UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZAÇÃO SEMIPRESENCIAL EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

FRANK DAMINELLI FREY

GESTÃO CENTRALIZADA DE SERVIDORES EM REDES COMPUTACIONAIS

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA
2018

FRANK DAMINELLI FREY

GESTÃO CENTRALIZADA DE SERVIDORES EM REDES COMPUTACIONAIS

Monografia de Especialização, apresentada ao Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientador: Prof. Dr. Kleber Kendy Horikawa Nabas

CURITIBA

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes

TERMO DE APROVAÇÃO

GESTÃO CENTRALIZADA DE SERVIDORES EM REDES COMPUTACIONAIS

por

FRANK DAMINELLI FREY

Esta monografia foi apresentada em 23 de novembro de 2018 como requisito parcial para a obtenção do título de Especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Orientador

_____
Prof. Dr. Edenilson José da Silva
Membro titular

_____
Prof. M.Sc. Omero Francisco Bertol
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho à Deus, meu Pai e minha Avó.

AGRADECIMENTOS

A DEUS acima de tudo.

Agradeço também ao meu amigo e orientador Prof. Dr. Kleber Kendy Horikawa Nabas, pela sabedoria com que me guiou nesta trajetória.

Enfim, a todos aqueles que por algum motivo contribuíram para a realização desta pesquisa.

RESUMO

FREY, Frank Daminelli. **Gestão centralizada de servidores em redes computacionais.** 2018. 35 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Com o passar dos tempos o tempo vem ficando cada vez mais escasso e valioso, as pessoas trabalham mais e precisam ser mais rápidas e para isso o acesso a informação também tem que ser mais rápidas, esse trabalho tem como objetivo buscar alternativas ao Microsoft Active Directory. Assim foi realizado uma pesquisa mais a profunda sobre o que é o Active Directory e quais seriam suas possíveis alternativas e descobrimos que existe diversas alternativas, pois o AD é uma plataforma de gestão que utiliza protocolos padrões, como LDAP, Kerberos, SMB, entre outros. Assim foi possível encontrar e realizar os estudos necessários para concluirmos que existem alternativas as ferramentas proprietárias.

Palavras-chave: LDAP. Centralização. Autenticação. Controle de Acesso. Samba.

ABSTRACT

FREY, Frank Daminelli. **Centralized management of servers in computer networks**. 2018. 35 p. Monografia de Especialização em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2018.

Over time, time has become increasingly scarce and valuable, people work harder and need to be faster, and access to information has to be faster as well, and this work aims to look for alternatives to Microsoft Active Directory . So we did a more in-depth research on what Active Directory is and what its possible alternatives would be and we discovered that there are several alternatives, since AD is a management platform that uses standard protocols such as LDAP, Kerberos, SMB, among others . Thus it was possible to find and carry out the necessary studies to conclude that there are alternatives to the proprietary tools.

Keywords: LDAP. Centralization. Autentication. Access Control. Samba.

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE SIGLAS

AD	*Active Directory* (ou Diretório Ativo)
ARC4	*Alleged RC4*, algoritmo simétrico de criptografia de fluxo
CAL	*Client Access License* (ou Licença de acesso ao cliente)
CLI	*Comand-Line Interface* (ou Interface de Linha de Comando)
DAP	*Directory Access Protocol* (ou Protocolo de Acesso a Diretório)
DC	*Domain Control* (ou Controlador de Domínio)
DHCP	*Dynamic Host Configuration Protocol* (ou Protocolo de Configuração Dinâmica de Host)
DNS	*Domain Name System* (ou Sistema de Nome de Domínio)
FQDN	*Fully Quallified Domain Name* (ou Domínio Completamente Expressado)
GPO	*Group Policy Object* (ou Objeto de Política de Grupo)
GUI	*Graphical User Interface* (ou Interfaces Gráficas de Usuários)
IP	*Internet Protocol* (ou Protocolo de Internet)
LDAP	*Lightweight Directory Access Protocol*
MIT	*Massachussets Institute of Technology*
OpenLDAP	*Open Lightweight Directory Access Protocol*
OSI	*Open Systems Interface*
OU	*Organization Unit* (ou Unidade Organizacional)
RC4	Algoritmo simétrico de criptografia de fluxo
TCP/IP	*Transmission Control Protocol / Internet Protocol* (ou Protocolo de Controle de Transmissão / Protocolo de Internet)
TI	Tecnologia de Informação

SUMÁRIO

1 INTRODUÇÃO

Diariamente a tecnologia vem se expandindo e as redes computacionais não poderia ficar de fora, que por sua vez demanda de uma grande necessidade de gerenciamento, segurança, disponibilidade entre outros quesitos.

Por essas necessidades é que existem diversas soluções para implementação, gestão e manutenção da sua rede buscando uma maior eficiência no atendimento do seu cliente, buscando suprir suas necessidades visando a facilitar as rotinas do dia a dia.

Para isso conta-se com ferramentas como o Active Directory da Microsoft ferramenta essa que vem acoplada nas versões de servidores da Microsoft desde a versão do Windows Server 2000 até as mais recentes. Para os sistemas UNIX, Linus e BSD pode-se contar com a ferramenta Samba ou OpenLDAP.

Tanto o AD como o Samba, o OpenLDAP o Sistema Librix AD, o OpenDS (OPENDS, 2018), OpenDJ (OPENDJ, 2018), permitem a interoperabilidade entre diversos sistemas operacionais pois utilizam o protocolo *Lightweight Directory Access Protocol* (LDAP), assim permitindo que se utilize servidores proprietários ou não como estações clientes da mesma maneira ou ainda sistemas mistos, podendo todas essas se comunicarem entre si além de acessar os recursos disponíveis na rede conforme as permissões ou negações determinadas pelas regras aplicadas.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Tendo como objetivo criar a interoperabilidade entre sistemas operacionais para aumentar a segurança das redes de computadores além de dificultar os acessos indevidos e não autorizados, ainda amenizando a incidência de vírus na rede e baixando custos de se ter um servidor proprietário em média e pequena empresa, assim utiliza-se como base servidor Linux pela sua robustez, segurança e baixo custo, e utiliza-se clientes Windows pela praticidade e facilidade na utilização e das ferramentas para os usuários finais.

1.1.2 Objetivos Específicos

Explanar a importância e a praticidade da gerencia de um servidor usando LDAP seja este em Linux, Windows, OpenDS (descontinuado), Librix AD (descontinuado), OpenDJ, ou qualquer sistema operacional. Para isso é necessário instalar e configurarar os seguintes serviços *Domain Name System* (DNS, ou Sistema de Nome de Domínio), *Dynamic Host Configuration Protocol* (DHCP, ou Protocolo de Configuração Dinâmica de Host), Kerberos, assim como outras ferramentas que trabalham em conjunto para facilitar a sua gestão.

1.2 JUSTIFICATIVA

O assunto abordado neste trabalho é de suma importância para as empresas buscando melhorar e facilitar a administração da sua rede pela gestão centralizada de seus servidores com a autenticação de usuários, aumentando a segurança com disponibilidade e replicação de dados. Além de facilitar outras necessidades que não serão abordadas em nossa pesquisa como as rotinas de backup.

2 REFERENCIAL TEÓRICO

2.1 O QUE É UM SERVIÇO DE DIRETÓRIO

Um serviço de diretório pode ser comparado com uma lista telefônica ou uma agenda pessoal. Nas agendas pode-se organizar, as horas, os dias, as semanas, os meses e até os anos, ou organizar por pessoa, nomes, sobrenomes, datas de aniversário, entre outros dados importantes (ROVER, 2012).

O serviço de diretório tem exatamente o mesmo sentido, o sentido de organizar e principalmente ter um local centralizado para a busca de informações necessárias no dia a dia, para nossos trabalhos (ROVER, 2012).

Quando cria um novo usuário, utilizando o serviço de diretório, nesta base de dados como em uma agenda, está por sua vez guarda os nomes, sobrenomes, endereços, logins, senhas, grupo(s) ao qual o usuário pertence dentre outras tantas opções que pode-se cadastrar, tudo isto ficará disponível dentro de uma base de dados o qual utilizara esses dados pelo(s) servidores para vários serviços o qual o usuário tenha sua permissão de acesso (ROVER, 2012).

Pode-se citar algumas soluções de serviço de diretório “Active Directory” para Sistemas Microsoft; EDirectory para Sistemas Novell; OpenLDAP, Samba para Sistemas Open Source.

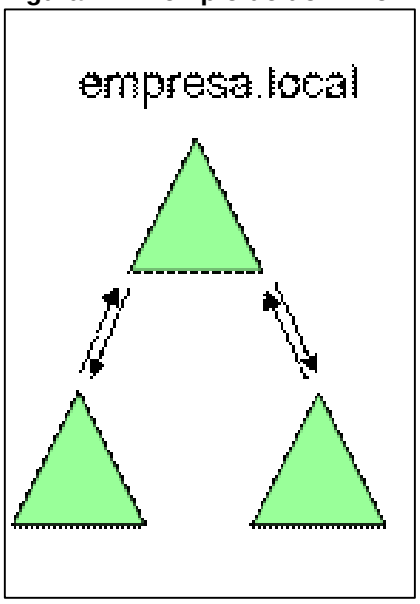
Nos dias de hoje as empresas precisam ter informações rápidas, atualizadas, com alta disponibilidade e com segurança o que pode ser proporcionado ao se utilizar uma rede em domínio com um sistema gerenciado pelo LDAP pode nos oferecer todos estes atributos e muito mais (ROVER, 2012).

2.2 DOMÍNIO

Para se configurar uma rede com uma gerencia centralizada é necessário se ter um domínio, que esse por sua desempenha um papel de suma importância, tendo como principal função limitar ou conceder acessos. Se uma determinada pessoa não detém um usuário no domínio logo não terá acesso, e por sua vez o usuário que tenha uma negação atribuída a um determinado recurso, não o terá salve alteração de diretivas administrativas no controlador LDAP. Com isso pode-se concluir que é criada

uma relação de confiança conforme mostrada na Figura 1, com diretivas de segurança. Essa relação de confiança pode ser entre servidor e estações ou entre servidores (outros domínios) (BATTISTI, 2018).

Figura 1 - Exemplo de domínio



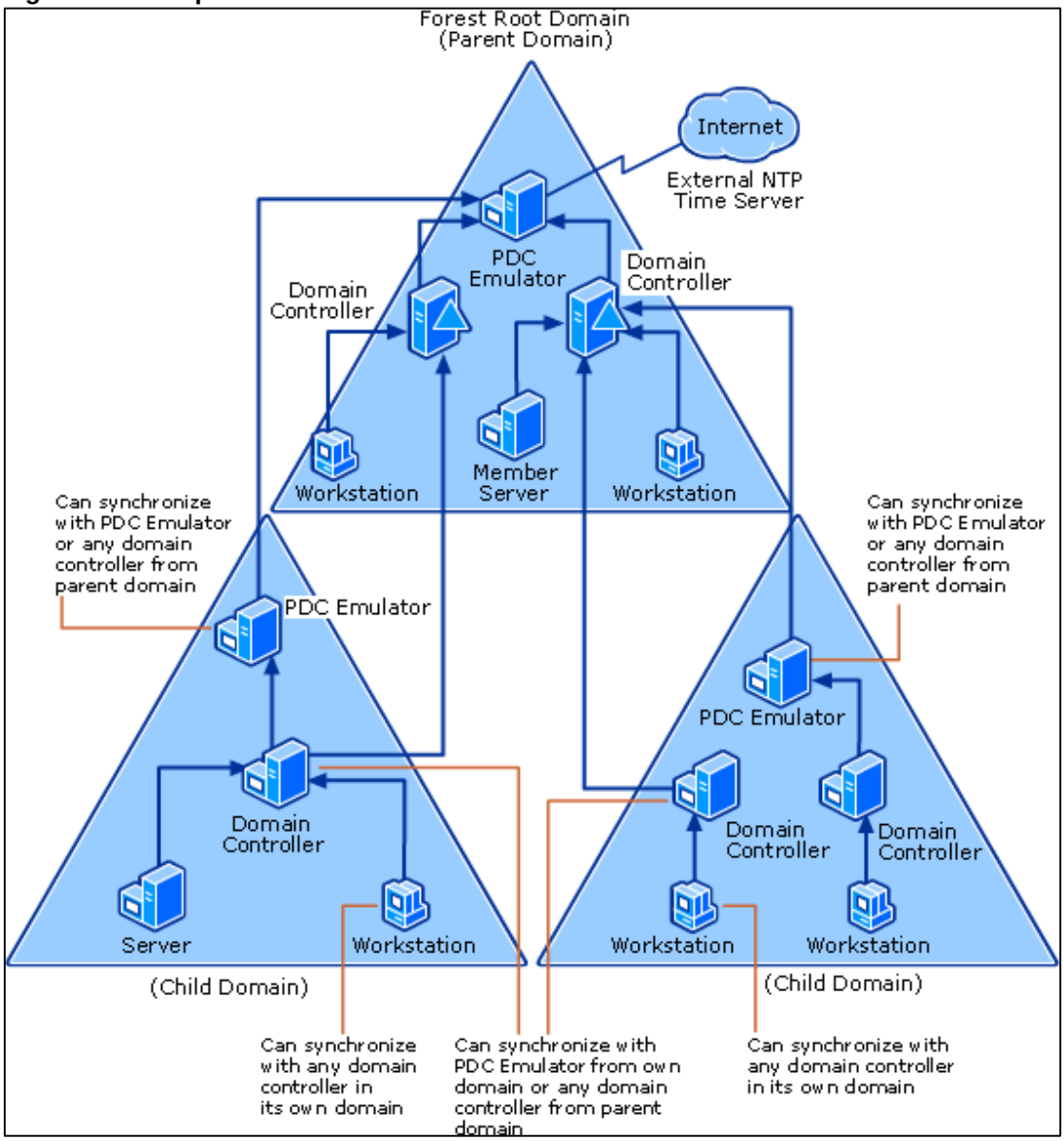
Fonte: Battisti (2018).

2.3 FLORESTA

Nada mais é do que um conjunto de árvores de uma empresa conforme pode-se verificar na Figura 2, que por sua vez delimitam e empregam diretivas no ambiente em relação aos controladores de domínio. Através das florestas pode-se efetuar as relações de confiança para os compartilhamentos de dados entre a matriz e suas filiais. Na floresta pode-se delimitar a segurança das informações contidas controlador LDAP, tornando o esquema único (ROVER, 2012).

O primeiro domínio de uma Floresta é chamado de domínio principal, assim está Floresta receberá o nome deste domínio, a floresta pode ser feita de um único domínio como também estar dividida com várias árvores dentro da mesma floresta, formando uma hierarquia (ROVER, 2012).

Figura 2 - Exemplo de floresta

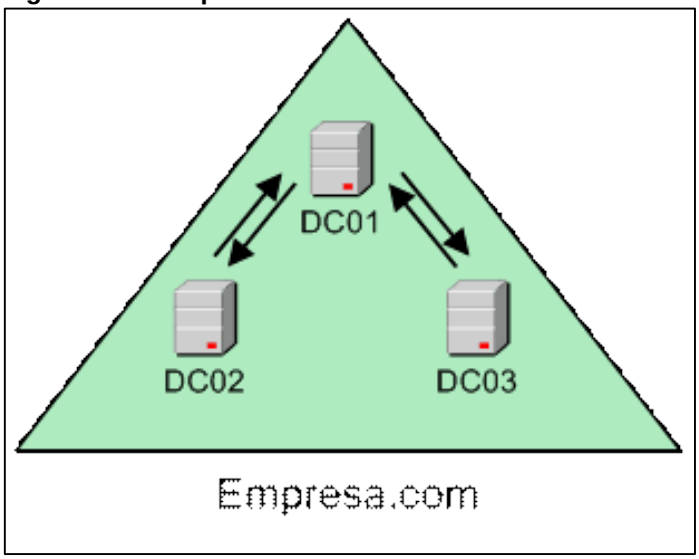


Fonte: Rover (2012).

2.4 CONTROLADOR DE DOMÍNIO

Um servidor quando na modalidade de controlador de domínio (ou *Domain Control* - DC) é encarregado de efetuar a gestão dos usuários dentro de uma rede, que por sua vez realiza as autenticações dos usuários, assim como replicação de dados entre outros controladores de domínio se assim delegados. É necessário no mínimo um controlador de domínio em uma rede, para que se possa ter um serviço de diretório instalado e funcional. Porém vale ressaltar que pode-se ter vários controladores de domínios em réplicas conforme pode-se verificar na Figura 3 mais somente um domínio na mesma floresta (ROVER, 2012).

Figura 3 - Exemplo de controlador de domínio



Fonte: Battisti (2018).

No Windows o “Active Directory” cria o arquivo NTDS.dit que é o seu banco de dados, esse por sua vez armazena os nomes de usuários, *logons*, *scripts* de *logon*, grupos aos quais o usuário pertence, horário permitido de acesso, entre muitas outras funcionalidades, assim este arquivo requer uma certa segurança o que o faz ser criptografado com o sistema de criptografia RC4, que geram chaves de 2048 bits para maior segurança e integridade da rede e seus dados (ROVER, 2012).

No Samba também tem-se um banco de dados com o algoritmo simétrico de criptografia RC4 ou ARC4 (SAMBA, 2018).

2.5 ESTRUTURA

Os serviços de diretórios são divididos basicamente em duas estruturas: as estruturas físicas e as estruturas logicas. As físicas otimizam os tráfegos de rede e logon, assim como determinam como e quando deverá ocorrer a sua replicação (se houver mais de um *Domain Control* - DC). A estrutura lógica consiste na arvore de domínio, domínio, floresta, objetos e unidades organizacionais (BATTISTI, 2018).

2.5.1 Objetos

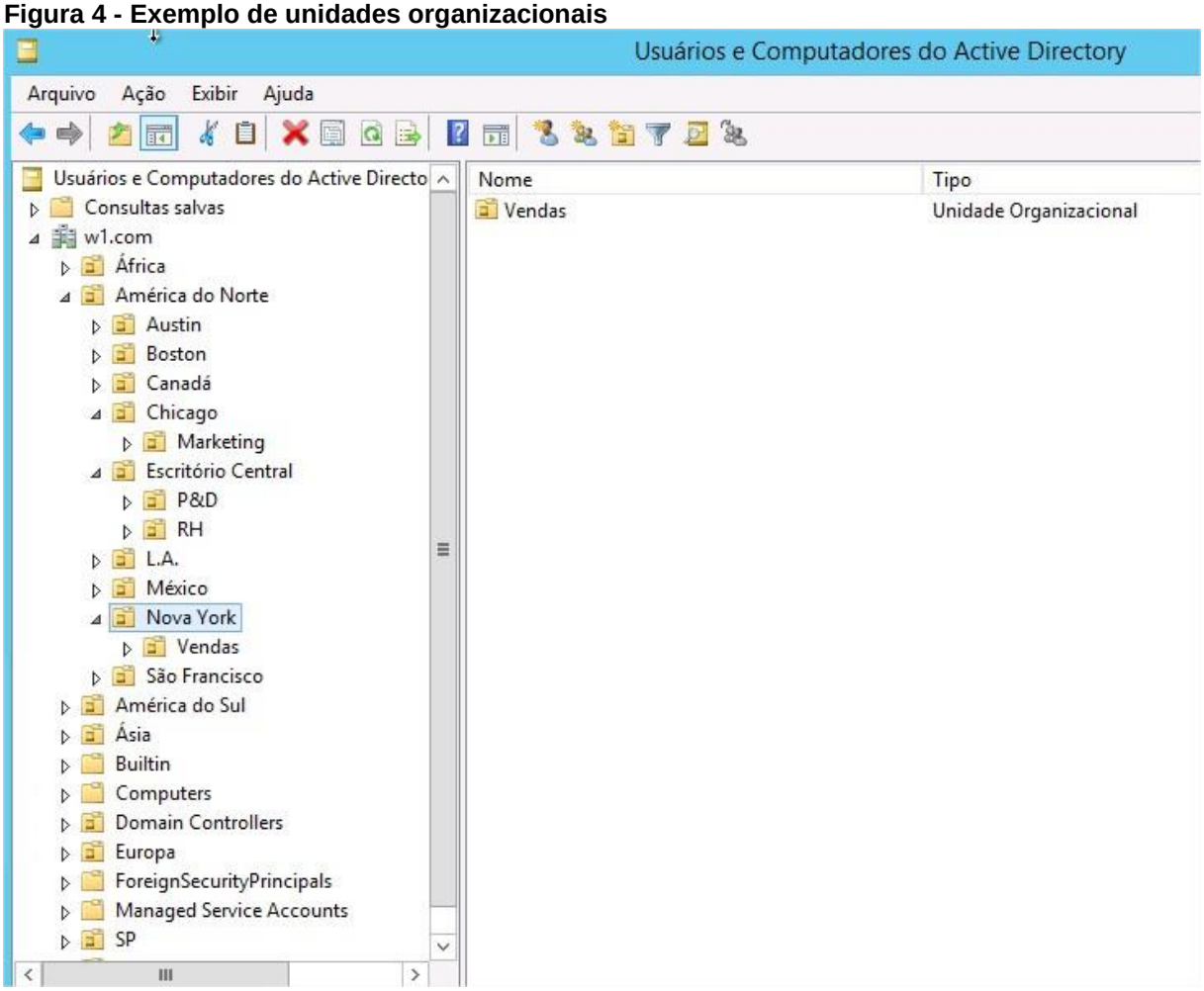
Esses são os componentes mais básicos da estrutura lógica. Os objetos de um domínio são: a) os computadores, b) as impressoras, e c) os usuários (ROVER, 2012).

2.5.2 Unidades Organizacionais

Uma unidade organizacional ou simplesmente “OU” é um objeto do tipo container que é utilizado para organizar os objetos conforme pode-se verificar na Figura 4, pondendo essa ser de várias maneiras, sendo elas (ROVER, 2012):

- Departamentais: representando setores físicos de uma determinada empresa como por exemplo: ADM, RH, entre outros.
- Geográfica: representado por cidades, estados, municípios ou mesmo países.
- Hibridas: esse mescla os demais tipos podendo se Geográfico, Departamental e/ou Setorial.
- Setorial: representando os setores físicos de uma determinada empresa como por exemplo: administrativo, contábil, diretoria, financeiro, entre outros.

Figura 4 - Exemplo de unidades organizacionais



Fonte: Autoria própria.

Segundo Battisti e Lima (2017), as OU’s podem ser utilizadas para separar os objetos em comum para a aplicação de determinadas diretivas de grupos, as *Group Policy Object* (GPO, ou Objeto de Política de Grupo).

2.6 LDAP

O LDAP é o protocolo de acesso aos diretórios do tipo X.500, seu serviço de diretório segue o modelo *Open Systems Interface* (OSI). Os clientes LDAP acessavam os gateways para o serviço de diretório X.500, onde esse *gateway* (também chamado de *proxy* ou *front-end*) rodando LDAP entre o cliente e o gateway. Anteriormente rodava o *Directory Access Protocol* (DAP, ou Protocolo de Acesso a Diretório) X.500 entre o servidor X.500 e o gateway (MACHADO; MORI JUNIOR, 2006).

O protocolo X.500 é pesado e opera sobre a pilha completa de protocolos OSI que requer uma grande quantidade significante de recursos computacionais. Já o protocolo LDAP é projetado para operar sobre TCP/IP fornecendo a maioria das funcionalidades do X.500 com um custo muito mais reduzido (MACHADO; MORI JUNIOR, 2006).

O protocolo LDAP é leve, pois não roda na pilha das camadas OSI, como o protocolo da camada de aplicação X.500. Os pacotes X.500 carregam mais informações, pois precisam de cabeçalhos para cada uma das camadas da pilha de protocolos OSI. Já o LDAP tem uma suite de protocolos TCP/IP, na qual roda, também necessita de cabeçalhos nos pacotes, mas tem um overhead menor (MACHADO; MORI JUNIOR, 2006).

O segundo motivo é que o LDAP omite várias operações do X.500 que são raramente usadas. LDAPv3 possui apenas nove operações principais e fornece um modelo mais simples para os programadores e administradores. Assim é possível que eles se foquem mais na semântica de seus programas, sem terem que se preocupar com características do protocolo raramente usadas (MACHADO; MORI JUNIOR, 2006).

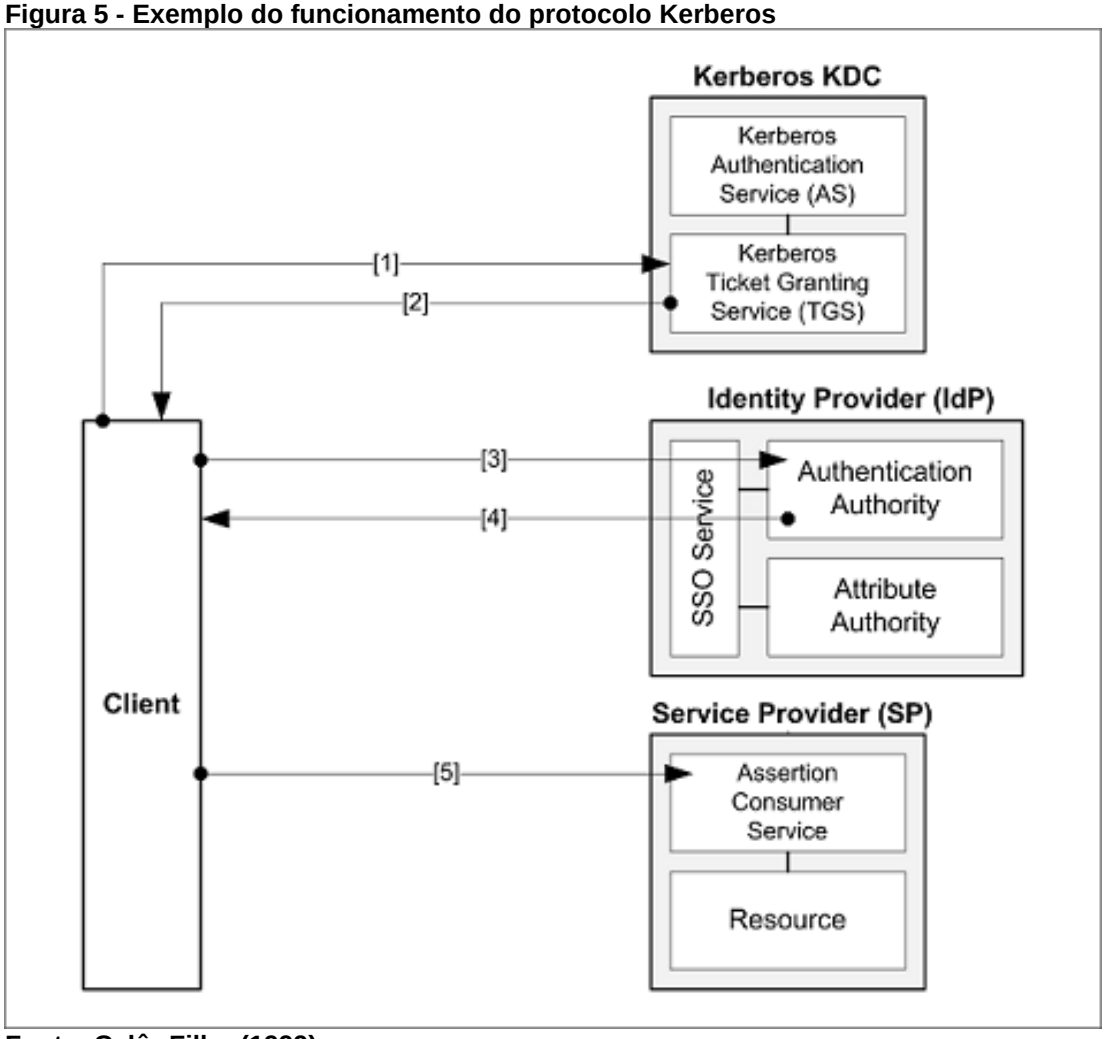
Além do LDAP ainda ser usado para acessar o serviço de diretório X.500 através de gateways, LDAP é também agora implementado direto em servidores LDAP do tipo X.500. Note o uso de "do tipo X.500" em vez de simplesmente "X.500", pois um servidor X.500 não entende mensagens LDAP. O segundo uso é o mais

comum atualmente, pois atende a praticamente todas necessidades (MACHADO; MORI JUNIOR, 2006).

2.7 KERBEROS

Kerberos é um protocolo que foi desenvolvido para fornecer uma poderosa autenticação nas aplicações usuário/servidor conforme pode-se verificar na Figura 5, onde funciona como a terceira parte neste processo, oferendo a autenticação do usuário (CALÔR FILHO, 1999).

Figura 5 - Exemplo do funcionamento do protocolo Kerberos



Fonte: Calôr Filho (1999).

O protocolo Kerberos, exemplificado ainda na Figura 5, foi desenvolvido como parte do Athena Project, no *Massachussets Institute of Technology* (MIT). Seu nome vem do grego “Kerberus”, onde Cerberus que é um cão de três cabeças que tem como objetivo proteger a entrada do inferno de Hades (CALÔR FILHO, 1999).

2.8 POLÍTICAS DE GRUPO

Os *Group Policy Object* (GPO, ou Objetos das Políticas de Grupos) permitem o gerenciamento centralizado e automatizado de uma vasta quantidade de configurações relacionadas com usuários e computadores de um determinado domínio. As GPO se aplicam a partir da versão do Windows 2000 em diante, assim como no Samba, OpenLDAP e demais ferramentas de Diretórios. A grande vantagem das GPO é que ao invés de fazer as configurações individualmente, para muitos de usuários e em muitos computadores, usando as GPO, o administrador da rede pode aplicar, automaticamente, as configurações desejadas, a um determinado grupo e a outro não, bloquear acessos ou recursos a um e a outro não. Selecionar scripts de login e/ou de logoff (BATTISTI; LIMA, 2017).

Além de usar as Diretivas de Grupo para definir configurações para grupo de usuários, grupos de usuários e computadores, você também pode usar as GPO para ajudar a gerenciar e configurar os próprios servidores, inclusive os Controladores de Domínio, aplicando configurações de segurança, políticas de senha para o domínio, configurações para as contas de Administrador e Administradores, configurações para os grupos de segurança (BATTISTI; LIMA, 2017).

É muito vasta a infinidade de recursos que pode-se aplicar utilizando-se das GPO, que é possível instalar programas específicos em um determinado grupo, ou mesmo restringir que um determinado grupo não instale impressoras da rede, entre muitos outros recursos (BATTISTI; LIMA, 2017).

3 DESENVOLVIMENTO

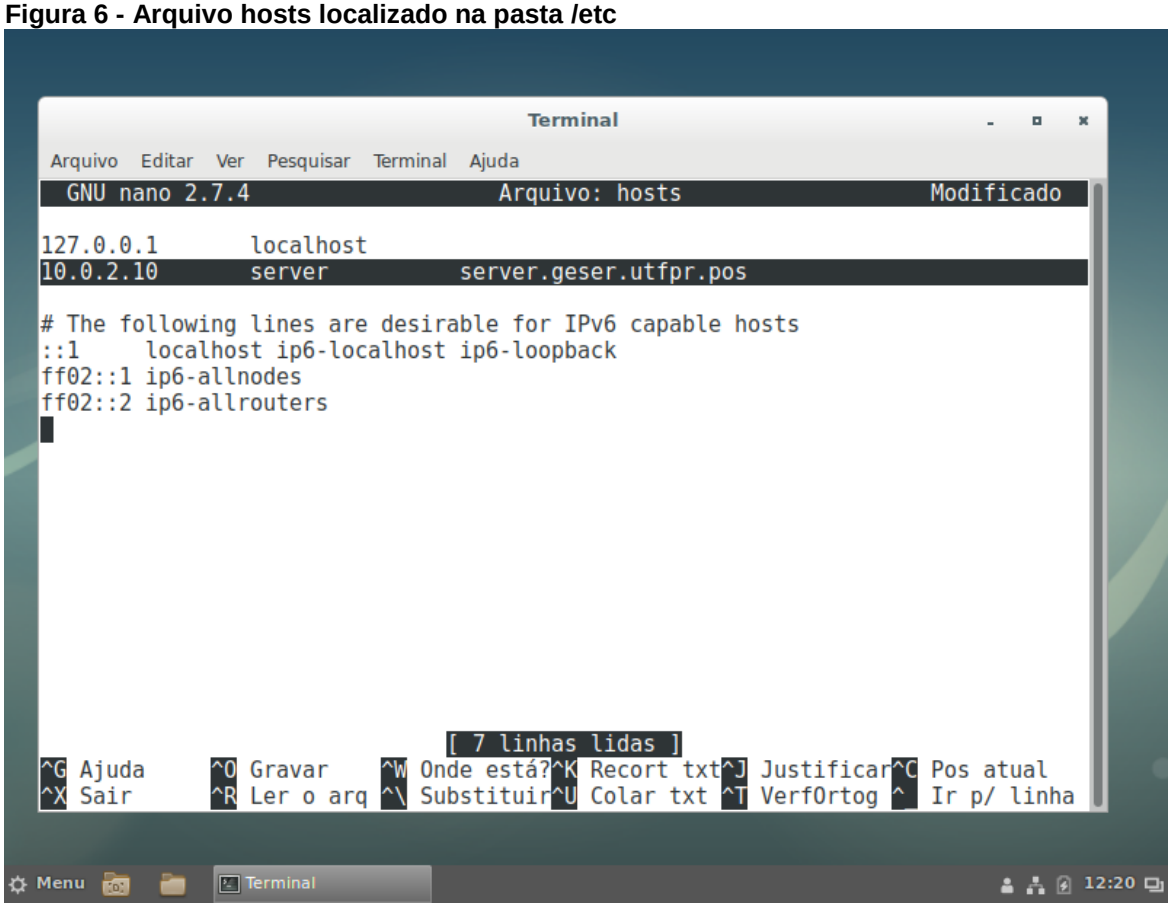
Para alcançar os objetivos desse trabalho, foi utilizado máquinas virtuais onde utiliza-se o Oracle Virtual Box na sua versão 5.2.20 r 125813 (Qt5.6.2), já com o Linux foi usada a versão do Linux Debian na sua versão 9.5.0 Stretch para configurações, testes e capturas de telas, após isso instalado o Samba na sua versão 4 (SAMBA, 2018).

3.1 LINUX DEBIAN 9.5.0 STRETCH

O Samba 4 vai além do simples compartilhamento de arquivos, pois também permite que o servidor Linux assuma o papel de um controlador de domínio (ou *Domain Control* - DC). Sendo assim é possível ingressar máquinas de qualquer natureza no seu domínio seja essa Windows, Linux, BSD, MAC OS, Unix com o serviço de diretório do servidor Linux para que se possa gerenciar seus objetos de um domínio como computadores, contas de usuários, impressoras, políticas, etc) ou seja, sem a necessidade do Windows Server, o que implicaria em uma grande economia pois não seria necessário a aquisição da licença do sistema operacional do servidor e também da quantidade de clientes de rede (ou *Client Access License* – CAL).

Nosso objetivo é listar as etapas necessárias para instalar o Samba 4 (e seus complementos) para transformar Linux Debian em um servidor como controlador do domínio que se denominará de geser.utfpr.pos. Assumi-se que o nosso controlador de domínio será configurado com o IP 10.0.2.10/24, assim nessa etapa preliminar define-se estaticamente o arquivo hosts localizado na pasta “/etc” para que o mapeamento do nome do servidor que posteriormente será configurado como controlador de domínio (Figura 6). Assim foi criado o mapeamento estático entre o nome versus o IP no qual o nome da máquina será composto com o sufixo do domínio (ou *Fully Quallified Domain Name* - FQDN) que será utilizado posteriormente. Com esse mapeamento o Samba irá sugerir o nome de domínio geser.utfpr.pos durante a sua instalação.

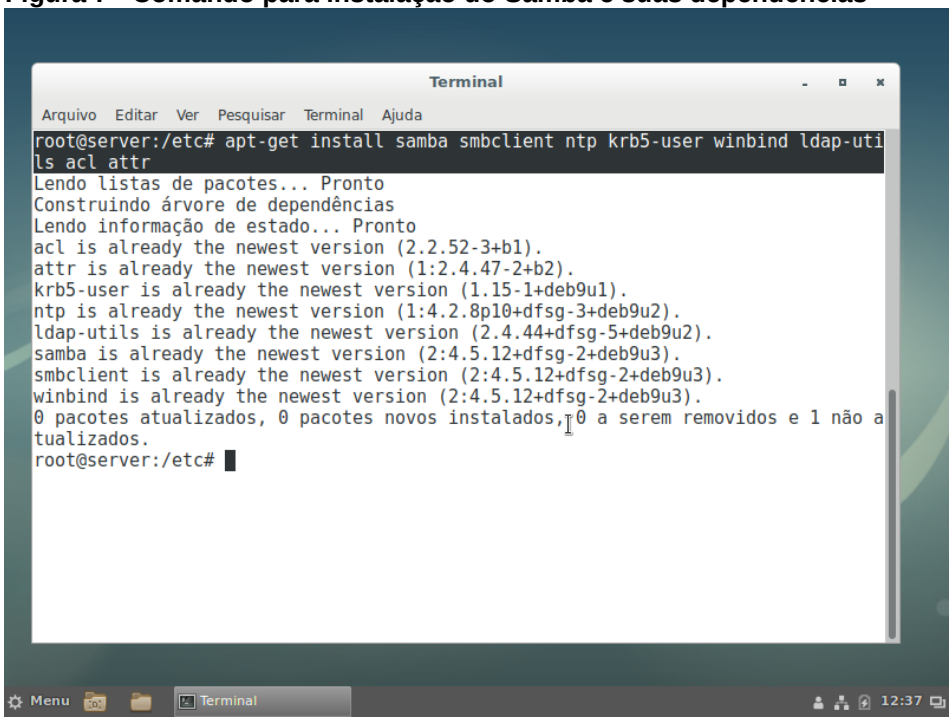
Figura 6 - Arquivo hosts localizado na pasta /etc



Fonte: Autoria própria.

Nessa etapa foi instalado o pacote do Samba para que seja posteriormente configurado o Linux como um controlador de domínio. Também se faz necessário instalar vários outros pacotes de serviços que serão necessários para o bom funcionamento desse nosso servidor, a exemplo o utilitário do sistema de arquivos para mapear as unidades do Windows (smbclient), o protocolo para sincronização dos relógios dos computadores (ntp), o utilitário do sistema para autenticação de usuários e serviços em rede (krb5-user), o sistema de integração, autenticação e mecanismos de serviços de diretório em um domínio Windows e Linux (winbind), os utilitários do pacote *Lightweight Directory Access Protocol* (LDAP), aos quais pode-se acessar um servidor LDAP local ou remotamente além de conter todos os programas clientes necessários para acessar estes servidores (ldap-utils), o utilitário necessário para manipulação das listas de controle de acesso (ACL) e por fim o utilitário para manipulação de atributos estendidos dos sistemas de arquivos (attr). Apesar de aparentar ser bastante coisa, essa tarefa é simples, rápida e facilmente implementada ao utilizar-se o comando que pode-se verificar na Figura 7, notem que como já havia instalado anteriormente esses pacotes, nenhum deles sofreu alterações.

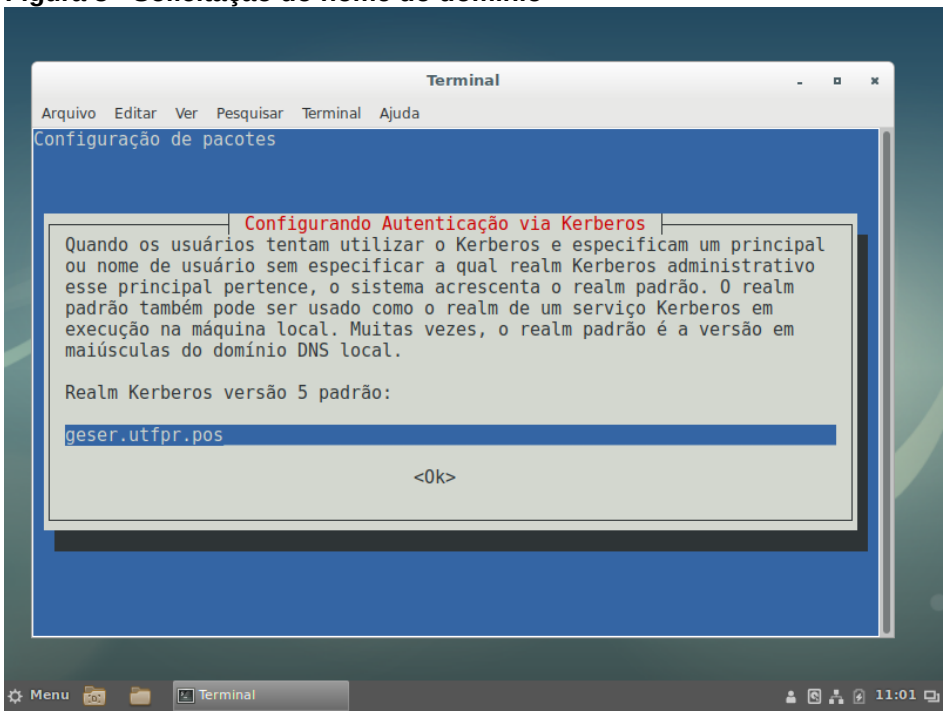
Figura 7 - Comando para instalação do Samba e suas dependências



Fonte: Autoria própria.

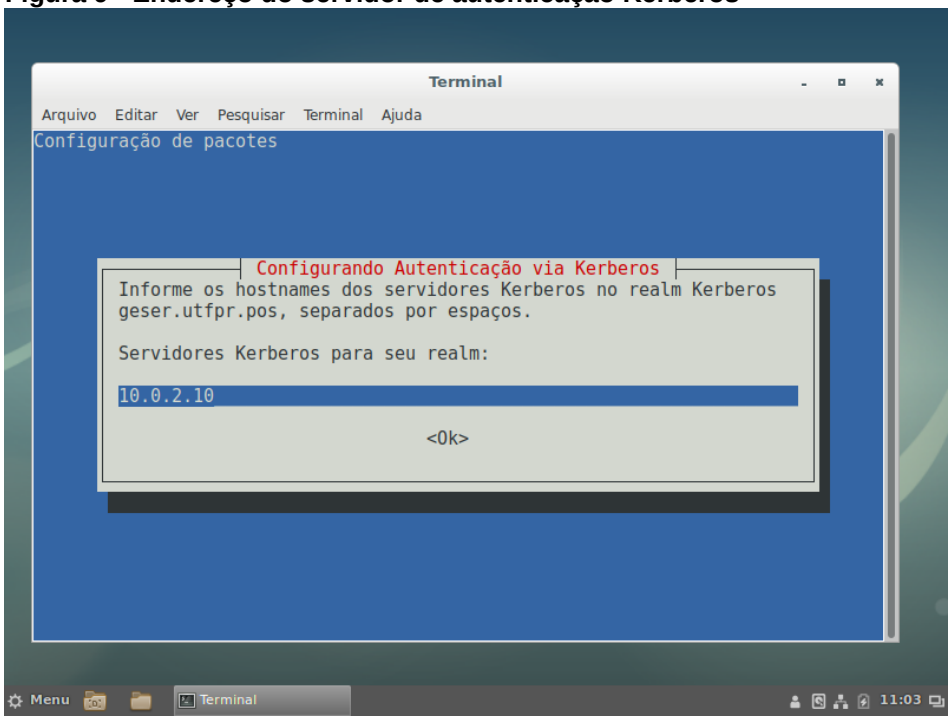
Durante o processo de instalação irão aparecer alguns diálogos (modo texto) solicitando 3 informações como nome do domínio, endereço do servidor de autenticação Kerberos e o endereço do servidor administrativo conforme pode-se verificar nas Figuras 8 (solicitação de domínio), 9 (endereço do servidor de autenticação) e 10 (endereço do servidor administrativo).

Figura 8 - Solicitação do nome do domínio



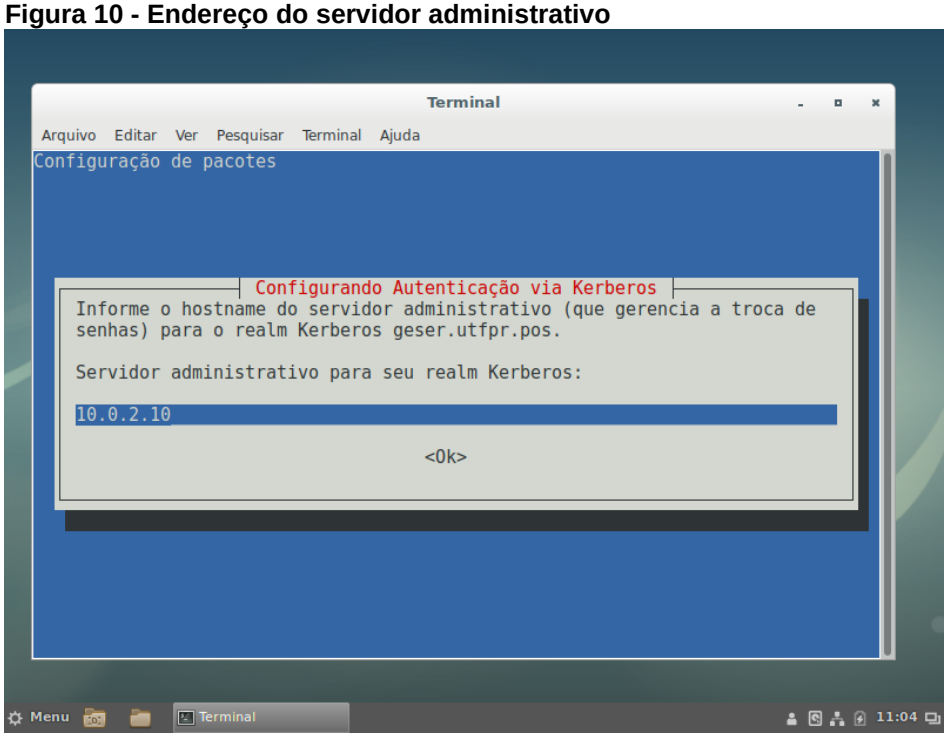
Fonte: Autoria própria.

Figura 9 - Endereço do servidor de autenticação Kerberos



Fonte: Autoria própria.

Figura 10 - Endereço do servidor administrativo



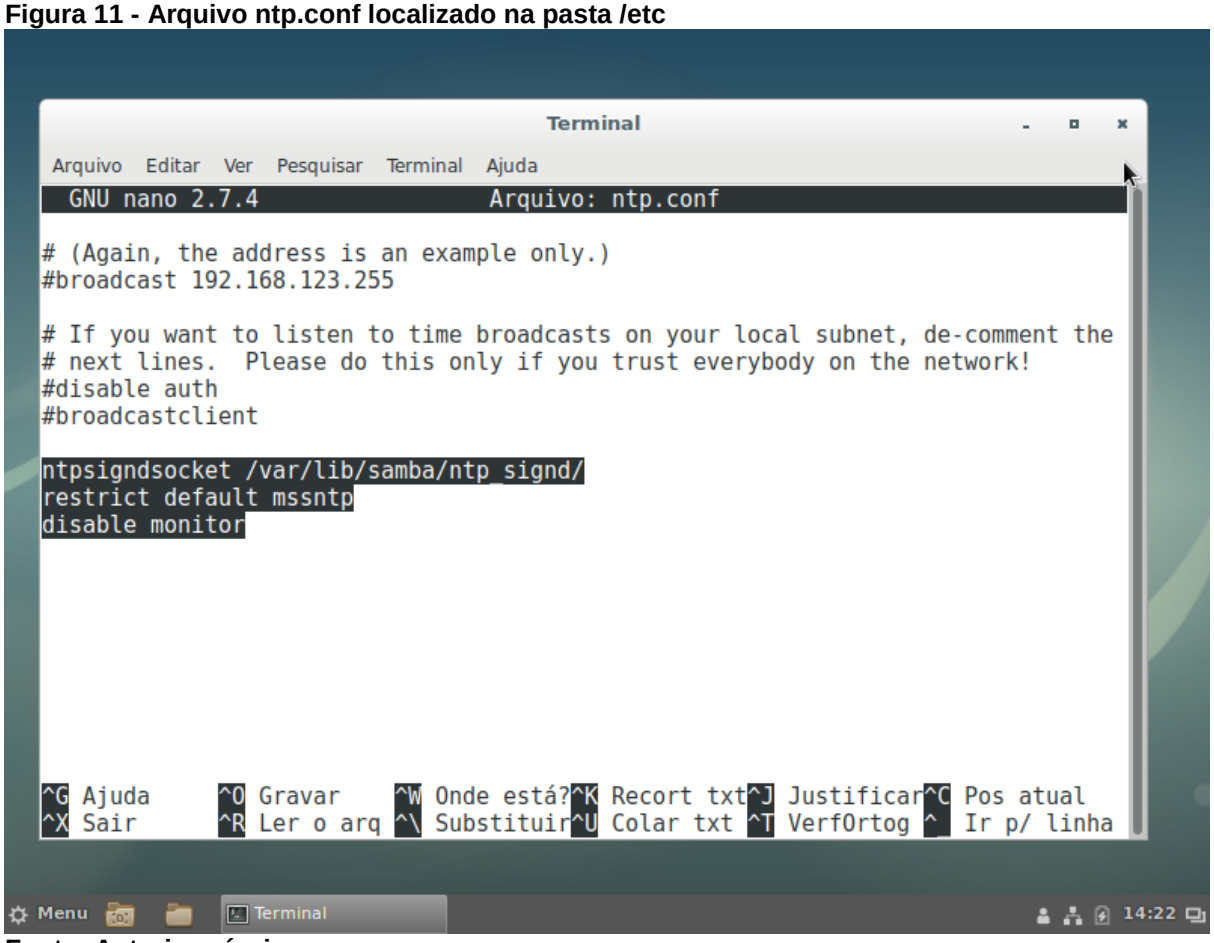
Fonte: Autoria própria.

Nessa próxima etapa será realizado os ajustes no serviço NTP responsável pela sincronização do relógio do servidor e logo este será responsável por sincronizar os relógios de todas as demais máquinas do domínio. Inicialmente será criado o “diretório ntp_signd” com as devidas permissões, após isso é necessário adicionar

algumas linhas ao final do arquivo de configuração “ntp.conf” localizado na pasta “/etc” conforme pode-se verificar na Figura 11 e por fim reiniciar o seu serviço conforme os seguintes comandos:

```
root@server:/# install -d /var/lib/samba/ntp_signd/
root@server:/# chown root:ntp /var/lib/samba/ntp_signd
root@server:/# chmod 750 /var/lib/samba/ntp_signd/
```

Figura 11 - Arquivo ntp.conf localizado na pasta /etc

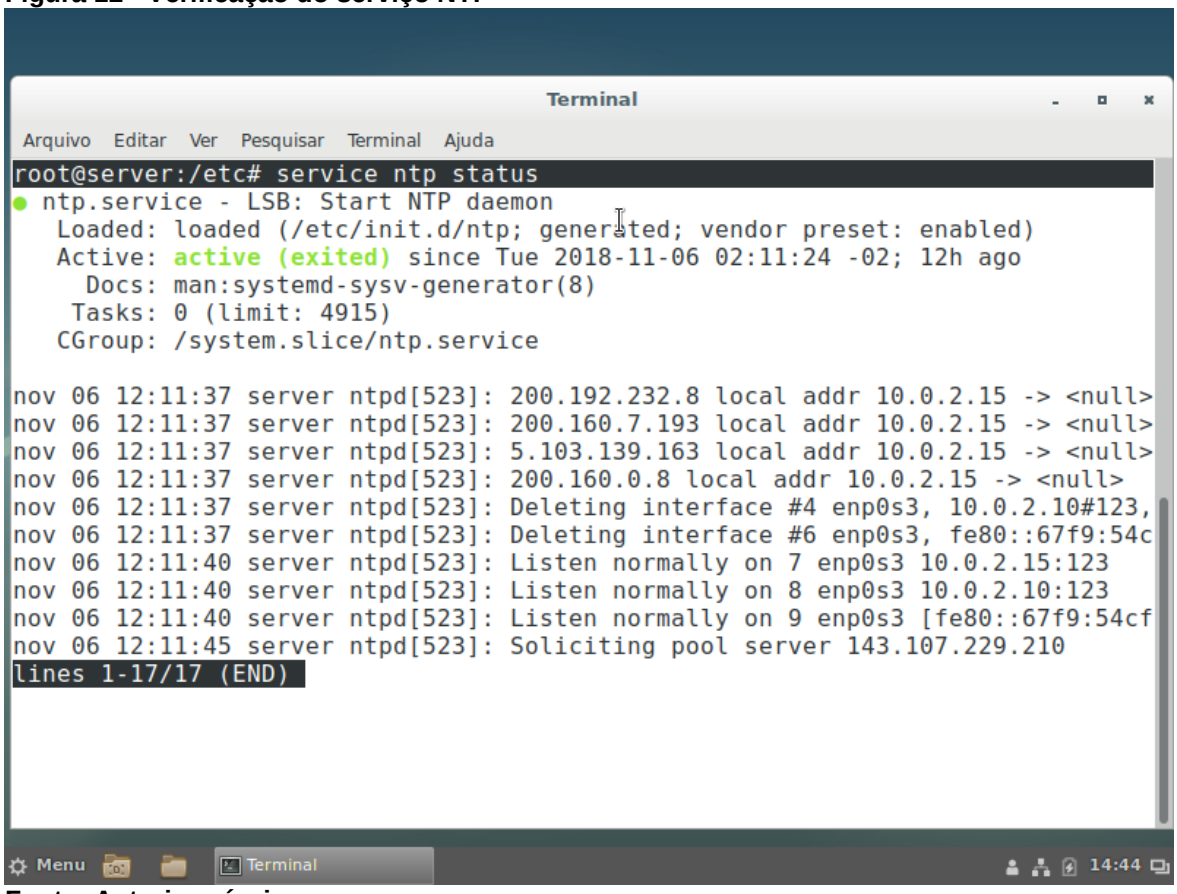


Fonte: Autoria própria.

Para reiniciar o serviço NTP basta executar o comando: “root@server:/# service ntp restart”.

Na Figura 12 pode-se verificar o status do serviço NTP em funcionamento.

Figura 12 - Verificação do serviço NTP



Fonte: Autoria própria.

Agora será configurado o domínio, através do processo de provisionamento do Samba, de ante mão basta parar alguns serviços que são executados automaticamente logo após a sua instalação, também será removido o arquivo de configuração original do Samba o arquivo smb.conf localizado na pasta /etc/samba. Para isso basta executar os seguintes comandos:

```
root@server:/# systemctl stop smbd nmbd winbind
root@server:/# rm /etc/samba/smb.conf
```

Essa é uma das etapas mais importantes, o provisionamento do domínio em que serão utilizadas ferramentas automatizadas do próprio Samba, preparando nosso servidor como um controlador do domínio (geser.utfpr.pos). Para isso utilizado o comando samba-tool que serve como frontend responsável por manipular o LDAP (backend), simplificando muito a tarefa de configuração. Para isso deve-se executar o comando: “root@server:/# samba-tool domain provision --use-rfc2307 --interactive”.

Durante esse processo o sistema irá questionar algumas informações necessárias, que já viram preconfiguradas por padrão ou capturadas pelas configurações que forão efetuadas:

```
Realm                           [GESER.UTFPR.POS]
Domain                          [GESER]
Server Role                     [DC]
DNS Backend                     [SAMBA_INTERNAL]
DNS Forwarder IP Address        (IP do DNS da REDE)
Administrator Password          (SENHA FORTE)
```

Agora será fixadas as configurações do DNS do servidor no arquivo “resolv.conf” localizado na pasta “/etc”, conforme pode-se verificar na Figura 13, e aplicar as características de imutabilidade (+i) no arquivo para que esse não seja mais dinamicamente atualizado. Após realizar esses procedimentos será necessário reiniciar o servidor implementando os seguintes comandos:

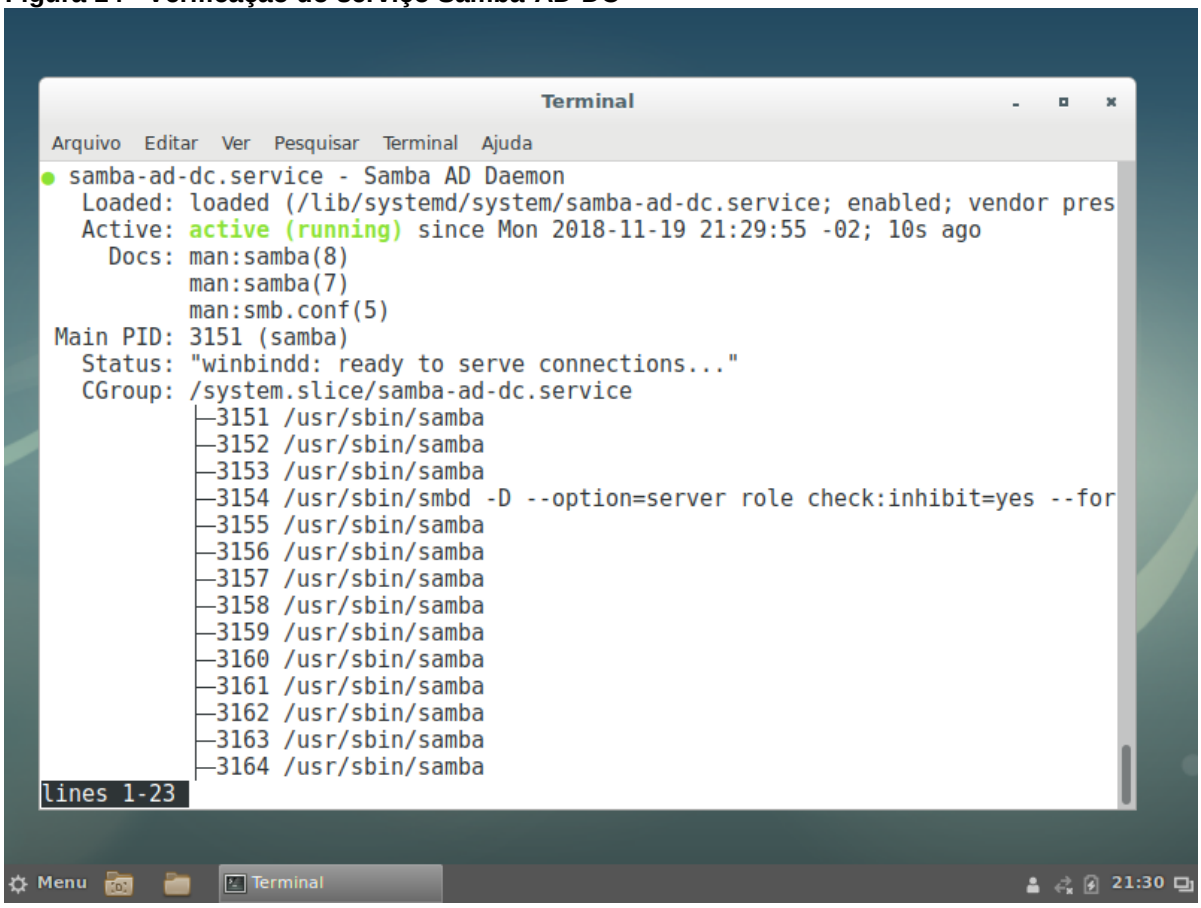
```
root@server:/# chattr +i /etc/resolv.conf
root@server:/# service samba-ad-dc restart
```

Figura 13 - Arquivo resolv.conf localizado na pasta /etc

Fonte: Autoria própria.

Agora será efetuada algumas verificações se o Samba está em execução. Para isso basta executar o comando “root@server:/# service samba-ad-dc status” e a seguir pode-se verificar o resultado na Figura 14.

Figura 14 - Verificação do serviço Samba-AD-DC



Fonte: Autoria própria.

Para fazer uma verificação mais apurada, vale testar a resolução de nomes internos de alguns registros automaticamente criados pelo controlador de domínio, além de testar a resolução dos nomes internos e externos:

```
root@server:/# host -t A geser.utfpr.pos
geser.utfpr.pos has address 10.0.2.10

root@server:/# host -t SRV _kerberos._udp.geser.utfpr.pos
_kerberos._udp.geser.utfpr.pos has SRV record 0 100 88
server.geser.utfpr.pos


root@server:/# host -t SRV _ldap._tcp.geser.utfpr.pos
_ldap._tcp.geser.utfpr.pos has SRV record 0 100 389
server.geser.utfpr.pos

root@server:/# host www.debian.org
www.debian.org has address 200.17.202.197
www.debian.org has IPv6 address
2801:82:80ff:8009:e61f:13ff:fe63:8e88
```

Vale testar a autenticação do Kerberos também, para isso deve-se executa os comandos:

```
root@server:/# kinit administrator@geser.utfpr.pos
Password for administrator@geser.utfpr.pos: ********
Warning: Your password will expire in 41 days on Mon Nov 19
20:00:00 2018
```

O servidor já está rodando Samba como controlador de domínio. Desde momento em diante o domínio pode ser administrado via interface de linha de comando (ou *Comand-Line Interface* - CLI) com a ferramenta samba-tool. Com essa tem-se uma vasta gama de opções para administração do domínio, nas Tabelas 1, 2 e 3 seguem os principais comandos e uma breve descrição.

Tabela 1 - Comandos samba-tool para manipulação de usuários

samba-tool user list	lista todos os usuários do domínio
samba-tool user add	adiciona novo usuário
samba-tool user del	exclui usuário existente
samba-tool user enable	habilita usuário desabilitado
samba-tool user disable	desabilita uma conta de usuário habilitada

Fonte: Autoria própria.

Tabela 2 - Comandos samba-tool para manipulação de grupos

samba-tool group addmembers	adiciona usuário a um grupo
samba-tool group listmembers	lista usuário do grupo

Fonte: Autoria própria.

Tabela 3 - Comandos samba-tool para manipulação de GPO

samba-tool gpo create	cria GPO
samba-tool gpo del	exclui uma GPO
samba-tool gpo dellink	exclui o link GPO/container
samba-tool gpo getlink	lista gpo de um determinado container
samba-tool gpo listall	lista todas as GPO
samba-tool gpo show	exibe as informações de um GPO
Samba-tool gpo setlink	adiciona ou atualiza uma gpo a um conteiner

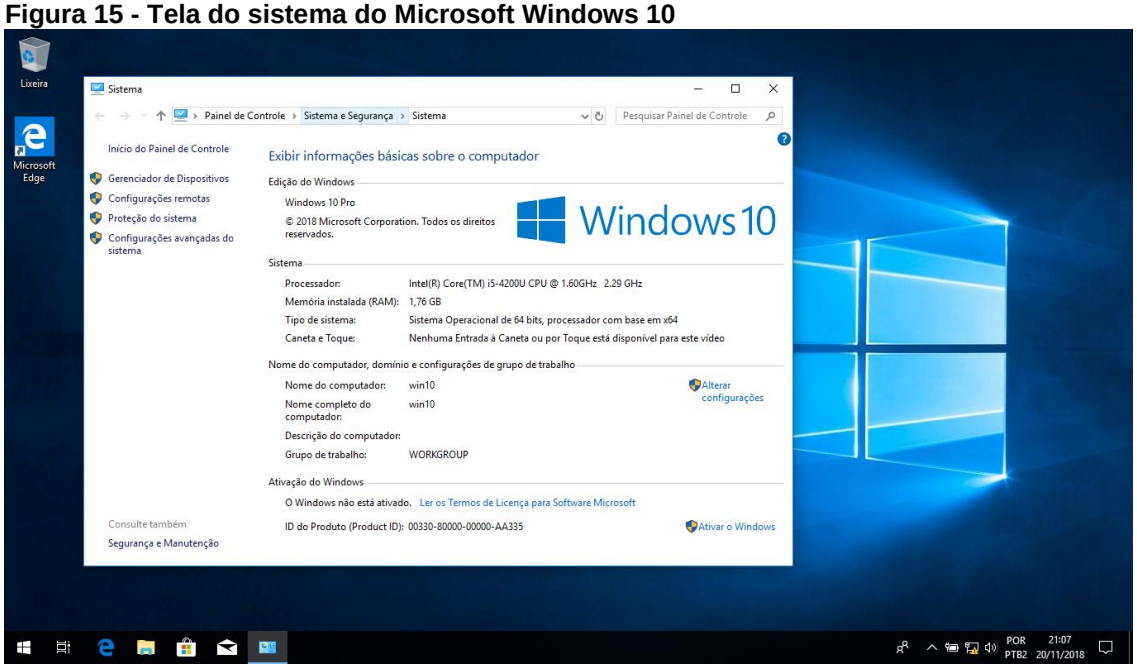
Fonte: Autoria própria.

Se algum usuário esquecer a sua senha, pode-se reseta-lá usando o comando abaixo forçando o usuário a alterá-la na próxima vez que efetuar login:

```
samba-tool user USUÁRIO --newpassword=SENHA --must-change-at-
next-login
```

Agora que o servidor encontra-se devidamente configurado é hora de adicionar uma máquina Windows 10 ao domínio (Figura 15). Para isso basta seguir o passo a passo para egresso ao domínio.

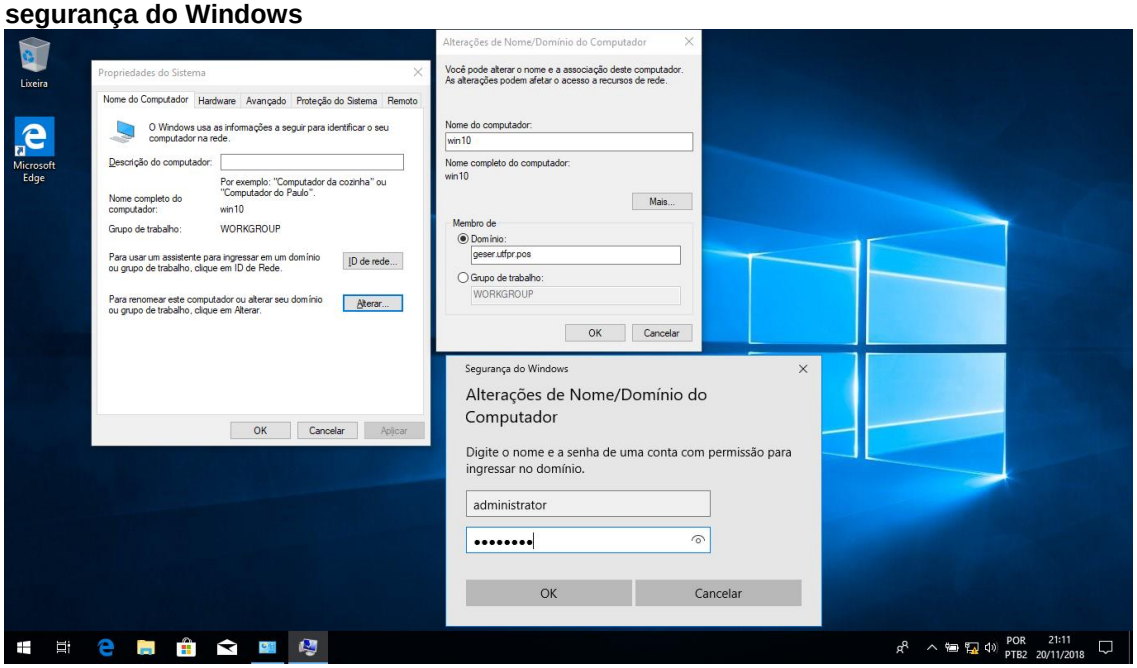
Figura 15 - Tela do sistema do Microsoft Windows 10



Fonte: Autoria própria.

Ao clicar em “Alterar configurações” que pode-se verificar ainda na Figura 15, aparecerá a janela de “Propriedades do Sistema” conforme pode-se verificar na Figura 16. Nesta janela clica-se no botão Alterar que nos levará a janela “Alterações de Nome/Domínio do Computador”, agora nessa janela adiciona-se o domínio “geser.utfpr.pos” e ao clicar no botão “ok” será solicitada as credenciais do Administrator lá do nosso servidor Linux, conforme pode-se verificar novamente na janela de Segurança do Windows (Figura 16).

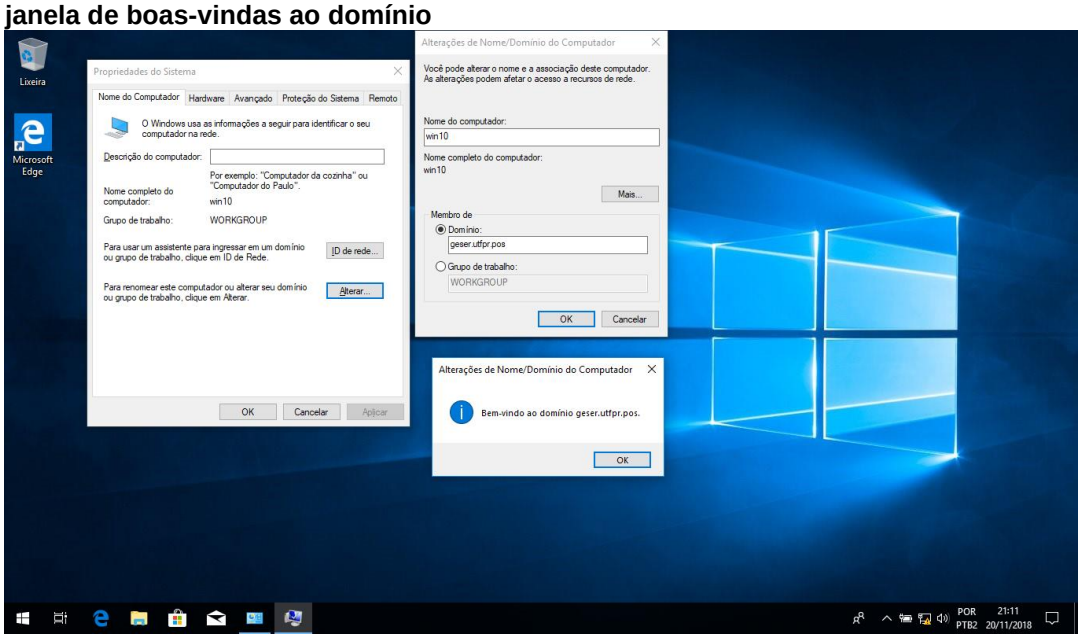
Figura 16 - Janela de propriedades do sistema; alteração de nome/domínio do computador; segurança do Windows



Fonte: Autoria própria.

É possível observar que após inseridas as credenciais do servidor “Samba4 Administrator” e a respectiva senha ao clicar-se em ok, o Windows nos apresenta a mensagem de boas-vindas “Bem-vindo ao domínio geser.utfpr.pos” conforme pode-se verificar na Figura 17.

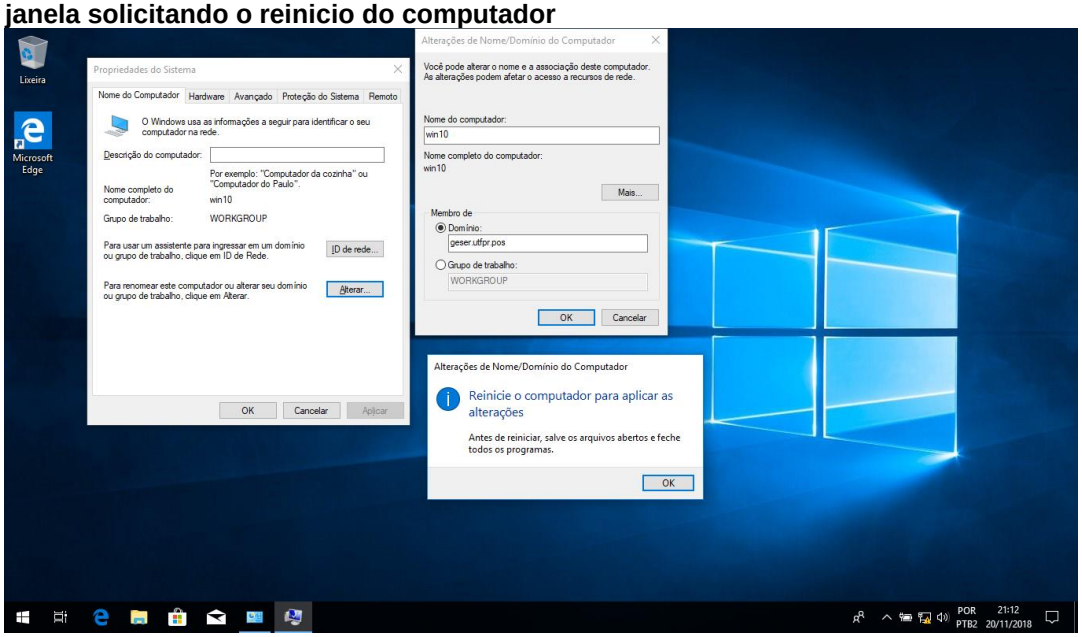
Figura 17 - Janela de propriedades do sistema; alteração de nome/domínio do computador; janela de boas-vindas ao domínio



Fonte: Autoria própria.

Após a mensagem de boas-vindas basta reiniciar o computador e logar no domínio, conforme pode-se verificar na Figura 18.

Figura 18 - Janela de propriedades do sistema; alteração de nome/domínio do computador; janela solicitando o reinicio do computador



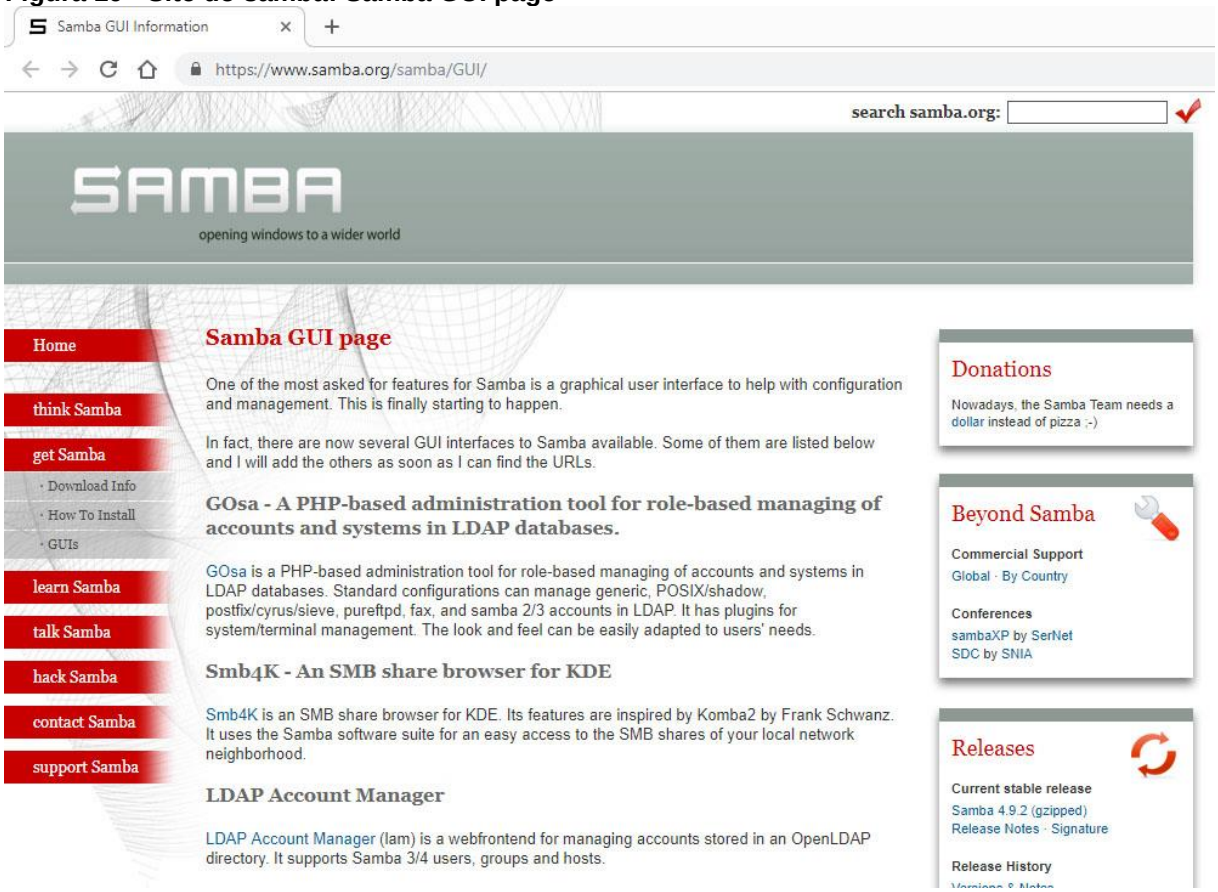
Fonte: Autoria própria.

3.2 SAMBA 4 - AMBIENTES GRÁFICOS

Assim como o Microsoft Windows Server tem o seu modo CLI e modo *Graphical User Interface* (GUI) o Samba 4 contam com algumas opções de ambientes gráficos para sua gestão, esses por sua vez podem ser conectados para gestão de qualquer um dos sistemas operacionais pois utilizam-se do mesmo protocolo LDAP.

A Figura 19, mostra como acessar a página oficial Samba (SAMBA, 2018), onde pode-se encontrar algumas das Interfaces Gráficas de Usuários (ou *Graphical User Interface* - GUI).

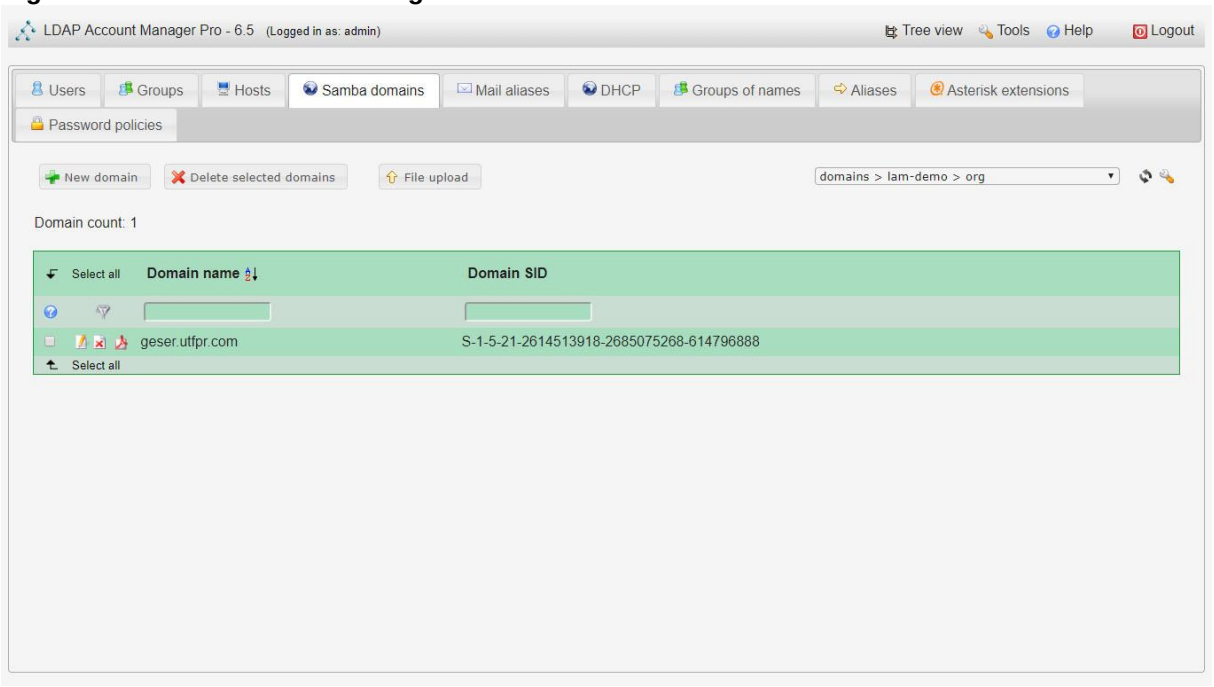
Figura 19 - Site do samba: Samba GUI page



Fonte: Autoria própria.

Na Figura 20, pode-se verificar uma das interfaces gráficas de usuários, está apenas para demonstrar que é possível ter uma gerencia amigável como temos no Windows, porem vale lembrar que em qualquer ambiente que seja as áreas gráficas são sempre mais engessadas, mesmo no Windows.

Figura 20 - LDAP Account manager Pro 6.5



Fonte: Autoria própria.

4 CONCLUSÃO

Para atender aos objetivos deste trabalho, o qual era realizar a gestão centralizada de servidores em redes computacionais constatamos que existem não somente o Microsoft Active Directory e que esse é apenas um gerenciador do protocolo LDAP.

Com esse trabalho pude concluir que muitas das vezes existem softwares livres tão bons ou melhores que muitos softwares proprietário porem o que pude perceber é a grande falta da disseminação de sua existência.

Assim pode-se concluir que mesmo não utilizando um software proprietário conseguimos realizar o mesmo propósito, com isso é possível economizar na compra de sistema operacional servidor e com as licenças de acesso (CALs).

A parte mais trabalhosa é a configuração entre o Samba, kerberos e winbind para que haja a interoperabilidade entre sistemas operacionais, assim Linux, Windows ou qualquer outro Sistema Operacional pode se conectar ao nosso domínio facilitando a usabilidade dos seus clientes de rede.

Com este posso afirmar que num futuro cliente ou mesmo no momento de uma mudança em algum servidor estudarei mais a fundo para implementação de servidores Linux como Controladores de Domínios com LDAP, Samba4, Kerberos e seus demais protocolos e ferramentas para se ter essa redução de custo e confiabilidade e segurança das informações.

REFERÊNCIAS

BATTISTI, Júlio. **Componentes do active directory: Parte I.** Copyright© Júlio Battisti, 2018. Disponível em: <https://www.juliobattisti.com.br/tutoriais/ricardogerhard/activedirectory002.asp>. Acesso em: 11 nov. 2018.

BATTISTI, Júlio; LIMA, Diego. **Tudo sobre GPOs no Windows Server 2008, 2012 e 2016: Teoria e exemplos práticos e úteis - passo a passo.** Juatuba/MG: Instituto Alpha, 2017. Disponível em: <https://juliobattisti.com.br/downloads/livros/tudo_sobre_gpos_degusta.pdf>. Acesso em: 11 nov.2018.

CALÔR FILHO, Marcos Muniz. **Kerberos**. Universidade Federal do Rio de Janeiro (UFRJ), Grupo de Teleinformática e Automação (GTA), Trabalho de Redes de Computadores I, Rio de Janeiro: 1999. Disponível em: <https://www.gta.ufrj.br/grad/99_2/marcos/kerberos.htm>. Acesso em: 09 nov. 2018.

MACHADO, Erich Soares; MORI JUNIOR, Flavio da Silva. **Autenticação integrada baseada em serviço de diretório LDAP.** Universidade de São Paulo, Instituto de Matemática e Estatística, São Paulo: 2006. Disponível em: <https://linux.ime.usp.br/~cef/mac499-06/monografias/erich/html/index.html>. Acesso em: 03 set. 2018.

OPENDJ. **OpenDJ 2.6 administration guide**. Copyright© 2010-2018 ForgeRock, 2018. Disponível em: <https://backstage.forgerock.com/docs/opendj/2.6/admin-guide/> Acesso em: 08 nov. 2018.

OPENDS. **Introducing the OpenDS Project**. Copyright© ORACLE, 2018. Disponível em: <https://www.oracle.com/technetwork/java/opends-142561.html>. Acesso em: 07 nov. 2018.

ROVER, Marinho. **O que é active directory, topologia física e lógica?: Parte1**. Copyright© Microsoft, jun. 2012. Disponível em: <https://technet.microsoft.com/pt-br/library/jj206711.aspx?f=255&MSPPError=-2147217396>. Acesso em: 25 out. 2018.

SAMBA. **Samba: opening windows to a wide world.** Copyright© samba.org, 2018. Disponível em: <https://www.samba.org>. Acesso em: 18 nov. 2018.