Rafael José Puiati Bergamaschi

Interoperabilidade com Kerberos + Samba + LDAP + Active Directory

Monografia de Pós-Graduação "*Lato Sensu*" apresentada ao Departamento de Ciência da Computação para obtenção do título de Especialista em "Administração em Redes Linux"

Orientador
Prof. Herlon Ayres Camargo

Lavras
Minas Gerais - Brasil
2011

Rafael José Puiati Bergamaschi

Interoperabilidade com Kerberos + Samba + LDAP + Active Directory

Monografia de Pós-Graduação "*Lato Sensu*" apresentada ao Departamento de Ciência da Computação para obtenção do título de Especialista em "Administração em Redes Linux"

Aprovada em *30 de abril de 2011*

Profa. Ana Paula Piovesan Melchiori

Prof. Arlindo Follador Neto

Prof. Herlon Ayres Camargo
(Orientador)

Lavras
Minas Gerais - Brasil
2011

Dedico esta monografia à minha mãe, que infelizmente não pode mais acompanhar meus passos na minha carreira.

Agradecimentos

Agradeço ao Senhor pela ajuda e força, principalmente nos momentos em que os erros eram persistentes. Em especial agradeço à minha querida Suellen, pela paciência, pelas orações e ajunda na revisão. Agradeço ao professor Herlon Camargo pela ajuda, paciência e compreensão.

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

Este trabalho apresenta uma simulação de como é possível realizar a interoperabilidade entres os sistemas operacionais Linux e Windows. Esta simulação é realizada em dois ambientes. No primeiro ambiente é discutido a integração do Kerberos, Samba e OpenLDAP, em um servidor Linux para autenticação de um cliente Windows. No segundo ambiente é discutido a instalação do Active Directory em um servidor Windows para autenticação de um cliente Linux.

Palavras-Chave: Interoperabilidade; Integração; Kerberos; LDAP; OpenLDAP; Samba; Active Directory; Linux; Windows.

Capítulo 1

Introdução

Atualmente, em ambientes corporativos, é comum encontrar redes heterogêneas. O cenário mais comum são servidores com Linux e estações de trabalho com Windows. Em redes heterogêneas, surge o problema quando um usuário precisa acessar algum arquivo ou serviço presente no servidor. Mas graças a ferramentas e soluções cada vez mais modernas e transparentes aos usuários, esse problema entre sistemas operacionais diferentes são minimizados.

A motivação deste trabalho é mostrar que existe a possibilidade de criar uma convivência harmoniosa entre o Linux e o Windows, e torná-la transparente ao usuário, facilitando assim o trabalho do administrador da rede.

Este trabalho tem como objetivo mostrar, através de simulação, como é possível interoperar[1] entre os sistemas operacionais Linux e Windows, utilizando a autenticação em domínio de forma segura, com um serviço de diretório. Para comprovar esta afirmativa, serão criados dois ambientes: o primeiro com o cliente Windows e servidor Linux e o segundo com o cliente Linux e servidor Windows. Em ambos os servidores será instalado um serviço de arquivo e um controlador de domínio, mas este trabalho focará na autenticação no domínio.

Existem soluções no mercado semelhante da apresentada neste trabalho, como por exemplo: Likewise[2] e System Security Services Daemon (SSSD)[3] da RedHat Enterprise Linux.

[1] A interoperabilidade é a capacidade de um sistema se comunicar com outro sistema (semelhando ou não), de forma mais transparente possível.

[2] Disponível em http://www.likewise.com/.

[3] Disponível em http://www.redhat.com/.

Nos dois servidores serão instalados um controlador de domínio, um serviço de diretório para armazenar os usuários da rede e um protocolo para promover a autenticação segura pela rede. No ambiente 1 serão utilizadas tecnologias em software livre, com o sistema operacional em Linux e a integração do Samba, OpenLDAP e Kerberos. No ambiente 2 serão utilizadas tecnologias proprietárias, com o sistema operacional Windows com Active Directory. Este trabalho não possui a finalidade mostrar qual o ambiente apresenta o melhor custo benefício, ficará restrito apenas ao seu objetivo.

Para desenvolver esse trabalho, foram criados dois ambientes com máquinas virtuais para simulação, utilizando o Oracle VM VirtualBox[4] versão 3.2.12. A Tabela 1.1 apresenta os sistemas operacionais instalados no ambiente 1 e a Tabela 1.2 apresenta os sistemas operacionais instalados no ambiente 2.

Tabela 1.1: Sistemas operacionais do ambiente 1.

Sistema Operacional	**Função**	***host***
`Ubuntu Server Edition 10.04 64-bit`	Servidor	ubuntuserver
`Windows 7 Professional 64-bit`	Cliente	windowscliente

Tabela 1.2: Sistemas operacionais do ambiente 2.

Sistema Operacional	**Função**	***host***
`Windows Server 2008 R2 Enterprise 64-bit`	Servidor	windowsserver
`Ubuntu Desktop Edition 10.04 64-bit`	Cliente	clientelinux

Importante destacar que este trabalho não tem por objetivo discutir a instalação dos sistemas operacionais GNU/Linux Ubuntu[5], Windows 7[6] e Windows 2008[7]. Para mais informações desses procedimentos consulte suas respectivas documentações.

O autor deste trabalho usa como referência as distribuições Ubuntu e Debian, para todas as configurações de arquivos e suas respectivas localizações. Outras

[4]Disponível em `http://www.virtualbox.org/`.

[5]Instalação disponível em `https://help.ubuntu.com/10.04/installation-guide/index.html`.

[6]Instalação disponível em `http://windows.microsoft.com/pt-BR/windows7/Installing-Windows-7-recommended-links`.

[7]Instalação disponível em `http://www.microsoft.com/windowsserver2008/en/us/product-documentation.aspx`.

distribuições Linux podem ter dado outro nome a esses arquivos, inclusive outras localizações, consulte a documentação de sua distribuição para mais detalhes.

As versões dos pacotes instalados nas distribuições Linux, das Tabelas 1.1 e 1.2, correspondem as versões mais atuais presentes no seus respectivos repositórios no momento da execução deste trabalho.

A escolha do Windows Server 2008 é justificada por ser a versão para servidores mais recente disponível da Microsoft, no momento da escrita desse trabalho e consequentemente o fato de apresentar recursos mais avançados que as versões anteriores. O cliente e servidor Windows utilizados neste trabalho foram licenciados pelo *MSDN Academic Alliance*[8]. Há uma versão de avaliação do Windiows Server 2008 disponível em `http://www.microsoft.com/windowsserver2008`.

O Capítulo 1 apresenta os objetivos deste trabalho, a motivação e um resumo da metodologia adotada. O Capítulo 2 apresenta a revisão de literatura das seguintes tecnologias: Kerberos, Samba, LDAP, OpenLDAP e Active Directory. O Capítulo 3 apresenta as instalações e configurações da integração do Kerberos, Samba e OpenLDAP no servidor Linux, e as configurações do cliente Windows para autenticação no servidor. O Capítulo 4 apresenta a instalação e configuração do Active Directory no servidor Windows, e as instalações e as configurações no cliente Linux para autenticação no servidor. O Capítulo 5 apresenta os resultados dos testes de autenticação, realizados nos dois ambientes. O Capítulo 6 apresenta a conclusão e sugestões para trabalhos futuros. O Apêndice A apresenta a lista dos principais arquivos de configuração utilizados no servidor Linux.

[8]Disponível em `http://www.microsoft.com/brasil/educacao/comunidadeacademica/msdnaa/default.mspx`.

Capítulo 2

Revisão da Literatura

2.1 Kerberos

2.1.1 Visão Geral

O Kerberos é um protocolo de autenticação, baseado no protocolo *Needham-Schroed*, utilizado para prover segurança em redes inseguras. O Kerberos foi desenvolvido pelo MIT (Massachusetts Institute of Technology), originalmente com o objetivo de atender as necessidades do projeto Athenas[1]. Atualmente, o MIT Kerberos Consortium[2] apresenta a seguinte proposta: "*Estabelecer o Kerberos como a plataforma de autenticação da rede de computadores do mundo.*" (BUCKLEY, 2008).

O objetivo principal do protocolo é eliminar a transmissão de senhas pela rede e prover a transmissão de dados criptografados entre o cliente e servidor. A implementação livre do Kerberos pode ser encontrada no MIT[3]. O protocolo passou por várias revisões e aprimoramentos e, no momento do desenvolvimento desse trabalho encontra-se na versão 5, especificado na RFC 1510. Há outras implementações livre do Kerberos como Heimdal[4] e Shishi[5].

[1] Disponível em `http://museum.mit.edu/150/26`
[2] Disponível em `http://www.kerberos.org/`.
[3] Disponível em `http://web.mit.edu/kerberos/`.
[4] Disponível em `http://www.h5l.org/`.
[5] Disponível em `http://www.gnu.org/software/shishi/`.

A palavra Kerberos é originária da mitologia grega *Cerberus*, um cão de três cabeças e calda de serpente. *Cerberus* possuía a função de guardar os portões do reino de *Hates*, deus do mundo inferior, com o objetivo de impedir a entrada de pessoas não autorizadas.

O KDC (*Key Distribution Center* – Centro de Distribuição de Chaves) é o servidor Kerberos. O KDC é dividido em três partes, como apresentado na Figura 2.1:

- AS (*Authentication Service* – Serviço de Autenticação), é responsável pela autenticação do cliente, isto é, confirmar a identidade do cliente. Fornece um TGT (*Ticket Granting Ticket* - Tíquete de Concessão) para o cliente acessar o *Ticket-Granting Service*.
- TGS (*Ticket-Granting Service* – Serviço de Concessão de Tíquetes), é responsável por fornecer tíquetes aos clientes já autenticados no AS. Fornece tíquetes para que o cliente possa se comunicar nos servidores específicos.
- *Database* (Base de dados), é responsável pelo armazenamento dos dados associados aos clientes e serviços, chaves secretas e informações sobre os tíquetes.

A chave de sessão é uma chave gerada pelo Kerberos de forma aleatória e emitida ao cliente. Assim o cliente com um tíquete e uma chave de sessão poderá se comunicar com um servidor de forma criptografada, durante o tempo de validade do tíquete.

A Figura 2.1 apresenta a troca de mensagens cliente/servidor utilizando o protocolo Kerberos:

- **AS_REQ** é o programa de *login*, do cliente enviando seu nome para o AS.
- **AS_REP** é a resposta do AS, se o cliente estiver presente na base de dados. Quando o cliente recebe o AS_REP, no próprio cliente a senha é conferida com o número cifrado recebido, descarta-se esse número, porque a senha já foi verificada, e obtém-se a chave de sessão e um TGT para se comunicar com o TGS.
- **TGS_REQ** é quando o cliente deseja solicitar o acesso a um serviço. A mensagem é criptografada com a chave de sessão e composta do TGT da mensagem anterior, um novo autenticador.

- **TGS_REP** é a permissão de acesso (tíquete) ao serviço, solicitada pelo cliente.
- **AP_REQ** é a requisição que o cliente envia ao serviço. Esta requisição é composta da autorização (tíquete) recebida na mensagem anterior do TGS, e uma autorização gerada pelo cliente, criptografada pela chave de sessão fornecida pelo TGS;
- **AP_REP** é a resposta do servidor da aplicação enviada ao cliente. Nem sempre este pacote é requerido, somente quando a autenticação é necessária.

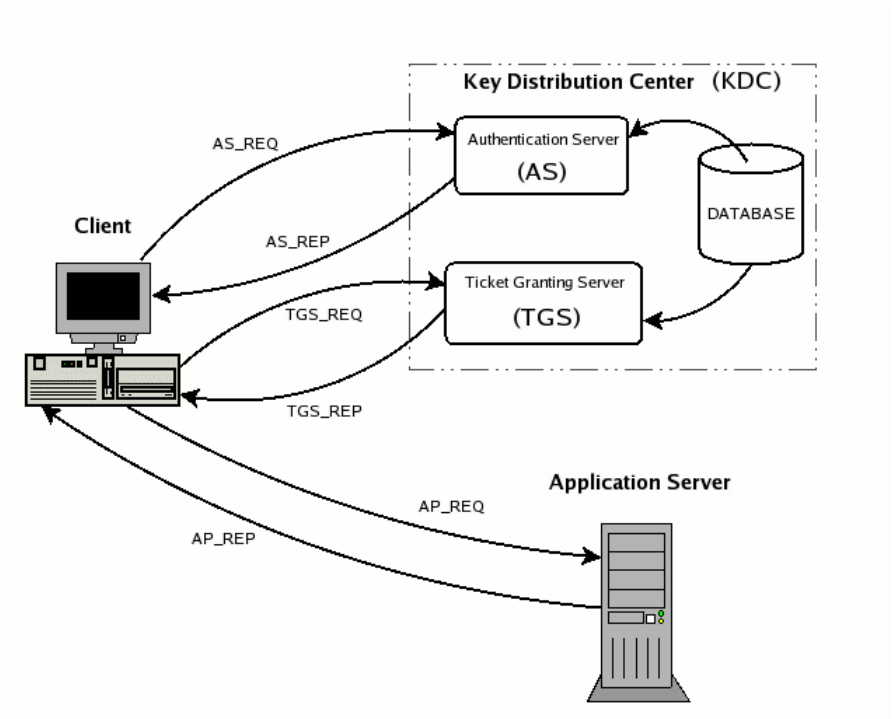

Figura 2.1: Troca de mensagens no Kerberos (RICCIARDI, 2007).

O TGT permite ao cliente solicitar outros tíquetes para acesso a serviços na rede. Desta forma o cliente é dispensado de utilizar sua senha. Todo este processo se torna transparente ao usuário. O KDC atua como um intermediador para autenticação entre o cliente e os demais serviços na rede.

Um *realm* é caracterizado pelo domínio do Kerberos, onde há máquinas que confiam no KDC. O cliente de um *realm* pode precisar acessar um serviço em

outro *realm*. Neste caso, o Kerberos possui um mecanismo chamado *cross-realm authentication* (autenticação entre *realms*), que compartilha as chaves entre os *realms*, através de uma relação de confiança entre eles.

Em (CHESWICK; BELLOVIN; RUBIN, 2005) e (COULOURIS; DOLLIMORE; KINDBERG, 2007), são apresentadas algumas críticas e limitações do Kerberos, entre elas:

- a utilização de um tíquete com validade de tempo de uso exige uma sincronização entre os relógios do cliente e do servidor;
- definir um tempo ideal para a sessão, geralmente é limitado a poucas horas, que seja suficiente para evitar interrupções do serviço e para que o recurso não fique disponível quando o cliente deixe de usá-lo;
- o protocolo foi projetado para autenticação de cliente/servidor e não para cliente/cliente.

Mais informações sobre o protocolo Kerberos são encontradas em (COULOURIS; DOLLIMORE; KINDBERG, 2007), (RICCIARDI, 2007) e (JORDAO, 2005).

2.1.2 Arquivos de Configurações

O primeiro arquivo é o `/etc/krb5.conf`, que é dividido em seções, das quais as principais são:

- `[libdefaults]` - define alguns valores padrões para serem usados pela biblioteca do Kerberos, como *realm* padrão;
- `[realms]` - contém subseções que definem informações sobre o *realm* do Kerberos, como o nome do servidor KDC, servidor que irá gerenciá-lo e suas respectivas portas;
- `[domain_realm]` - esta seção faz o mapeamento entre domínios DNS e *realms* Kerberos;
- `[logging]` - define a localização dos arquivos de *log* do Kerberos;
- `[login]` - contém valores que serão usados pelo programa de *login* do Kerberos.

O segundo arquivo é o `/etc/krb5kdc/kdc.conf`. Nele há informações de configurações do próprio servidor KDC, padrões para emissão do *tickets*, e também é divido em seções, as principais são:

- `[kdcdefaults]` - define valores padrões do comportamento geral do KDC, como portas de acesso;
- `[realms]` - contém subseções que definem informações sobre o *realm* do Kerberos, como a localização dos arquivos de configuração, da base de dados, de *log*, tipos de criptografias suportadas.

O arquivo *ACL* define as permissões dos usuários ao banco de dados Kerberos. O arquivo *ACL* deve corresponder ao valor do parâmetro `acl_file` no arquivo `kdc.conf`. Nesse trabalho está definido como `/etc/krb5kdc/kadm5.acl`. Uma linha *ACL* é composta pela entidade denominada *principal* (diretora) e suas respectivas permissões, como: `primário/instância@realm permissões`. O *principal* é divido em três partes:

- primário - corresponde ao usuário, serviço ou *host*, sendo primeiro o usuário, segundo o serviço e terceiro o *host*.
- instância - corresponde ao papel do usuário, por exemplo *admin* ou *root*, o usuário pode ter a instância *null*;
- *realm* - faz referência ao reino servido pelo Kerberos.

A Tabela 2.1 apresenta as opções de permissão usadas na entidade *principal*.

A Figura 2.2 mostra um exemplo de *ACL*. Na primeira linha qualquer usuário com instância *admin* terá todas as permissões. Na segunda linha o usuário *rafael*, com instância *null*, pode acrescentar, listar, modificar e consultar todos os usuários.

```
*/admin@UBUNTUSERVER.EMPRESALINUX.COM.BR *
rafael@UBUNTUSERVER.EMPRESALINUX.COM.BR alci
```

Figura 2.2: Exemplo de *ACL*.

Mais detalhes sobre os arquivos de configuração do Kerberos poderão ser encontrados em (MIT, 2010a) e em (MIT, 2010b).

Tabela 2.1: Permissões para um *principal* (TRIGO, 2007).

Permissão	Descrição
a	Permite acrescentar *principals* ou políticas.
A	Proíbe acrescentar *principals* ou políticas.
d	Permite remover *principals* ou políticas.
D	Proíbe remover *principals* ou políticas.
m	Permite modificar *principals* ou políticas.
M	Proíbe modificar *principals* ou políticas.
c	Permite modificar senhas de *principals*.
C	Proíbe modificar senhas de *principals*.
i	Permite consultar o banco de dados Kerberos.
I	Proíbe consultar o banco de dados Kerberos.
l	Permite listar *principals* ou polítcas.
L	Proíbe listar *principals* ou polítcas.
s	Permite a configuração explícita da chave de um *principal*.
S	Proíbe a configuração explícita da chave de um *principal*.
*	Todos os privilégios (o mesmo que admcil).
x	Idêntico ao *.

2.1.3 Principais Comandos

- `kdb5_util` - fornece um meio para criar, apagar, restaurar e fazer cópia de segurança do banco de dados Kerberos. Alguns parâmetros:
  - `dump` - realiza um *dump* da base de dados Kerberos para um arquivo;
  - `load` - restaura a base de dados Kerberos de um arquivo *dump*;
  - `create [-s]` - cria uma nova base de dados Kerberos. Com a opção *-s*, força a criação de uma senha;
  - `destroy [-f]` - apaga a base de dados Kerberos. Com a opção *-f*, não solicita confirmação.
- `kadmin.local` e `kadmin` - programas para fazer entradas e manutenção na base de dados do Kerberos, como gerenciar contas e tabelas de serviços essenciais (*keytabs*). O `kadmin.local` executa diretamente no KDC sem autenticação Kerberos, enquanto `kadmin` usa autenticação Kerberos e um RPC criptografado. Os dois programas oferecem as mesmas funcionalidades. Alguns parâmetros:
  - `addprinc` - é um *aliases* para `add_principal`, utilizado para criar *principals*;

  - `modprinc` - é um *aliases* para `modify_principal`, utilizado para modificar *principals*;
  - `ktadd` - utilizado para gerar um *keytag* ou adicionar um *principal* a um *keytag* existente, requer privilégios de administrador;
  - `ktremove` - utilizado para remover um *principal* de um *keytag* existente;
  - `cpw` - é um *aliases* para `change_password`, utilizado para alterar a senha de um *principal*.

- `kinit` - emite um *ticket* para um usuário Kerberos;
- `klist` - lista os *tickets* obtidos.

Mais detalhes sobre os comandos do Kerberos poderão ser encontrados em (MIT, 2010b).

2.2 Samba

2.2.1 Visão Geral

O Samba[6] atua como um servidor de arquivos em uma rede com servidor Linux e clientes Windows. Samba foi criado em 1992 por Andrew Tridgell, seu objetivo inicial era montar um espaço em disco em uma máquina com DOS para um servidor Unix. Tridgell criou um software com suporte ao protocolo NetBEUI e implementou o protocolo SMB (*Server Message Block*) no Unix, fazendo com que o Unix funcionasse como um servidor de arquivos Windows. Tridgell, satisfeito com o resultado, resolveu levar seu trabalho mais a fundo implementando novas melhorias e funções.

O Samba é um software de código-fonte aberto, um projeto membro do *Software Freedom Conservancy*[7], no momento do desenvolvimento deste trabalho, encontra-se na versão 3.5.8.

A lista abaixo apresenta algumas das principais características do Samba:

- trabalhar em rede TCP/IP, utilizando a porta 445 do protocolo TCP;

[6] Disponível em `http://www.samba.org/`.
[7] Disponível em `http://conservancy.softwarefreedom.org/`.

- atender clientes Windows e Linux;
- compartilhar arquivos;
- compartilhar impressoras;
- centralizar autenticação de usuários;
- atuar como Controlador Primário de Domínio - PDC;
- suportar autenticação pelo sistema (`/etc/passwd`), Kerberos, LDAP e PAM;
- suportar servidor WINS (*Windows Internetworking Name Server*).

2.2.2 Arquivo de Configuração

Toda configuração do Samba é centralizada em um único arquivo de texto simples, `/etc/samba/smb.conf`. Este arquivo é divido em seções, a lista a seguir destaca algumas das principais seções e suas opções:

- `[global]` - seção que contém as opções gerais do servidor. As configurações desta seção afetam todo o servidor:
  - `netbios name = [nome]` - nome do servidor;
  - `workgroup = [nome]` - nome do grupo de trabalho/domínio que o servidor pertencerá;
  - `server string = [identificação]` - identificação enviada do servidor Samba para o ambiente de rede;
  - `wins support = [yes]` - permite que o servidor Samba passe a trabalhar como um servidor WINS;
  - `guest account = [conta]` - nome da conta Convidado;
  - `valid users = [usuário]` - define os usuários que terão acesso aos recursos do servidor Samba;
  - `invalid users = [usuário]` - define os usuários que não terão acesso aos recursos do servidor Samba;
  - `hosts allow = [máquinas]` - define através dos *hosts* ou IPs as máquinas que terão acesso aos recursos do servidor Samba;
  - `hosts deny = [máquinas]` - define através dos *hosts* ou IPs as máquinas que não terão acesso aos recursos do servidor Samba;

  - `os level = [num]` - define o nível do sistema operacional para eleições de controlador local ou de domínio;
  - `domain master = [yes/no/auto]` - define se o servidor tentará ou não se tornar DMB (*Domain Master Browser*) da rede;
  - `local master = [yes/no]` - define se o servidor tentará ou não se tornar LMB (*Local Master Browser*) da rede local;
  - `preferred master = [yes/no/auto]` - informa se o servidor Samba terá ou não vantagens para ganhar uma eleição local;

- `[homes]` - seção que contém as opções de acesso a diretórios *homes* de usuários:
  - `path = [localização]` - define a localização do diretório compartilhado do usuário, caso não seja o diretório `home` padrão da conta;
  - `comment = [comentário]` - define um comentário para o compartilhamento;
  - `writable = [yes/no]` - define se o compartilhamento terá permissão somente de leitura ou de leitura e escrita;
  - `read only = [yes/no]` - equivalente ao `writable`, porém com a lógica invertida;
  - `browseable = [yes/no]` - define se cada usuário pode enxergar somente seu próprio diretório ou não.

No arquivo `smb.conf` é possível definir seções adicionais, para cada compartilhamento. Neste caso o nome da seção, receberá o nome do compartilhamento.

2.2.3 Principais Comandos

- `testparm` - verifica se as configurações do arquivo `smb.conf` estão corretas.
- `smbpasswd` - o uso de senha criptografada é um requisito desejável nas configurações do Samba. As senhas criptografadas são armazenadas no arquivo `/etc/samba/smbpasswd` ao invés do `/etc/passwd`. O programa `smbpasswd` gerencia este arquivo de senhas e o status de contas de usuários/ máquinas do domínio. A Tabela 2.2 apresenta alguns parâmetros.

Mais informações sobre Samba são encontradas em (MORIMOTO, 2008), (SILVA, 2010), (SOUSA, 2010) e (VERNOOIJ; TERPSTRA; CARTER, 2003).

Tabela 2.2: Alguns parâmetros do comando `smbpasswd`.

Parâmetro	Descrição
`-a`	Adiciona um usuário. O usuário já deve existir em `/etc/passwd`. Caso o usuário já exista em `/etc/samba/smbpasswd`, sua senha será alterada.
`-U`	Altera a senha do usuário, porém a antiga senha será solicitada.
`-r servidor`	Permite utilizar o comando de forma remota.
`-n`	Define o acesso sem senha para o usuário.
`-x`	Exclui o usuário do arquivo `/etc/samba/smbpasswd`.
`-d`	Desabilita o usuário.
`-e`	Habilita o usuário desabilitado.
`-m`	Adiciona uma conta de máquina. A conta de máquina já deve existir em `/etc/passwd`. Usa-se juntamente com o parâmetro `-a`.

2.3 LDAP

2.3.1 Visão Geral

Lightweight Directory Access Protocol - "LDAP, ou Protocolo Leve de Acesso a Diretórios, é um conjunto de regras que controla a comunicação entre serviços de diretórios e seus clientes." (TRIGO, 2007).

O LDAP foi originalmente construído para se comunicar com o serviço de diretório X.500[8], atualmente obsoleto. Ao longo do tempo foi evoluindo para um sistema de diretório completo e independente, por isso o nome *leightweight*, ou leve. O LDAP é um protocolo que é executado sobre o TCP/IP, encontra-se na versão 3, denominado LDAPv3, e é especificado pela RFC 4510.

O LDAP foi adotado pela empresa de *softwares* Microsoft como a base do seu serviço de diretório, Active Diretory – AD (seção 2.5). No mundo UNIX e Linux, sua implementação padrão é o pacote OpenLDAP (seção 2.4).

[8] X.500 difine uma série de padrões para rede de computadores relacionados ao serviço de diretório.

2.3.2 Árvore de diretório do LDAP

O serviço de diretório LDAP possui uma estrutura organizada em árvore de forma hierárquica. Como toda estrutura em árvore, existem os elementos: raiz, ramos e folhas. *"A raiz e os ramos são diretórios. Cada diretório pode conter outros diretórios ou elementos que são chamados de entradas; cada entrada possui um ou mais atributos que, por sua vez, podem ter um ou mais valores associados a eles, todos de acordo com um tipo de dados predefinido."* (TRIGO, 2007).

A árvore de diretório pode estar organizada de duas formas: no padrão X.500 ou no padrão DNS[9].

O padrão X.500, apresentado na Figura 2.3, é o mais tradicional. Reflete uma estrutura geográfica e/ou uma estrutura organizacional. É possível perceber referências de país, estado e cidade, como também representação de uma organização: departamentos e pessoas.

Com o advento da Internet, o padrão baseado em nomes de domínios tornou-se mais adequado. O padrão DNS, apresentado na Figura 2.4, é o mais utilizado atualmente. Os elementos são organizados como se fossem domínios, permitindo utilizar o próprio domínio da empresa, tornando-se uma configuração única.

2.3.3 Estrutura de dados LDAP

O modelo de informações do LDAP é baseado em entradas. Cada entrada é identifacada por um único nome distinto, chamado DN - *Distinguished Name*. Um arquivo chamado *schema* define a estrutura de entrada e quais atributos serão inseridos. As entradas são definidas em um *objectClass*, que especifica os atributos que a entrada deve conter, podendo ser obrigatórios ou opcionais.

Os atributos ou objetos possuem um número de controle, denominado OID - *Object ID*, registrados na IANA[10], assim como os *schemas*. Devido a complexidade para a criação de *schemas*, o LDAP fornece alguns *schemas* prontos. Na Tabela 2.3 são apresentados alguns atributos comuns encontrados em hierarquias LDAP.

LDAP Data Interchange Format - `LDIF`, é o formato em que as informações devem estar definidas para importação e exportação dos dados LDAP. Para criar

[9] *Domain Name System* - Sistema de Nomes de Domínio é um banco de dados distribuído, estruturado no formato de árvore, utilizado para traduzir nomes de domínios em IP, e vice-versa.

[10] Disponível em `http://www.iana.org/`.

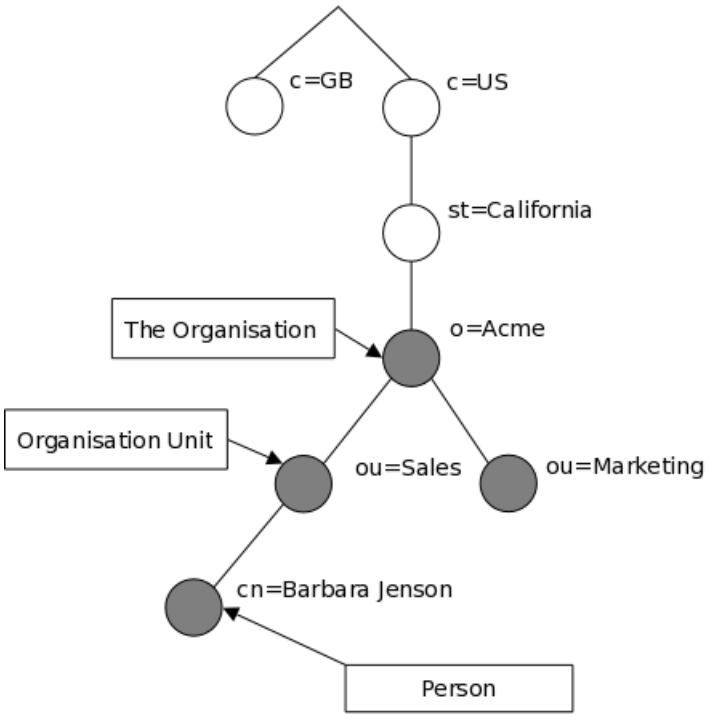

Figura 2.3: Padrão X.500. (THE OPENLDAP PROJECT, 2010).

Tabela 2.3: Exemplo de alguns atributos comuns do LDAP.

Atributo	Descrição
`o`	Organização
`ou`	Unidade organizacional
`cn`	Nome comum
`uid`	Identificação do usuário
`gn`	Nome de uma pessoa
`sn`	Sobrenome de uma pessoa
`objectClass`	Classe de objetos

um arquivo `LDIF`, deve-se utilizar um arquivo no formato texto puro e definir seus atributos de entrada, começando pela definição do domínio `dn`. A Figura 2.5 apresenta um exemplo de um arquivo `LDIF`.

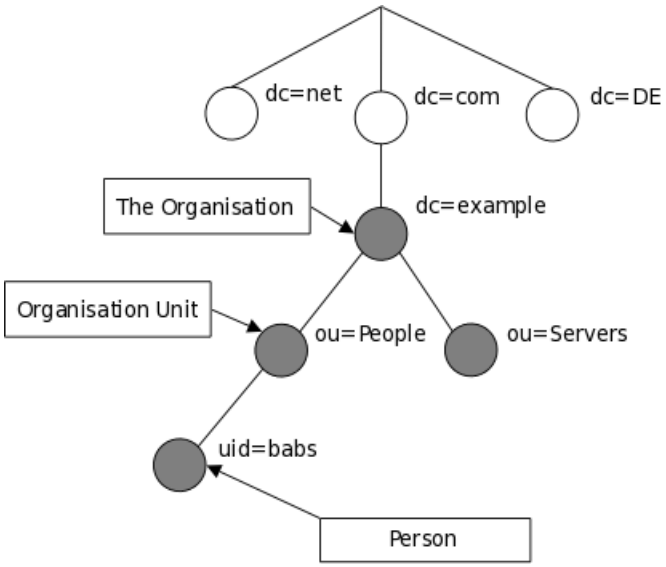

Figura 2.4: Padrão DNS. (THE OPENLDAP PROJECT, 2010).

```
# exemplo.ldif
dn: dc=exemplo,dc=com,dc=br
objectclass: dcObject
objectclass: organization
o: Exemplo Ltda
dc: exemplo
```

Figura 2.5: Exemplo de um arquivo `LDIF`.

2.3.4 Vantagens do LDAP

A lista abaixo apresenta algumas vantagens para motivação em utilizar o LDAP:

- com uma estrutura em formato de árvore é altamente otimizado para consultas;
- a forma hierárquica de como os dados são armazenados nos diretórios segue uma padronização;
- centraliza e organiza as informações em uma única estrutura, mas apresenta um modelo distribuído para armazenamento de informações, ou seja, permite que sejam usados diferentes servidores para armazenagem;

- facilidade de acesso aos dados LDAP através de ferramentas de linha de comando, como `ldapsearch`, ou com ferramentas Web, como o phpLDAPadmin[11];
- LDAP é suportado por grande parte das linguagens de programação, facilitando o desenvolvimento de ferramentas para manipulação de seus dados;
- vários serviços de redes, como e-mail, web, domínio de rede, *proxy*, entre outros, suportam o LDAP como sua base de dados.

Mais informações sobre o protocolo LDAP são encontradas em (TRIGO, 2007), (THE OPENLDAP PROJECT, 2010) e (NEMETH; SNYDER; HEIN, 2007).

2.4 OpenLDAP

2.4.1 Visão Geral

OpenLDAP[12] é uma implementação do LDAP (seção 2.3). Originário de um trabalho realizado pela Universidade de Michigan, agora mantido pela comunidade da Internet, é um projeto de código-fonte aberto, e no momento do desenvolvimento deste trabalho, encontra-se na versão 2.4.23.

O OpenLDAP possui as seguintes características, de acordo com (TRIGO, 2007):

- suporte a IPv4 e IPv6;
- autenticação (Cryrus Sasl-Kerberos V, GSSAPI, Digest-MD5);
- segurança no transporte - SSL e TLS;
- controle de acessos;
- escolha entre banco de dados;
- capacidade de atender a múltiplos bancos de dados simultaneamente;
- alta performance em múltiplas chamadas;

[11] Disponível em `http://phpldapadmin.sourceforge.net/`.
[12] Disponível em `http://www.openldap.org/`.

- replicação de base.

`Slapd` - *Stand Alone LDAP Daemon*, é o *deamon* de servidor padrão. Ele pode escutar as conexões em qualquer porta, mas a padrão é 389. O `slurpd` - *Standalone LDAP Update Replication Daemon*, é o *deamon* utilizado para propagar as alterações de um banco de dados do `slapd` para outro, ou seja, trata de replicação.

2.4.2 Arquivos de Configurações

O arquivo de configuração `/etc/ldap/slapd.conf` apresenta uma série de opções globais que se aplicam ao `slapd`.

- `include` - define os *schemas* que serão utilizados e sua respectiva localização;
- `database` - define o tipo de banco de dados a ser utilizado, entre `ldbm` e `bdb`, ou outro;
- `suffix` - define o domínio a ser utilizado;
- `rootdn` - define o nome do administrador do OpenLDAP, seguindo a hierarquia definida no `suffix`;
- `rootpw` - define a senha do administrador do OpenLDAP, pode ser uma senha texto puro ou criptografada, gerada pelo comando `slappasswd`;
- `directory` - define onde ficarão armazenados os arquivos binários da base do OpenLDAP.

A Figura 2.6 apresenta um exemplo de configuração do arquivo `slapd.conf`.

```
database bdb
suffix "dc=empresalinux,dc=com,dc=br"
rootdn "cn=admin,dc=empresalinux,dc=com,dc=br"
rootpw secret
directory /usr/local/var/openldap-data
```

Figura 2.6: Exemplo do arquivo `slapd.conf`.

O arquivo de configuração `/etc/ldap/ldap.conf` é usado para definir os padrões do sistema que se aplicam aos clientes LDAP. As principais opções deste arquivo são:

- `BASE` - especifica a base DN utilizada nas execuções das operações LDAP, está relacionado com o parâmetro `suffix` no arquivo `slapd.conf`.
- `HOST` - especifica o nome ou endereço IP do servidor LDAP.

A Figura 2.7 apresenta um exemplo de configuração do arquivo `ldap.conf`.

```
BASE dc=empresalinux, dc=com, dc=br
HOST 127.0.0.1
```

Figura 2.7: Exemplo do arquivo `ldap.conf`.

2.4.3 Principais Comandos

- `ldapsearch` - utilizado para realizar pesquisas. A Tabela 2.4 apresenta alguns parâmetros.

Tabela 2.4: Alguns parâmetros do comando `ldapsearch`.

Parâmetro	Descrição
`-x`	Autenticação simples.
`-h`	Nome do *host* do servidor OpenLDAP, caso seja diferente do valor definido no arquivo `ldap.conf`.
`-b`	Base de pesquisa, caso seja diferente do valor definido no arquivo `ldap.conf`
`-L`	Saída no formado `LDIF`, pode ser usado para obter três formatos diferentes: -L, -LL ou -LLL.
`[filtro]`	Define filtro de pesquisa, seu valor padrão é `'(objectClass=*)'`.
`[atributos]`	Especifica os atributos que devem retornar na pesquisa.

- `ldapadd` - utilizado para adicionar informações. A Tabela 2.5 apresenta alguns parâmetros.
- `ldapdelete` - utilizado para apagar registros. A Tabela 2.6 apresenta alguns parâmetros.
- `ldapmodify` - utilizado para alterar campos do registro. A Tabela 2.7 apresenta alguns parâmetros.

Tabela 2.5: Alguns parâmetros do comando `ldapadd`.

Parâmetro	Descrição
`-x`	Autenticação simples.
`-D`	Especifica o domínio.
`-w`	Especifica a senha ou -W para solicitar a senha no *prompt*.
`-f arquivo`	Especifica o arquivo no formato `LDIF`.
`-v`	Modo *verbose*, exibe informações após execução do comando.

Tabela 2.6: Alguns parâmetros do comando `ldapdelete`.

Parâmetro	Descrição
`-x`	Autenticação simples.
`-D`	Especifica o domínio.
`-w`	Especifica a senha ou -W para solicitar a senha no *prompt*.
`-f arquivo`	Especifica o arquivo no formato `LDIF`, que contém os registros a serem apagados.
`-v`	Modo *verbose*, exibe informações após execução do comando.
`dn`	Especifica a entrada a ser apagada, definindo atributos e seus respectivos valores.

Tabela 2.7: Alguns parâmetros do comando `ldapmodify`.

Parâmetro	Descrição
`-x`	Autenticação simples.
`-D`	Especifica o domínio.
`-w`	Especifica a senha ou -W para solicitar a senha no *prompt*.
`-f arquivo`	Especifica o arquivo no formato `LDIF`, que contém os campos a serem alterados.
`-v`	Modo *verbose*, exibe informações após execução do comando.

- `slapcat` - utilizado para listar o conteúdo da base no formato `LDIF`, muito útil para gerar um *dump* do conteúdo da base. A Tabela 2.8 apresenta alguns parâmetros.

Tabela 2.8: Alguns parâmetros do comando `slapcat`.

Parâmetro	Descrição
`-b`	Especifica a base a ser gerada.
`-a`	Especifica um filtro, para retornar apenas os registros que combinem com o filtro.
`-s`	Especifica a a árvore que será pesquisada.
`-f arquivo`	Especifica o arquivo do configuração `lsapd.conf`.
`-l arquivo`	Especifica o arquivo no formato `LDIF`, a ser gerado.
`-v`	Modo *verbose*, exibe informações após execução do comando.

- `slapadd` - utilizado para adicionar informações quando o `slapd` não estiver em execução, muito útil para inserir grande quantidade de dados. A Tabela 2.9 apresenta alguns parâmetros.

Tabela 2.9: Alguns parâmetros do comando `slapadd`.

Parâmetro	Descrição
`-b`	Especifica a base a ser modificada.
`-w`	Escreve informações de contexto para o *syncrepl* utilizar na replicação da base LDAP.
`-f arquivo`	Especifica o arquivo do configuração `slapd.conf`.
`-l arquivo`	Especifica o arquivo no formato `LDIF` de entrada.
`-v`	Modo *verbose*, exibe informações após execução do comando.

Mais informações sobre OpenLDAP são encontradas em (TRIGO, 2007), (THE OPENLDAP PROJECT, 2010), (SOUSA, 2010) e (SUNGAILA, 2007).

2.5 Active Directory

2.5.1 Visão Geral

Active Directory - AD é um serviço de diretório para Windows Server versões 2000, 2003 e 2008. No Windows NT já existia o PDC (*Primary Domain Controller* – Controlador Primário de Domínio), um servidor central para armazenar e gerenciar senhas das estações. Mas só a partir do Windows 2000 que se originou o Active Directory, baseado nos protocolos Kerberos (seção 2.1) e LDAP (seção 2.3), com mais recursos que o Windows NT e permitindo outros servidores no mesmo domínio.

Em síntese, o Active Directory é capaz de realizar as seguintes funções:

> "*Ele permite que os administradores gerenciem as informações de toda a empresa de forma eficiente a partir de um repositório central que pode ser distribuído globalmente. Uma vez que informações sobre os usuários e grupos, computadores e impressoras, aplicativos e serviços foram adicionadas ao Active Directory, podem ser disponibilizadas para utilização em toda a rede para muitas ou poucas pessoas, como você preferir. A estrutura da informação pode corresponder à estrutura da sua organização e seus usuários podem consultar o Active Directory para encontrar a localização de uma impressora ou o endereço de e-mail de um colega. Com unidades organizacionais, você pode delegar controle e gestão dos dados, contudo, você vê o ajuste.*"(DESMOND *et al.*, 2009).

O Active Directory fornece a solução chamada *Identity and Access* - IDA (Identidade e Acesso), que possui o objetivo de manter a segurança dos recursos de rede. Uma infraestrutura IDA deve:

- armazenar informações das identidades - uma identidade pode ser usuários, grupos, computadores, serviço, ou outro objeto que realiza uma ação na rede;
- autenticar uma identidade - o Active Directory utiliza o protocolo Kerberos para autenticar as identidades;
- controlar acesso - o controle de acesso é realizado através de *ACL's*, que especifica os níveis de acesso a determinadas identidades, por exemplo, a um documento;

- fornecer auditoria - fornece um mecanismo por meio do qual gerencia a auditoria, sobre as atividades dentro da infraestrutura IDA.

O Active Directory, na versão do Windows Server 2008, é composta por cinco tecnologias, formando um solução IDA completa, como mostra a Figura 2.8.

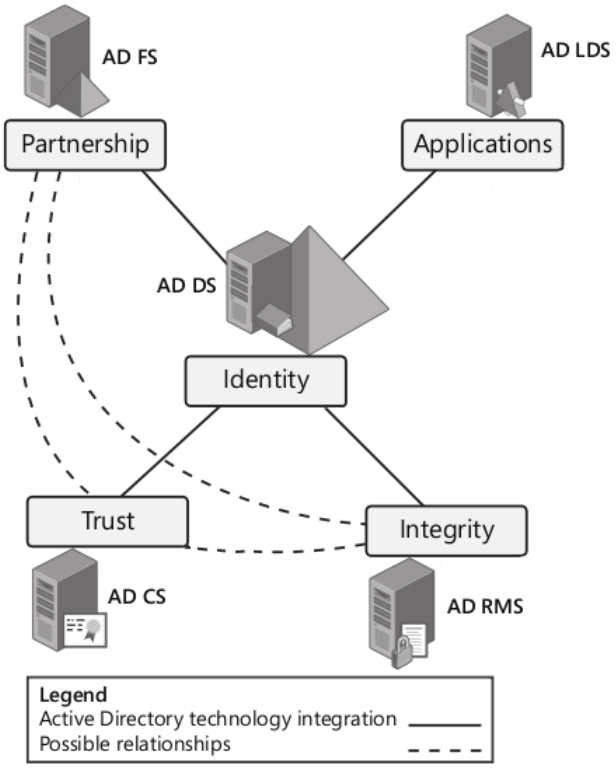

Figura 2.8: A integração das cinco tecnologias do Active Directory, segundo (HOLME; RUEST; RUEST, 2008).

As cinco tecnologias mencionadas são:

- **Active Directory Domain Services (Identidade)** - o AD DS é a principal tecnologia do Active Directory. Ele é o centro de gerenciamento de identidades, é responsável pela autenticação, autorização e gerenciamento das informações de objetos que realizam ações na rede. É no AD DS que os protocolos LDAP e Kerberos são implementados.
- **Active Directory Certificate Services (Confiabilidade)** - o AD CS é usado para criar, distribuir e gerenciar certificados de chave pública para assegurar

os recursos de rede. Desta forma, ele pode ser usado para configurar uma autoridade certificadora para emitir certificados digitais como parte de uma infraestrutura de chave pública (Publik Key Infrastructure - PKI), que vincula a identidade de uma pessoa, dispositivo ou serviço a uma chave privada correspondente. Se vinculado à autoridade de certificação externa conhecida, o AD CS pode emitir certificados à comunidade externa, ou apenas integrar ao AD DS, para fornecer automaticamente certificados aos usuários e computadores da rede interna.

- **Active Directory Federation Services (Parceria)** - o AD FS permite estender a solução IDA a outras plataformas Windows ou não Windows. Com o AD FS é possível autenticar em uma rede e usar os serviços de outra rede, quando ele promove uma relação de confiabilidade entre as redes. Na realidade ele estende a estrutura interna do AD DS ao mundo externo, para isto é necessário a integração com o AD CS e o AD RMS.

- **Active Directory Lightweight Directory Services (Aplicações)** - o AD LDS, conhecido anteriormente como Active Directory Application Mode (ADAM), pode funcionar de forma autônoma com relação ao AD DS. Ele pode ser usado por aplicações que exigem apenas o serviço de diretório, sem o serviço de domínio. Como o próprio nome sugere, ele é uma implementação leve do AD DS.

- **Active Directory Rights Management Services (Integridade)** - o AD RMS é responsável pela proteção das informações que permite implementar modelos persistentes de política de uso, que definem o uso autorizado e não autorizado. Na prática ele irá definir, por exemplo, se o documento poderá ter permissões de escrita ou leitura ou de cópia ou de impressão, entre outras permissões, ou seja, seu principal objetivo é manter a integridade dos dados e proteger a propriedade intelectual.

Além da solução IDA, o Active Directory pode gerenciar recursos da rede. Isto é possível porque ele utiliza um *schema* para definir objetos e atributos de usuários, grupos e computadores. O Active Directory possui um tipo de índice, chamado *catálogo global*, que permite localizar os objetos no diretório. Esta tarefa é possível graças a Active Directory Services Interface (ADSI)[13] e ao protocolo LDAP que são utilizados para ler e manipular o armazenamento de dados.

[13] ADSI é uma interface utilizada para manibular objetos do Active Directory.

2.5.2 Componentes de uma infraestrutura do Active Directory

O AD DS fornece a base da solução IDA e o gerenciamento de uma rede, e segundo (HOLME; RUEST; RUEST, 2008) apresenta os componentes de uma infraestrutura do Active Directory da seguinte forma:

- **Armazenamento de dados** - o AD DS armazena suas identidades no diretório (um armazenamento de dados hospedado nos controladores de domínio). O banco de dados é dividido em várias partições, incluindo o esquema, configuração, catálogo global e o contexto de nomeação de domínios que contém os dados sobre objetos dentro de um domínio - os usuários, grupos e computadores, por exemplo.

- **Controladores de domínio** - os controladores de domínios ou DCs são servidores que executam a função de AD DS. Como parte dessa função, eles executam o serviço Kerberos Key Distribution Center (KDC), que realiza a autenticação e outros serviços do Active Directory.

- **Domínio** - são necessários um ou mais controladores de domínio para criar um domínio no Active Directory. Um domínio é uma unidade administrativa dentro da qual certas capacidades e características são compartilhadas. Os controladores de domínio replicam a partição de armazenamento de dados do domínio, que contém os dados da identidade dos usuários ou grupos ou computadores do domínio. Assim, os controladores de domínio mantém uma consistência dos dados da identidade, podendo qualquer DC autenticar com qualquer identidade em um domínio.

- **Floresta** - uma floresta é uma coleção de domínios do Active Directory. O primeiro domínio é definido como *domínio raiz de floresta*. A floresta define o limite do armazenamento e replicagem dos dados, porque ela possui uma única instância do esquema de diretório e uma única definição de configuração de rede.

- **Árvore** - as árvores são o resultado direto dos nomes de DNS escolhidos para os domínios na floresta. Por exemplo, se há dois nomes no DNS chamados *universidade.com* e *escola.com*, estes dois domínios são considerados duas árvores em uma floresta, porque são nomes distintos. Se os nomes no DNS forem *universidade.com* e *graduacao.universidade.com*, são dois domínios e uma única árvore em uma floresta, porque são nomes contínuos no DNS, um domínio é subdomínio do outro e estão todos na mesma árvore.

- **Nível funcional** - o nível funcional indica o nível de recursos disponíveis do AD DS em um domínio ou por toda a floresta. O nível funcional está relacionado com a versão do Windows, quanto mais alta a versão, mais recursos estarão disponíveis. Há três níveis funcionais de domínio: Windows 2000, Windows Server 2003 e Windows Server 2008; e dois níveis funcionais de floresta: Windows Server 2003 e Windows Server 2008.

- **Unidade organizacional** - um contêiner é a classe de objeto. Os contêineres padrões, são Users, Computers e Builtin, a unidade organizacional (*Organizational Unit* - OU) é outro tipo de contêiner. As OUs podem fornecer um escopo para gerenciar um objeto, por exemplo, muito útil quando deseja-se aplicar uma política de uso a usuários e computadores, então aplica-se diretamente em uma OU, a qual os objetos pertencem.

- **Sites** - no Active Directory, um site é um objeto que representa uma parte da empresa, onde há boa conectividade na rede. Sendo assim, um site representa os limites de replicação e serviços dentro do Active Diretocry. Controladores de domínio trabalham com maior eficiência dentro de um site, por exemplo, a autenticação de um usuário no domínio de um site diferente pode se tornar lenta, dispendiosa e insegura.

Em uma infraestrutura Active Directory, para que o AD DS funcione como um controlador de domínio corretamente, deve atender os seguintes itens:

- o nome do domínio e o nome DNS devem ser únicos;

- ao criar uma floresta, o nível funcional deve ser configurado corretamente, caso exista controladores de domínio que rodam em versões anteriores do Windows;

- é necessário que se tenha um DNS respondendo pelos domínios do Active Directory, pode se usar o Windows DNS Service ou um serviço DNS de terceiros;

- o servidor controlador de domínio exige configuração de IP estático;

- a senha da conta de usuário *Administrador* do servidor controlador de domínio não pode ser em branco;

- o dados do controlador de domínio e o volume do sistema (SYSVOL) podem ser armazenados em uma unidade (partição) diferente do sistema operacional.

2.5.3 Objetos do Active Directory

O Active Directory é um serviço de diretório, e a função de um serviço de diretório, é manter informações sobre os recursos conectados a sua rede, como usuário, grupos e computadores. Estes recursos são divididos em unidades organizacionais, que possuem o papel de coletar objetos que compartilham requisitos comuns da administração, configuração ou visibilidade, fornecendo uma hierarquia administrativa. As OUs são uma divisão lógica dentro do domínio, com elas é possível restringir os direitos administrativos apenas a nível de OUs, sem que um usuário tenha poderes sobre outros objetos do domínio.

Para que um usuário possa ter acesso aos recursos da rede é necessário criar uma conta. Uma conta no domínio é um objeto Active Directory. Os objetos possuem atributos para armazenar suas informações. Os três principais objetos do Active Directory são:

- Usuários ou Users - o objeto Users armazena informações para que o usuário do domínio possa acessar os recursos da rede. Possui atributos como: logon, senha, nome, e-mail, entre outros.

- Grupos ou Groups - gerenciar recursos da rede com base em contas individuais de usuário, torna-se inviável para o administrador da rede. O objeto Groups agrupa os usuários, para facilitar o gerenciamento, assim todas as contas de usuário relacionadas com o mesmo grupo estarão sujeitas às mesmas políticas de uso do grupo.

- Computadores ou Computers - todo computador que deseja acessar o domínio, deve ter uma conta cadastrada no domínio. Esta conta do computador é representada no domínio pelo objeto Computers. O nome desta conta dever ser o mesmo nome do *host* da máquina.

2.5.4 Ferramentas Administrativas do Active Directory

As ferramentas administrativas do Active Directory, ou *snap-ins* como são chamadas, fornecem as funcionalidades necessárias para o suporte do serviço de diretório. Estas ferramentas utilizam uma estrutura comum chamada Microsoft Management Console (MMC). São janelas personalizáveis semelhantes ao Windows Explorer.

Os *snap-ins* são encontrados em `Iniciar -> Painel de Controle -> Ferramentas Administrativas`, e são os seguintes:

- **Usuários e Computadores do Active Directory** - gerencia os objetos usuários, computadores, grupos, entre outros;
- **Serviços e Sites do Active Directory** - gerencia replicação, topologia de rede e serviços relacionados;
- **Domínios e Relações de Confiança do Active Directory** - configura e mantém relações de confiança e os níveis funcionais do domínio e da floresta;
- **Schema do Active Directory** - examina e modifica a configuração dos atributos e das classes de objeto do Active Directory. Como não é comum alterar o *schema*, não é instalado por padrão.

A versão do Windows Server 2008 R2 possui todos os *snap-ins* mencionados, e uma ferramenta exclusiva, a Central Administrativa do Active Directory. Localizada em `Ferramentas Administrativas` no `Painel de Controle`, com uma única interface gráfica aprimorada, é possível: gerenciar os objetos, conectar e gerenciar a um ou vários domínios ou controladores de domínio na mesma instância da Central Administrativa e realizar pesquisas de dados do Active Directory.

Mais informações sobre o Active Directory são encontradas em (HOLME; RUEST; RUEST, 2008), (REIMER *et al.*, 2008) e (RUEST; RUEST, 2008).

Capítulo 3

Implementação com Servidor Linux e Cliente Windows

Neste capítulo serão descritos os procedimentos para instalação e configuração do Kerberos, Samba e OpenLDAP no servidor Linux, como também as configurações para autenticação do cliente Windows no servidor Linux.

3.1 Instalação e configuração no servidor Linux

Nesta seção serão descritos de forma progressiva os procedimentos para instalação e configurações dos respectivos serviços: Kerberos, Samba e OpenLDAP, todos realizados no servidor Linux.

É importante lembrar que os procedimentos de instalação e configuração desta seção foram realizados na distribuição Ubuntu Server Edition 10.04 64-bit (Capítulo 1), o que é válido para a maioria das distribuições baseadas no Debian. Outras distribuições Linux podem ter dado outros nomes a esses arquivos, inclusive outras localizações. Consulte a documentação de sua distribuição para mais detalhes.

3.1.1 Instalação e configuração do Kerberos

O Kerberos necessita de alguns pré-requisitos para seu correto funcionamento. Um deles é que todos os computadores da rede estejam com seus relógios sincroniza-

dos, isto é possível instalando o NTP[1] (*Network Time Protocol*). Outro serviço necessário é o DNS[2], para correta resolução dos nomes dos computadores da rede.

A instalação do Kerberos utilizando pacotes pré-compilados está descrita conforme a Figura 3.1. O pacote `krb5-kdc` corresponde ao servidor Kerberos (KDC). O pacote `krb5-admin-server` responsável pela criação, remoção, mudanças de senhas e outros comandos de administração através do protocolo Kerberos. E o pacote `libkrb5-dev` contém os *links* simbólicos, cabeçalhos e bibliotecas de desenvolvimento necessárias para compilar e *linkar* programas que usam as bibliotecas do Kerberos.

```
ubuntuServer:~# aptitude install krb5-kdc krb5-admin-server libkrb5-dev
```

Figura 3.1: Instalação do Kerberos.

Para configurar o Kerberos, deve-se alterar o arquivo `/etc/krb5.conf`. A Figura 3.2 apresenta as modificações necessárias para o correto funcionamento do Kerberos. Na seção `[libdefaults]` a *tag* `default_realm` recebe o nome do *realm*. Na seção `[realms]` deve-se definir o nome do servidor KDC e o nome do servidor que irá gerenciá-lo. Esta seção permite adicionar outros *realms* quando houver. Na seção `[domain_realm]` deve-se definir a relação entre nome de domínio e *realm* na biblioteca do Kerberos.

```
[libdefaults]
        default_realm = EMPRESALINUX.COM.BR

[realms]
        EMPRESALINUX.COM.BR = {
                kdc = ubuntuserver.empresalinux.com.br
                admin_server = ubuntuserver.empresalinux.com.br
                default_domain = EMPRESALINUX.COM.BR
        }
[domain_realm]
        .empresalinux.com.br = EMPRESALINUX.COM.BR
        empresalinux.com.br = EMPRESALINUX.COM.BR
```

Figura 3.2: Arquivo krb5.conf

[1] Instalação disponível em `http://www.eecis.udel.edu/~mills/ntp/html/build.html`

[2] Instalação do DNS com BIND, disponível em `http://www.isc.org/software/bind/documentation`

A Figura 3.2 contém somente as configurações que devem ser modificas ou adicionadas no arquivo `krb5.conf`. No Apêndice A.2, encontra-se a configuração completa realizada no arquivo.

No arquivo `/etc/krb5kdc/kdc.conf` contém a localização dos principais arquivos do *realm* criado, conforme a Figura 3.3

```
[kdcdefaults]
    kdc_ports = 750,88

[realms]
    EMPRESALINUX.COM.BR = {
        database_name = /var/lib/krb5kdc/principal
        admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
        acl_file = /etc/krb5kdc/kadm5.acl
        key_stash_file = /etc/krb5kdc/stash
        kdc_ports = 750,88
        max_life = 10h 0m 0s
        max_renewable_life = 7d 0h 0m 0s
        master_key_type = des3-hmac-sha1
        supported_enctypes = aes256-cts:normal arcfour-hmac:normal
des3-hmac-sha1:normal des-cbc-crc:normal des:normal des:v4 des:norealm
des:onlyrealm des:afs3
        default_principal_flags = +preauth
    }
```

Figura 3.3: Arquivo kdc.conf

Após a configuração dos arquivos, deve-se criar o banco de dados do Kerberos com o comando `kdb5_util`. Com a opção *-s* deve-se criar uma senha conforme a Figura 3.4. Antes de executar este comando, certifique-se que os diretórios referenciados no arquivo `kdc.conf` já existam.

As permissões dos usuários e servidores serão definidas no arquivo ACL `kadm5.acl`, conforme o valor do parâmetro `acl_file` no arquivo `kdc.conf`. A Figura 3.5 apresenta o arquivo `kadm5.acl`. Mais detalhes sobre o arquivo ACL podem ser encontrados na subseção 2.1.2.

Após definir as políticas para os usuários, deve-se criá-las no banco de dados, com o comando `kadmin.local`. O comando interno `addprinc` irá adicionar *principals*, e o comando interno `ktadd` irá adicionar o mesmo em um *keytag*, caso não exista, um *keytag* será gerado, conforme a Figura 3.6. O usuário `root` será adicionado com uma instância `admin`, conforme a Figura 3.7.

```
ubuntuServer:~# kdb5_util create -s
Loading random data
Initializing database '/var/lib/krb5kdc/principal' for realm
    'EMPRESALINUX.COM.BR',
master key name 'K/M@EMPRESALINUX.COM.BR'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
```

Figura 3.4: Criando banco de dados do Kerberos.

```
*/admin@UBUNTUSERVER.EMPRESALINUX.COM.BR *
rafael@UBUNTUSERVER.EMPRESALINUX.COM.BR alci
*/root@UBUNTUSERVER.EMPRESALINUX.COM.BR
```

Figura 3.5: Arquivo `kadm5.acl`.

Para inicializar o Kerberos, são necessários dois comandos: `krb5kdc` e `kadmin`. A Figura 3.8 mostra os dois comandos, observe que o segundo comando ficará em execução. O programa `krb5kdc` é o KDC, responsável pela distribuição dos *tickets* aos usuários e o `kadmin` é responsável pelo gerenciamento de contas, como: criar, alterar e remover usuários.

Após realizar as configurações, as primeiras contas poderão ser criadas com o comando `kadmin.local` e o comando interno `addprinc`, conforme a Figura 3.9. Observe que uma senha será solicitada ao usuário `rafael`. Como mencionado anteriormente, a instância do usuário pode ser *null*, ou seja, opcional.

Neste momento, antes do cliente autenticar-se no servidor Kerberos, seus relógios já devem estar sincronizados e o DNS funcionando corretamente. Um teste para verificar o correto funcionamento do Kerberos pode ser feito com o comando `kinit`, para gerar um *ticket* ao usuário, e o comando `klist` para listar o *ticket*, conforme a Figura 3.10.

Mais detalhes sobre a instalação do Kerberos poderão ser encontrados em (MIT, 2010a) e em (TRIGO, 2007).

```
ubuntuServer:~# kadmin.local
Authenticating as principal root/admin@EMPRESALINUX.COM.BR with
    password.
kadmin.local:  addprinc kadmin/admin@EMPRESALINUX.COM.BR
WARNING: no policy specified for kadmin/admin@EMPRESALINUX.COM.BR;
    defaulting to no policy
Enter password for principal "kadmin/admin@EMPRESALINUX.COM.BR":
Re-enter password for principal "kadmin/admin@EMPRESALINUX.COM.BR":
add_principal: Principal or policy already exists while creating
    "kadmin/admin@EMPRESALINUX.COM.BR".
kadmin.local:  ktadd -k /etc/krb5kdc/kadm5.keytab kadmin/admin
    kadmin/changepw
Entry for principal kadmin/admin with kvno 3, encryption type
    AES-256 CTS mode with 96-bit SHA-1 HMAC added to keytab
    WRFILE:/etc/krb5kdc/kadm5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type ArcFour
    with HMAC/md5 added to keytab WRFILE:/etc/krb5kdc/kadm5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type Triple
    DES cbc mode with HMAC/sha1 added to keytab
    WRFILE:/etc/krb5kdc/kadm5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type DES cbc
    mode with CRC-32 added to keytab WRFILE:/etc/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type
    AES-256 CTS mode with 96-bit SHA-1 HMAC added to keytab
    WRFILE:/etc/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type
    ArcFour with HMAC/md5 added to keytab
    WRFILE:/etc/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type
    Triple DES cbc mode with HMAC/sha1 added to keytab
    WRFILE:/etc/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type DES
    cbc mode with CRC-32 added to keytab
    WRFILE:/etc/krb5kdc/kadm5.keytab.
kadmin.local:  quit
```

Figura 3.6: Adicionar *principal*.

3.1.2 Instalação e configuração do Samba

A instalação do Samba utilizando pacotes pré-compilados está descrita conforme a Figura 3.11. O pacote `samba` corresponde o *deamon* do servidor Samba, o `smbclient` é um pacote para instalar uma interface de linha de comando do cliente

```
ubuntuServer:~# kadmin.local -q "addprinc root/admin"
Authenticating as principal root/admin@EMPRESALINUX.COM.BR with
    password.
WARNING: no policy specified for root/admin@EMPRESALINUX.COM.BR;
    defaulting to no policy
Enter password for principal "root/admin@EMPRESALINUX.COM.BR":
Re-enter password for principal "root/admin@EMPRESALINUX.COM.BR":
Principal "root/admin@EMPRESALINUX.COM.BR" created.
```

Figura 3.7: Adicionar usuário `root`.

```
ubuntuServer:~# krb5kdc &
[1] 923
root@ubuntuServer:~# kadmin &
[2] 925
[1]   Fim da execução com status 1      krb5kdc
ubuntuServer:~# Authenticating as principal
    root/admin@EMPRESALINUX.COM.BR with password.
```

Figura 3.8: Inicializar o Kerberos.

```
ubuntuServer:~# kadmin.local
Authenticating as principal root/admin@EMPRESALINUX.COM.BR with
    password.
kadmin.local:  addprinc rafael
WARNING: no policy specified for rafael@EMPRESALINUX.COM.BR;
    defaulting to no policy
Enter password for principal "rafael@EMPRESALINUX.COM.BR":
Re-enter password for principal "rafael@EMPRESALINUX.COM.BR":
Principal "rafael@EMPRESALINUX.COM.BR" created.
kadmin.local:  quit
```

Figura 3.9: Adicionar usuário a base de dados Kerberos.

Samba para Linux e o pacote `samba-doc` corresponte à documentação do Samba. Como o objetivo desta parte do trabalho é a interoperabilidade com o Windows 7, é exigido que se instale o Samba versão 3.3 ou superior. Para consultar a versão do Samba instalado utilize o comando `smbd -V`.

O servidor Samba será configurado para atuar como PDC - *Primary Domain Controler*. As configurações do Samba como servidor de autenticação serão priorizadas neste trabalho. Para as configurações de serviços de arquivos e impressora,

```
ubuntuServer:~# kinit rafael
Password for rafael@EMPRESALINUX.COM.BR:
ubuntuServer:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: rafael@EMPRESALINUX.COM.BR

Valid starting     Expires            Service principal
02/09/11 23:53:11  02/10/11 09:53:11
    krbtgt/EMPRESALINUX.COM.BR@EMPRESALINUX.COM.BR
        renew until 02/10/11 23:53:08
```

Figura 3.10: Gerar e listar o *ticket*.

```
ubuntuServer:~# aptitude install samba smbclient samba-doc
```

Figura 3.11: Instalação do Samba.

consulte (MORIMOTO, 2008). A Figura 3.12 mostra como o arquivo `smb.conf` deve estar configurado.

A configuração completa realizada no arquivo `smb.conf` poderá ser encontrada no Apêndice A.3.

Para verificar se há algum erro de sintaxe no arquivo `smb.conf`, e se está corretamente configurado para atuar como um PDC, execute o comando `testparm`, conforme a Figura 3.13.

Com as configurações realizadas, deve-se reiniciar o servidor Samba, conforme a Figura 3.14 e adicionar os usuários, começando pelo administrador do Samba, `root`, com o seguinte comando: `smbpasswd -a root`. Um outro usuário deve ser adicionado para testes, e deve-se criar um conta para a máquina da rede, neste caso o cliente Windows, a Figura 3.15 mostra como adicionar as contas. É importante evitar de se cadastrar um usuário no Samba com o mesmo nome do usário local já existente do cliente Windows 7.

3.1.3 Instalação e configuração do OpenLDAP

A instalação do OpenLDAP utilizando pacotes pré-compilados, está descrita conforme a Figura 3.16. O pacote `slapd` corresponde o *deamon* do servidor OpenLDAP e o `ldap-utils` é um pacote de utilitários do OpenLDAP.

```
[global]
        workgroup = EMPRESALINUX
        server string = Servidor PDC
        interfaces = eth0, lo
        bind interfaces only = Yes
        map to guest = Bad User
        obey pam restrictions = Yes
        pam password change = Yes
        passwd program = /usr/bin/passwd %u
        passwd chat = *Enter\snew\s*\spassword:* %n\n
*Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully* .
        unix password sync = Yes
        syslog = 0
        log file = /var/log/samba/log.%m
        max log size = 1000
        name resolve order = lmhosts wins bcast
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        domain logons = Yes
        os level = 200
        preferred master = Yes
        domain master = Yes
        dns proxy = No
        wins support = Yes
        usershare allow guests = Yes
        panic action = /usr/share/samba/panic-action %d
```

Figura 3.12: Arquivo `smb.conf`.

```
ubuntuServer:~# testparm
Load smb config files from /etc/samba/smb.conf
rlimit_max: rlimit_max (1024) below minimum Windows limit (16384)
Loaded services file OK.
Server role: ROLE_DOMAIN_PDC
Press enter to see a dump of your service definitions
```

Figura 3.13: Comando `testparm`.

```
ubuntuServer:~# service smbd stop
ubuntuServer:~# service smbd start
```

Figura 3.14: Reiniciando o servidor Samba.

```
# adduser teste
# smbpasswd -a teste
# useradd -d /dev/null -s /bin/false windowscliente$
# passwd -l windowscliente$
# smbpasswd -a -m windowscliente
```

Figura 3.15: Adicionar contas de usuário e de máquina ao Samba.

```
ubuntuServer:~# aptitude install slapd ldap-utils
```

Figura 3.16: Instalação do OpenLDAP.

As principais configurações serão definidas no arquivo `/etc/ldap/slapd.conf`: tipo de base, estrutura de diretório, administrador e a senha do administrador, conforme a Figura 3.17. As opções deste arquivo são detalhadas em (TRIGO, 2007).

```
# Parâmetros específicos do tipo de base
backend                bdb

# Base de dados
database                bdb

# Estrutura do Diretório e administrador
suffix                 "dc=empresalinux,dc=com,dc=br"
rootdn                 "cn=admin,dc=empresalinux,dc=com,dc=br"
rootpw                 {SSHA}h/lquPXJhvDumeh8uaoaUFAv+RBUBRFQ
```

Figura 3.17: Arquivo `slapd.conf`.

A configuração completa realizada no arquivo `slapd.conf` poderá ser encontrada no Apêndice A.1.

No arquivo `/etc/default/slapd`, deve-se definir a localização da configuração, conforme a Figura 3.18.

```
SLAPD_CONF=/etc/ldap/slapd.conf
```

Figura 3.18: Arquivo `slapd`.

Inicialmente será utilizado o próprio servidor para testar e validar as configurações do OpenLDAP. Para facilitar as consultas no arquivo `/etc/ldap/ldap.conf`, será definida a base a ser pesquisada, conforme a Figura 3.19.

```
BASE dc=empresalinux, dc=com, dc=br
HOST 127.0.0.1
```

Figura 3.19: Arquivo `ldap.conf`.

Agora deve-se reiniciar o servidor OpenLDAP, para aplicar as alterações feitas, conforme a Figura 3.20. Se a inicialização ocorreu como esperado, o resultado da pesquisa para verificar se a definição da base está correta deve ser conforme a Figura 3.21. Para possíveis problemas encontrados na inicialização do servidor e mais detalhes podem ser encontrados em (TRIGO, 2007) e (SUNGAILA, 2007).

```
ubuntuServer:~# /etc/init.d/slapd stop
Stopping OpenLDAP: slapd.
ubuntuServer:~# /etc/init.d/slapd start
Starting OpenLDAP: slapd.
```

Figura 3.20: Reinicializando o servidor OpenLDAP.

```
ubuntuServer:~# ldapsearch -x '(objectClass=*)'
# extended LDIF
#
# LDAPv3
# base <dc=empresalinux,dc=com,dc=br> (default) with scope subtree
# filter: (objectClass=*)
# requesting: ALL
#

# search result
search: 2
result: 32 No such object

# numResponses: 1
```

Figura 3.21: Verificando a base.

Para inserir os dados na estrutura LDAP, é necessário a criação de arquivos `LDIF`. Para criar a estrutura, é necessário começar pelo domínio. A Figura 3.22 cria um arquivo chamado `empresalinux.ldif` para demonstrar como definir o domínio. A Figura 3.23 demonstra a utilização do comando `ldapadd` para inserir os dados do arquivo `empresalinux.ldif` na base.

```
# arquvivo empresalinux.ldif
dn: dc=empresalinux,dc=com,dc=br
objectClass: top
objectClass: dcObject
objectClass: organization
dc: empreasalinux
o: Empresa Linux LTDA
```

Figura 3.22: Arquivo `empresalinux.ldif`.

```
ubuntuServer:~/ldifs# ldapadd -x -D "cn=admin,dc=empresalinux,dc=com,dc=br" \
-W -f empresalinux.ldif
Enter LDAP Password:
adding new entry "dc=empresalinux,dc=com,dc=br"
```

Figura 3.23: Comando `ldapadd`.

Como o ponto forte do LDAP é a organização e hierarquia, serão criados grupos, as chamadas unidades organizacionais, para agrupar os dados. A Figura 3.24 apresenta a estrutura para criar as unidades organizacionais *Usuários* e *Grupos*, utilizando o arquivo `unidades.ldif`. A inserção destes dados na base é semelhante ao comando da Figura 3.23.

```
# arquvivo unidades.ldif
dn: ou=usuarios,dc=empresalinux,dc=com,dc=br
objectClass: top
objectClass: organizationalunit
objectClass: dcObject
dc: empresalinux
ou: usuarios

dn: ou=grupos,dc=empresalinux,dc=com,dc=br
objectClass: top
objectClass: organizationalunit
objectClass: dcObject
dc: empresalinux
ou: grupos
```

Figura 3.24: Arquivo `unidades.ldif`.

Com a hierarquia da árvore já criada, agora deve-se inserir os usuários. A Figura 3.25 apresenta o arquivo `usuarios.lidf` para a inserção de uma conta de

usuário no padrão *POSIX*. A inserção dos demais usuários será semelhante a esta. Para inserir o usuário base, faz-se semelhante ao comando da Figura 3.23.

```
dn: uid=rafael,ou=usuarios,dc=empresalinux,dc=com,dc=br
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: inetOrgPerson
cn: rafael
sn: Bergamaschi
mail: rafael@empresalinux.com.br
telephonenumber: 31-3636-1212
uid: rafael
userPassword: {SSHA}vawx0PRxhhz2PPh7QZ7jaC4dyyRO5oSO
homeDirectory: /home/rafael
displayName: Rafael Bergamaschi
loginShell: /dev/null
uidNumber: 1001
gidNumber: 1001
```

Figura 3.25: Arquivo `usuarios.ldif`.

Através de uma pesquisa na base, pode-se confirmar o sucesso da inserção dos dados, conforme a Figura 3.26.

3.1.4 Integrando Samba + OpenLDAP

Antes das configurações para a integração do Samba ao OpenLDAP, será instalado um pacote pré-compilado, conforme mostrado na Figura 3.27. O pacote `smbldap-tools` traz um conjunto de *scripts* desenvolvidos em *Perl*, para facilitar na integração do Samba ao OpenLDAP, gerenciando contas de usuários, grupos e computadores armazenados na base LDAP.

O arquivo `samba.schema` não existe no diretório `/etc/ldap/schema`, mas está presente no pacote `samba-doc`. É necessário descompactar o arquivo do diretório `/usr/share/doc/samba-doc/exmaples/LDAP/` e copiar para o diretório `/etc/ldap/schema/`. Após esta operação, deve-se incluir o arquivo `samba.schema` nas configurações do arquivo `slapd.conf`.

A configuração completa realizada no arquivo `slapd.conf`, poderá ser encontrada no Apêndice A.1.

```
ubuntuServer:~/ldifs# ldapsearch -x '(cn=rafael)'
# extended LDIF
#
# LDAPv3
# base <dc=empresalinux,dc=com,dc=br> (default) with scope subtree
# filter: (cn=rafael)
# requesting: ALL
#

# rafael, usuarios, empresalinux.com.br
dn: uid=rafael,ou=usuarios,dc=empresalinux,dc=com,dc=br
objectClass: top
objectClass: person
objectClass: posixAccount
objectClass: inetOrgPerson
cn: rafael
sn: Bergamaschi
mail: rafael@empresalinux.com.br
telephoneNumber: 31-3636-1212
uid: rafael
userPassword:: e1NTSEF9dmF3eDBQUnhoaHoyUFBoN1FaN2phQzRkeXlSTzVvU08=
homeDirectory: /home/rafael
displayName:: UmFmYWVsIEJlcmdhbWFzY2hpIA==
loginShell: /dev/null
uidNumber: 1001
gidNumber: 1001

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

Figura 3.26: Verificando os dados na base.

```
ubuntuServer:~# aptitude install smbldap-tools
```

Figura 3.27: Instalação do pacote para integrar Samba + OpenLDAP.

No arquivo `smb.conf`, na seção `[global]`, serão adicionadas algumas configurações para a integração com OpenLDAP, conforme a Figura 3.28.

```
# Integração ao OpenLDAP
passdb backend = ldapsam:ldap://127.0.0.1
ldap admin dn = cn=admin,dc=empresalinux,dc=com,dc=br
ldap ssl = off
ldap delete dn = no
ldap user suffix = ou=Users
ldap group suffix = ou=Groups
ldap machine suffix = ou=Computers
ldap suffix = dc=empresalinux,dc=com,dc=br

# Scripts das Smbldaptools
add user script = /usr/sbin/smbldap-useradd -m "%u"
delete user script = /usr/sbin/smbldap-userdel "%u"
add group script = /usr/sbin/smbldap-groupadd -p "%g"
delete group script = /usr/sbin/smbldap-groupdel "%g"
add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
set primary group script = /usr/sbin/smbldap-usermod -g '%g' '%u'
add machine script = /usr/sbin/smbldap-useradd -t 0 -w "%u"
```

Figura 3.28: Alterar o `smb.conf` para integrar o OpenLDAP .

Será necessário adicionar as unidades organizacionais da Figura 3.29. Para isto, deve-se executar o comando:

```
ldapadd -x -D cn=admin,dc=empresalinux,dc=com,dc=br -W -f units.ldif
```

Com o Samba parado, é necessário armazenar a senha do administrador do OpenLDAP (neste caso, *admin*), ao arquivo de controle do Samba `secrets.tdb`, com o seguinte comando: `smbpasswd -W`.

Os arquivos `smbldap.conf` e `smbldap_bind.conf` não existem no diretório `/etc/smbldap-tools/`, mas vêm junto com o pacote `smbldap-tools`. É necessário copiar os arquivos do diretório `/usr/share/doc/smbldap-tools/examples/`, para o diretório `/etc/smbldap-tools/`, e no caso do `smbldap.conf` deve ser descompactado.

Em seguida, configurando a ferramenta `smbldap-tools`, deve-se gerar o código SID (*Samba ID*) de identificação do domínio, e inseri-lo no arquivo `smbldap.conf`, conforme a Figura 3.30. Este comando também insere na base LDAP um registro do tipo `sambaDomainName`.

```
# units.ldif
dn: ou=Users,dc=empresalinux,dc=com,dc=br
ou: Users
objectClass: top
objectClass: organizationalUnit

dn: ou=Groups,dc=empresalinux,dc=com,dc=br
ou: Groups
objectClass: top
objectClass: organizationalUnit

dn: ou=Computers,dc=empresa,dc=com,dc=br
ou: Computers
objectClass: top
objectClass: organizationalUnit
```

Figura 3.29: Arquivo `units.ldif`.

```
ubuntuServer# net getlocalsid EMPRESALINUX
SID for domain EMPRESALINUX is: S-1-5-21-3362332767-3512035659-2527167089
```

Figura 3.30: Cadastrar código SID.

Insira o código SID no arquivo `/etc/smbldap-tools/smbldap.conf` e adicione as demais configurações, conforme a Figura 3.31.

As configurações do arquivo `smbldap_bind.conf` devem estar conforme a Figura 3.32.

Depois destas configurações, é necessário popular a base LDAP, nos padrões utilizados em servidores Windows. Para isto deve-se executar o script `smbldap-populate`, conforme a Figura 3.33. Este script solicitará uma senha para o administrador do LDAP.

Com o servidor Samba e OpenLDAP iniciados, deve-se cadastrar um usuário, como uma forma de teste da integração entre os serviços. A Figura 3.34 apresenta a adição do usuário `testeadmin`, como administrador do domínio Samba, em seguida um usuário comum será cadastrado.

Mais informações sobre a integração do Samba ao OpenLDAP, poderão ser encontradas em (SUNGAILA, 2007) e (AMORIM; HESS, 2010).

```
SID="S-1-5-21-3362332767-3512035659-2527167089"
sambaDomain="EMPRESALINUX"
slaveLDAP="127.0.0.1"
slavePort="389"
masterLDAP="127.0.0.1"
masterPort="389"
ldapTLS="0"
ldapSSL="0"
verify="require"
suffix="dc=empresalinux,dc=com,dc=br"
usersdn="ou=Users,${suffix}"
groupsdn="ou=Groups,${suffix}"
computersdn="ou=Computers,${suffix}"
sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
scope="sub"
hash_encrypt="SSHA"
```

Figura 3.31: Configurar arquivo `smbldap.conf`.

```
slaveDN="cn=admin,dc=empresalinux,dc=com,dc=br"
slavePw="123456"
masterDN="cn=admin,dc=empresalinux,dc=com,dc=br"
masterPw="123456"
```

Figura 3.32: Configurar arquivo `smbldap_bind.conf`.

3.1.5 Integrando Kerberos + Samba + OpenLDAP

O Cyrus-SASL[3] é uma ferramenta para prover autenticação e comunicação criptografada para protocolos orientados a conexão. A instalação do Cyrus-SASL utilizando pacotes pré-compilados está descrita conforme a Figura 3.35. Sua instalação é necessária porque ele faz a ligação entre o Kerberos e o LDAP.

O pacote `krb5-kdc-ldap` contém um *plugin* LDAP para o servidor KDC e alguns utilitários. Este *plugin* permite que os dados KDC sejam armazenados no servidor LDAP ao invés do banco de dados local padrão. Sua instalação utilizando pacotes pré-instalados está descrita conforme a Figura 3.35.

[3]Disponível em `http://asg.web.cmu.edu/`.

```
ubuntuServer:~# smbldap-populate
Populating LDAP directory for domain EMPRESALINUX
    (S-1-5-21-3362332767-3512035659-2527167089)
(using builtin directory structure)

entry dc=empresalinux,dc=com,dc=br already exist.
entry ou=Users,dc=empresalinux,dc=com,dc=br already exist.
entry ou=Groups,dc=empresalinux,dc=com,dc=br already exist.
adding new entry: ou=Computers,dc=empresalinux,dc=com,dc=br
adding new entry: uid=root,ou=Users,dc=empresalinux,dc=com,dc=br
adding new entry: uid=nobody,ou=Users,dc=empresalinux,dc=com,dc=br
adding new entry:
    cn=Domain Admins,ou=Groups,dc=empresalinux,dc=com,dc=br
adding new entry:
    cn=Domain Users,ou=Groups,dc=empresalinux,dc=com,dc=br
adding new entry:
    cn=Domain Guests,ou=Groups,dc=empresalinux,dc=com,dc=br
adding new entry:
    cn=Domain Computers,ou=Groups,dc=empresalinux,dc=com,dc=br
adding new entry:
    cn=Administrators,ou=Groups,dc=empresalinux,dc=com,dc=br
adding new entry:
    cn=Account Operators,ou=Groups,dc=empresalinux,dc=com,dc=br
adding new entry:
    cn=Print Operators,ou=Groups,dc=empresalinux,dc=com,dc=br
adding new entry:
    cn=Backup Operators,ou=Groups,dc=empresalinux,dc=com,dc=br
adding new entry:
   cn=Replicators,ou=Groups,dc=empresalinux,dc=com,dc=br
entry sambaDomainName=EMPRESALINUX,dc=empresalinux,dc=com,dc=br
   already exist.
    Updating it...

Please provide a password for the domain root:
Changing UNIX and samba passwords for root
New password:
Retype new password:
```

Figura 3.33: *Script* `smbldap-populate`.

O próximo passo é criar uma conta do Kerberos para o LDAP e gerar uma *keytab* para que o servidor LDAP consiga autenticar no servidor Kerberos, conforme a Figura 3.36.

```
# smbldap-useradd -m -a testeadmin
# smbldap-passwd testeadmin
# smbldap-usermod -G "Domain Admins" testeadmin
# smbldap-useradd -P -a userteste
```

Figura 3.34: Adicionar usuários com `smbldap`.

```
ubuntuServer:~# aptitude install sasl2-bin libsasl2-2 libsasl2-modules \
    libsasl2-modules-ldap libsasl2-modules-gssapi-mit krb5-kdc-ldap
```

Figura 3.35: Instalar Cyrus-SASL e o `krb5-kdc-ldap`.

```
ubuntuServer:~# kadmin.local -q \
    "addprinc -randkey ldap/ubuntuserver.empresalinux.com.br"
ubuntuServer:~# kadmin.local -q \
    "ktadd ldap/ubuntuserver.empresalinux.com.br"
```

Figura 3.36: Adicionar conta no Kerberos para o LDAP.

Para que o LDAP dê suporte ao Kerberos, no arquivo `slapd.conf` deve-se adicionar o schema para o Kerberos. Porém, o schema não acompanha a instalação do Kerberos e nem do OpenLDAP, mas está presente no pacote `krb5-kdc-ldap`. No diretório `/usr/share/doc/krb5-kdc-ldap/`, o arquivo `kerberos.schema.gz` deve ser descompactado e copiado para o diretório `/etc/ldap/schema/`. Após esta operação, deve-se incluir o arquivo `kerberos.schema` nas configurações do arquivo `slapd.conf`. As devidas alterações no arquivo `slapd.conf` estão presentes na Figura 3.37.

```
# Arquivo de Schema
include /etc/ldap/schema/kerberos.schema

# Chave de Criptografia
TLSCertificateFile /etc/ldap/ssl/ldap.crt
TLSCertificateKeyFile /etc/ldap/ssl/ldap.key

# Suporte ao Kerberos
sasl-realm EMPRESALINUX.COM.BR
sasl-host ubuntuserver.empresalinux.com.br
```

Figura 3.37: Suporte ao Kerberos em `slapd.conf`.

Normalmente utilizam-se certificados de uma CA (*Certificate Authority* - Autoridade Certificadora) oficialmente reconhecida. Como o ojetivo deste trabalho é apenas demonstrativo, deve-se gerar um certificado autoassinado, conforme a Figura 3.38. Ao solicitar o `Common Name`, deve ser o nome do *host* do servidor, como: `ubuntuserver.empresalinux.com.br`.

```
ubuntuServer:~# openssl req -newkey rsa:1024 -x509 -nodes -out \
    ldap.pem -keyout ldap.key -days 365
```

Figura 3.38: Gerar certificado autoassinado.

A configuração completa realizada no arquivo `slapd.conf`, poderá ser encontrada no Apêndice A.1.

Para habilitar a porta ldaps (636) altere o arquivo `/etc/defaults/slapd`, conforme a Figura 3.39.

```
SLAPD_SERVICES="ldap:/// ldaps:/// ldapi:///"
```

Figura 3.39: Alterar `slapd`.

Alguns problemas podem surgir pelo uso de certificados autoassinados. Para que as ferramentas do LDAP localizem e aceitem sua autenticidade, altere o arquivo `/etc/ldap/ldap.conf`, conforme a Figura 3.40.

```
TLS_CACERT /etc/ldap/ssl/ldap.pem
TLS_REQCERT never
```

Figura 3.40: Alterar `ldap.conf`.

O arquivo `krb5.conf` deve ser alterado para fornecer suporte ao LDAP. As alterações necessárias são mostradas na Figura 3.41.

A configuração completa realizada no arquivo `krb5.conf` poderá ser encontrada no Apêndice A.2.

O utilitário `kdb5_ldap_util` deve ser usado para criar o *realm* e integrá-lo ao domínio do LDAP, conforme a Figura 3.42.

Deve-se criar um *stash* da senha usada para vincular ao servidor LDAP, conforme a Figura 3.43. Esta senha é usada nas opções `ldap_kdc_dn` e `ldap_kadmin_dn` no arquivo `krb5.conf`,

```
...
[realms]
        EMPRESALINUX.COM.BR = {
                kdc = ubuntuserver.empresalinux.com.br
                admin_server = ubuntuserver.empresalinux.com.br
                default_domain = empresalinux.com.br
                database_module = openldap_ldapconf
        }
...

[dbdefaults]
        ldap_kerberos_container_dn =
    cn=admin,dc=empresalinux,dc=com,dc=br

[dbmodules]
        openldap_ldapconf = {
            db_library = kldap
            ldap_kerberos_container_dn =
    cn=admin,dc=empresalinux,dc=com,dc=br
            ldap_kdc_dn = "cn=admin,dc=empresalinux,dc=com,dc=br"
            ldap_kadmind_dn = "cn=admin,dc=empresalinux,dc=com,dc=br"
            ldap_service_password_file = /etc/krb5kdc/service.keyfile
            ldap_servers = ldaps://ubuntuserver.empresalinux.com.br/
            ldap_conns_per_server = 5
        }
...
```

Figura 3.41: Alterar `krb5.conf`.

```
ubuntuServer:~# kdb5_ldap_util -D cn=admin,dc=empresalinux,dc=com,dc=br \
    create -subtrees dc=empresalinux,dc=com,dc=br -r EMPRESALINUX.COM.BR \
    -s -H ldap://ubuntuserver.empresalinux.com.br
```

Figura 3.42: Criar *realm* para integrar ao LDAP.

```
ubuntuServer:~# kdb5_ldap_util -D cn=admin,dc=empresalinux,dc=com,dc=br \
    stashsrvpw -f /etc/krb5kdc/service.keyfile \
    cn=admin,dc=empresalinux,dc=com,dc=br
```

Figura 3.43: Criar *stash* da senha para o LDAP.

É necessário criar um objeto com os atributos do Kerberos na base LDAP. Utilizando o usuário com os atributos do Samba, apresentado na Figura 3.34, o

comando `addprinc` com a opção `-x` irá adicionar apenas os atributos do Kerberos ao objeto existente, conforme a Figura 3.44

```
ubuntuServer:~# kadmin.local
Authenticating as principal root/admin@EMPRESALINUX.COM.BR with password.
kadmin.local:  addprinc -x
    dn="uid=userteste,ou=Users,dc=empresalinux,dc=com,dc=br" userteste
WARNING: no policy specified for userteste@EMPRESALINUX.COM.BR;
    defaulting to no policy
Enter password for principal "userteste@EMPRESALINUX.COM.BR":
Re-enter password for principal "userteste@EMPRESALINUX.COM.BR":
Principal "userteste@EMPRESALINUX.COM.BR" created.
kadmin.local:  quit
```

Figura 3.44: Adicionar os atributos do Kerberos ao objeto do LDAP.

As alterações no arquivo `smb.conf` do Samba para integrar ao Kerberos, estão descritas na Figura 3.45. A opção `security` deve receber o valor `ads`, para que o Samba atue como um membro do domínio em um *realm* AD.

```
realm = EMPRESALINUX.COM.BR
security = ads
encrypt passwords = yes
```

Figura 3.45: Suporte ao Kerberos em `smb.conf`

A configuração completa realizada no arquivo `smb.conf` poderá ser encontrada no Apêndice A.3.

As configurações de integração do Samba ao OpenLDAP foram apresentadas na Seção 3.1.4. Neste ponto completa-se a integração entre Kerberos, Samba e OpenLDAP.

3.2 Configuração no cliente Windows

O cliente Windows também deve atender às exigências do Kerberos, possuir um DNS para resolver seu nome e seu relógio deve estar sincronizado com o do servidor Linux. Ambos devem estar na mesma rede, com a configuração do servidor *wins* apontando para o servidor Samba.

Para permitir a conexão do cliente Windows 7 ao domínio Samba, é necessário adicionar ou alterar o registro do Windows, conforme a Figura 3.46. A primeira alteração, está relacionada ao "modo de compatibilidade" de domínios, e a segunda, às requisições de resolução de nomes do DNS.

Na tela *Iniciar -> Computador -> Propriedades -> Alterar Configurações -> Alterar -> Mais...*, a opção *Alterar sufixo DNS primário ...* deve ser desmarcada e o cliente Windows deve ser reiniciado.

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\
   LanmanWorkstation\Parameters]
DWORD "DomainCompatibilityMode"=dword:00000001
DWORD "DNSNameResolutionRequired"=dword:00000000
```

Figura 3.46: Alterar registro do Windows.

Com as pré-configurações realizadas, na tela *Iniciar -> Computador -> Propriedades -> Alterar Configurações -> Alterar*, deve-se selecionar a opção *Domínio* e digitar o nome do domínio, neste caso *EMPRESALINUX*. Ao pressionar o botão *OK* e após alguns instantes deve-se digitar o nome e a senha do administrador do Samba, conforme a Figura 3.47 , neste caso o usuário *root*. Uma mensagem de boas vindas será exibida, e o cliente Windows deve ser reiniciado e fazer um *logon* com um dos usuários cadastrados no Samba. Para possíveis problemas ou dúvidas sobre o Windows 7 com Samba, consulte `http://wiki.samba.org/index.php/Windows7`.

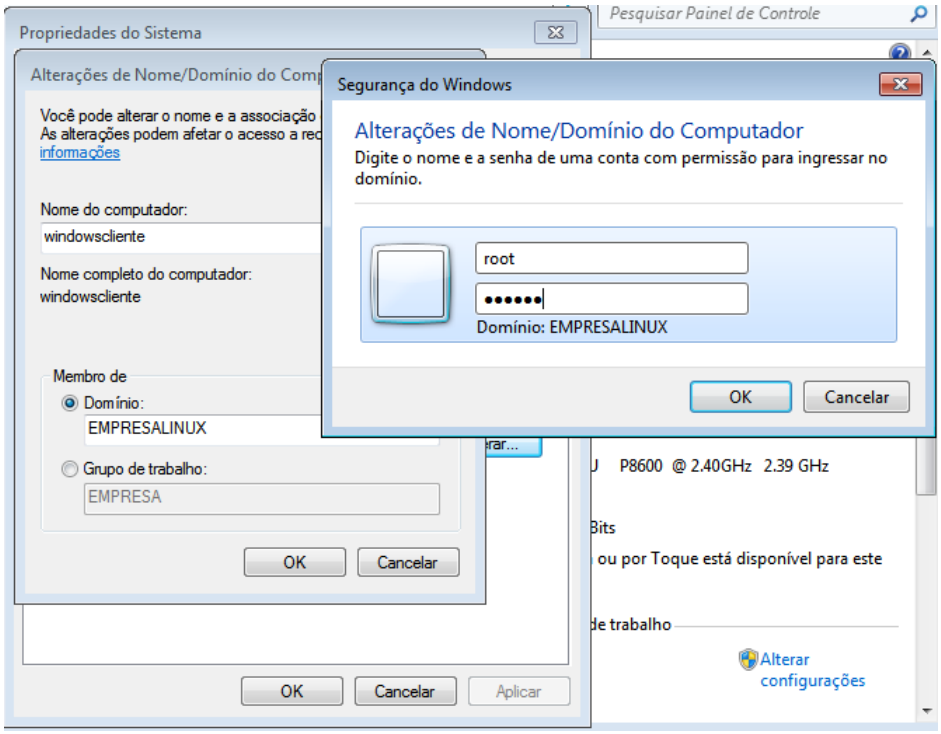

Figura 3.47: Entrar no domínio com Windows 7.

Capítulo 4

Implementação com Servidor Windows e Cliente Linux

Neste capítulo serão descritos os procedimentos para instalação e configuração Active Directory no servidor Windows. Como também as instalações e configurações para autenticação do cliente Linux, no servidor Windows.

4.1 Instalação e configuração no servidor Windows

De acordo com a proposta deste trabalho, ficará limitado somente à implementação da tecnologia AD DS do Active Directory. Há duas formas de adicionar a função do AD DS a um servidor Windows: utilizando a interface Windows ou a linha de comando. Este trabalho contemplará apenas a instalação com a interface Windows.

O primeiro passo é abrir o "Gerenciador de Servidores", em `Iniciar -> Painel de Controle -> Ferramentas Administrativas -> Gerenciador de Servidores`. Na seção "Resumo de Funções" deve-se selecionar a opção "Adicionar Funções", conforme a Figura 4.1, e o "Assistente para Adicionar Funções" irá abrir.

Com o "Assistente para Adicionar Funções" aberto, deve-se avançar até a tela de "Selecionar Funções do Servidor", selecionar a opção "Serviços de Domínio Active Directory", avançar até a tela de "Confirmar Seleções de Instalação" e selecionar o botão "Instalar". Após o processo de instalação, uma tela indicando que a instalação foi bem-sucedida irá aparecer.

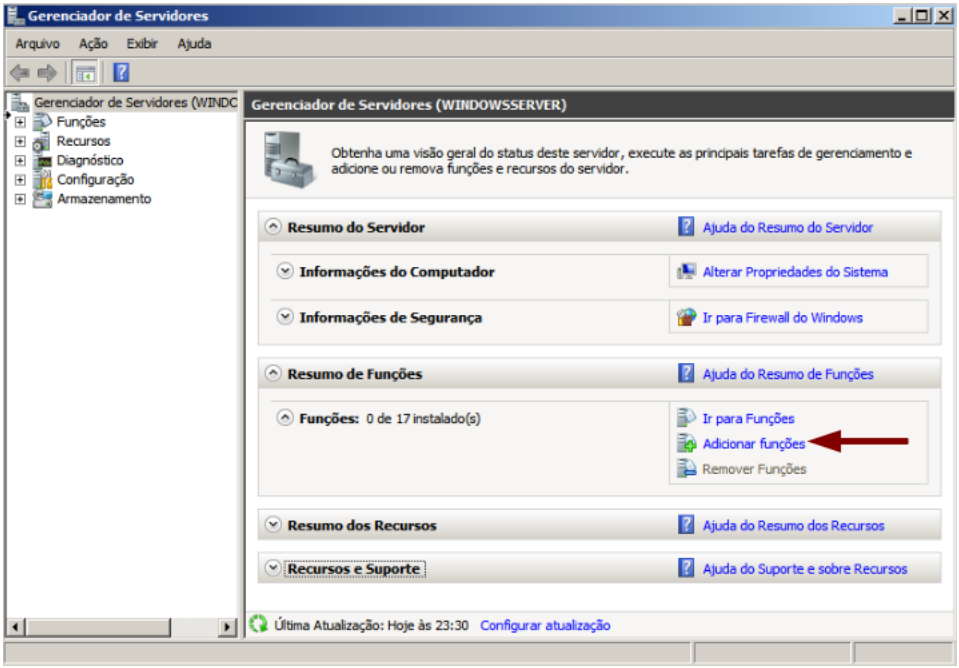

Figura 4.1: Adicionar Funções no Gerenciador de Servidores.

Na seção "Funções -> Serviços de Domínio Active Directory", do "Gerenciador de Servidores", haverá uma mensagem informando que o servidor não está operando como controlador de domínio, até que se execute o assistente de instalação do AD DS, conforme a Figura 4.2. Para tal tarefa deve-se ir ao `Iniciar -> Executar` e digitar `Dcpromo.exe`.

Com o "Assistente de Instalação de Serviços de Domínio Active Directory" aberto, deve-se avançar até a tela "Escolher uma Configuração de Implantação", selecionar a opção "Criar um novo domínio em uma nova floresta" e avançar. Na tela "Nomear o Domínio da Floresta", deve-se escolher um nome de domínio raiz da floresta, neste caso, `empresawindows.com.br`. Ao avançar com a tela deve-se selecionar o nível funcional "Windows Server 2008" e em seguida avançar. Na tela "Opções Adicionais de Controlador de Domínio", a opção "Servidor DNS" deve ser mantida para que seja criada um infraestrutura de DNS durante a instalação do AD DS. Deve-se avançar até a tela "Senha do Administrador do Modo de Restauração dos Serviços de Diretório", e escolher uma senha e avançar até a concluir a instalação. Após a instalação o servidor deve ser reiniciado.

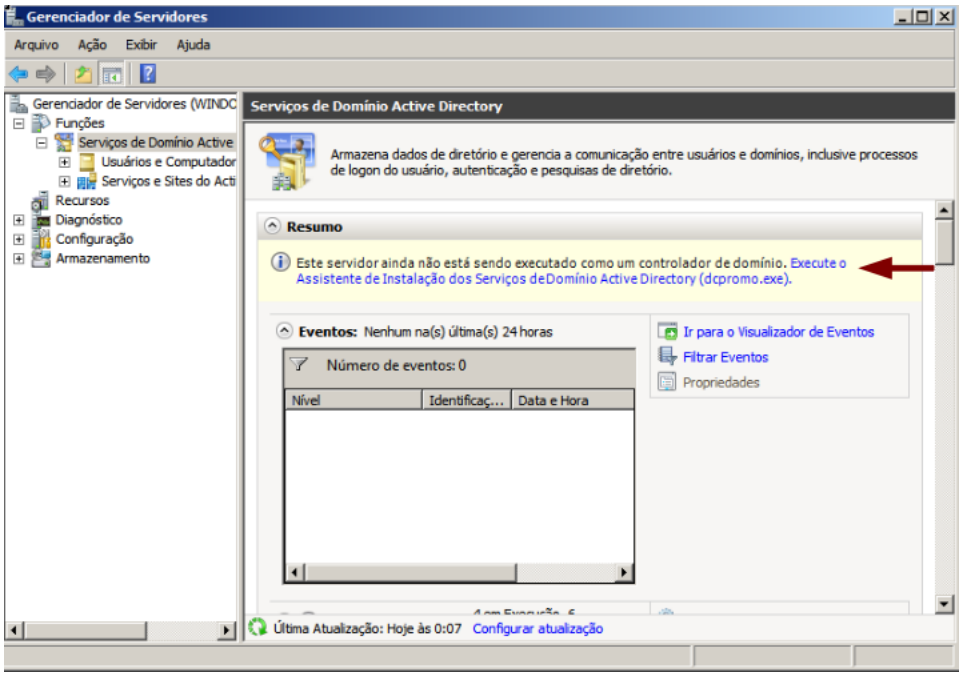

Figura 4.2: Controlador de domínio não está disponível no "Serviços de Domínio Active Directory".

O próximo passo depois da instalação do AD DS, é criar uma OU. Para isto, deve-se acessar o *snap-in* "Usuários e Computadores do Active Directory" em `Iniciar -> Painel de Controle -> Ferramentas Administrativas`, selecionar o domínio com o botão direito do mouse, em seguinda: *Novo -> Unidade Organizacional*. Deve-se digitar um nome para a OU e selecionar o botão "Ok".

Para criar o objeto usuário, deve-se acessar o *snap-in* "Usuários e Computadores do Active Directory", selecionar a OU desejada com o botão direito do mouse, em seguinda: *Novo -> Usuário*. Na caixa de diálogo "Novo Objeto - Usuário", deve-se digitar o nome e sobrenome do usuário. O campo "Nome Completo" será preenchido automaticamente, se tornará um CN (*Common Name*), por isso deve ser único dentro de uma OU. Em "Nome de logon de usuário", deve-se digitar o nome com o qual o usuário fará o logon, como mostrado na Figura 4.3, depois avançar para digitar a senha do usuário e, em seguida, avançar até concluir.

Para criar o objeto grupo, deve-se acessar o *snap-in* "Usuários e Computadores do Active Directory", selecionar a OU desejada com o botão direito do mouse, em seguinda: *Novo -> Grupo*. Na caixa de diálogo "Novo Objeto - Grupo", deve-se digitar o nome do grupo e selecionar o botão "Ok". Para adicionar o usuário

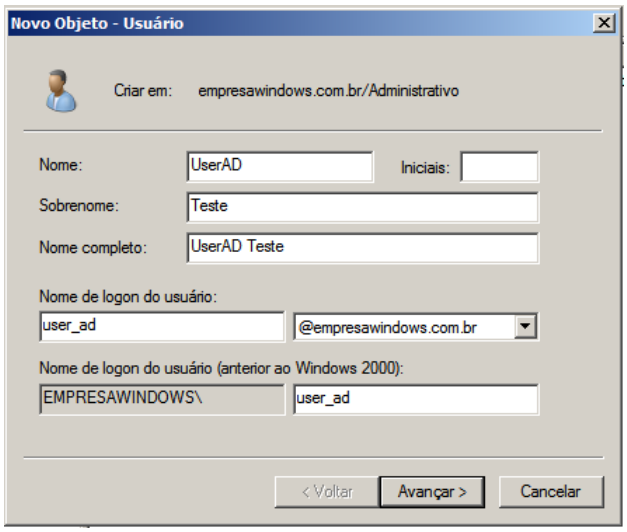

Figura 4.3: Adicionar objeto usuário.

criado anteriormente neste grupo, deve-se selecionar o grupo com o botão direito do mouse e selecionar a opção "Propriedades". Na guia "Membros", deve-se selecionar o botão "Adicionar", digitar o nome do usuário e em seguida "Ok" e "Ok" novamente para fechar a caixa de diálogo.

Para criar o objeto computador, deve-se acessar o *snap-in* "Usuários e Computadores do Active Directory", selecionar a OU desejada com o botão direito do mouse e em seguinda: *Novo -> Computador*. Na caixa de diálogo "Novo Objeto - Computador", deve-se digitar o nome do computador, e no campo "Usuários ou Grupos", deve-se selecionar a qual grupo ou usuário este computador pertence e em seguida selecionar o botão "Ok".

Neste momento o Active Directory já possui as configurações necessárias, um usuário e um computador cadastrados no domínio, para permitir a realização de testes. O Active Directory possui muito mais opções de configurações e recursos, para serem explorados, porém estão fora do escopo deste trabalho. Para mais informações sobre a utilização dessas outras opções e recursos, consulte (HOLME; RUEST; RUEST, 2008).

4.2 Instalação e configuração no cliente Linux

O cliente Linux também deve atender às exigências do Kerberos: possuir um DNS para resolver seu nome e seu relógio deve estar sincronizado com o do servidor Windows, e ambos na mesma rede. Para sincronizar o relógio com o do servidor, pode-se utilizar o seguinte comando: `# ntpdate <ip_servidor>`.

A instalação do Kerberos e Samba utilizando pacotes pré-compilados, está descrita conforme a Figura 4.4. As novidades são: o pacote `winbind`, junto com o pacote `samba`, é utilizado para gerenciamento centralizado de usuários em Windows e Linux; e o pacote `libpam-krb5`, que realiza a integração do PAM (*Pluggable Authentication Modules*) com o Kerberos.

```
clientelinux:~# aptitude install krb5-config krb5-user winbind samba \
    smbfs libpam-krb5
```

Figura 4.4: Instalação dos pacotes para o cliente Linux.

O *realm empresawindows.com.br* deve ser configurado no Kerberos no arquivo `/etc/krb5.conf`, conforme a Figura 4.5.

```
[libdefaults]
        default_realm = EMPRESAWINDOWS.COM.BR

[realms]
        EMPRESAWINDOWS.COM.BR = {
                kdc = windowsserver.empresawindows.com.br
                default_domain = EMPRESAWINDOWS.COM.BR
                kpasswd_server = windowsserver.empresawindows.com.br
                admin_server = windowsserver.empresawindows.com.br
        }

[domain_realm]
        .empresawindows.com.br = EMPRESAWINDOWS.COM.BR
```

Figura 4.5: Arquivo `krb5.conf` no cliente Linux.

A próxima etapa é inserir o cliente Linux como membro do domínio Active Directory. Para isto, é necessário configurar o Samba e o Winbind. Os dois serviços são configurados no arquivo `/etc/samba/smb.conf`, na seção `[global]`, conforme a Figura 4.6.

```
[global]
        workgroup = EMPRESAWINDOWS
        realm = EMPRESAWINDOWS.COM.BR
        security = ADS
        password server = windowsserver.empresawindows.com.br
        encrypt passwords = Yes
        syslog = 0
        log file = /var/log/samba/log.%m
        max log size = 1000
        os level = 0
        local master = No
        domain master = No
        preferred master = No
        idmap uid = 10000-20000
        idmap gid = 10000-20000
        template shell = /bin/bash
        winbind separator = +
        winbind enum users = Yes
        winbind enum groups = Yes
        winbind use default domain = Yes
```

Figura 4.6: Arquivo `smb.conf` no cliente Linux.

O Linux utiliza uma API universal, o NSS, para mapear nomes. Por padrão, o NSS vem configurado para buscar primeiro no arquivo `/etc/passwd`, mas ele deve consultar um servidor Active Directory, caso o módulo esteja carregado. Desta forma, os usuários do AD estarão como se fossem usuários locais. Para isto, deve-se alterar o arquivo `/etc/nsswitch.conf`, conforme a Figura 4.7.

```
passwd: compat winbind
group: compat winbind
```

Figura 4.7: Arquivo `nsswitch.conf` no cliente Linux.

Para completar a integração do Linux com o AD, é necessário adicionar o computador Linux no domínio AD. Para isto, deve-se executar o comando `net ads`, conforme a Figura 4.8. O usuário `Administrador`, passado como parâmetro do comando, corresponde ao usuário do servidor Windows.

Neste momento o Linux consegue identificar todos os usuário do domínio Active Directory. Para possibilitar o *login* no Linux com um usuário AD, é necessário integrar o Kerberos com o PAM. Para isto, deve-se alterar as configurações dos ar-

```
clientelinux:~# net ads join -U Administrador
```

Figura 4.8: Adicionar o computador Linux ao domínio AD.

quivos presentes no diretório `/etc/pam.d/`, que corresponde aos quatro tipos de módulos do PAM: `auth`, `account`, `password` e `session`. A Figura 4.9 apresenta as modificações necessárias.

```
# /etc/pam.d/common-auth
auth sufficient pam_krb5.so forwardable
auth required pam_unix.so nullok_secure use_first_pass
auth required pam_deny.so

# /etc/pam.d/common-account
account sufficient pam_krb5.so forwardable
account required pam_unix.so

# /etc/pam.d/common-password
password sufficient pam_krb5.so nullok obscure md5
password required pam_unix.so nullok obscure md5

# /etc/pam.d/common-session
session required pam_mkhomedir.so silent skel=/etc/skel/ umask=0022
session sufficient pam_kerb5.so
session required pam_unix.so
```

Figura 4.9: Integrar Kerberos com o PAM.

Mais informações sobre a integração do Linux com Active Directory, consulte (NEU, 2008).

Capítulo 5

Testes e Resultados

É importante lembrar que o autor deste trabalho utilizou máquinas virtuais, para os clientes e servidores, como descrito no Capítulo 1. Para a realização dos testes de autenticação nos clientes foram utilizados os seguintes métodos:

- instalação básica do sistema operacional nos clientes, com somente as instalações e configurações necessárias para autenticação em domínio;
- os servidores foram reiniciados antes dos testes;
- foram realizados dez testes de autenticação em cada cliente nos dois ambientes, após primeira autenticação, quando o perfil dos usuários são criados;
- o cliente foi reiniciado antes de cada teste de autenticação;
- o tempo de autenticação foi cronometrado da seguinte forma: após a senha do usuário ter sido digitada na tela de *login*, até o momento em que a área de trabalho tornou-se disponível para uso, com todos os aplicativos inicializados;

Na simulação do primeiro ambiente, com o servidor Linux e cliente Windows, deve-se fazer o *logon* no cliente Windows, com o usuário do LDAP com os atributos do Kerberos e do Samba. O usuário que atende estas características é o `userteste`, criado no Capítulo 3, como mostra as Figura 5.1 e Figura 5.2.

A Figura 5.3 mostra que um usuário da integração Kerberos+Samba+OpenLDAP está logado no cliente Windows. No servidor Linux com Samba, executando-se o

```
dn: uid=userteste,ou=Users,dc=empresalinux,dc=com,dc=br
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: sambaSamAccount
objectClass: krbPrincipalAux
objectClass: krbTicketPolicyAux
cn: userteste
sn: userteste
givenName: userteste
uid: userteste
uidNumber: 1006
gidNumber: 513
homeDirectory: /home/userteste
loginShell: /bin/bash
gecos: System User
sambaLogonTime: 0
sambaLogoffTime: 2147483647
sambaKickoffTime: 2147483647
sambaPwdCanChange: 0
displayName: userteste
sambaSID: S-1-5-21-3362332767-3512035659-2527167089-3012
sambaPrimaryGroupSID: S-1-5-21-3362332767-3512035659-2527167089-513
sambaLogonScript: logon.bat
sambaProfilePath: \\PDC-SRV\profiles\userteste
sambaHomePath: \\PDC-SRV\userteste
sambaHomeDrive: H:
sambaLMPassword: 02D093CE93078E8FAAD3B435B51404EE
sambaAcctFlags: [U]
sambaNTPassword: CAF13C4F321B608B27FD75D2549BA53C
sambaPwdLastSet: 1297803821
sambaPwdMustChange: 1301691821
userPassword:: e1NTSEF9aTIybUp3YjZaUkh1ckE5Q0ZsUS8zYjVMZldkUlZtdG0=
shadowLastChange: 15020
shadowMax: 45
```

Figura 5.1: Atributos do usuário `userteste`.

comando `smbstatus` é possível identificar se o cliente Windows autenticou-se no servidor Samba conforme a Figura 5.4. O tempo médio de autenticação no domí-

```
krbPrincipalName: userteste@EMPRESALINUX.COM.BR
krbTicketFlags: 128
krbPrincipalKey:: MIICd6ADAgEBoQMCAQGiAwIBAqMDAgEBpIICXzCCAlswVKAHMAWgAwIBAKFJ
 MEegAwIBEqFABD4gAMOuIwJLV4FpHi1QtPJXmi/5JA+PqNVuPo6lo5N67zvba3UdJsOe3CMZ8U6b9
 fTHniU9LxmsyCbO27rnizBEoAcwBaADAgEAoTkwN6ADAgEXoTAELhAAfQCVU0WRoWLLn/SNPhbmlL
 doCbgIPC9QEMHC8WucWL+L0j77xlKsRW/H4FYwTKAHMAWgAwIBAKFBMD+gAwIBEKE4BDYYADejkVf
 0lOkEspB+tWm2AY8Uu0axePjeF1yt21/f2ZSpZoorizC8qq+38KjZfGhrGBjNvPcwPKAHMAWgAwIB
 AKExMC+gAwIBAaEoBCYIADzlD/LaxE+otYo1KGtIrrMgaOPj9sUV0wFhVeQ4Kfbo6NUaiTA8oAcwB
 aADAgEBoTEwL6ADAgEDoSgEJggAqT/ClDn0FQdfDVXindQrHTLV00aGUkQrfm4ruq2cwTkvkMjaME
 mgFDASoAMCAQKhCwQJdXNlcnRlc3RloTEwL6ADAgEDoSgEJggATXiR4QK++OpPc4wA/G9R62FYBkI
 bh0oahPIwgf4T79ZIAw+7MFOgHjAcoAMCAQOhFQQTRU1QUkVTQUxJTlVYLkNPTS5CUqExMC+gAwIB
 A6EoBCYIAG7P2A6yK4BaMkOGQoxO++5U49qlMO/b/cs7lL/NVJ8+SONRIDBToB4wHKADAgEFoRUEE
 0VNUFJFU0FMSU5VWC5DT00uQlKhMTAvoAMCAQOhKAQmCADwo09SzPt+R0A1MtbFsVhVhIfd4fStz6
 gYyo2ZR/LwtaGkUa8=
krbPasswordExpiration: 197001010000000Z
krbLastPwdChange: 20110307201524Z
krbLastSuccessfulAuth: 20110307201538Z
krbLoginFailedCount: 0
krbExtraData:: AALcPHVNdXNlcnRlc3RlMi9hZG1pbkBFTVBSRVNBTElOVVguQ09NLkJSAA==
krbExtraData:: AAgBAA==
```

Figura 5.2: Atributos do usuário `userteste` (continuação).

nio foi de aproximadamente 78 (setenta e oito) segundos, o tempo de autenticação local no cliente era de aproximadamente 15 (quinze) segundos. Utilizando um cliente Linux, o tempo de autenticação no servidor Linux foi de aproximadamente 15 (quinze) segundos, como apresentado na Tabela 5.1.

Na simulação do segundo ambiente, com o servidor Windows e cliente Linux, o programa de *login* solicita um TGT ao servidor. Com o tíquete, é possível o cliente acessar o serviço de domínio com um usuário cadastrado no servidor, como se fosse um usuário local. Isto é possível, porque o PAM do cliente Linux foi configurado para primeiro carregar o módulo Kerberos na autenticação. A Figura 5.5 mostra que um usuário do Active Directory está logado no cliente Linux.

O tempo médio de autenticação no domínio foi de aproximadamente 13 (treze) segundos, o tempo de autenticação local no cliente era de aproximadamente 10 (dez) segundos. Utilizando um cliente Windows (versão 7 de 64bits), o tempo de autenticação no servidor Windows foi de aproximadamente 15 (quinze) segundos, como apresentado na Tabela 5.1.

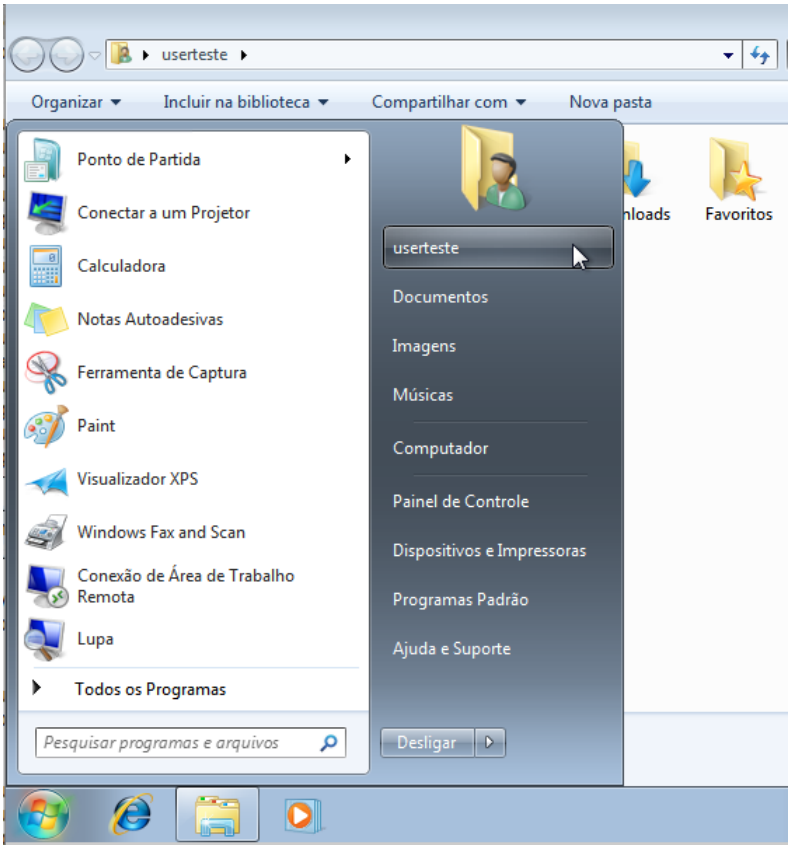

Figura 5.3: Usuário Windows autenticado no servidor Linux.

```
ubuntuServer:~# smbstatus -b

Samba version 3.4.7
PID     Username      Group         Machine
-------------------------------------------------------------------
854       userteste        userteste        windowscliente (10.0.0.100)
```

Figura 5.4: *Status* dos clientes no servidor Samba.

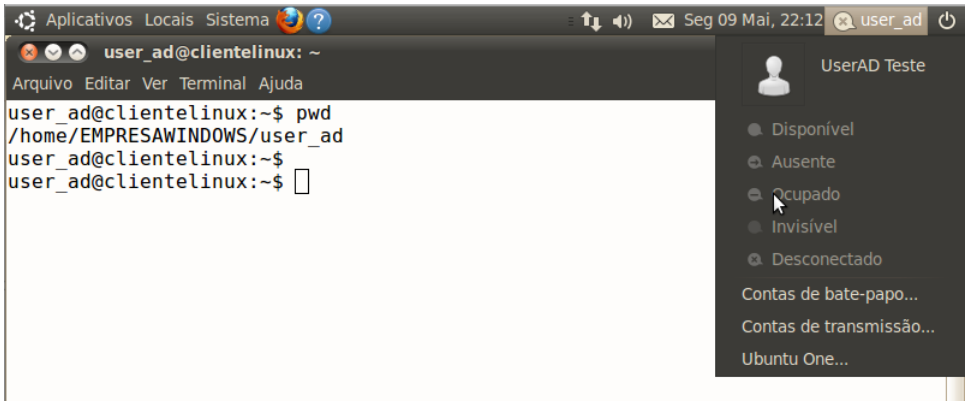

Figura 5.5: Usuário AD autenticado no cliente Linux.

Tabela 5.1: Resultados dos testes de autenticação.

Método do teste	Cliente	Servidor	Tempo de autenticação
`Cliente/servidor`	Windows	Linux	78 segundos
`Cliente/servidor`	Linux	Linux	15 segundos
`Local`	Windows	—	15 segundos
`Cliente/servidor`	Linux	Windows	13 segundos
`Cliente/servidor`	Windows	Windows	15 segundos
`Local`	Linux	—	10 segundos

Capítulo 6

Conclusão

Este trabalho mostrou que é possível realizar a interoperabilidade entre os sistemas operacionais Linux e Windows, realizando a autenticação segura em domínios, nos dois ambientes propostos. A simulação do primeiro ambiente, mostrou-se mais trabalhosa no lado do servidor, porém mais flexível para o administrador, na questão de configurações e ajustes de acordo com as necessidades da rede. O cliente Windows mostrou-se bem simples na configuração. A simulação do segundo ambiente, mostrou-se mais simples e pouco flexível no lado do servidor. A configuração no cliente Linux mostrou-se um pouco complexa e mais flexível, comparada ao cliente Windows. De acordo com os testes de tempo de autenticação realizados, o Linux mostrou-se mais eficiente, ou seja, mais preparado para interoperar com o Windows.

Uma primeira proposta para trabalho futuro é utilizar máquinas reais nos ambientes, com servidor de domínio e arquivos, cronometrar o tempo de autenticação e transferência de arquivos com vários clientes acessando o servidor de forma simultânea.

Uma segunda proposta para trabalho futuro é utilizar o mecanismo *cross-realm* do Kerberos, nos ambientes propostos deste trabalho, onde um cliente Windows do *realm* do servidor Linux também possa autenticar no *realm* do servidor Windows, demonstrando a interação entre os dois *realm*, em sistemas operacionais diferentes.

Uma terceira proposta para trabalho futuro é realizar a interoperabilidade com um cliente Windows e um Servidor Linux, utilizando o Samba na versão 4.

Referências Bibliográficas

AMORIM, M.; HESS, P. Samba com Windows 7. *Linux Magazine*, v. 62, p. 38, jan. 2010.

BUCKLEY, S. C. *MIT Kerberos Consortium Proposal to Sponsors*. [S.l.], 2008. Disponível em: <http://www.kerberos.org/join/overview.pdf>.

CHESWICK, W. R.; BELLOVIN, S. M.; RUBIN, A. D. *Firewalls e Segurança na Internet - Repelindo o hacker Ardiloso*. 2. ed. São Paulo: Bookman, 2005.

COULOURIS, G.; DOLLIMORE, J.; KINDBERG, T. *Sistemas Distribuídos - Conceitos e Projetos*. 4. ed. Porto Alegre: Bookman, 2007.

DESMOND, B.; RICHARDS, J.; ALLEN, R.; LOWE-NORRIS, A. G. *Active Directory, Designing, Deploying, and Running Active Directory*. 4. ed. Sebastopol: O'Reilly, 2009.

HOLME, D.; RUEST, N.; RUEST, D. *MCTS Self-Paced Training Kit (Exam 70-640): Configuring Windows Server 2008 Active Directory - Resource Kit*. 1. ed. Redmond: Microsoft Press, 2008.

JORDAO, L. d. B. *Uso do Protocolo de Autenticação Kerberos em Redes Linux*. Lavras: [s.n.], 2005. Disponível em: <http://www.ginux.ufla.br/files/mono-LeonardoJordao.pdf>.

MIT, M. I. O. T. *Kerberos V5 Installation Guide*. [S.l.], 2010. Disponível em: <http://web.mit.edu/kerberos/krb5-1.8/krb5-1.8.3/doc/krb5-install.html>.

MIT, M. I. O. T. *Kerberos V5 System Administrator's Guide*. [S.l.], 2010. Disponível em: <http://web.mit.edu/kerberos/krb5-1.8/krb5-1.8.3/doc/krb5-admin.html>.

MORIMOTO, C. E. *Servidores Linux - Guia Prático*. Porto Alegre: Sul Editores, 2008.

NEMETH, E.; SNYDER, G.; HEIN, T. R. *Manual Completo do Linux - Guia do administrador*. 2. ed. São Paulo: Pearson, 2007.

NEU, W. Autenticação no Linux com Active Directory e Kerberos 5 - Domando os cães do inferno. *Linux Magazine*, v. 48, p. 40, nov. 2008.

REIMER, S.; KEZEMA, C.; MULCARE, M.; WRIGHT, B. *Windows Server 2008 Active Directory - Resource Kit*. 1. ed. Redmond: Microsoft Press, 2008.

RICCIARDI, F. *KERBEROS PROTOCOL TUTORIAL*. Italy, 2007. Disponível em: <http://www.kerberos.org/software/tutorial% -.html>.

RUEST, D.; RUEST, N. *Microsoft Windows Server 2008: The Complete Reference*. [S.l.]: McGraw-Hill Osborne Media, 2008.

SILVA, G. M. d. *Guia Foca GNU/Linux*. [s.n.], 2010. Disponível em: <http://www.guiafoca.org/>.

SOUSA, L. J. M. d. *Consolidação de Bases LDAP distintas em Ambiente Samba: Proposição para um Caso Real*. Lavras: [s.n.], 2010. Disponível em: <http://www.ginux.ufla.br/files/mono-LuisSousa.pdf>.

SUNGAILA, M. *Autenticação Centralizada com OpenLDAP - Integrando Serviços de Forma Simples e Rápida*. 1. ed. São Paulo: Novatec, 2007.

THE OPENLDAP PROJECT. *OpenLDAP Software 2.4 Administrator's Guide*. [S.l.], 2010. Disponível em: <http://www.openldap.org/doc/admin24/index-.html>.

TRIGO, C. H. *OpenLDAP - Uma Abordagem Integrada*. 1. ed. São Paulo: Novatec, 2007.

VERNOOIJ, J.; TERPSTRA, J.; CARTER, G. *The Official Samba 3.5.x HOWTO and Reference Guide*. Prentice Hall, 2003. Disponível em: <http://www.samba-.org/samba/docs/man/Samba-HOWTO-Collection/index.html>.

Apêndice A

Arquivos de Configurações do Servidor Linux

A.1 Arquivo `sladp.conf`

```
# Versão de protocolo utilizado para conexão pelos clientes
allow bind_v2

# Schemas e definições de classes de objeto
include        /etc/ldap/schema/core.schema
include        /etc/ldap/schema/cosine.schema
include        /etc/ldap/schema/nis.schema
include        /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/samba.schema
include /etc/ldap/schema/kerberos.schema

# Arquivos de controle dos processos do servidor slapd
pidfile                /var/run/slapd/slapd.pid
argsfile        /var/run/slapd/slapd.args

# Nível de log
loglevel 256

# Arquivo de log
logfile /var/log/slapd.log
```

```
# Módulos
modulepath        /usr/lib/ldap
moduleload        back_bdb

# Parâmetros específicos do tipo de base
backend                bdb

# Base de dados
database                bdb

# Chave de Criptografia
TLSCertificateFile /etc/ldap/ssl/ldap.pem
TLSCertificateKeyFile /etc/ldap/ssl/ldap.key

# Suporte ao Kerberos
sasl-realm EMPRESALINUX.COM.BR
sasl-host ubuntuserver.empresalinux.com.br

# Estrutura do Diretório e administrador
suffix                "dc=empresalinux,dc=com,dc=br"
rootdn                "cn=admin,dc=empresalinux,dc=com,dc=br"
rootpw                {SSHA}h/lquPXJhvDumeh8uaoaUFAv+RBUBRFQ

# Local de armazenamento dos dados
directory        /var/lib/ldap
```

A.2 Arquivo `krb5.conf`

```
[libdefaults]
  default_realm = EMPRESALINUX.COM.BR

[realms]
  EMPRESALINUX.COM.BR = {
        kdc = ubuntuserver.empresalinux.com.br
        admin_server = ubuntuserver.empresalinux.com.br
        default_domain = EMPRESALINUX.COM.BR
        database_module = openldap_ldapconf
```

```
  }

[domain_realm]
  .empresalinux.com.br = EMPRESALINUX.COM.BR
  empresalinux.com.br = EMPRESALINUX.COM.BR

[logging]
  kdc = FILE:/var/log/krb5kdc.log
  admin_server = FILE:/var/log/kadim.log
  default = FILE:/var/log/krb5lib.log

[dbdefaults]
  ldap_kerberos_container_dn =
cn=admin,dc=empresalinux,dc=com,dc=br

[dbmodules]
  openldap_ldapconf = {
        db_library = kldap
        ldap_kerberos_container_dn =
cn=admin,dc=empresalinux,dc=com,dc=br
        ldap_kdc_dn =
"cn=admin,dc=empresalinux,dc=com,dc=br"
        ldap_kadmind_dn =
"cn=admin,dc=empresalinux,dc=com,dc=br"
        ldap_service_password_file = /etc/krb5kdc/service.keyfile
        ldap_servers =
ldaps://ubuntuserver.empresalinux.com.br/
        ldap_conns_per_server = 5
  }

[login]
  krb4_convert = true
  krb4_get_tickets = false
```

A.3 Arquivo `smb.conf`

```
[global]
```

```
   workgroup = EMPRESALINUX
   realm = EMPRESALINUX.COM.BR
   netbios name = pdc
   server string = Servidor PDC
   wins support = yes
   dns proxy = no
   name resolve order = lmhosts wins bcast
   local master = yes
   preferred master = yes
   os level = 200
   interfaces = eth0, lo
   bind interfaces only = yes
   host allow = 10.0.0. 127.
   log file = /var/log/samba/log.%m
   max log size = 1000
   syslog = 2
   panic action = /usr/share/samba/panic-action %d
   security = ads
   password server = ubuntuserver.empresalinux.com.br
   kerberos method = system keytab
   dedicated keytab file = /etc/krb5kdc/krb5.keytab
   encrypt passwords = true
   enable privileges = yes
   unix password sync = yes
   domain logons = yes
   socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
   domain master = yes
   usershare allow guests = yes
# Integração ao OpenLDAP
   passdb backend =
ldapsam:ldaps://ubuntuserver.empresalinux.com.br/
   ldap admin dn = cn=admin,dc=empresalinux,dc=com,dc=br
   ldap ssl = On
   ldap delete dn = no
   ldap user suffix = ou=Users
   ldap group suffix = ou=Groups
   ldap machine suffix = ou=Computers
   ldap suffix = dc=empresalinux,dc=com,dc=br
   add user script = /usr/sbin/smbldap-useradd -m "%u"
```

```
   delete user script = /usr/sbin/smbldap-userdel "%u"
   add machine script =
/usr/sbin/smbldap-useradd -t 0 -w "%u"
   add group script = /usr/sbin/smbldap-groupadd -p "%g"
   delete group script = /usr/sbin/smbldap-groupdel "%g"
   add user to group script =
/usr/sbin/smbldap-groupmod -m "%u" "%g"
   delete user from group script =
/usr/sbin/smbldap-groupmod -x "%u" "%g"
   set primary group script =
/usr/sbin/smbldap-usermod -g '%g' '%u'
```