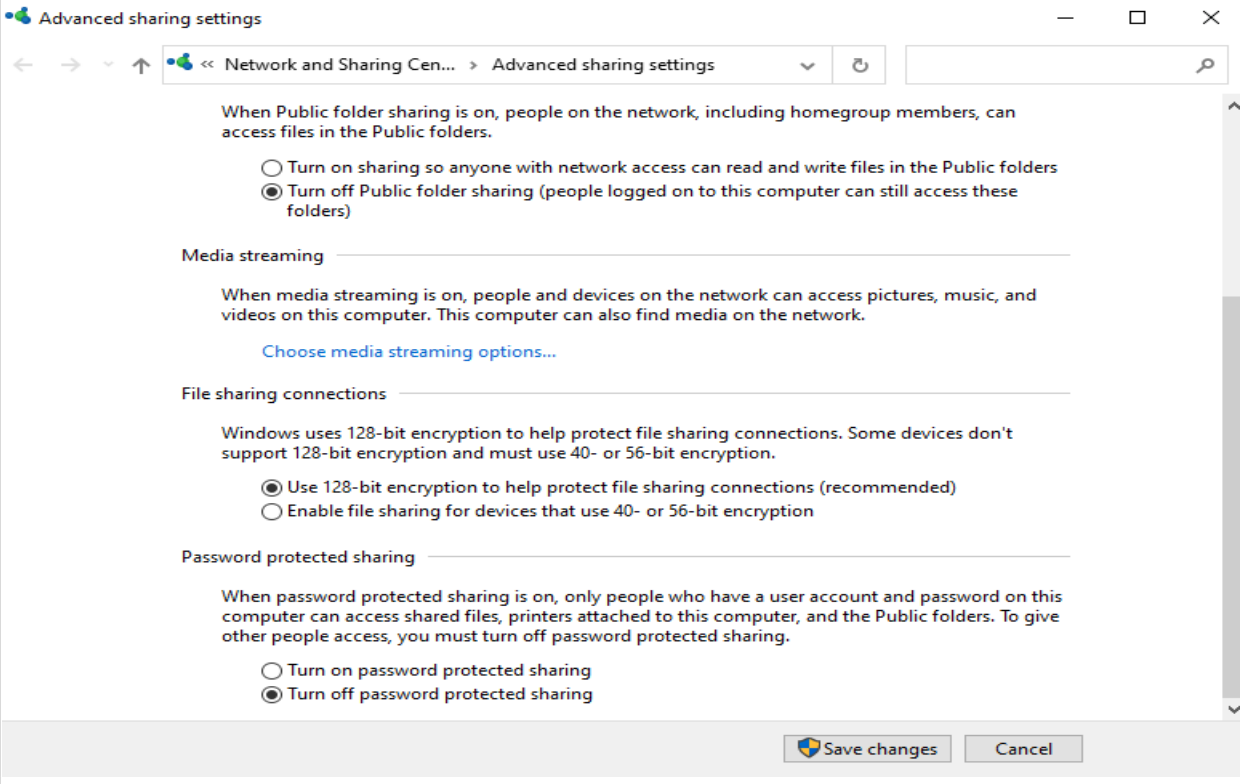


Em seguida foram alteradas as permissões, clicando em permissões, e dando acesso total (Na prática deveria ser mais restrito, uma leitura apenas, por exemplo):



Foi alterado também, o modo compartilhamento para que seja realizado sem senha:


Advanced sharing settings
Network and Sharing Cen... › Advanced sharing settings
Change sharing options for different network profiles
Windows creates a separate network profile for each network you use. You can choose specific options for each profile.
Private (current profile)
Network discovery
When network discovery is on, this computer can see other network computers and devices and is visible to other network computers.
Turn on network discovery
Turn on automatic setup of network connected devices.
Turn off network discovery
File and printer sharing
When file and printer sharing is on, files and printers that you have shared from this computer can be accessed by people on the network.
Turn on file and printer sharing
Turn off file and printer sharing
Guest or Public
All Networks
Save changes
Cancel


Advanced sharing settings
Network and Sharing Cen... › Advanced sharing settings
When Public folder sharing is on, people on the network, including homegroup members, can access files in the Public folders.
Turn on sharing so anyone with network access can read and write files in the Public folders
Turn off Public folder sharing (people logged on to this computer can still access these folders)
Media streaming
When media streaming is on, people and devices on the network can access pictures, music, and videos on this computer. This computer can also find media on the network.
Choose media streaming options...
File sharing connections
Windows uses 128-bit encryption to help protect file sharing connections. Some devices don't support 128-bit encryption and must use 40- or 56-bit encryption.
Use 128-bit encryption to help protect file sharing connections (recommended)
Enable file sharing for devices that use 40- or 56-bit encryption
Password protected sharing
When password protected sharing is on, only people who have a user account and password on this computer can access shared files, printers attached to this computer, and the Public folders. To give other people access, you must turn off password protected sharing.
Turn on password protected sharing
Turn off password protected sharing
Save changes
Cancel

E pronto!