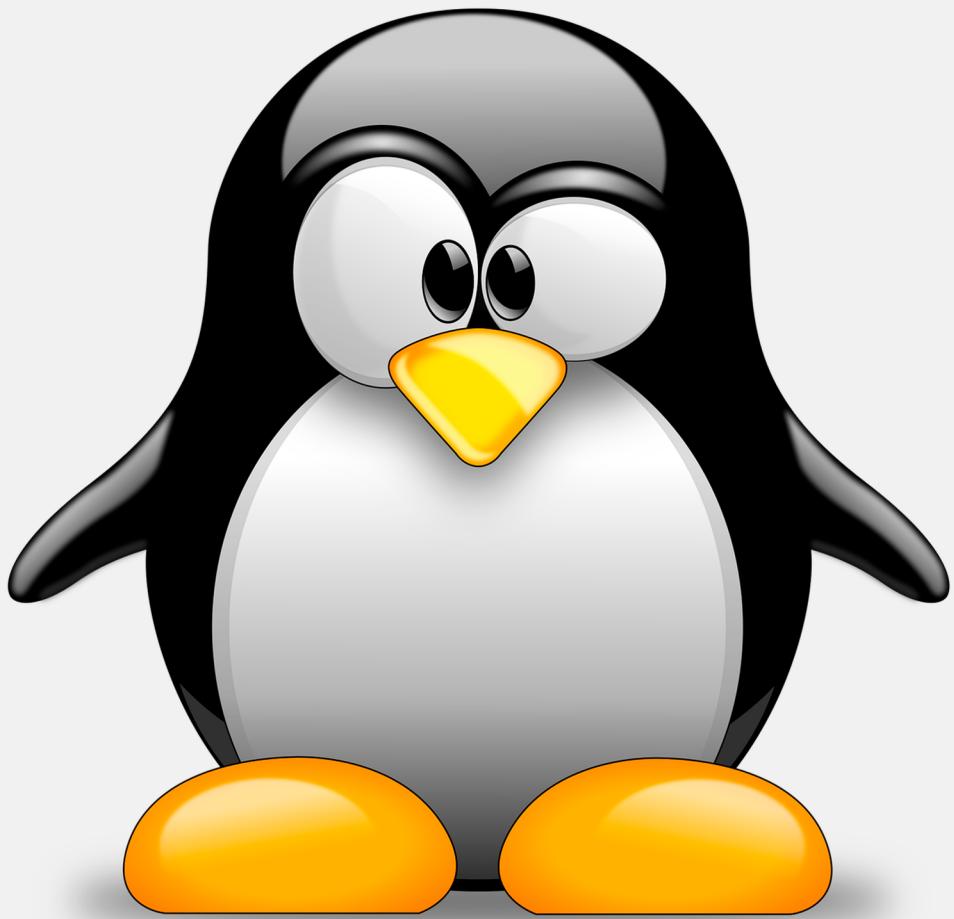




E-BOOK %100 GRATUITO

COMO GANHAR DINHEIRO COM O LINUX



FATURANDO COM LINUX, SEM CERTIFICAÇÃO.



Introdução

@LINUX.GNU

Esse material que esta na suas mãos é incrível, e o conhecimento que está nele é o suficiente para você dar aquele diferencial na sua carreira de TI, **principalmente se você é um técnico ou analista.**

Nesse e-book você vai descobrir como é possível substituir o **Windows Server PIRATA** ou se livrar das licenças que custam uma verdadeira **FORTUNA** e como é possível ganhar dinheiro com o Linux de forma estratégica, utilizando **um sistema chamado SAMBA 4** que é instalado no Linux.

Você pode ganhar em média R\$: 5.000,00 por projeto implementado, basta aprender os passos simples e necessários para implementar um servidor de respeito, original, seguro, gratuito, estável e de fácil gerenciamento.

É importante que você já tenha algum conhecimento em Linux para seguir **esse passo a passo incrível**, desenvolvido para te ajudar a trabalhar com ferramentas open source e te levar a outro nível, para você surpreender a todos a ponto de deixar eles com uma certa inveja de você.

Contato

- ✉ fernando@linuxcurso.com
- 📞 [11 97412-8091](tel:11 97412-8091)
- 🌐 linuxcurso.com

Os primeiros passos podem parecer complexo, mas é normal, quantas vezes algo te pareceu complexo e no final era bem simples, como, por exemplo quando formatou **seu primeiro PC instalando Windows XP, 7 ou 10** (esqueça o 8) ou quando usou Linux na VM a primeira vez, parecia complexo e agora parece tão simples, já está praticamente no piloto automático.

É a mesma coisa aqui, tem que seguir o passo a passo até o final e rever, para assim **INSTALAR esses passos simples no seu cérebro**, deixando tudo praticamente no automático, para quando for usar esse conhecimento você **FATURAR R\$: 5.000,00 de forma rápida e eficiente**.

Isso é para você parar de **formatar computadores por R\$: 50,00 ou 100,00** e ir para outro nível, o nível mais ALTO, o de empresas que estão precisando de você nesse momento, mas não sabem disso, querem se livrar das licenças que custam uma FORTUNA para **reduzir custos**, mas não sabem o que fazer, ou **utilizam CRACKs colocando os dados de todos em alto risco**, imagine perder dados importantes e não ter os backups ou tomar uma multa gigante por simplesmente utilizar a pirataria, daria para ouvir os gritos de desespero do gestou ou cliente.

Aproveite o máximo esse e-book !

@linux.gnu
#linux.gnu

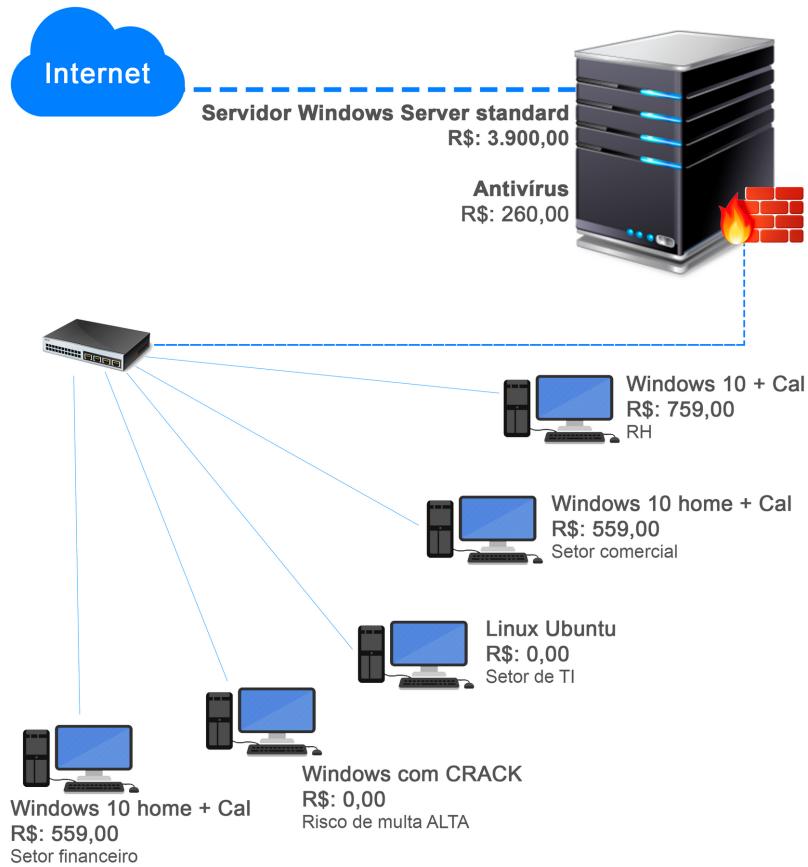
Contato

- ✉ fernando@linuxcurso.com
- 📞 [11 97412-8091](tel:1197412-8091)
- 🌐 linuxcurso.com



Cenário 01

O QUE VOCÊ VAI ENCONTRAR NA EMPRESA



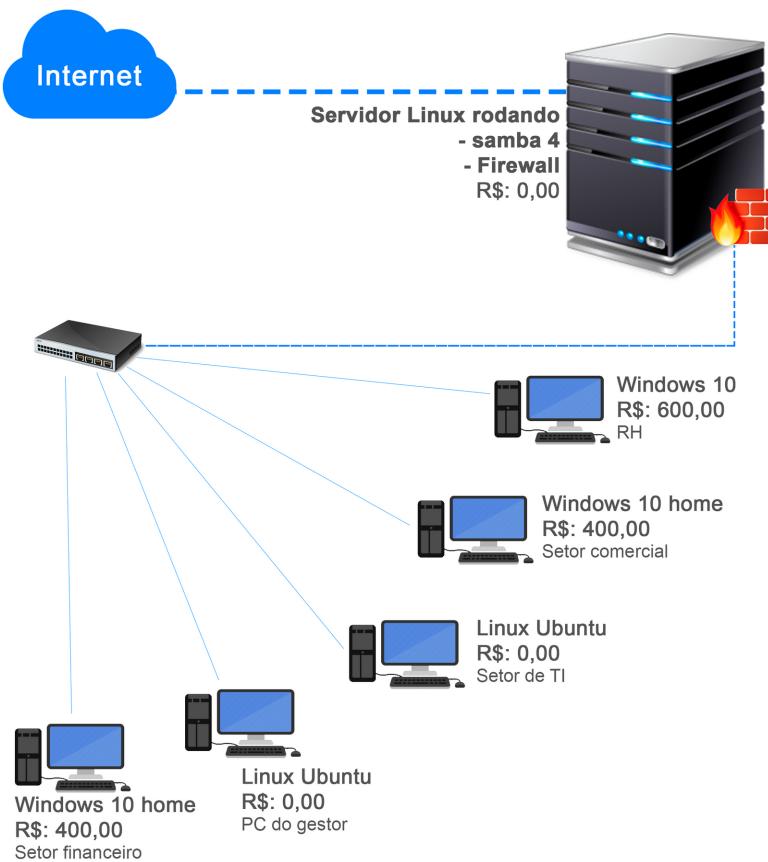
CAL: é uma licença de acesso, cada usuário precisa de uma para poder acessar o servidor.

Nesse pequeno cenário o valor gasto com licenças já passa dos **R\$:6.000,00**
Imagine isso em um cenário onde está **1 servidor com 50 máquinas**
O valor seria bem mais alto que R\$: 6.000,00



Cenário 02

O QUE VOCÊ SERÁ CAPAZ DE IMPLEMENTAR



SAMBA 4: software open source que **substitui perfeitamente** o Windows Server e pode ser gerenciado com a mesma **interface gráfica** do Windows.

Não precisa utilizar CALs.

Nesse cenário o valor foi **reduzido para R\$: 1.400,00** uma diferença de **R\$: 4.637,00** do cenário anterior. **Cobre pelo menos 50%** desse valor que você acabou de economizar, que seria R\$: 2.318,50 desse jeito você e a empresa ganha, a empresa acabou de se livrar das licenças para sempre.

Alguns Pcs continuaram com Windows, esses usuários precisam realmente dele para realizar devidas tarefas.



OBJETIVO

@LINUX.GNU

Agora você vai aprender o passo a passo a implementação do servidor **Samba 4** como **Active Directory e Servidor de Arquivos para ser implantado em um ambiente de TI** de uma organização que necessite utilizar os recursos de um Controlador de Domínio centralizado, seja para redução de custos ou substituir um domínio Microsoft Windows PIRATA.

Nesse passo a passo você vai ver os seguintes recursos:

- Samba4 - Active Directory Domain Server;
- Samba4 – File Server;
- Serviço NTP (Network Time Protocol);
- Encaminhamento de DNS do Samba;
- Autenticação de usuários e grupos e computadores;
- Instalação da ferramenta RSAT em máquina Windows, para administrar os objetos presentes no AD.



Descrição do cenário utilizado

Ambiente de Virtualização: O cenário utilizado na elaboração desse e-book foi criado em um ambiente virtualizado, com a utilização do Software Livre de virtualização VirtualBox, versão 6.1.

Firewall: O pfSense é Open Source (não há necessidade de aquisição de licença para instalar e utilizar seus recursos no ambiente corporativo), ele também possui os recursos necessários para assumir o papel de roteador da rede, além de diversos outros recursos que possibilitam a implantação de vários recursos de segurança para proteger e controlar o ambiente de Tecnologia da Informação da organização.

Servidor Linux: o sistema operacional escolhido para instalar o Servidor Samba 4 nas funções de Domain Controller e File Server foi Debian GNU/Linux-10 (Buster), versão 10.3.3 –64bits. Nessa escolha foi considerada a estabilidade conhecida do Linux Debian aliada a facilidade de instalação e configuração dos pacotes, por meio dos repositórios APT mantidos pela plataforma do Debian.

Máquinas Windows: foram escolhidos para instalação no ambiente uma máquina virtual com Windows 7 e outra com Windows 10. Essa escolha foi feita considerando que a maioria dos ambientes de rede das corporações é composta atualmente por esses dois sistemas



Descrição do cenário utilizado

O cenário proposto para simular a implementação do servidor Samba como DomainController e File Server está composto por um ...

Firewall: com os recursos de internet, DNS e DHCP ativados

Servidor Linux Debian 10: com os recursos do servidor Samba instalados

2 Pcs Windows: um sendo Windows 10 e outro com Windows 7

Requisitos básicos do ambiente para instalar e testar a solução proposta:

Recurso	Disco	Memória	Esquema de Rede
Firewall pfSense	16 GB	512 MB	<p>Interface Externa: <u>modo bridge</u> e recebendo IP via DHCP</p> <p>Interface Interna: rede exclusiva de hospedeiro e endereço IP configurado em: 192.168.50.1</p>
Servidor Linux Debian 10	10 GB	512 MB	<p>Interface única: rede exclusiva de hospedeiro e endereço IP configurado em: 192.168.50.4</p>
Computador Windows 7	30 GB	1 GB	<p>Interface única: rede exclusiva de hospedeiro e endereço IP configurado em: 192.168.50.7</p>
Computador Windows 10	50 GB	2 GB	<p>Interface única: rede exclusiva de hospedeiro e endereço IP configurado em: 192.168.50.10</p>



Controlador de Domínio

@LINUX.GNU

Conceitualmente um **Domain Controller** (Active Directory) consiste em um servidor/serviço de diretórios (atualmente ele conta com um servidor LDAP integrado), no qual **constam informações sobre usuários, grupos, políticas de grupos (GPOs),** computadores e outros objetos para simplificar o acesso e a integração entre os diversos recursos de Tecnologia da Informação em uso no ambiente colaborativo.

Os recursos do Active Directory podem ser implementados por meio do Servidor Windows **e também pelo Servidor Linux Samba.**

O servidor Samba, a partir da versão 4, disponibiliza todos os recursos existentes no Active Directory é totalmente compatível com as estações de trabalho Windows, **inclusive com o Microsoft Windows 10**, sem necessidade de nenhuma modificação nesses sistemas para que eles ingressem no domínio mantido pelo servidor Samba 4.



Vantagens na adoção do Active Directory no Servidor Samba 4:

SAMBA 4

Com a adoção do Servidor Samba como Domain Controller Active directory a organização estará usufruindo de um dos servidores mais utilizados para **interoperabilidade de sistemas e redes heterogêneas** (integração entre Linux e Windows), além de não necessitar adquirir licenças para uso dos recursos do Active Directory mantidos pelo Samba 4.

Em relação ao licenciamento, esse é um dos grandes diferenciais que fazem com que **pequenas e médias organizações optem pela implantação dos recursos** do Active Directory em um servidor Linux com Samba 4, em detrimento do Windows Server, visto que **não é necessário adquirir licenças** para disponibilizar os serviços no Servidor Samba e nem para que as estações de trabalho se conectem e utilizem esses recursos.

Dessa forma o projeto Samba 4 poderá ser utilizado tanto por empresas que pretendam estruturar seus ambientes de redes para melhorar a integração dos serviços e o controle dos recursos quanto por corporações que já possuam um ambiente rodando Windows Server **mas querem economizar com licenciamento ou queiram legalizar** seu ambiente que porventura estejam rodando softwares não licenciados.



Recursos disponíveis no Servidor Samba 4:

ALGUNS RECURSOS

Active Directory Domain Controller:

Servidor de DNS interno: responsável pela manutenção e resolução dos nomes das máquinas locais e também pelo cache de DNS para resolver as consultas originadas na rede interna com destino à internet;

File Server: servidor de arquivos com capacidade de proporcionar a interoperabilidade e a integração entre sistemas Windows e Linux;

NTP Server: serviço de hora para proporcionar a sincronização dos relógios ativos de rede conectados ao domínio Samba 4;

Lixeira de rede: recurso de proteção contra perda accidental de informação;

Auditoria de acessos às pastas e arquivos: capacidade de auditar os acessos e manipulações de pastas e arquivos no file server.



Instalação e configuração do Samba 4

AJUSTES - DOMAIN CONTROLLER E FILE SERVER

Verificar compatibilidade do sistema de arquivos: é necessário que o sistema de arquivos esteja pronto para suportar o uso de ACLs estendidas, recurso exigido pelo Samba 4

```
# grep -i ext4 /boot/config-$(uname -r) | grep -iE 'acl|security'
```

```
192.168.50.4 - PuTTY
root@adLivre:~# grep -i ext4 /boot/config-$(uname -r) | grep -iE 'acl|security'
CONFIG_EXT4_FS_POSIX_ACL=y
CONFIG_EXT4_FS_SECURITY=y
```

```
# tune2fs -l /dev/sda1 | grep 'mount options'
```

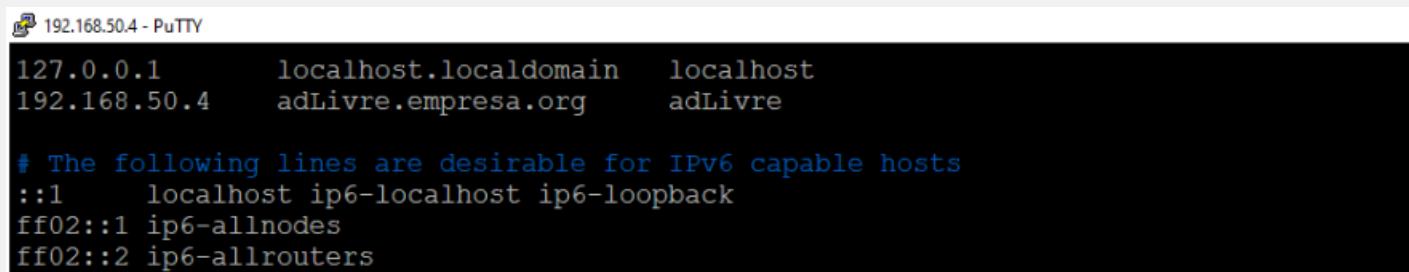
```
192.168.50.4 - PuTTY
root@adLivre:~# tune2fs -l /dev/sda1 | grep 'mount options'
Default mount options:    user_xattr acl
```

Ajustar os parâmetros do host: nesse exemplo foi definido o domínio “empresa.org”.

Observação: essa configuração é de extrema importância, porque no momento em que o serviço do Samba e formos subir o domínio será verificado nome do host nesse local.

```
# nano /etc/hosts
```

```
127.0.0.1      localhost.localdomain  localhost
192.168.50.4   adLivre.empresa.org   adLivre
```



```
192.168.50.4 - PuTTY
127.0.0.1      localhost.localdomain  localhost
192.168.50.4   adLivre.empresa.org   adLivre

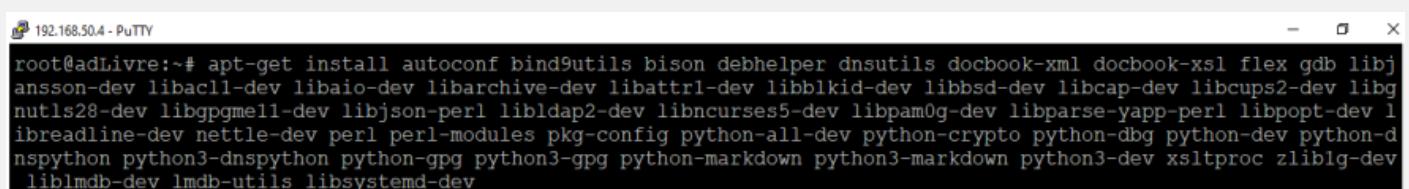
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

Importante: antes de realizar a instalação é necessário configurar IP manual no servidor. Não devem ser feitas as configurações com o servidor recebendo IP via DHCP. Recomenda-se **desinstalar o DHCP Client** do servidor para evitar surpresas.

Instalar as dependências: Nesse passo serão instaladas as dependências que o Samba necessitará para executar os recursos do domínio.

Algumas não serão utilizadas por completo nesse ambiente, mas é sempre recomendável instalá-las para que **fiquem disponíveis em caso de necessidade futura**.

```
apt-get install autoconf bind9utils bison debhelper dnsutils docbook-xml
docbook-xsl flex gdb libjansson-dev libacl1-dev libaio-dev libarchive-dev libattr1-
dev libblkid-dev libbsd-dev libcap-dev libcups2-dev libgnutls28-dev libgpgme11-
dev libjson-perl libldap2-dev libncurses5-dev libpam0g-dev libparse-yapp-perl
libpopt-dev libreadline-dev nettle-dev perl perl-modules pkg-config python-all-dev
python-crypto python-dbg python-dev python-dnspython python3-dnspython
python-gpg python3-gpg python-markdown python3-markdown python3-dev
xsltproc zlib1g-dev liblmbdb-dev lmdb-utils libsystemd-dev
```



```
root@adLivre:~# apt-get install autoconf bind9utils bison debhelper dnsutils docbook-xml docbook-xsl flex gdb libjansson-dev libacl1-dev libaio-dev libarchive-dev libattr1-dev libblkid-dev libbsd-dev libcap-dev libcups2-dev libgnutls28-dev libgpgme11-dev libjson-perl libldap2-dev libncurses5-dev libpam0g-dev libparse-yapp-perl libpopt-dev libreadline-dev nettle-dev perl perl-modules pkg-config python-all-dev python-crypto python-dbg python-dev python-dnspython python3-dnspython python-gpg python3-gpg python-markdown python3-markdown python3-dev xsltproc zlib1g-dev liblmbdb-dev lmdb-utils libsystemd-dev
```



Instalar o Samba 4:

Com ambiente pronto, passaremos a instalação dos serviços do Samba, para isso serão instalados os seguintes pacotes:

Samba: pacote com os recursos do módulo servidor Samba, nele serão instalados todos os recursos providos pela Samba;

Kerberos: instalado por meio do pacote “ krb5-user ”. Será o responsável pela camada de segurança, na concessão de tickets para autenticação de usuários e dispositivos;

Winbind: esse serviço é responsável por fazer o reconhecimento e a integração de usuários e recursos entre os sistemas padrão Microsoft e os padrão GNU/Linux;

Smbclient: módulo Cliente do Samba, responsável pelas conexões do servidor Samba e compartilhamentos mantidos em outros locais;

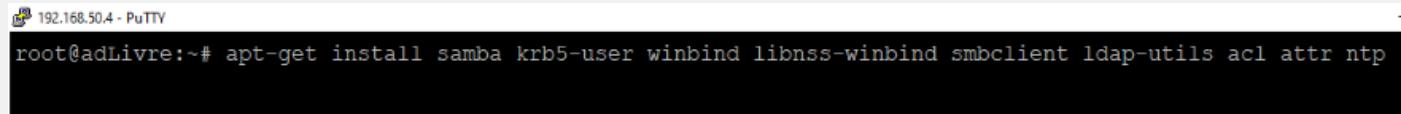
Idap-utils: pacote que realizará a instalação e integração de um servidor LDAP interno no Samba 4. Esse recurso é o responsável pela armazenamento, organização e manipulação dos serviços de diretório;

acl: Recurso para uso de ACLs estendidas pelo Samba;

attr: Recurso para uso de ACLs estendidas pelo Samba;

ntp: serviço responsável por manter os relógios dos computadores sincronizados com o do servidor. Caso os relógios dos computadores não estejam corretos, serão recusados pelo Kerberos e não autenticarão no domínio.

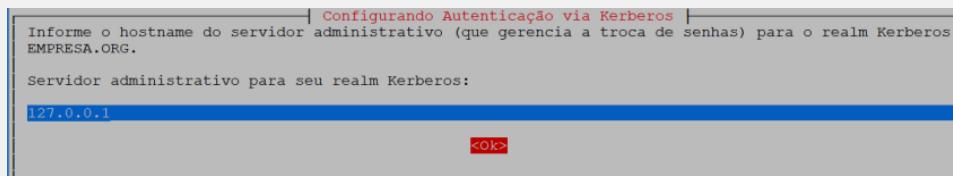
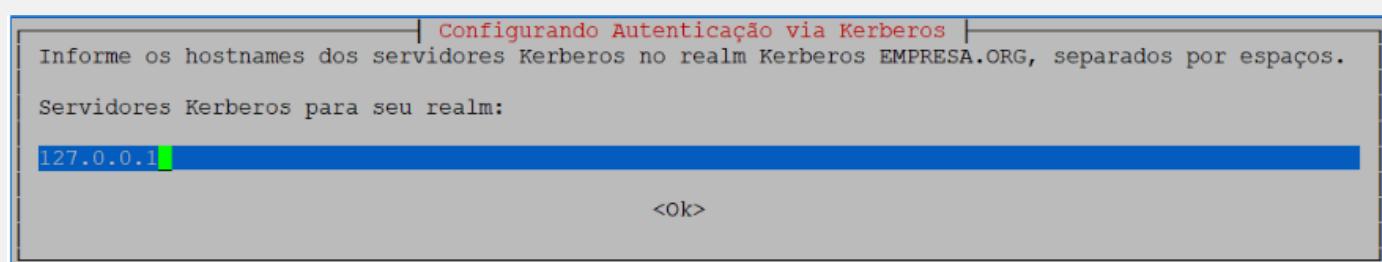
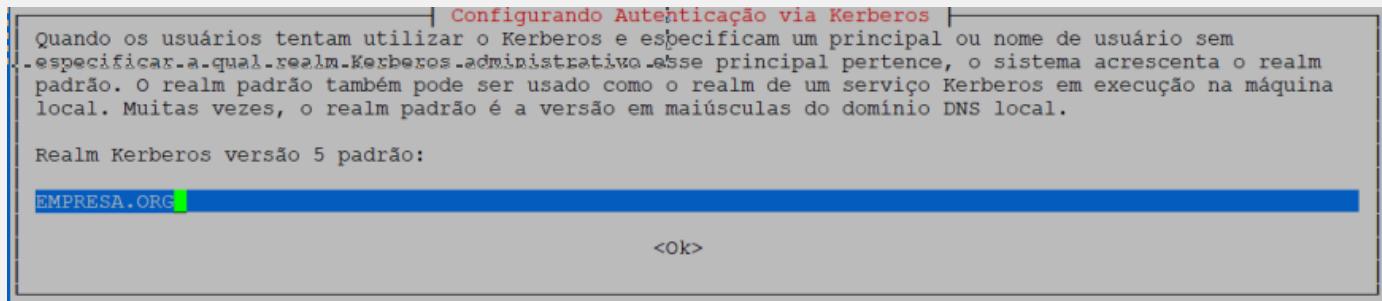
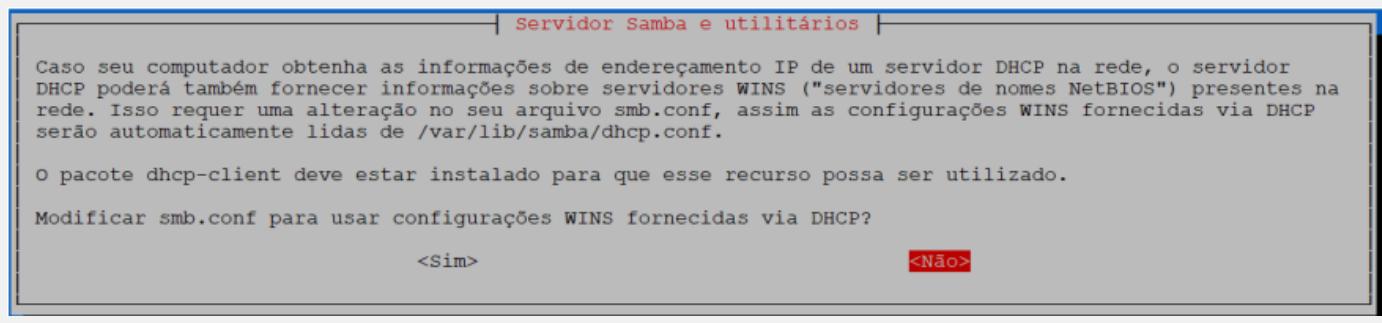
```
# apt-get install samba krb5-user winbind libnss-winbind smbclient ldap-utils acl attr ntp
```



```
192.168.50.4 - PuTTY
root@adLivre:~# apt-get install samba krb5-user winbind libnss-winbind smbclient ldap-utils acl attr ntp
```

Observação: durante o processo de instalação serão feitas algumas perguntas que poderão ser respondidas conforme as imagens abaixo:

(Caso algumas das perguntas seja respondida de maneira diferente não há problemas, visto que serão configurados os recursos na ativação dos serviços do Samba)





Configurar o NTP (Network Time Protocol):

Abrir o arquivo “/etc/ntp.conf” e acrescentar no final do arquivo o conteúdo abaixo

```
#nano /etc/ntp.conf
#(/etc/ntp.conf)
```

```
# Relogio Local
server 127.127.1.0
fudge 127.127.1.0 stratum 10
```

```
# Configurações adicionais para o Samba 4
ntpsigndsocket /var/lib/samba/ntp_signd/ # necessário criar esse diretório
restrict default mssntp
disable monitor
```

```
# If you want to listen to time broadcasts on your local subnet, de-comment the
# next lines. Please do this only if you trust everybody on the network!
#disable auth
#broadcastclient

# Relogio Local
server 127.127.1.0
fudge 127.127.1.0 stratum 10

# Configurações adicionais para o Samba 4
ntpsigndsocket /var/lib/samba/ntp_signd/ # necessário criar esse diretório
restrict default mssntp
disable monitor
```

É necessário também alterar o Pool dos servidores de NTP.

Abrir novamente o arquivo “/etc/ntp.conf” e substituir o Pool do Debian pelo do NTP.BR

```
# nano /etc/ntp.conf (substituir o Pool do Debian pelo do ntp.br)
```

```
#### remover ou comentar as linhas abaixo:
```

```
pool 0.debian.pool.ntp.org iburst
pool 1.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
pool 2.debian.pool.ntp.org iburst
```

```
#### Acrescentar as seguintes:
```

```
server a.ntp.br iburst
server b.ntp.br iburst
server c.ntp.br iburst
```

```
# You do need to talk to an NTP server or two (or three).
#server ntp.your-provider.example

# pool.ntp.org maps to about 1000 low-stratum NTP servers. Your server will
# pick a different set every time it starts up. Please consider joining the
# pool: <http://www.pool.ntp.org/join.html>
server a.ntp.br iburst
server b.ntp.br iburst
server c.ntp.br iburst
```

Criar e configurar o diretório que será utilizado pelo serviço do NTP

```
# mkdir /var/lib/samba/ntp_signd/
# chown -v root:ntp /var/lib/samba/ntp_signd/
# chmod -v 750 /var/lib/samba/ntp_signd/
```

```
192.168.50.4 - PuTTY
root@adLivre:~# mkdir /var/lib/samba/ntp_signd/
root@adLivre:~#
root@adLivre:~# chown -v root:ntp /var/lib/samba/ntp_signd/
alterado o dono de '/var/lib/samba/ntp_signd/' de root:root para root:ntp
root@adLivre:~#
root@adLivre:~# chmod -v 750 /var/lib/samba/ntp_signd/
modo de '/var/lib/samba/ntp_signd/' alterado de 0755 (rwxr-xr-x) para 0750 (rwxr-x---)
root@adLivre:~#
```

Reiniciar e testar os serviços do NTP

```
# systemctl restart ntp
```

```
# ntpq -p
```

```
192.168.50.4 - PuTTY
root@adLivre:~# systemctl restart ntp
root@adLivre:~#
root@adLivre:~# ntpq -p
      remote          refid      st t when poll reach      delay      offset      jitter
===== 
 LOCAL(0)        .LOCL.      10 l      3   64      1    0.000    0.000    0.000
 a.ntp.br        200.160.7.186  2 u      1   64      1   32.916   -2.085   0.911
 b.ntp.br        200.160.7.186  2 u      2   64      1   73.852   -2.798   0.000
 c.ntp.br        .INIT.      16 u     -   64      0    0.000    0.000    0.000
root@adLivre:~#
root@adLivre:~#
root@adLivre:~# ntpq -p
      remote          refid      st t when poll reach      delay      offset      jitter
===== 
 LOCAL(0)        .LOCL.      10 l      7   64      1    0.000    0.000    0.000
 *a.ntp.br       200.160.7.186  2 u      1   64      1   34.856   -1.727   0.953
 b.ntp.br        200.160.7.186  2 u     -   64      1  113.334  -17.754  15.648
 c.ntp.br        200.160.7.186  2 u     -   64      1   55.059  -22.728  17.401
```

Remover o serviço timesyncd (esse serviço é desnecessário e conflita com o NTP)

```
# systemctl status systemd-timesyncd.service
```

```
# systemctl disabled systemd-timesyncd.service
```

```
# systemctl stop systemd-timesyncd.service
```

```
192.168.50.4 - PuTTY
root@adLivre:~# systemctl status systemd-timesyncd.service
● systemd-timesyncd.service - Network Time Synchronization
  Loaded: loaded (/lib/systemd/system/systemd-timesyncd.service; enabled; vendor preset: enabled)
  Drop-In: /usr/lib/systemd/system/systemd-timesyncd.service.d
            └--disable-with-time-daemon.conf
    Active: inactive (dead)
      Docs: man:systemd-timesyncd.service(8)
root@adLivre:~#
root@adLivre:~# systemctl disable systemd-timesyncd.service
Removed /etc/systemd/system/dbus-org.freedesktop.timesync1.service.
Removed /etc/systemd/system/sysinit.target.wants/systemd-timesyncd.service.
root@adLivre:~#
root@adLivre:~# systemctl stop systemd-timesyncd.service
root@adLivre:~#
root@adLivre:~#
```



Provisionar e iniciar o DOMÍNIO:

Antes de realizar o provisionamento do domínio são necessários alguns ajustes

Parar alguns serviços antes de configurar o Samba 4:

```
# systemctl stop smbd.service  
# systemctl stop nmbd.service  
# systemctl stop winbind.service
```

```
192.168.50.4 - PuTTY  
root@adLivre:~# systemctl stop smbd.service  
root@adLivre:~# systemctl stop nmbd.service  
root@adLivre:~# systemctl stop winbind.service  
root@adLivre:~#
```

Remover o smb.conf da distribuição (Após o provisionamento do novo domínio esse arquivo será recriado:

```
# cd /etc/samba  
# mv smb.conf smb.conf.original
```

```
192.168.50.4 - PuTTY  
root@adLivre:~# cd /etc/samba/  
root@adLivre:/etc/samba#  
root@adLivre:/etc/samba# mv smb.conf smb.conf_original  
root@adLivre:/etc/samba#
```

Provisionar o Samba 4 (observar os parâmetros “--domain=” e “--realm=”, deverão constar os nomes que a organização utilizará):

```
# samba-tool domain provision --use-rfc2307 --domain=EMPRESA --realm=EMPRESA.ORG
```

```
192.168.50.4 - PuTTY
root@adLivre:~# samba-tool domain provision --use-rfc2307 --domain=EMPRESA --realm=EMPRESA.ORG
Administrator password will be set randomly!

Once the above files are installed, your Samba AD server will be ready to use
Admin password: xVs,M7FH$_VYo5$9-I~).
Server Role: active directory domain controller
Hostname: adLivre
NetBIOS Domain: EMPRESA
DNS Domain: empresa.org
DOMAIN SID: S-1-5-21-2730157239-2509255529-1947189257
root@adLivre:~#
```

Observação: durante o provisionamento foi definida uma senha aleatória para o usuário Administrator, portanto é necessário definir uma senha para esse usuário.

```
# samba-tool user setpassword Administrator
```

```
192.168.50.4 - PuTTY
root@adLivre:~# samba-tool user setpassword Administrator
New Password:
Retype Password:
Changed password OK
root@adLivre:~#
```

Iniciar os serviços que foram parados anteriormente:

```
# /etc/init.d/samba-ad-dc restart
```

Ajustar os scripts para que os serviços inicializem corretamente

```
# systemctl unmask samba-ad-dc.service
# systemctl enable samba-ad-dc.service
# systemctl restart samba-ad-dc.service
```

```
192.168.50.4 - PuTTY
root@adLivre:~# systemctl unmask samba-ad-dc.service
root@adLivre:~#
root@adLivre:~# systemctl enable samba-ad-dc.service
Synchronizing state of samba-ad-dc.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable samba-ad-dc
root@adLivre:~#
root@adLivre:~# systemctl restart samba-ad-dc.service
root@adLivre:~#
```

Verificar o status do serviço do Samba:

```
# systemctl status samba-ad-dc.service
```



```
192.168.50.4 - PuTTY
● samba-ad-dc.service - Samba AD Daemon
  Loaded: loaded (/lib/systemd/system/samba-ad-dc.service; enabled; vendor preset: enabled)
  Active: active (running) since Thu 2020-04-09 14:55:56 -03; 35s ago
    Docs: man:samba(8)
          man:samba(7)
          man:smb.conf(5)
  Main PID: 1333 (samba)
    Status: "smbd: ready to serve connections..."
      Tasks: 24 (limit: 545)
     Memory: 133.0M
        CGroup: /system.slice/samba-ad-dc.service
                  ├─1333 samba: root process
                  ├─1334 samba: task[s3fs_parent]
                  └─1335 samba: task[dcesrv]
```

Configurar a resolução de nomes e as configurações do Kerberos:

Esse é um dos pontos que mais provocam erros no funcionamento do Samba4, para evitar erros deve-se dedicar certo cuidado ao arquivo "/etc/resolv.conf"

Desativar o serviço `systemd-resolved`: (para que não modifique automaticamente o arquivo "/etc/resolv.conf")

```
# systemctl disable systemd-resolved.service
# systemctl stop systemd-resolved.service
```

Abrir o arquivo "/etc/resolv.conf" e ajustar as configurações

```
# nano /etc/resolv.conf
```



```
192.168.50.4 - PuTTY
domain empresa.org
search empresa.org
nameserver 192.168.50.4
```

Copiar o arquivo “krb5.conf” do Samba 4 para o “/etc” e sobrescrever o existente:

```
# cp -vb /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

```
192.168.50.4 - PuTTY
root@adLivre:~# cp -vb /var/lib/samba/private/krb5.conf /etc/krb5.conf
'/var/lib/samba/private/krb5.conf' -> '/etc/krb5.conf' (cópia de segurança: '/etc/krb5.conf~')
```

Ajustar as permissões para o servidor NTP acessar o socket do Samba 4:

```
# chown -v root:ntp /var/lib/samba/ntp_signd/
# chmod -v 750 /var/lib/samba/ntp_signd/
# systemctl restart ntp
```

```
192.168.50.4 - PuTTY
root@adLivre:~# chown -v root:ntp /var/lib/samba/ntp_signd/
dono de '/var/lib/samba/ntp_signd/' mantido como root:ntp
root@adLivre:~#
root@adLivre:~# chmod -v 750 /var/lib/samba/ntp_signd/
modo de '/var/lib/samba/ntp_signd/' mantido como 0750 (rwxr-x---)
root@adLivre:~#
root@adLivre:~# systemctl restart ntp
root@adLivre:~#
```

Realização de testes e verificações de funcionamento do Samba 4:

Verificar se o serviço do Samba está ativo e listando os compartilhamentos

```
# smbclient -L localhost -U%
```

```
192.168.50.4 - PuTTY
root@adLivre:~# smbclient -L localhost -U%
      Sharename      Type      Comment
      -----
      netlogon       Disk
      sysvol         Disk
      IPC$          IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      -----
      Workgroup       Master
      -----
      WORKGROUP      ADLIVRE
root@adLivre:~#
```

Verificar se o serviço de DNS está funcionando fazendo as resoluções:

```
# host -t A empresa.org
```

```
192.168.50.4 - PuTTY
root@adLivre:~# host -t A empresa.org
empresa.org has address 192.168.50.4
root@adLivre:~#
```

```
# host -t SRV _kerberos._udp.empresa.org
```

```
# host -t SRV _ldap._tcp.empresa.org
```

```
192.168.50.4 - PuTTY
root@adLivre:~# host -t SRV _kerberos._udp.empresa.org
_kerberos._udp.empresa.org has SRV record 0 100 88 adlivre.empresa.org.
root@adLivre:~#
root@adLivre:~# host -t SRV _ldap._tcp.empresa.org
_ldap._tcp.empresa.org has SRV record 0 100 389 adlivre.empresa.org.
root@adLivre:~#
```

Verificar o funcionamento do KERBEROS:

```
# kinit administrator@EMPRESA.ORG
```

```
192.168.50.4 - PuTTY
root@adLivre:~# kinit administrator@EMPRESA.ORG
Password for administrator@EMPRESA.ORG:
Warning: Your password will expire in 41 days on qui 21 mai 2020 14:43:04 -03
root@adLivre:~#
```

```
# klist
```

```
192.168.50.4 - PuTTY
root@adLivre:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@EMPRESA.ORG

Valid starting     Expires            Service principal
09/04/2020 15:59:43 10/04/2020 01:59:43  krbtgt/EMPRESA.ORG@EMPRESA.ORG
      renew until 10/04/2020 15:59:37
root@adLivre:~#
```

Conclusão do provisionamento do domínio:

Neste momento o Servidor Samba 4 já está provisionado e testado, o domínio “EMPRESA.ORG” já está online e aceitando o ingresso de computadores, tanto **Windows 7** quanto **Windows 10** e também servidor Windows.

Ainda faltam alguns ajustes nos serviços de compartilhamento de arquivos e pastas, mas esses ajustes serão feitos quando as máquinas Windows já estiverem no domínio.



Ingresso de máquinas Clientes Windows no domínio

Antes de ingressar o computador cliente no domínio é necessário configurá-lo para que utilize com **DNS primário** o **IP do Servidor Samba 4** (192.168.50.4)

Adaptador Ethernet Ethernet:

```
Sufixo DNS específico de conexão. . . . . : empresa.org
Descrição . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Endereço Físico . . . . . : 08-00-27-5B-28-E4
DHCP Habilitado . . . . . : Sim
Configuração Automática Habilitada. . . . . : Sim
Endereço IPv6 de link local . . . . . : fe80::384e:90c2:2af:d398%4(Preferencial)
Endereço IPv4. . . . . : 192.168.50.10(Preferencial)
Máscara de Sub-rede . . . . . : 255.255.255.0
Concessão Obtida. . . . . : quinta-feira, 9 de abril de 2020 16:35:16
Concessão Expira. . . . . : quinta-feira, 9 de abril de 2020 18:35:14
Gateway Padrão. . . . . : 192.168.50.1
Servidor DHCP . . . . . : 192.168.50.1
IAID de DHCPv6. . . . . : 101187623
DUID de Cliente DHCPv6. . . . . : 00-01-00-01-26-1F-6F-26-08-00-27-5B-28-E4
Servidores DNS. . . . . : 192.168.50.4
NetBIOS em Tcpip. . . . . : Habilicitado
```

C:\Users\lopes>

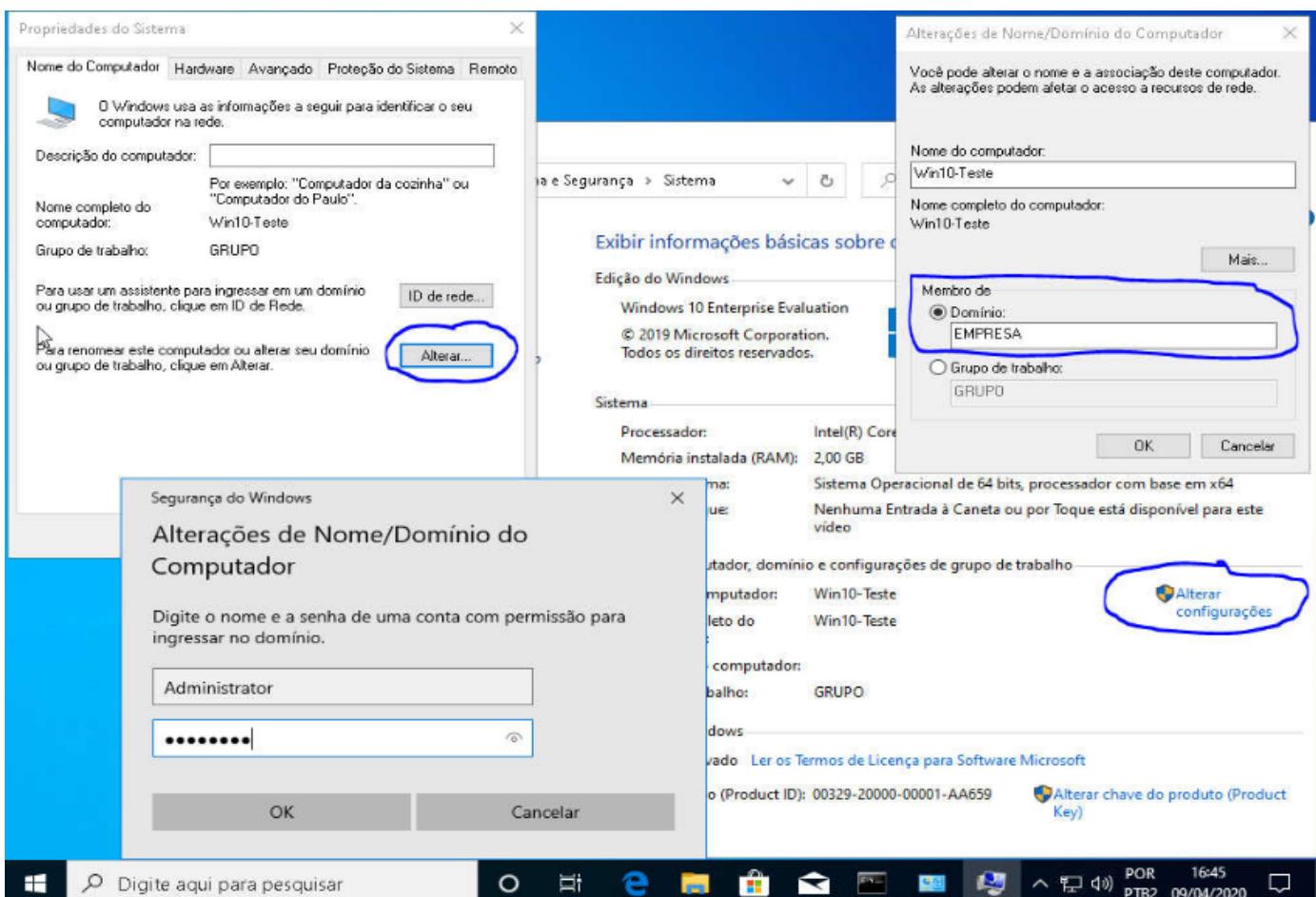
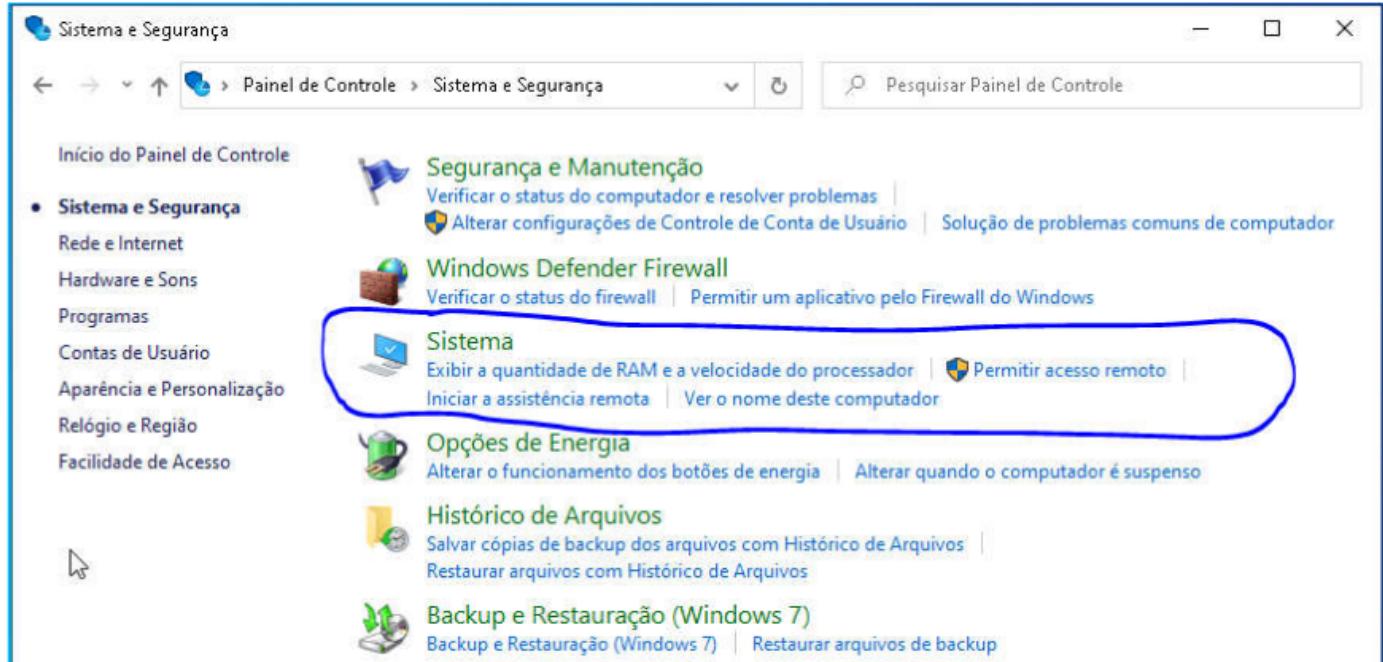


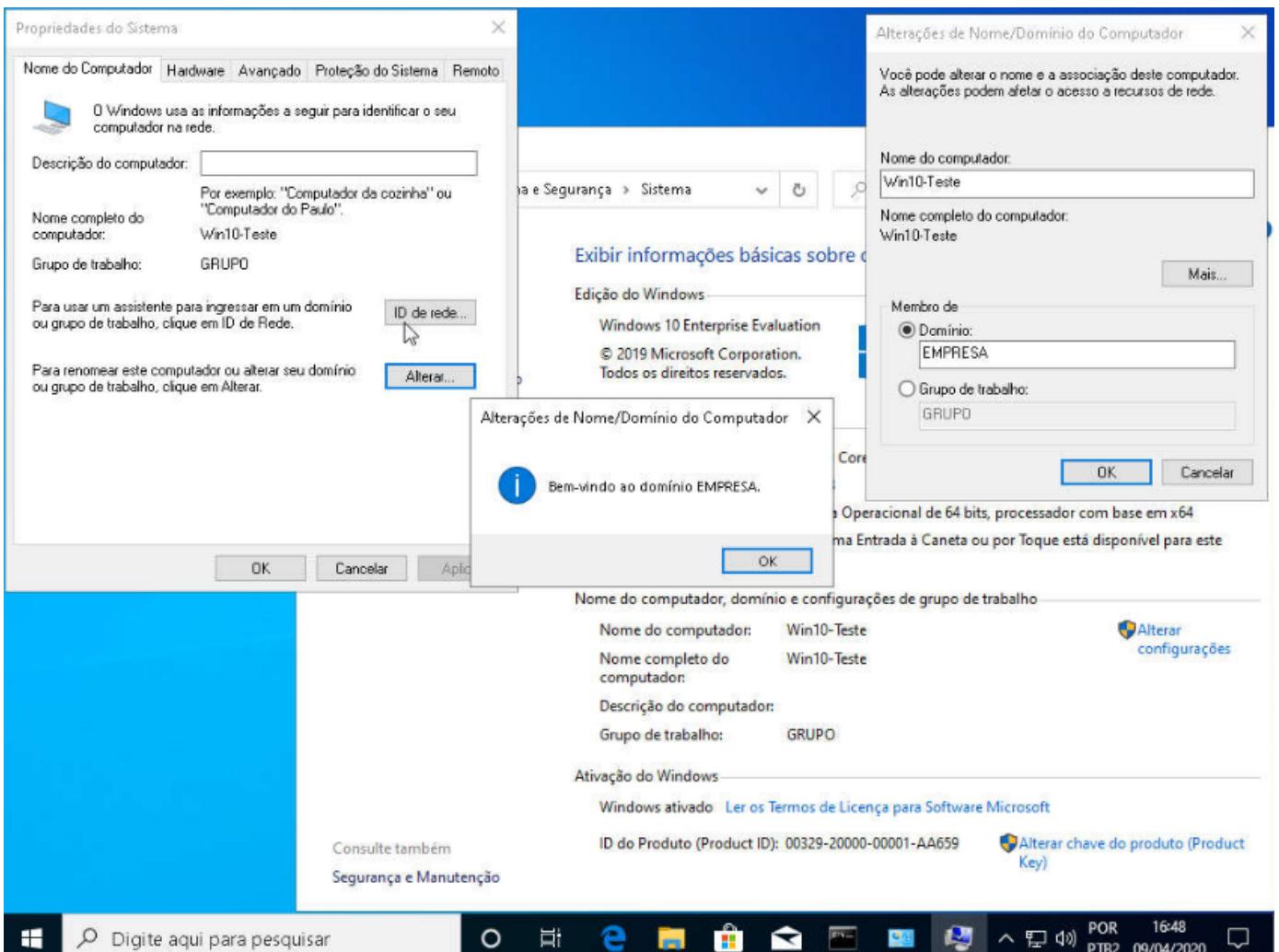
Digite aqui para pesquisar



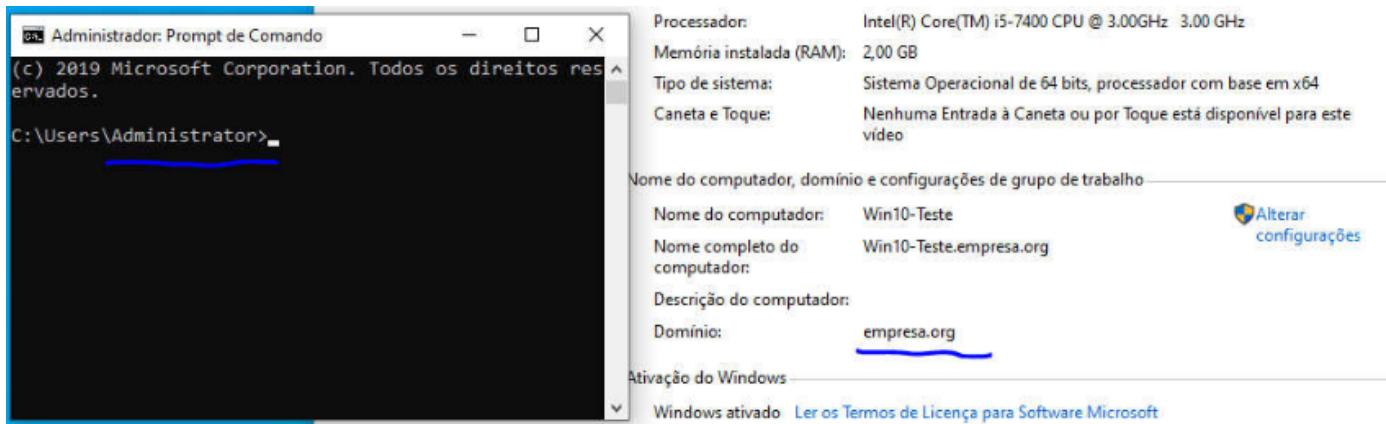
Ingressar computador Windows 10 no domínio “EMPRESA.ORG”:

- Abrir a tela Sistema em: “Painel de Controle\Sistema e Segurança\Sistema”;
- Selecionar “Alterar configurações”;
- Clicar no Alterar na tela de “Propriedades do Sistema”
- Marcar o CheckBox “Domínio” e digitar o nome do domínio: EMPRESA;
- Após esses passos será exigida a credencial de Administrator do domínio;





Reiniciar o computador e autenticar com o usuário Administrator, por enquanto ainda não foram criados outros usuários no domínio

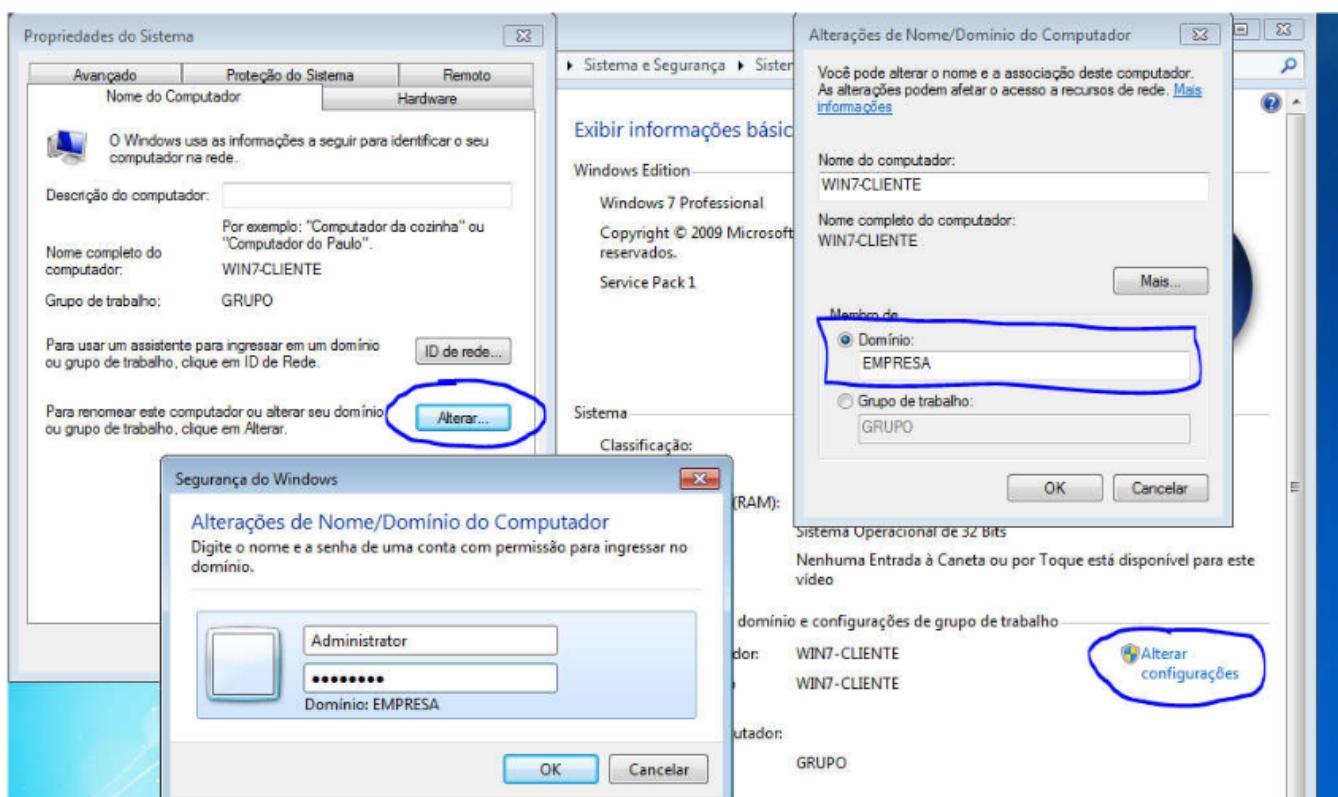


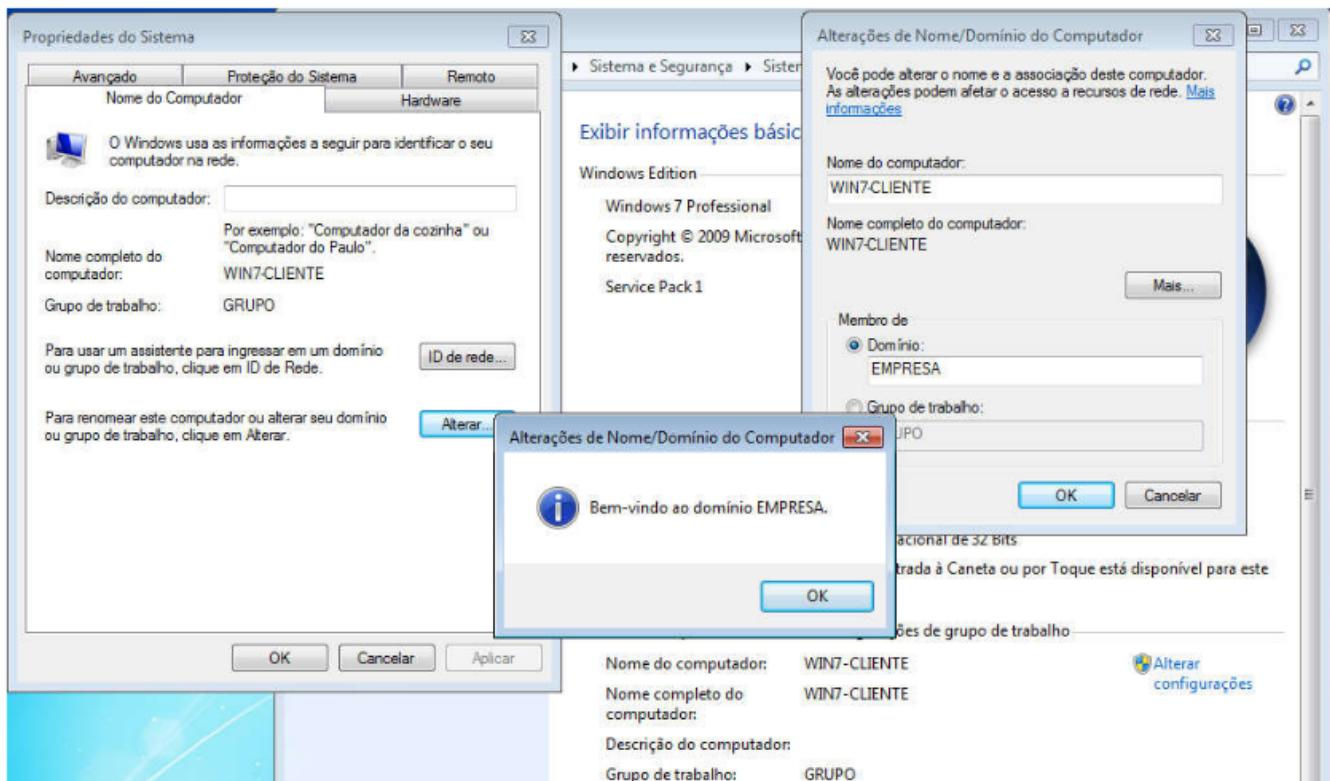
Após a reinicialização foi utilizado o usuário Administrator para logar no domínio EMPRESA, esse acesso foi realizado com sucesso.



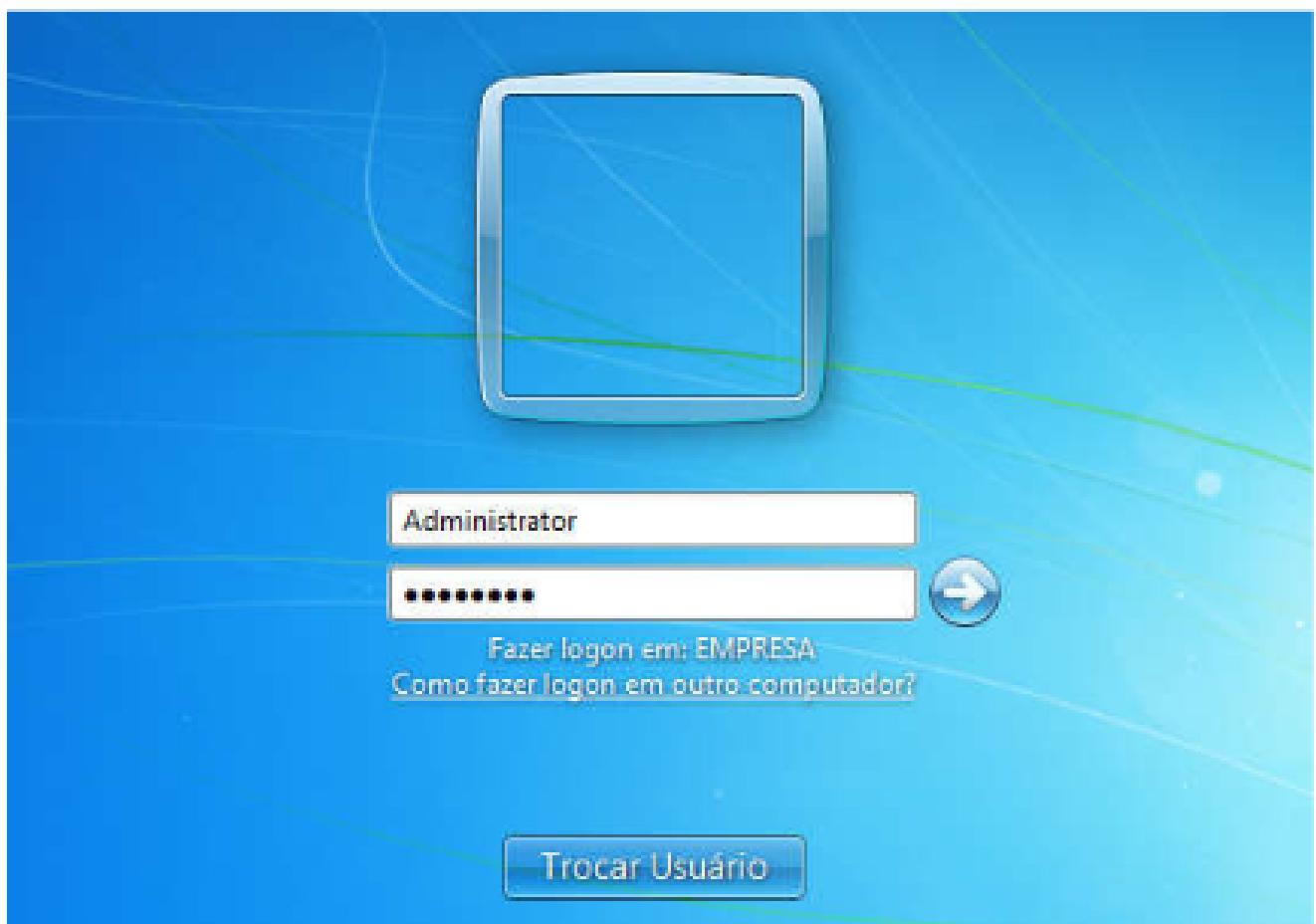
Ingressar computador Windows 7 no domínio “EMPRESA.ORG”:

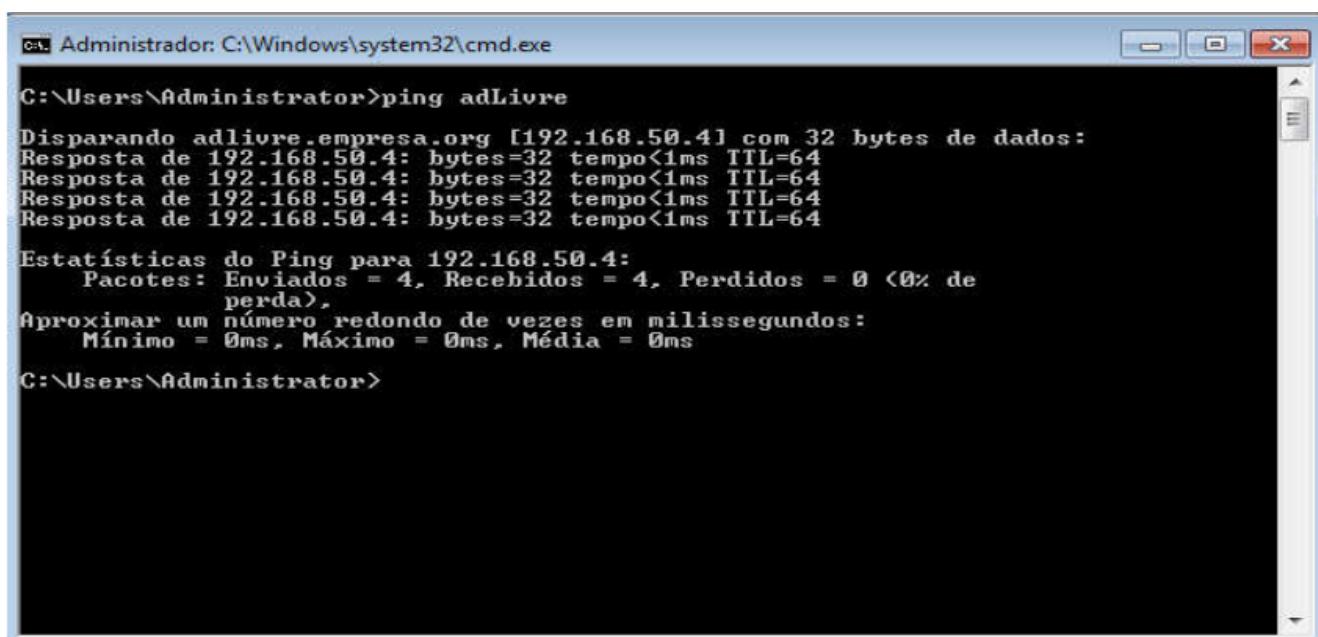
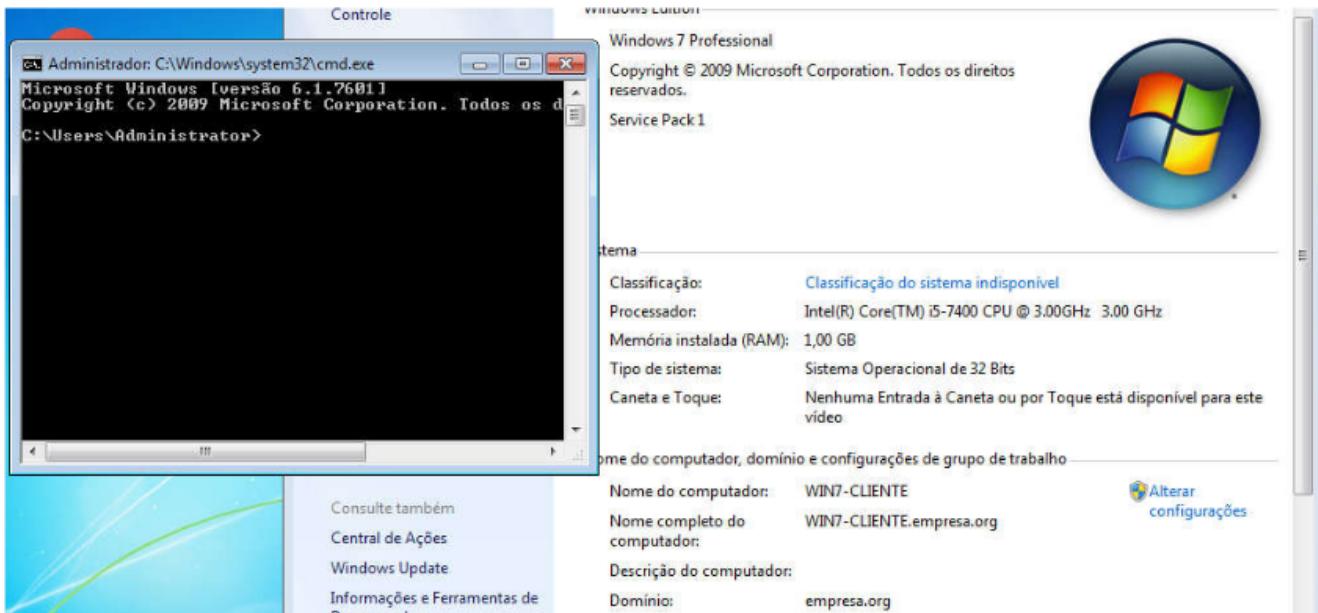
- Abrir a tela Sistema em: “Painel de Controle\Sistema e Segurança\Sistema”;
- Selecionar “Alterar configurações”;
- Clicar no Alterar na tela de “Propriedades do Sistema”
- Marcar o CheckBox “Domínio” e digitar o nome do domínio: EMPRESA;
- Após esses passos será exigida a credencial de Administrator do domínio;





Reiniciar o computador e autenticar com o usuário Administrator, por enquanto ainda não foram criados outros usuários no domínio





Mesmo princípio do Windows 10, acesso com o usuário Administrator foi realizado com sucesso.

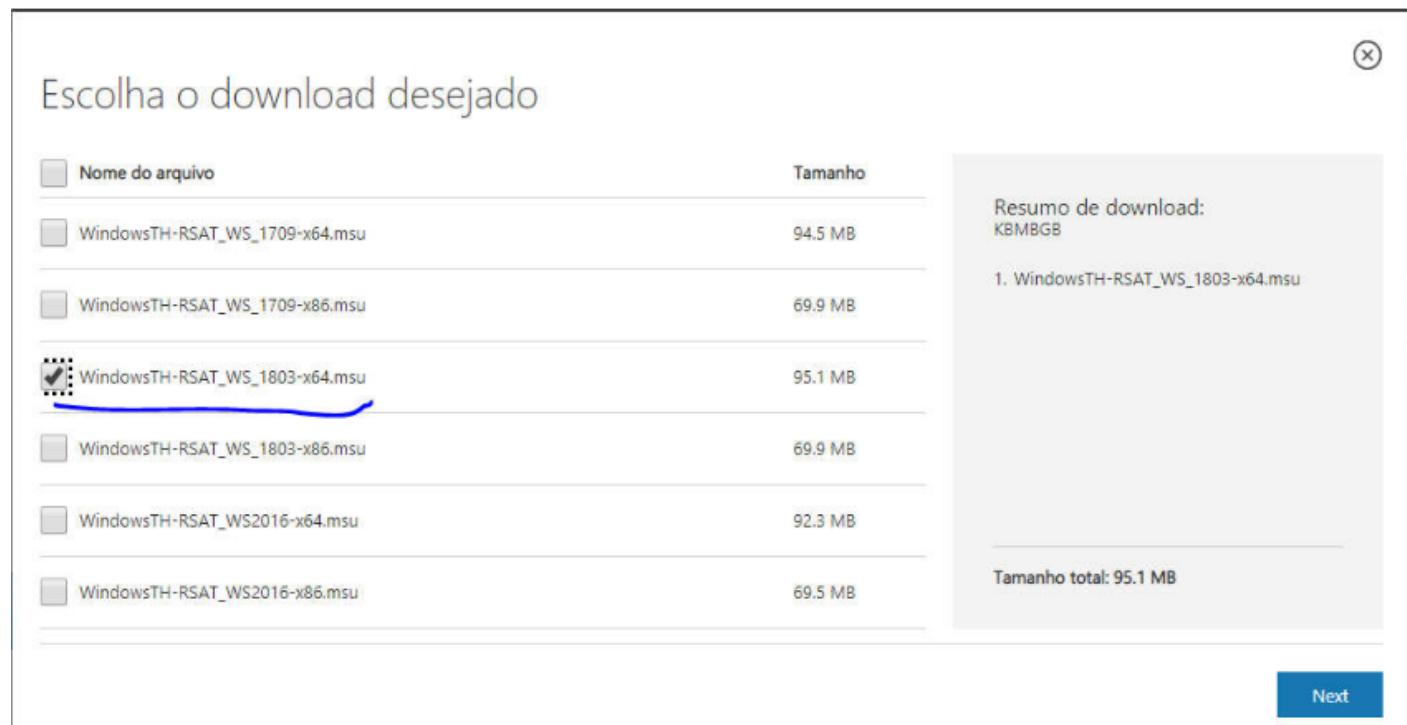


Instalar as Ferramentas de Administração de Servidor Remoto (RSAT):

Realizar o download do RSAT diretamente do portal da Microsoft pelo seguinte link:

https://download.microsoft.com/download/1/D/8/1D8B5022-5477-4B9A-8104-6A71FF9D98AB/WindowsTH-RSAT_WS_1803-x64.msu

Observação: caso o link pare de funcionar, basta pesquisar por RSAT e seguir até encontrar a seguinte tela:



The screenshot shows a download manager interface. On the left, a list of files is displayed with checkboxes. The file 'WindowsTH-RSAT_WS_1803-x64.msu' is checked and highlighted with a blue underline. On the right, a summary box shows the selected file and its total size.

Nome do arquivo	Tamanho
WindowsTH-RSAT_WS_1709-x64.msu	94.5 MB
WindowsTH-RSAT_WS_1709-x86.msu	69.9 MB
<input checked="" type="checkbox"/> WindowsTH-RSAT_WS_1803-x64.msu	95.1 MB
WindowsTH-RSAT_WS_1803-x86.msu	69.9 MB
WindowsTH-RSAT_WS2016-x64.msu	92.3 MB
WindowsTH-RSAT_WS2016-x86.msu	69.5 MB

Resumo de download:
KBMBGB

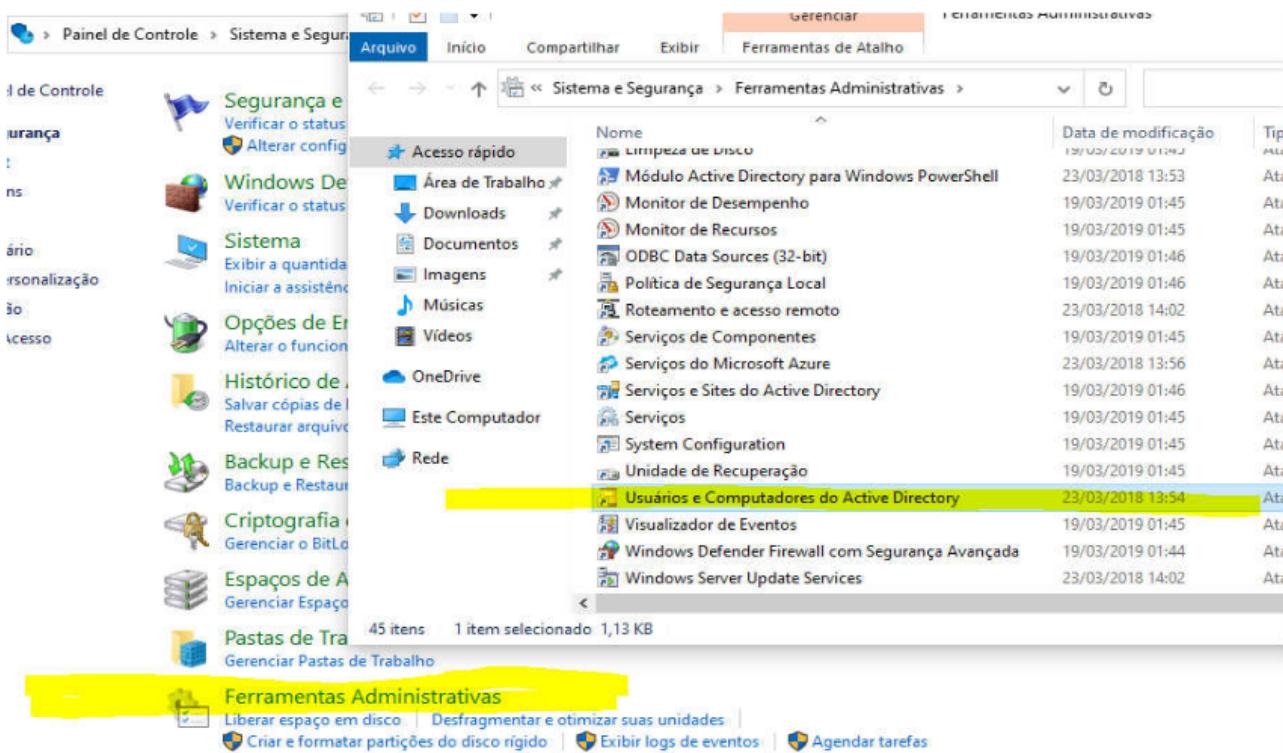
1. WindowsTH-RSAT_WS_1803-x64.msu

Tamanho total: 95.1 MB

Next

Executar e instalar o pacote do RSAT

Abrir a ferramenta “Usuários e Computadores do Active Directory”, localizada em: “Painel de Controle\Sistema e Segurança\Ferramentas Administrativas”

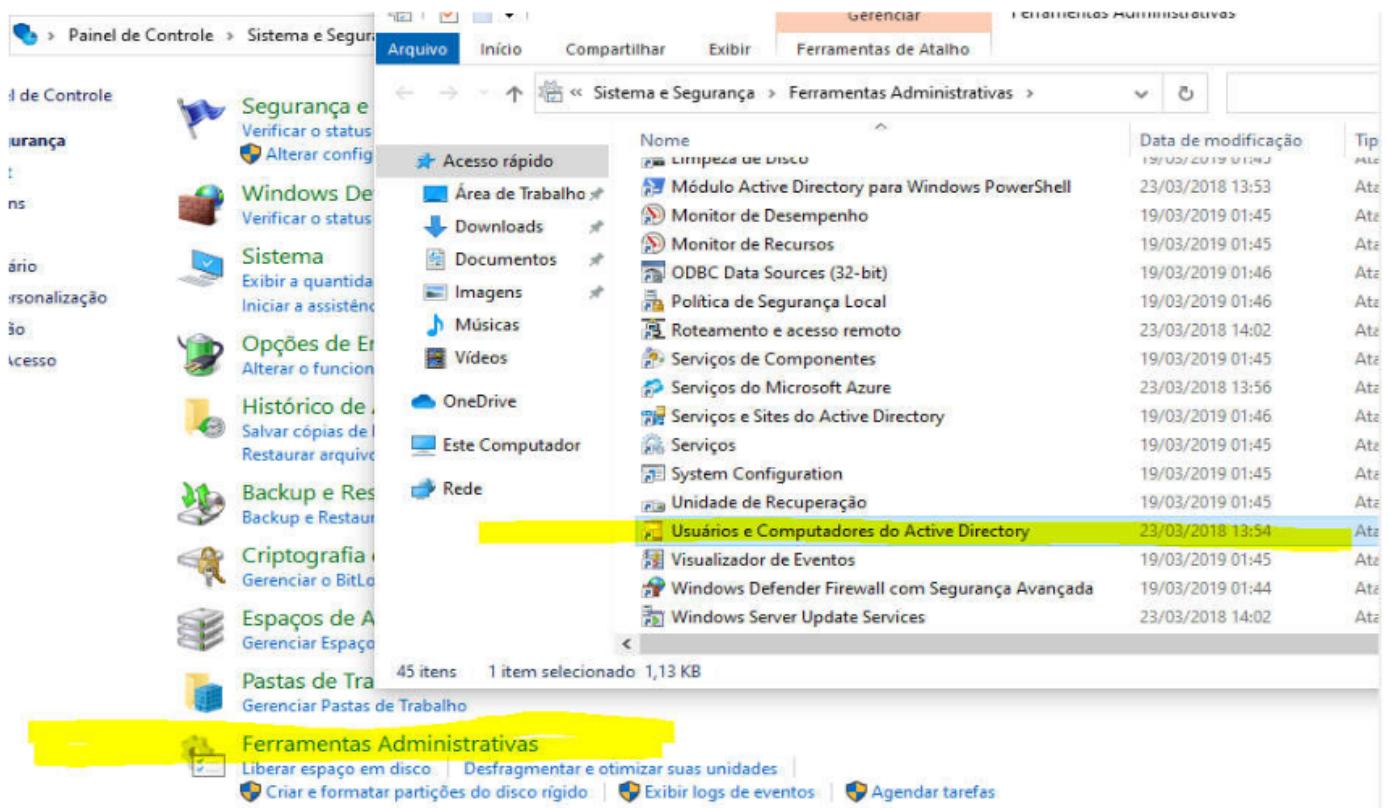


Ao abrir a ferramenta “Usuários e Computadores do Active Directory” será mostrada a seguinte tela, já com os recursos do domínio disponíveis para serem gerenciados e manuseados:

The screenshot shows the 'Usuários e Computadores do Active Directory' management console. The left pane displays a tree view of the Active Directory structure, including 'Consultas salvas', 'empresa.org' (with 'Domain Controllers', 'Users', 'Managed Service Accounts', 'Builtin', 'ForeignSecurityPrincipals', and 'Computers' children), and 'Read-only Domain Controllers'. The right pane is a table listing security groups:

Nome	Tipo	Descrição
Administrator	Usuário	Built-in account for ad...
Allowed RODC Password Repl...	Grupo de segurança - Domí...	Members in this group ...
Cert Publishers	Grupo de segurança - Domí...	Members of this group ...
Denied RODC Password Repl...	Grupo de segurança - Domí...	Members in this group ...
DnsAdmins	Grupo de segurança - Domí...	DNS Administrators Gro...
DnsUpdateProxy	Grupo de segurança - Global	DNS clients who are per...
Domain Admins	Grupo de segurança - Global	Designated administrato...
Domain Computers	Grupo de segurança - Global	All workstations and ser...
Domain Controllers	Grupo de segurança - Global	All domain controllers i...
Domain Guests	Grupo de segurança - Global	All domain guests
Domain Users	Grupo de segurança - Global	All domain users
Enterprise Admins	Grupo de segurança - Unive...	Designated administrato...
Enterprise Read-only Domain ...	Grupo de segurança - Unive...	Members of this group ...
Group Policy Creator Owners	Grupo de segurança - Global	Members in this group c...
Guest	Usuário	Built-in account for gue...
RAS and IAS Servers	Grupo de segurança - Domí...	Servers in this group ca...
Read-only Domain Controllers	Grupo de segurança - Global	Members of this group ...
Schema Admins	Grupo de segurança - Unive...	Designated administrato...

Essas ferramentas facilitam bastante o trabalho do administrador do domínio, visto que todas as operações são realizadas diretamente pelo Windows, inclusive, a criação ou alteração de contas de USUÁRIOS ou GRUPOS.



Ao abrir a ferramenta “**Usuários e Computadores do Active Directory**” será mostrada a seguinte tela, já com os recursos do domínio disponíveis para serem gerenciados e manuseados:



Configuração dos compartilhamentos – File Server

Configurar as bibliotecas do winbind:

Localizar a biblioteca "libnss_winbind.so.2"

```
# smbd -b | grep LIBDIR
```

192.168.50.4 - PuTTY

```
root@adLivre:~# smbd -b | grep LIBDIR
LIBDIR: /usr/lib/x86_64-linux-gnu
```

Configurar o uso das bibliotecas do winbind:

```
# ln -s /usr/lib/x86_64-linux-gnu/libnss_winbind.so.2 /usr/lib/x86_64-
linux-gnu/libnss_winbind.so
```

```
# ldconfig
```

192.168.50.4 - PuTTY

```
root@adLivre:~# ln -s /lib/x86_64-linux-gnu/libnss_winbind.so.2 /lib/x86_64-linux-gnu/libnss_winbind.so
root@adLivre:~#
root@adLivre:~# ldconfig
root@adLivre:~#
```

Configurar e testar o Name Service Switch:

Abrir o arquivo /etc/nsswitch

```
# nano /etc/nsswitch
```

Alterar os campos “passwd” e “group”

```
#(/etc/nsswitch)  
passwd: files winbind  
group: files winbind
```

Testar a conectividade com o Winbindd

```
# wbinfo --ping-dc
```

```
192.168.50.4 - PuTTY  
root@adLivre:~# wbinfo --ping-dc  
checking the NETLOGON for domain[EMPRESA] dc connection to "adlivre.empresa.org" succeeded  
root@adLivre:~#
```

```
# getent passwd EMPRESA\\Administrator  
# getent group "EMPRESA\\Domain Users"
```

```
192.168.50.4 - PuTTY  
root@adLivre:~# getent passwd EMPRESA\\Administrator  
EMPRESA\\administrator:*:0:100::/home/EMPRESA/administrator:/bin/false  
root@adLivre:~#  
root@adLivre:~# getent group "EMPRESA\\Domain Users"  
EMPRESA\\domain users:x:100:  
root@adLivre:~#
```

Criar e ajustar os diretórios compartilhados:

Criar o diretório e acertar as permissões

```
# mkdir /mnt/pastaSamba  
# chmod -v 777 /mnt/pastaSamba
```

```
192.168.50.4 - PuTTY  
root@adLivre:~# mkdir /mnt/pastaSamba  
root@adLivre:~#  
root@adLivre:~# chmod -v 777 /mnt/pastaSamba  
modo de '/mnt/pastaSamba' alterado de 0755 (rwxr-xr-x) para 0777 (rwxrwxrwx)  
root@adLivre:~#
```

Observação: a permissão para o diretório ser configurada em com a máscara 777, visto que o controle de segurança será realizado pelo uso das ACLs.

Conceder privilégios para configurar ACLs por meio do Windows

```
# net rpc rights grant "EMPRESA\Administrator" SeDiskOperatorPrivilege
-U "EMPRESA\Administrator"
```

Testar a conectividade com o Winbindd

```
# wbinfo --ping-dc
```

```
192.168.50.4 - PuTTY
root@adLivre:~# wbinfo --ping-dc
checking the NETLOGON for domain[EMPRESA] dc connection to "adlivre.empresa.org" succeeded
root@adLivre:~#
```

```
# getent passwd EMPRESA\\Administrator
```

```
# getent group "EMPRESA\\Domain Users"
```

```
192.168.50.4 - PuTTY
root@adLivre:~# getent passwd EMPRESA\\Administrator
EMPRESA\administrator:*:0:100::/home/EMPRESA/administrator:/bin/false
root@adLivre:~#
root@adLivre:~# getent group "EMPRESA\\Domain Users"
EMPRESA\domain users:x:100:
root@adLivre:~#
```

Criar e ajustar os diretórios compartilhados:

Criar o diretório e acertar as permissões

```
# mkdir /mnt/pastaSamba
```

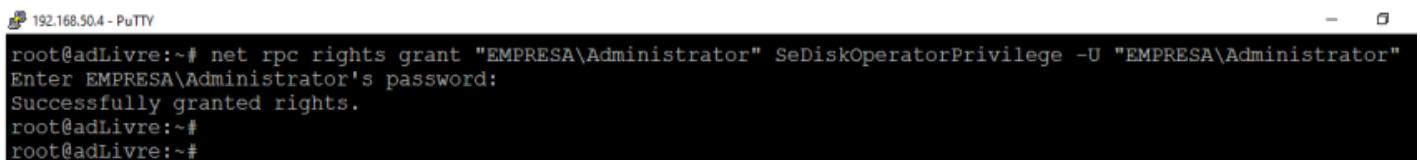
```
# chmod -v 777 /mnt/pastaSamba
```

```
192.168.50.4 - PuTTY
root@adLivre:~# mkdir /mnt/pastaSamba
root@adLivre:~#
root@adLivre:~# chmod -v 777 /mnt/pastaSamba
modo de '/mnt/pastaSamba' alterado de 0755 (rwxr-xr-x) para 0777 (rwxrwxrwx)
root@adLivre:~#
```

Observação: a permissão para o diretório ser configurada em com a máscara 777, visto que o controle de segurança será realizado pelo uso das ACLs.

Conceder privilégios para configurar ACLs por meio do Windows

```
# net rpc rights grant "EMPRESA\Administrator" SeDiskOperatorPrivilege  
-U "EMPRESA\Administrator"
```



```
192.168.50.4 - PuTTY  
root@adLivre:~# net rpc rights grant "EMPRESA\Administrator" SeDiskOperatorPrivilege -U "EMPRESA\Administrator"  
Enter EMPRESA\Administrator's password:  
Successfully granted rights.  
root@adLivre:~#  
root@adLivre:~#
```

Consultar os privilégios concedidos:

```
# net rpc rights list privileges SeDiskOperatorPrivilege -U  
"EMPRESA\Administrator"
```

Revogar privilégios

```
# net rpc rights revoke "EMPRESA\Administrator"  
SeDiskOperatorPrivilege -U "EMPRESA\Administrator"
```

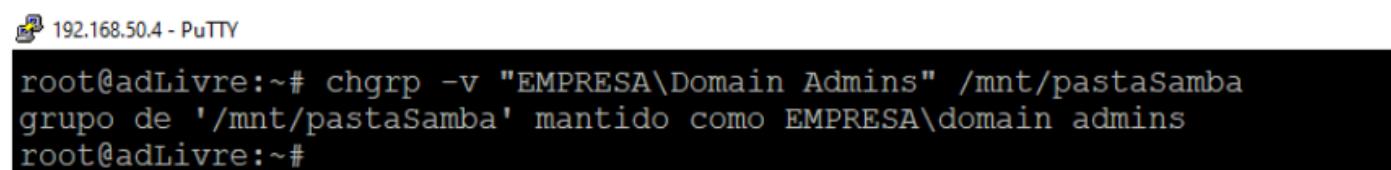
Definir grupo dono da pasta (necessário para que utilize as permissões ACLs)

```
# chgrp -v "EMPRESA\Domain Admins" /mnt/pastaSamba
```

Criar e ajustar os diretórios compartilhados:

Criar o diretório e acertar as permissões

```
# mkdir /mnt/pastaSamba  
# chmod -v 777 /mnt/pastaSamba
```



```
192.168.50.4 - PuTTY  
root@adLivre:~# chgrp -v "EMPRESA\Domain Admins" /mnt/pastaSamba  
grupo de '/mnt/pastaSamba' mantido como EMPRESA\domain admins  
root@adLivre:~#
```

Ajustar o "smb.conf" para rodar os diretórios compartilhados:

Criar o diretório no smb.conf

```
# nano /etc/samba/smb.conf
```

```
[Compartilhamento]
path = /mnt/pastaSamba
read only = no
```

Observação: Inserir esses valores no final do arquivo

Habilitar o suporte à ACL estendida (inserir na Seção Global do smb.conf)

```
vfs objects = acl_xattr
map acl inherit = yes
# the next line is only required on Samba versions less than 4.9.0
store dos attributes = yes
```

Terminada a configuração o arquivo /etc/samba/smb.conf deverá ficar conforme o preenchido abaixo:

```
# Global parameters
[global]
dns forwarder = 192.168.50.1
netbios name = ADLIVRE
realm = EMPRESA.ORG
server role = active directory domain controller
workgroup = EMPRESA
idmap_ldb:use rfc2307 = yes
ldap server require strong auth = no
```

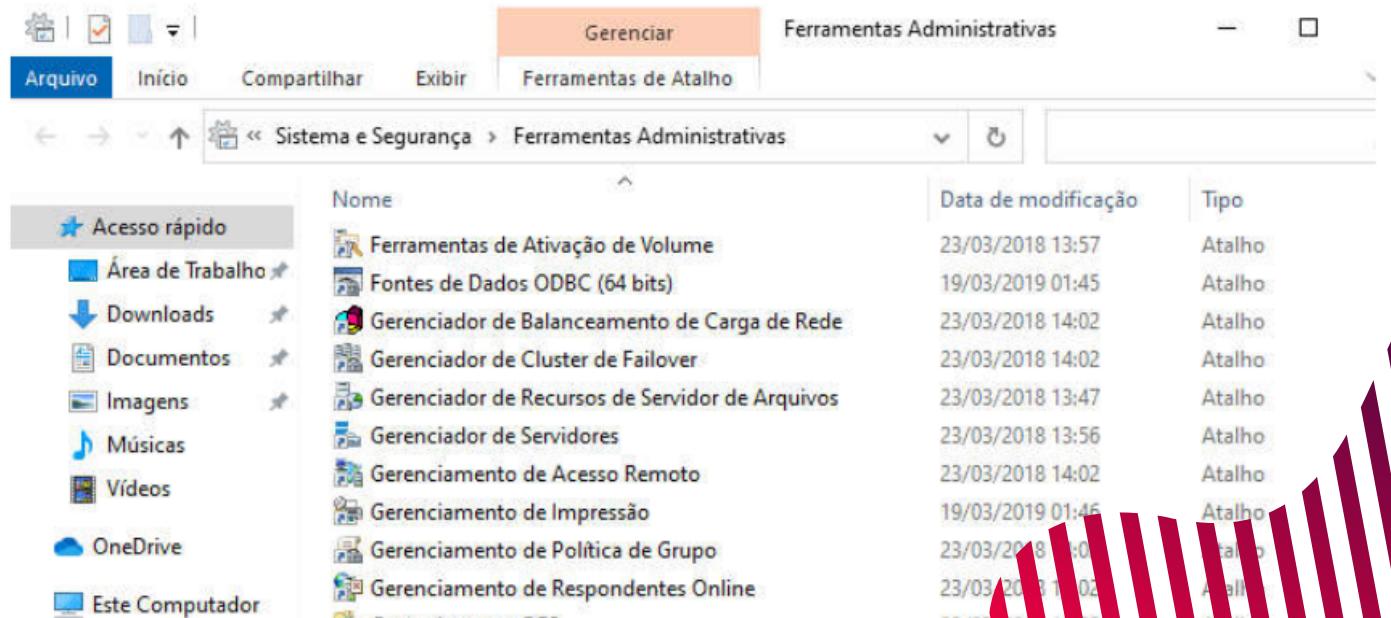
```
vfs objects = acl_xattr
map acl inherit = yes
# the next line is only required on Samba versions less than 4.9.0
store dos attributes = yes
[netlogon]
path = /var/lib/samba/sysvol/empresa.org/scripts
read only = No
[sysvol]
path = /var/lib/samba/sysvol
read only = No
[Compartilhamento]
path = /mnt/pastaSamba
read only = no
```

Recarregar as configurações

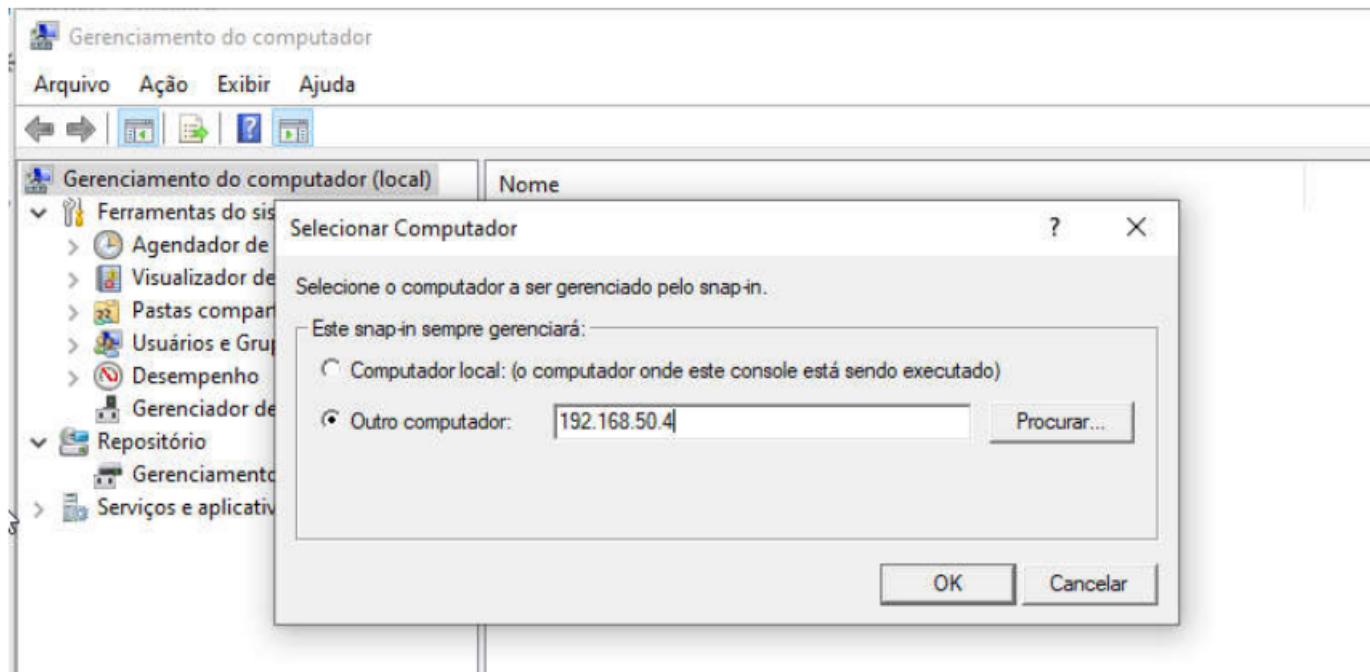
```
# smbcontrol all reload-config
```

Ajustar as permissões com o uso das ACLs estendidas:

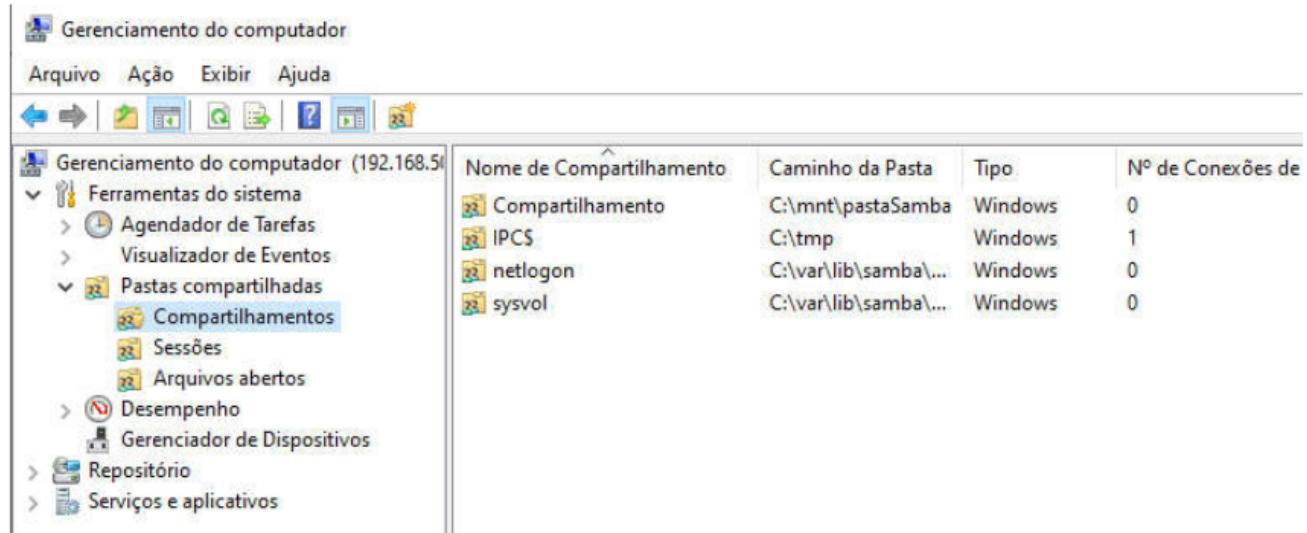
As configurações dos recursos das ACLs estendidas são feitas por meio do recurso “Gerenciamento do Computador” do Windows, que também consta em “Ferramentas Administrativas”.



Ao abrir a tela clique como o botão direito do mouse em: do Gerenciamento do Computador (local) e escolha: Conectar a outro computador e digite o endereço IP do Servidor Samba 4.



Em seguida, expandir Ferramentas do sistema >> Pastas compartilhadas >> Compartilhamentos (caso apareça um erro, basta ignorá-lo)

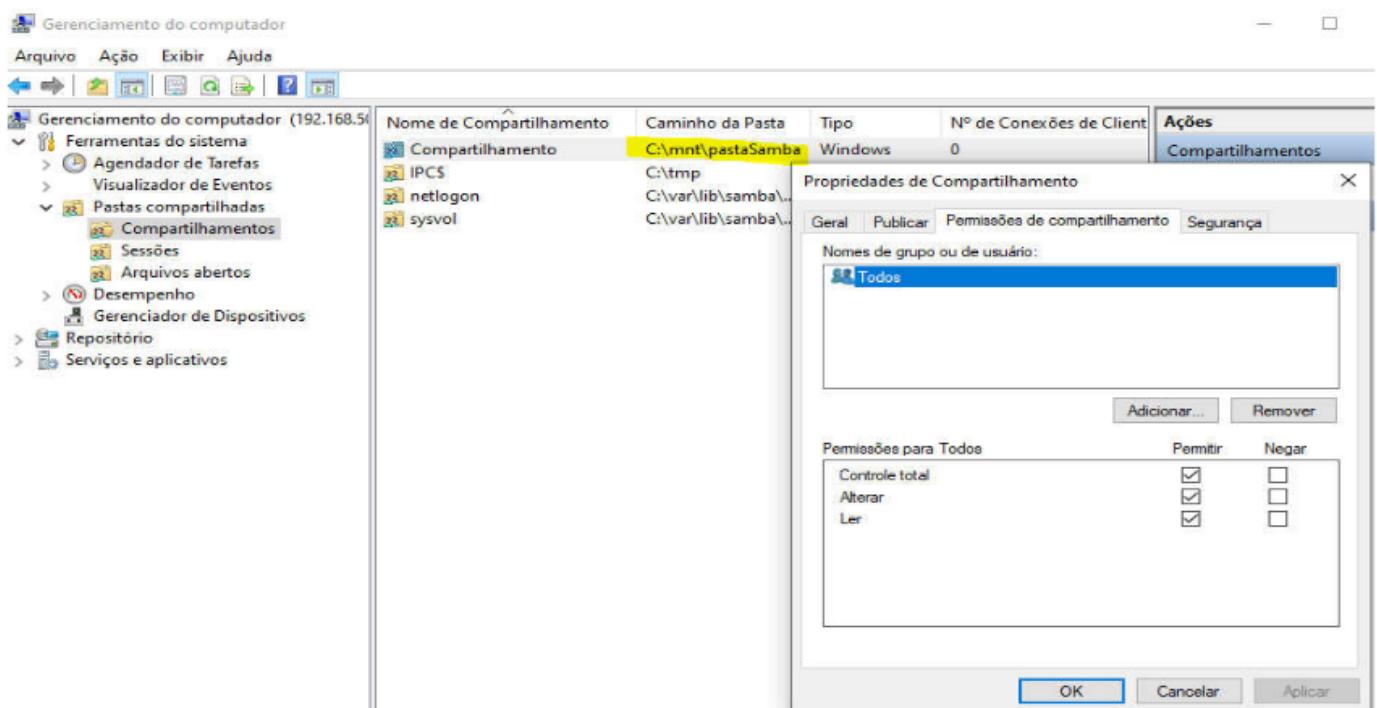


Nesse local temos a nossa pasta “Compartilhamento”, na qual poderemos realizar as configurações de permissões NTFS.

Podemos definir permissões da mesma forma como são definidas em um ambiente de Windows Server com o Active Directory.

Observação: Todas as vezes que houver necessidade de conceder ou alterar privilégios em diretórios compartilhados é importante que essa operação seja realizada pelo usuário Administrator ou algum outro que tenha sido concedido os privilégios de SeDiskOperatorPrivilege, conforme configuração já realizada anteriormente.

Permissões de compartilhamento:



Permissões NTFS (essas são as regras de segurança que são mantidas pelos recursos de ACLs estendidas):

The screenshot shows the Windows Server 2012 Shared Folders Properties dialog box. The 'Segurança' (Security) tab is selected. The 'Nome do objeto:' field contains '\\192.168.50.4\Compartilhamento'. The 'Nomes de grupo ou de usuário:' list includes 'GRUPO CRIADOR', 'Administrator', and 'Domain Admins (EMPRESA\Domain Admins)', with 'Domain Admins' highlighted. The 'Permissões para Domain Admins' table shows the following permissions: 'Controle total', 'Modificar', 'Ler & executar', 'Listar conteúdo da pasta', and 'Leitura'. The 'Avançadas' (Advanced) button is visible at the bottom right. The background shows the Windows Server 2012 Control Panel with the 'Pastas compartilhadas' (Shared Folders) option selected.

Nome de Compartilhamento	Caminho da Pasta	Tipo	Nº d
Compartilhamento	C:\mnt\pastaSamba	Windows	0
IPC\$	C:\tmp	Windows	1
netlogon	C:\var\lib\samba\...	Windows	0
sysvol	C:\var\lib\samba\...	Windows	0

Para trabalhar com as permissões do Compartilhamento e também com as permissões de segurança do NTFS basta acessar conforme demonstrado nos passos anteriores e aplicar as concessões nos dois níveis de segurança sem a necessidade de acessar diretamente o Servidor Linux para configurar qualquer permissão de usuário ou grupo.

Configurações das opções de senhas

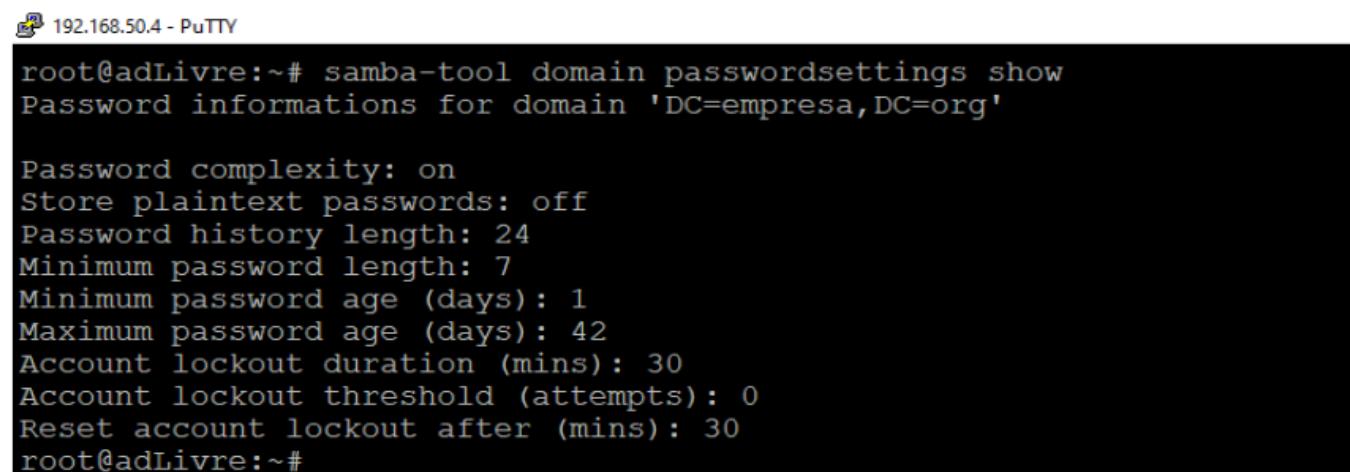
Esses recursos definem as políticas de senhas que poderão ser utilizadas no domínio e deverão ser definidas conforme as políticas de cada organização.

Observação: a política inicial implantada pelo Domínio Samba 4 é bem restritiva e em alguns casos a complexidade padrão das senhas não agrada em algumas corporações. Nesse caso recomenda-se desativar ou trabalhar uma forma de complexidade de atenda à organização.

Seguem abaixo as políticas básicas que podem ser definidas no Domínio de Rede mantido pelo Servidor Samba 4:

Verificar as configurações de políticas de senha

```
# samba-tool domain passwordsettings show
```



```
192.168.50.4 - PuTTY
root@adLivre:~# samba-tool domain passwordsettings show
Password informations for domain 'DC=empresa,DC=org'

Password complexity: on
Store plaintext passwords: off
Password history length: 24
Minimum password length: 7
Minimum password age (days): 1
Maximum password age (days): 42
Account lockout duration (mins): 30
Account lockout threshold (attempts): 0
Reset account lockout after (mins): 30
root@adLivre:~#
```

Desabilitar expiração de Senha de administrador no Samba 4.

```
# samba-tool user setexpiry administrator --noexpiry
```

Definir quantos dias a senha do administrador expirará no Samba 4.

```
# samba-tool user setexpiry --days=20 Administrator
```

Desabilitar complexidade de senha no Samba 4

```
# samba-tool domain passwordsettings set --complexity=off
```

Desabilitar o histórico de senha no Samba 4.

```
# samba-tool domain passwordsettings set --history-length=0
```

Desabilitar idade mínima de senha.

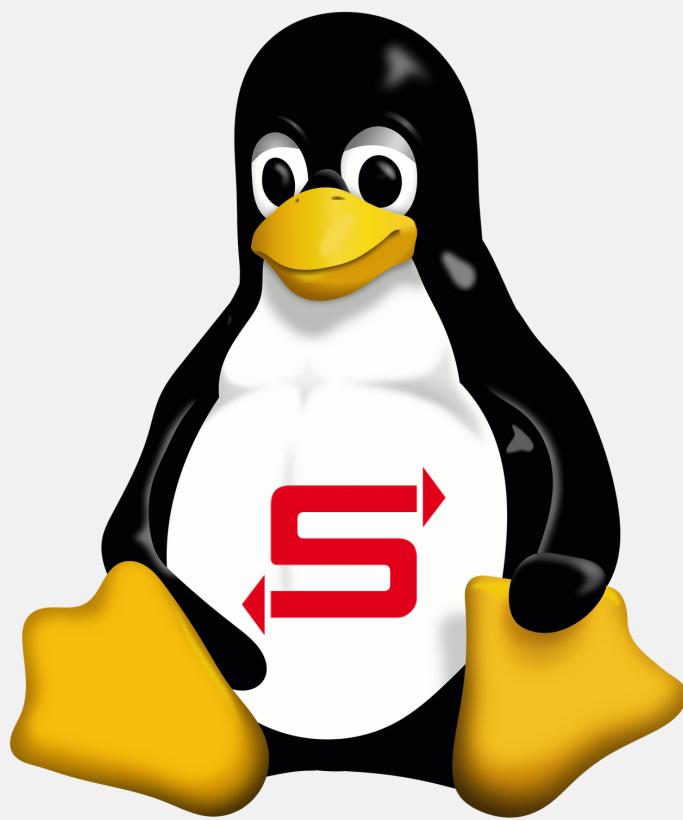
```
# samba-tool domain passwordsettings set --min-pwd-age=0
```

Desabilitar idade máxima da senha no Samba 4.

```
# samba-tool domain passwordsettings set --max-pwd-age=0
```

Desabilitar tamanho mínimo da senha no Samba 4.

```
# samba-tool domain passwordsettings set --min-pwd-length=0
```





Método Active Directory Linux PRO

RENDA EXTRA COM O LINUX

O que é esse método, é um curso completo com mais **6 bônus exclusivos** para você garantir o seu aprendizado mais **rápido e ter todo o suporte necessário** para fazer suas implementações de servidor com SAMBA 4 e Pfsense. Faturando com o Linux.

Bônus do método:

- 1. Curso de Backups inteligentes**
- 2. Curso de Pfsense Firewall/UTM**
- 3. Monitoramento de Servidores**
- 4. Curso Linux/GNU do Zero**
- 5. Super Script de automação desse sistema completo**
- 6. Comunidade ativa de profissional SAMBA 4**

Para saber mais sobre o método clique no botão abaixo.

Quero saber mais agora



Método Active Directory Linux PRO

CENÁRIO DO MÉTODO

GPO
Gerenciamento de usuário e grupos
Administração centralizada
Automação
Ganho de produtividade
Fácil gerenciamento
Interface fácil
Política de senhas

Você configurando



Controle de armazenamento
dos usuários da rede.

Servidor Linux com SAMBA 4

Conexão SSH com Servidor



Usuários Windows acessando arquivos
no servidor Linux.

- Painel de controle bloqueado
- cmd bloqueado
- Horário de funcionamento das 9h às 16h
- Sites pornográficos bloqueados

Novos usuários herdaram as configurações
ao entrar no domínio.

Quero saber mais agora