JACKSON RIBEIRO DE SOUZA

AUTENTICAÇÃO CRUZADA EM AMBIENTES HETEROGÊNEOS (*WINDOWS* X *LINUX*)

LAVRAS - MG

2010

JACKSON RIBEIRO DE SOUZA

AUTENTICAÇÃO CRUZADA EM AMBIENTES HETEROGÊNEOS (*WINDOWS* X *LINUX*)

Monografia apresentada ao Colegiado do Curso de Ciência da Computação, para a obtenção do título de Bacharel em Ciência da Computação.

Orientador

Prof. PhD Luiz Henrique Andrade Correia

LAVRAS - MG

2010

JACKSON RIBEIRO DE SOUZA

AUTENTICAÇÃO CRUZADA EM AMBIENTES HETEROGÊNEOS (*WINDOWS* X *LINUX*)

Monografia apresentada ao Colegiado do Curso de Ciência da Computação, para a obtenção do título de Bacharel em Ciência da Computação.

Aprovada em *16 de Novembro de 2010*

Prof[a]. Dr[a]. Marluce Rodrigues Pereira

Prof. MSc. Eric Fernandes de Mello Araújo

Prof. PhD Luiz Henrique Andrade Correia

Orientador

LAVRAS - MG

2010

Dedico esta monografia ao meu maior amigo, companheiro e exemplo...Deus, que sempre com seu amor, compreensão e justiça, me manteve em seu caminho, me mostrando sempre quais deveriam ser os próximos passos mesmo quando as infinitas opções tentavam me confundir.

AGRADECIMENTOS

Agradeço à todos que me ajudaram, diretamente ou indiretamente na conclusão desse trabalho, pois estes tiveram a paciência de me aguentar em momentos que nem eu mesmo me suportava.

Agradeço ao meu orientador, Prof. Dr. Luiz Henrique de Andrade Correia pelos conselhos, correções e ajuda imprescindível neste trabalho.

Agradeço também a minha mãe, Adagilza Chagas Ribeiro, mulher especial em minha vida que foi fundamental para que hoje alcançasse meus objetivos e me tornasse uma pessoa melhor.

E em especial a uma pessoa que com poucas palavras e atitudes me mostrou que a vida vai muito além do que os olhos podem ver, Elayne Cristina Ramos Hoffmann.

Por fim, aos colegas e amigos que, mesmo sem saber me ajudaram muito.

RESUMO

Este trabalho tem por objetivo a implementação de um ambiente de rede heterogêneo interoperável, onde estações clientes estarão habilitadas a realizarem a verificação de credenciais através de servidores em plataformas distintas, promovendo assim a autenticação cruzada. Para alcançar tal objetivo foi implementado um servidor em plataforma *Linux (openSUSE 11.3)* e outro *Microsoft® (Windows Server 2008 Enterprise®)*, proporcionando assim uma vertente *open source* e outra proprietária, para a análise da viabilidade e vantagens da integração proposta.

Palavras-chave: *Active Directory*. Autenticação Cruzada. Interoperabilidade. *LDAP*. *OpenLDAP*.

ABSTRACT

This paper aims to implement an interoperable heterogeneous network environments, where client stations will enable to obtain the authentication servers using different platforms, thus promoting the cross-authentication. To achieve this goal was implemented a *Linux (openSUSE 11.3)* and other *Microsoft ® (Windows ® Server 2008 Enterprise)*, thus providing an *open source* component and the other owner, to the feasibility and advantages of the proposed integration.

Keywords: Active Directory. Cross-Authentication. Interoperability. LDAP. OpenLDAP.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

1.1 Contextualização

O alto custo na adoção de uma plataforma que seja totalmente proprietária para a estruturação de um ambiente de TI (Tecnologia da Informação) é um problema permanente e que tem se tornado um grande desafio para muitas organizações. Em particular podemos destacar as pequenas, onde em sua maioria possuem orçamentos e recursos limitados. Muitas dessas organizações acabam por adotar medidas de contenção de gastos levando serviços e departamentos de TI a sofrerem déficits em resposta a este problema. Como conseqüência, elas são muitas vezes limitadas a tecnologias mais antigas e até mesmo a versões obsoletas do *software*, devido ao alto custo de atualizações constantes e aquisições de novas licenças (WILKINS; COLE; NELSON, 2004).

A confiabilidade dos sistemas atuais também se tornou uma questão importante e preocupante devido ao grande crescimento das redes de computadores locais e da internet. Em decorrência de tal fato temos como conseqüência uma disseminação de vírus cada vez mais acelerada e dinâmica em um âmbito global, colocando em risco diariamente todos os processos organizacionais que rodam sobre a infraestrutura de TI. Assim temos um ambiente onde empresas estão cada vez mais preocupadas com a segurança de seus sistemas e proteção de seus dados.

Todo esse cenário, aliado à crescente popularização dos sistemas operacionais *open source*, tem elevado o número de empresas interessadas na adoção dos serviços baseados nesta plataforma. Em parte devido principalmente a fatores como: segurança, disponibilidade e também ao baixo custo de implementação e licenciamento. Com isso nos deparamos cada vez mais com uma mudança na estruturação dos *Data Centers* atuais. Atualmente não encontramos mais um am-

biente homogêneo e com predominância de uma única tecnologia, mas sim uma diversificação de plataformas aonde *software* proprietário e *software* livre se juntam em um mesmo cenário (RIGOLETO, 2006). Na perspectiva de Figueiredo (1999), grande parte das organizações acabam por adotar múltiplas plataformas em seus ambientes de TI devido a razões históricas e pragmáticas. Tendo como intuito, atender as suas diversas necessidades as quais não podem ser sanadas com apenas uma única tecnologia.

Entretanto, novos desafios são gerados ao se unir tecnologias distintas em um mesmo ambiente, um desses desafios é continuar provendo de forma eficiente e segura a autenticação e acesso a rede através dos serviços de diretório para os diferentes tipos de sistemas operacionais clientes. Atualmente, as grandes empresas possuem uma gama diversificada de plataformas, onde cada uma possui seu próprio gerenciamento de usuários. Essa descentralização gera uma demanda enorme aos responsáveis pela administração dos objetos de diretório (contas de usuários, contas de computador, diretivas de segurança). E com essa arquitetura de controle baseada em banco de dados distribuídos acaba por criar desafios como, replicação e consistência nas múltiplas bases de diretórios, aumentando também assim a exposição a ataques e falhas de segurança (JUNIOR, 2009).

De acordo com Reinhardt *et al.* (2009), com o aumento das redes de computadores e as constantes mudanças e evoluções, o gerenciamento de identidade torna-se cada vez mais complexo. Uma organização não pode esperar um longo período para que um determinado empregado consiga se autenticar na rede e obter acesso a uma determinada aplicação. As exigências de produtividade dos ambientes corporativos exigem que o acesso do usuário aos recursos da rede seja imediata e satisfatória, não prejudicando assim seu desempenho.

Porém, mais do que implementar diferentes plataformas nas redes de computadores contemporâneas, existe hoje uma alta necessidade de integração desses novos sistemas *open source* com as tecnologias proprietárias já utilizadas, permitindo assim que os serviços oferecidos pelos mesmos continuem operando de forma ininterrupta e consistente. Em especial destacamos o serviço de diretório, pois é através desse poderoso recurso que provemos de forma centralizada e segura todo o gerenciamento e autenticação dos usuários corporativos.

Existem alguns mecanismos que permitem tal gerenciamento e autenticação em ambientes mistos, em particular o LDAP *(Lightweight Directory Access Protocol)* merece destaque. O foco principal deste trabalho é apresentar este protocolo, procurando analisar e descrever duas de suas implementações, *Active Directory*® e *OpenLDAP*, tendo como foco a interoperabilidade através da autenticação cruzada.

1.2 Motivação

De acordo com pesquisa realizada pela Fundação Getúlio Vargas, foi constatado que nos *Data Centers* atuais 12% dos servidores são Unix, 20% Linux, 66% Windows e 2% outros. Isso mostra a grande heterogeneidade das redes de computadores contemporâneas e que há um grande desafio a ser vencido no gerenciamento de identidade entre essas plataformas distintas. A autenticação entre sistemas proprietários e de código aberto já é uma realidade no meio empresarial. Devido a esse cenário, e as inúmeras mudanças no mundo dinâmico da TI com foco cada vez maior em interoperabilidade, se faz necessário uma maior explanação e pesquisa sobre a capacidade de tecnologias distintas coexistirem no mesmo ambiente, provendo a autenticação cruzada de forma harmoniosa e mais do que isso, produtiva (MEIRELLES, 2010).

1.3 Objetivo

Este trabalho tem por objetivo a implementação de um ambiente de rede heterogêneo e interoperável através da autenticação cruzada, utilizando para isso ferramentas que estejam disponíveis nas plataformas adotadas e que permitam a comunicação entre os sistemas. Este ambiente tem como propósito que usuários de estações clientes *Linux* ou *Windows* possam ser autenticados usando o protocolo LDAP, tanto no serviço de diretório da *Microsoft*, o *Active Directory*®, quanto em sua versão livre, o *OpenLDAP*, de forma que estes possam usufruir das potencialidades de ambas as tecnologias, garantido assim maior segurança e versatilidade no acesso às informações.

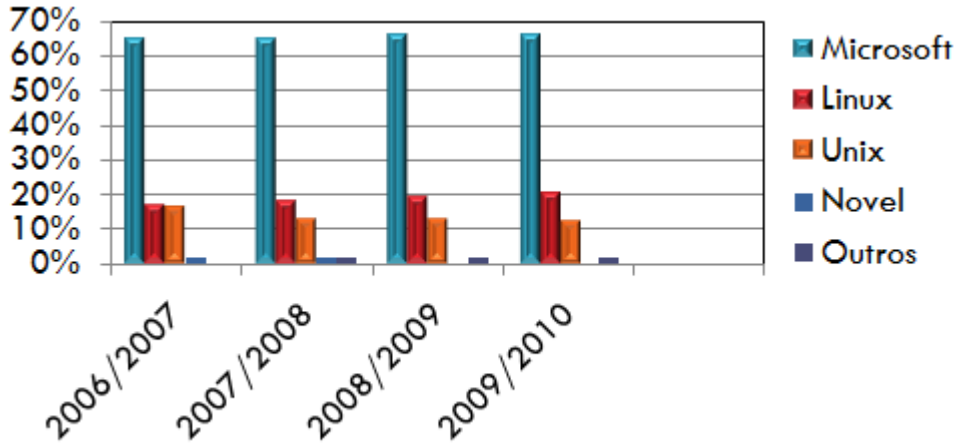

Figura 1: Gráfico evolução 2006/2010

1.4 Estrutura do Trabalho

Para possibilitar uma melhor organização do trabalho, o mesmo foi dividido em 7 capítulos. O resumo que se segue deverá assim permitir uma leitura rápida, facilitando a escolha do tema que mais suscite dúvidas ao leitor, permitindo-

lhe deste modo concentrar-se nas questões que considere mais importantes. O capítulo 2 apresenta o referencial teórico, mostrando os principais conceitos necessários para um melhor entendimento e explanação sobre o assunto, delineando assim uma base sólida para a construção da interoperabilidade proposta. A metodologia utilizada neste trabalho é apresentada no capítulo 3, juntamente com informações sobre o ambiente computacional utilizado. No capítulo 4 tem-se o início da parte prática, onde encontra-se a documentação das instalações dos sistemas adotados e das ferramentas necessárias para cumprimento dos objetivos. Esta parte foi estruturada em forma de tutoriais para facilitar a sua reprodução em qualquer ambiente posteriormente. Ainda dando prosseguimento à parte prática, no capítulo 5 são documentados os procedimentos e configurações necessárias para a interoperabilidade entre as plataformas através da autenticação cruzada com *Active Directory*® e *OpenLDAP*. No capítulo 6 temos os resultados e discussão, onde analisamos a viabilidade do projeto e suas dificuldades. O Capítulo 7 finaliza apresentando a conclusão e trazendo sugestões para trabalhos futuros.

2 REFERENCIAL TEÓRICO

Para uma melhor compreensão do trabalho apresenta-se neste capítulo os conceitos e ferramentas necessárias para a implementação e desenvolvimento do ambiente de autenticação cruzada proposto.

2.1 Conceitos Fundamentais

2.1.1 Domínio

Podemos definir um domínio como um limite administrativo e de segurança. Administrativo, pois as contas que possuem tais privilégios têm permissões de acesso em todos os recursos do domínio ao qual estão inseridas, mas não em recursos de outros domínios, ou seja, o domínio é quem define as fronteiras de permissões (BATTISTI, 2003).

Já a caracterização como um limite de segurança se dá pelo fato de que cada domínio em particular tem suas definições de políticas de segurança que se aplicam às contas de usuários e demais recursos dentro do domínio e não a outros domínios. Assim, diferentes domínios podem ter diferentes políticas e configurações de segurança. Por exemplo, no domínio A, posso ter uma política de segurança que define um tamanho mínimo de senha como 8 caracteres. Esta política será válida para todas as contas de usuário do domínio A. Um segundo domínio B, pode ter uma política de segurança diferente, a qual define um tamanho mínimo de senha de 12 caracteres. Esta política será válida somente para as contas de usuários do domínio B (BATTISTI, 2003).

O conjunto de contas de computadores e de usuários cadastrados de forma centralizada em um banco de dados compartilhado por toda a rede também é uma das formas de definirmos um domínio. Por contas de usuários e computadores

entende-se ser o nome e a senha dos mesmos, credenciais necessárias para que possam acessar os recursos da rede, ou seja, o domínio ao qual pertençam.

Em se tratando de domínios podemos enumerar várias vantagens, dentre as mais pertinentes destacam-se: escalabilidade, portabilidade e a facilidade de administração.

- Escalabilidade: A utilização da estrutura de domínio promove um crescimento da rede computacional de forma organizada e simples, nesse ambiente os usuários possuem apenas um nome e uma senha e conseguem acessar todos os recursos da rede aos quais tenham permissão (MINASI, 2003).

- Portabilidade: Pois habilita os usuários que pertencem ao domínio se autenticarem e usarem qualquer computador que esteja nesse domínio, permitindo que os mesmos tenham suas configurações disponíveis em qualquer máquina da rede, alcançando assim uma maior portabilidade (MINASI, 2003).

- Facilidade de administração: Ambientes que possuem um domínio de rede, ao contratar um funcionário, basta apenas cadastrá-lo no banco de dados do domínio, com as permissões aos recursos de rede necessários. Não é necessária nenhuma alteração nas estações de trabalho para que esse usuário possa ser um membro de toda a rede do domínio. Para excluir um usuário demitido o raciocínio é o mesmo, basta excluí-lo do banco de dados do domínio (MINASI, 2003).

A criação de um domínio é realizada através da instalação e manutenção de serviços de diretórios como o *Active Directory*® e *OpenLDAP*, às páginas seguintes ilustram esses conceitos.

2.1.2 Diretório

Uma das formas de sintetizar e entender o conceito de diretório é imaginar um banco de dados centralizado com informações sobre usuários, senhas, computadores e outros elementos necessários ao funcionamento de um sistema. Esse sistema pode ser representado por um conjunto de aplicações em um servidor, serviços de email ou autenticação. Pode-se também fazer um paralelo com um exemplo mais simples e mais presente em nosso dia a dia, como por exemplo uma lista telefônica com o cadastro do nome do usuário, telefone e endereço, que também reflete uma analogia com um típico diretório (BATTISTI, 2003).

Em termos gerais, grande parte dos profissionais de informática associa o termo diretório ao contexto de sistemas de arquivos, o que só em parte é verdadeiro. Ao pesquisar o conceito da palavra diretório percebe-se que a mesma tem vários significados, se diferenciando de acordo com o contexto. No contexto de sistemas de arquivos possui um significado, no contexto de redes e ambientes distribuídos outro e no contexto de banco de dados um terceiro significado (NAGUEL, 2001).

Esses significados não são excludentes como pode-se supor em princípio. Em um nível mais elementar diretório significa lista. E lista nada mais é do que um depósito de informação. A partir daí é possível entender porque diretório é usado nesses contextos.

Diretório em sistemas de arquivos nada mais é do que um arquivo especial que contém as lista dos arquivos pertencentes a esse diretório. No contexto de redes e ambientes distribuídos, diretório é uma lista que contém informações de serviços de rede que, por exemplo, exigem algum tipo de autenticação, obrigando que os serviços mantenham um diretório de usuários, ou seja, uma lista de

usuários. Já no contexto de banco de dados é mais intuitivo, uma vez que lista é na verdade um depósito de informação (NAGUEL, 2001).

Nas redes de computadores com modelo baseado em diretório, há uma base única de informações, que podem ser contas de usuários, contas de computador ou qualquer outro recurso da rede. Porém, na prática não é que existe uma única base armazenada em um determinado servidor e todos os demais acessam esta base. O que ocorre na prática, é que todos contêm uma cópia do diretório e alterações efetuadas em um dos servidores são repassadas para os demais, para que todos fiquem com uma cópia idêntica da base de dados do diretório. Esta sincronização entre os servidores é conhecida como replicação (BATTISTI, 2003).

De acordo com Querino e Júnior (2005), a utilização de um diretório varia de acordo com a necessidade. Em resumo, pode-se citar os seguintes:

- Sistemas de Arquivos: Nesse contexto, um diretório é simplesmente definido como um arquivo especial que contém as informações pertencentes a esse diretório;

- Redes em Ambientes Distribuídos: Com esse contexto o diretório corresponde a uma lista que contém informações dos serviços da rede para o efeito de autenticação da mesma.

- Base de Dados: No que diz respeito à base de dados, um diretório é um estrutura (*schema*), que armazena diversas tabelas, sendo estas tabelas com características comuns.

Em resumo, pode-se definir um diretório como uma base de dados especializada com o propósito de prover o acesso rápido aos dados de forma padronizada, contendo diferentes tipos de informações e oferecendo uma versatilidade muito grande na hora de buscar o dado desejado.

2.1.3 Serviço de Diretório

Em termos gerais, um serviço de diretório é um repositório de informações de rede, aplicações, ou NOS *(Network Operation System)* que são úteis para múltiplos sistemas ou usuários. De fato, há muitos tipos de diretórios diferentes, incluindo páginas de internet, servidores de email, e até mesmo serviço de DNS *(Domain Name System)* (DESMOND et all., 2009)

Segundo Bosque e Macedo (2007), um serviço de diretório contém informações em formas de entradas. Um bom exemplo poderia ser uma lista telefônica, que contém entradas como: nomes de pessoas, nomes de empresas, endereços e telefones. Cada entrada representada nessa lista contém uma série de dados que, de maneira formal, chamamos de atributos. A figura 1 exibe um exemplo de diretório estruturado. Nesta imagem é possível visualizar o conjunto de dados dispostos de forma hierárquica formando uma árvore, onde cada nó representa um objeto.

Um serviço de diretório desempenha também um papel importante dentro da empresa, pois ele fornece uma estrutura que facilita e padroniza o acesso a diversas informações, como por exemplo, dados de usuário, computadores, impressoras, servindo como um ponto de integração entre os diversos sistemas e minimizando os problemas de administração dos mesmos.

Os recursos de redes de grande porte são compartilhados por vários usuários e aplicativos. Para permitir que usuários e aplicativos acessem os recursos e as informações sobre eles, você precisa de um modo consistente de nomear, descrever, localizar, acessar, gerenciar e proteger informações sobre esses recursos. Um serviço de diretório desempenha essa função, sendo um repositório estruturado de informações sobre pessoas e recursos de uma organização (MICROSOFT®, 2003).

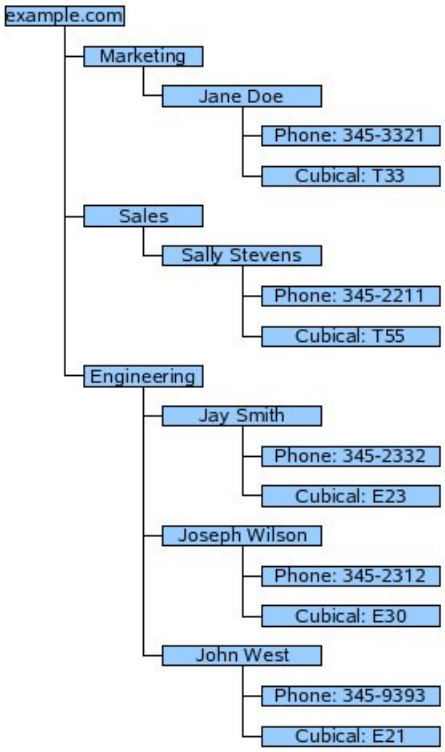

Figura 2: Árvore de Diretório (COOMBS, 2005)

Os serviços de diretório despontam atualmente como a última moda nos domínios de softwares para gestão de redes de computadores, principalmente no campo de servidores. Esses tipos de serviços, implementam uma base de dados distribuída, onde a informação é armazenada de forma hierarquizada, seguindo a estrutura de uma árvore (PEREIRA, 2003).

Se o diretório é uma base de dados organizada, ou seja, uma lista de dados, um serviço de diretório nada mais é do que uma aplicação que controla os objetos e seus atributos em um diretório. Com o serviço de diretório, os objetos e os atributos podem estar disponíveis aos usuários e a outras aplicações de forma ininterrupta e centralizada. Existem hoje, muitas implementações de software que

desempenham a função de diretório, por exemplo, o *Active Directory*® e o *Openldap*. Serviço de diretório é a implementação cliente/servidor para o conceito de diretório (NAGUEL, 2001).

Dada a necessidade crescente de informações, em particular através da Internet, a popularidade do diretório tem crescido na última década e hoje é uma escolha comum para aplicações distribuídas (KOUTSONIKOLA; VAKALI, 2004).

Para o cumprimento dos objetivos de integração das plataformas heterogêneas através da autenticação cruzada, será necessária a implementação de servidores *Microsoft*® e *Linux*, com os serviços de diretório do *Active Directory*® e *OpenLDAP* respectivamente, atuando no mesmo domínio.

Nesse sentido, faz-se necessário a partir daqui explanar a respeito das ferramentas e técnicas que farão esse ambiente possível. Em resumo, tratam-se dos conceitos do protocolo LDAP e suas implementações, além de mais algumas técnicas e recursos que serão úteis para conclusão da interoperabilidade.

2.2 O protocolo LDAP *(Lightweight Directory Access Protocol)*

O LDAP (*Lightweight Directory Access Protocol*) é um protocolo padrão inicialmente projetado para o acesso a serviços de diretório com o padrão X.500. O LDAP é a versão reduzida de um protocolo chamado DAP (*Directory Access Protocol*). A principal função do DAP era a de estabelecer, de forma padrão, regras de comunicação de acesso com um diretório baseado no padrão X.500, mas por ser complexo permitiu o surgimento do LDAP que implementa apenas as operações básicas do DAP como: *Bind*, *Read*, *List*, *Search*, *Compare*, *Modify*, *Add*, *Delete* e *ModifyRDN* (BOSQUE; MACEDO, 2007).

De acordo com Gomes *et all* (2001), o LDAP trabalha diretamente sobre o protocolo TCP/IP e oferece mais funcionalidades do que o DAP e a um custo

menor. Como se trata também de um diretório, ele baseia-se fundamentalmente no modelo cliente/servidor e fornece autenticação e o serviço de diretório para os utilizadores.

O protocolo LDAP é utilizado pela arquitetura do *Active Directory*® e ainda é possível de ser implementado usando o *OpenLDAP* em plataforma livre, que será visto mais adiante. Serviços de diretórios implementando LDAP podem conter informações particulares de funcionários e informações sobre a organização (SENA, 2005).

O *OpenLDAP* se tornou o primeiro serviço de diretório de código aberto em decorrência da Universidade de *Michigan* que trabalhava em um projeto com o objetivo de desenvolver o seu próprio servidor LDAP e decidiu abrir o código-fonte do seu *software*, surgindo assim a versão de código aberto, o *OpenLDAP*, colocando esses recursos disponíveis para usuários do mundo *Linux* (SENA, 2005).

2.3 Implementações do Protocolo LDAP

Nesta seção iremos abordar duas implementações do protocolo LDAP que serão utilizadas para a criação do ambiente misto proposto, *Active Directory*® da *Microsoft*® e a vertente livre o, *OpenLDAP*.

2.3.1 *OpenLDAP*

O *OpenLDAP* pode ser descrito como uma composição de um conjunto de aplicativos LDAP *open source*, no qual estão dispostas todas as ferramentas necessárias para fornecer um serviço de diretório padrão LDAP v.3 em um ambiente de rede, disponível em várias plataformas (Linux, Solaris, MacOS). É uma solução considerada madura hoje em dia e possui amplo suporte, sendo largamente utilizada como alternativa às implementações comerciais existentes como, *Active*

Directory®, *Novell eDirectory*, *Sun Java System Directory Server* (MACHADO; JUNIOR, 2006).

Para Gamito e Oliveira (2003), o *OpenLDAP* é definido como uma implementação livre do protocolo LDAP, que foi criado inicialmente com o objetivo de permitir acesso a serviços de diretório, através da *Internet*, embora seja possível utilizar qualquer tipo de dados.

A autenticação usando o *OpenLDAP*, na opinião de Querino e Júnior (2005), baseia-se fundamentalmente em dois métodos básicos que são os seguintes:

- LDAP *Bind*: Método que consiste em fazer *login* enviando sua senha, em seguida o serviço dá-lhe a permissão de autenticação ou então nega-lhe o acesso aos recursos solicitados. Neste caso, o utilizador apenas faz a requisição do serviço sem se preocupar com a forma como a validação do seu pedido será executado.

- LDAP *Compare*: Outro método de autenticação onde a filosofia utilizada para o efeito é a comparação. O utilizador envia sua senha e pede ao servidor para compará-la com a que se encontra armazenada no diretório e a resposta é retornada com a permissão ou negação de acesso.

Como um de seus recursos nativos, o *OpenLDAP* também possui o suporte a replicação de vários mestres, onde dois servidores LDAP podem aceitar atualizações, sincronizar uns com os outros, e atualizar suas bases de dados, criando assim uma consistência entre as replicas (KOUTSONIKOLA; VAKALI, 2004).

É interessante observar que toda essa maturidade e robustez se deve em parte ao fato do *OpenLDAP* suportar os padrões LDAP v.3 (RFCs 2251-2256 e 2829-28), assim como umas RFCs adicionais, por exemplo (SHERESH, 2002):

- RFC 2596: Uso de linguagens de programação no LDAP;

- RFC 2829: Métodos de autenticação para o LDAP;
- RFC 2830: LDAP v.3, extensão para a camada de transporte seguro;
- RFC 2849: Inclusão do formato *LDAP Data Interchange Format* (LDIF) v.1;
- RFC 3062: Operações extendidas para a modificação de senhas.

Todo esse projeto é mantido por uma série de programadores voluntários no mundo inteiro, que juntos criam novas soluções e desenvolvem a gama de aplicativos do *OpenLDAP* (GEYER; KELLERMANN; SILVELLO, 2005).

2.3.2 *Active Directory*

O *Active Directory* armazena informações sobre usuários, computadores e recursos de rede, tornando os recursos acessíveis aos aplicativos. Ele fornece uma forma consistente de nomear, descrever, localizar, acessar, gerenciar e garantir a segurança de informações sobre os recursos. *O Active Directory* possui as seguintes funções (MICROSOFT, 2003):

- Centraliza o controle de recursos de rede: Com a centralização do controle de recursos como servidores, arquivos compartilhados e impressoras, apenas usuários autorizados podem acessar os recursos no *Active Directory*.
- Centraliza e descentraliza o gerenciamento de recursos: Os administradores podem gerenciar os computadores de clientes distribuídos, serviços de rede e aplicativos a partir de um local central usando uma interface de gerenciamento consistente. Também podem distribuir tarefas administrativas, delegando o controle de recursos a outros administradores.

- Armazena objetos de modo seguro em uma estrutura lógica: O *Active Directory* armazena todos os recursos como objetos em uma estrutura lógica, hierárquica e segura.

- Otimiza o tráfego de rede: A estrutura física do *Active Directory* permite usar a largura de banda da rede de modo mais eficiente. Por exemplo, ela garante que os usuários, ao fazerem *logon*, sejam autenticados pela autoridade mais próxima, o que reduz o tráfego de rede.

Na opinião de Loureiro (2001), a introdução do *Active Directory* no Windows 2000, constitui uma das mais ou se não a mais importante novidade do sistema operacional proprietário. Esse protocolo trouxe um outro dinamismo para o Windows 2000 e revolucionou na sua totalidade não só a administração e organização da rede, mas também veio preencher as lacunas nas redes NT, que se notavam tanto na criação como na gestão de redes geograficamente separadas. O *Active Directory* constitui assim, um elemento central das versões de servidores Windows 2000 e posteriores.

Com a instalação do *Active Directory* em servidores *Microsoft* tem-se a criação de um domínio de rede baseado nessa plataforma. O *Active Directory* é a implementação LDAP da *Microsoft*®, constituindo um novo servidor de diretórios, como escrito acima. É, tecnicamente, um servidor LDAP versão 3 (MICROSOFT, 2003).

O *Active Directory* da *Microsoft*® é um sistema totalmente integrado ao sistema operacional *Windows*®, sendo o primeiro serviço de diretório da *Microsoft* escalável, projetado para utilizar tecnologias de padrão *Internet*. Ele inclui características de desempenho como armazenamento indexado para recuperação rápida de informações e suporte nativo a LDAP, além de características de segu-

rança, como a impossibilidade de se fazer pesquisas anônimas (sem informar as credenciais do pesquisador) em sua base de dados (MICROSOFT, 2003).

2.4 Virtualização

Define-se máquina virtual como sendo uma cópia eficiente e separada de uma máquina física. A máquina virtual é essencialmente idêntica a uma máquina real, ou seja, qualquer instrução executada em uma máquina virtualizada deve exibir o mesmo efeito que seria observado se fosse executada em uma máquina física (POPEK; GOLDBERG, 1974).

Devido ao fato de serem eficientes, se faz necessário que uma parte das instruções dominantes seja executada diretamente no hardware da máquina. Isto exclui do âmbito das máquinas virtuais os tradicionais simuladores (tentativa de imitar as funções de um dispositivo) e emuladores (tentativa de imitar o desenho do hardware de um dispositivo), por precisarem simular quase a totalidade das instruções antes de executá-las no hardware. A máquina virtual encontrase em um nível de abstração intermediário entre a máquina real e o emulador, no que se refere à forma como os recursos de hardware e de controle são abstraídos e usados pelas aplicações (LAUREANO, 2004).

Pode-se entender o termo separada como o fato da máquina virtual ter que trabalhar como se fosse um computador independente. Essa característica possíbilita que o usuário não perceba que está executando suas tarefas em uma máquina virtualizada ao invés de uma máquina física. Além disso, falhas em uma máquina virtual não serão propagadas para as outras máquinas virtuais (POPEK; GOLDBERG, 1974).

O conceito de virtualização tanto para *desktops* quanto para servidores é o mesmo, ou seja, executar diversos sistemas operacionais em um único *hardware*.

Uma forma já bastante difundida, apesar de não utilizar esta mesma terminologia, é a virtualização de desktops, através do uso de servidores de terminais, onde cada utilizador ligado ao sistema possui a sua sessão dentro de um mesmo sistema operacional.

2.5 Literatura Relacionada

Neste capítulo apresenta-se alguns trabalhos e pesquisas feitas sobre o tema em questão. Forão mapeados trabalhos científicos e publicações que abordam a metodologia adotada. O objetivo é determinar o estado da arte sobre o tema desta monografia.

2.5.1 Trabalhos

Dos trabalhos pesquisados, selecionou-se um artigo utilizando a biblioteca *pGINA*, um livro sobre interoperabilidade entre as plataformas *Linux* e *Windows* e duas monografias sobre autenticação cruzada utilizando o protocolo LDAP.

- *Using pGINA to Authenticate Users in MicrosoftWindows Environments*;
- *Linux and Windows interoperability guide*;
- Implementação de Ambientes Mistos Linux Windows para Compartilhamento de Recursos e Autenticação de Usuários;
- Integração dos Sistemas Operativos Windows e Linux.

A análise desses materiais resultou em uma base sólida para o alcançe dos objetivos e proporcionou uma forma mais eficaz e agíl para a resolução dos problemas e dificuldades encontradas. O artigo *Using pGINA to Authenticate Users in Microsoft Windows Environments* apresenta a utilização da biblioteca *pGINA*,

que simplifica a autenticação de usuários *Windows* em um ambiente que inclue sistemas *Linux* e *UNIX*. O artigo tem como objetivo prover um entendimento sobre como a autenticação na plataforma *Microsoft* funciona, e como o pGINA pode ser usado para proporcionar uma alternativa ao mecanismo de autenticação em ambientes heterogêneos.

O livro *Linux and Windows interoperability guide* vem com a proposta de fornecer uma maneira de se criar a interoperabilidade de forma harmoniosa e produtiva em ambientes Linux e Windows. Cobrindo para isso pontos como: problemas mais comuns com interoperabilidade, serviços de diretório, internet/intranet, arquivos etc.

Os trabalhos acadêmicos utilizados como base (Implementação de Ambientes Mistos Linux Windows para Compartilhamento de Recursos e Autenticação de Usuários e Integração dos Sistemas Operacionais Windows e Linux), mostraram-se utéis na delimitação da metodologia que deveria ser empregada, porém apresentaram um alto grau de desatualização, uma vez que a interoperabilidade é realizada entre sistemas legados como *Windows Server 2003* e *Windows XP*. Neste trabalho apresenta-se a interoperabilidade entre os sistemas mais atuais como *Windows Server 2008*, *Windows 7* e *Ubuntu LTS 10.04*.

3 METODOLOGIA

Este capítulo descreve a metodologia utilizada no trabalho a qual permitiu que os objetivos da pesquisa fossem alcançados. Na primeira seção deste capítulo será apresentada a classificação da pesquisa quanto à natureza, objetivo e aos procedimentos. Em seguida serão descritos os procedimentos metodológicos e o ambiente computacional utilizado.

3.1 Tipo de Pesquisa

O presente trabalho pode ser classificado quanto a sua natureza como uma pesquisa aplicada, pois seu objetivo principal se concentra na geração de conhecimento para a solução de um problema prático. Quanto aos objetivos ela pode ser enquadrada como pesquisa descritiva, uma vez que visa observar, registrar e analisar os fenômenos ou sistemas técnicos a partir do ambiente interoperável implantado. Em relação aos procedimentos, a pesquisa é caracterizada como experimental e em laboratório, pois tem como finalidade a descoberta de novos métodos, técnicas, ensaios e estudos de laboratório através de simulação. Entende-se por uma pesquisa em laboratório aquela que permite o controle das variáveis que possam interferir no experimento (ZAMBALDE; PADUA; ALVES, 2008).

3.2 Procedimentos Metodológicos

3.2.1 Etapas da Pesquisa

A pesquisa foi estruturada essencialmente em três etapas: levantamento bibliográfico, instalações dos sistemas e ferramentas necessárias e configurações para a autenticação cruzada.

A primeira delas consistiu basicamente na aquisição de referências e documentos para o desenvolvimento e evolução do trabalho, possibilitando assim um maior embasamento teórico. Nessa etapa ocorreu a pesquisa bibliográfica que serviu como base para a aquisição de conhecimento acerca dos temas envolvidos no projeto como: serviço de diretório, autenticação cruzada, interoperabilidade, *Active Directory* e *OpenLDAP*. O acervo bibliográfico basicamente foi formado por consultas a livros, monografias, teses de mestrado e artigos da área, consultados a partir do mês de novembro do ano de 2009.

Na etapa seguinte foi realizada a criação do ambiente heterogêneo, onde ocorreram as instalações dos sistemas e ferramentas necessárias para a autenticação cruzada, incluindo os sistemas operacionais de servidores, estações clientes e demais recursos.

Em seguida foram feitas as devidas configurações no cenário descrito acima, possibilitando assim a autenticação cruzada entre as plataformas *Linux* e *Windows*. Essas configurações foram documentadas para possibilitar assim sua reprodução posterior.

3.3 Ambiente Computacional

3.3.1 Sistemas Operacionais Clientes e Servidores

Como sistemas operacionais de servidores foram adotados o *Windows Server 2008 Enterprise* da *Microsoft* e o *openSUSE 11.3* da *Novell*. A escolha do *Windows Server 2008 Enterprise* se deu por motivo como a adoção no mercado, pois como informado anteriormente segundo pesquisa realizada, esse sistema representa mais de 60% dos sistemas operacionais utilizados em servidores no Brasil atualmente (MEIRELLES, 2010).

Em relação a escolha da distribuição *Linux* a ser utilizada, o acordo realizado entre *Microsoft* e *Novell* favoreceu a opção pelo *openSUSE 11.3*, pois ambas as plataformas vem trabalhando para alcançar a interoperabilidade entre seus produtos e serviços, facilitando assim a comunicação entre seus sistemas e consequentemente a autenticação cruzada. Para as estações clientes os seguintes sistemas foram implantados: Windows 7 da Microsoft e Ubuntu 10.04 LTS. O uso do *Windows 7* se faz necessário uma vez que foi adotado um servidor na mesma plataforma (Windows Server 2008 Enterprise), e a vertente *open source Ubuntu 10.04 LTS*, devido à sua grande usabilidade, popularidade e adoção em *desktops Linux*.

3.3.2 Serviços de Diretório

Os serviços de diretório utilizados nos servidores *Windows* e *Linux* foram o *Active Directory* e *OpenLDAP* respectivamente. O *Active Directory* é a opção de serviço de diretório que está disponível para a instalação no *Windows Server 2008 Enterprise* e vem desde o *Windows Server 2000* onde se tornou a grande novidade. Já o *OpenLDAP* é um pacote o qual implementa o protocolo *LDAP* e está presente na maioria das distribuições *Linux*, e tem se tornado a grande opção para usuários dessa plataforma quando necessitam criar um serviço de diretório.

3.3.3 Ferramentas para a Autenticação Cruzada

Para o ingresso de máquinas *Linux* em um domínio do *Active Directory* e sua posterior autenticação, foi utilizada a ferramenta *Likewise Open*, uma aplicação *open source* a qual permite que máquinas *Linux*, *Unix* e *Mac* possam ingressar em um domínio do *Active Directory* e serem autenticadas de maneira segura com suas credenciais de domínio. Para autenticação de clientes *Windows* no

OpenLDAP foi adotada a ferramenta *pGina*. O *pGina* é um software livre de autenticação cujo propósito é substituir de forma parcial a biblioteca *GINA* (*Graphical Identification and Authentication*) a qual é carregada pelo sistema *winlogon* do *Windows* e é responsável pelos processos de *login* e de *logout* dos usuários.

3.3.4 Topologia

Para a instalação dos sistemas operacionais clientes, servidores e ferramentas mencionadas acima, foi projetado um cenário utilizando uma única máquina física com a seguinte configuração de hardware:

- Processador: Intel(R) Core(TM)2 Duo T6400 2.0 GHz
- Memória RAM: DDR2 667MHz 4,0 GB
- Disco Rígido: HD sata 7200rpm 500 GB
- Placa de Rede Ethernet 100Mbits Realtek

Todos os sistemas foram virtualizados utilizando o *software VMware Server 2.0.2*. Sua adoção deu-se por motivos como o acesso gratuito, experiência prévia e conhecimento do produto, facilitando assim sua instalação e configuração. VMware Server é um produto gratuito de virtualização para servidores em ambas as plataformas, *Windows* e *Linux*. Ele permite particionar um servidor físico em várias máquinas virtuais para assim poder usufruir das vantagens da virtualização. É um produto potente e, ao mesmo tempo, de fácil utilização por usuários. Com isso tem-se uma cenário virtualizado conforme é apresentado na Figura 2, onde temos um switch virtual representando a ligação feita entre os sistemas virtualizados.

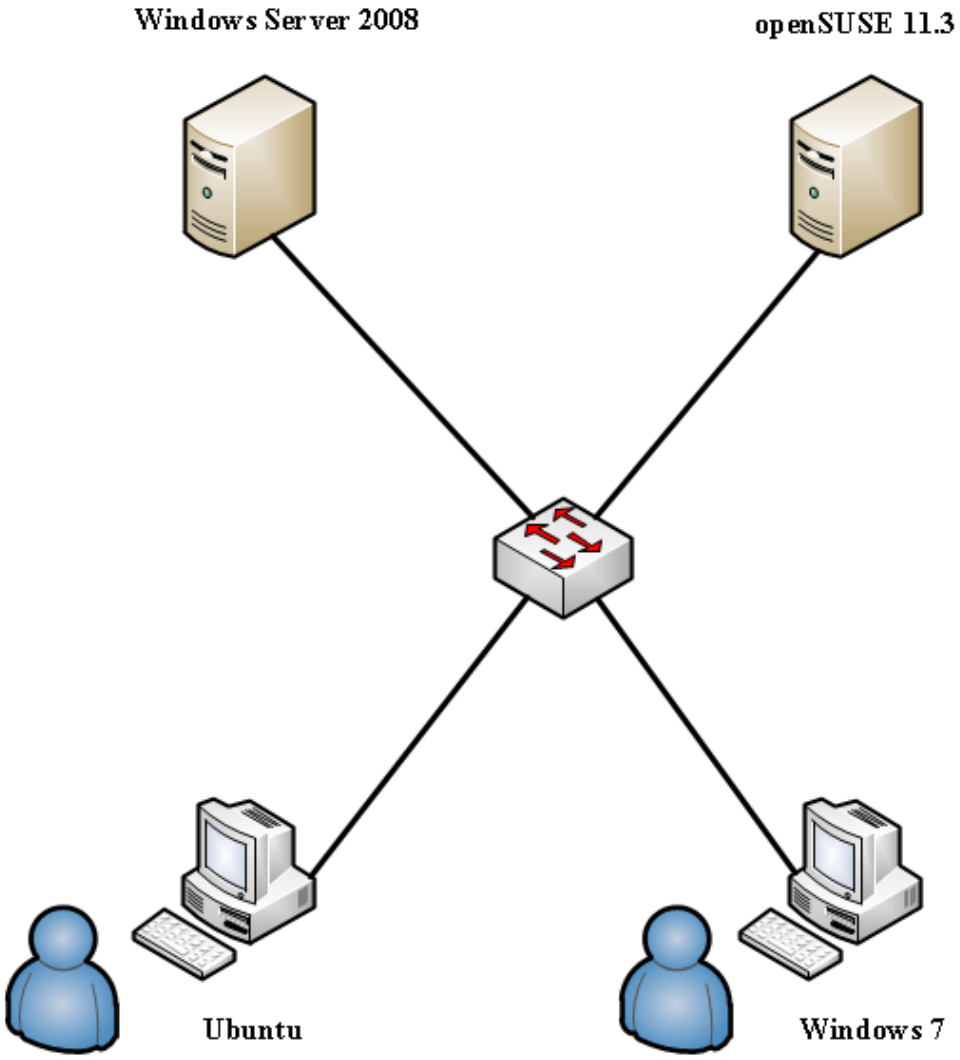

Figura 3: Switch Virtual e ligações entre as máquinas virtualizadas

4 DOCUMENTAÇÃO DAS INSTALAÇÕES DOS SISTEMAS E FERRAMENTAS

Este capítulo tem por objetivo documentar as instalações dos sistemas e ferramentas necessárias para alcançar a integração de plataformas *Linux* e *Windows* através da autenticação cruzada.

4.1 Instalação dos Sistemas Operacionais Servidores

Nesta primeira fase de implantação do cenário proposto foi dada ênfase às instalações dos sistemas operacionais de servidores *Linux* e *Windows*, que são respectivamente, *openSUSE 11.3* e *Windows Server 2008 Enterprise.*

Não houve a preocupação de uma documentação formal visto que as configurações feitas em suas opções padrões já atendem às necessidades do ambiente.

Segue, nos próximos itens, uma breve documentação sobre as instalações realizadas.

4.1.1 Instalação do *openSUSE 11.3*

A demonstração a seguir leva em consideração o modo de instalação em ambiente gráfico. A ferramenta de instalação e administração do *openSUSE 11.3* é o *YasT*. Logo na primeira tela, seleciona-se a opção instalação, como mostra a figura 3.

Selecionada a opção o instalador irá carregar em seguida o *kernel* do *Linux*. Como em todas as distribuições robustas, o instalador do *openSUSE 11.3* irá reconhecer os periféricos disponíveis na máquina e também sugerir uma forma de particionamento do HD *(Hard Disk)*, pacotes de *softwares* a serem instalados, dentre outras opções. A partir daqui todas as configurações sugeridas pelo insta-

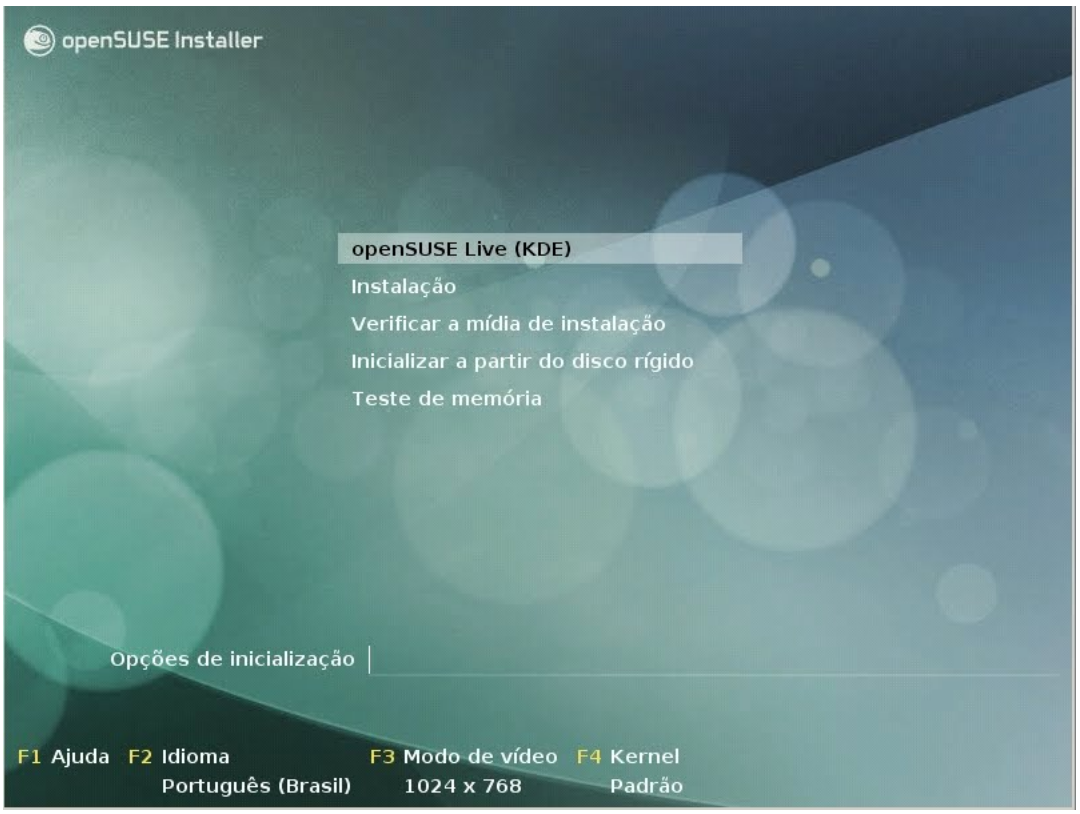

Figura 4: Tela Inicial de Instalação do *openSUSE 11.3*

lador foram aceitas no padrão, com exceção das configurações da placa de rede, onde foram definidos um endereço IP *(Internet Protocol)* e uma máscara de sub-rede, de acordo com figura 4.

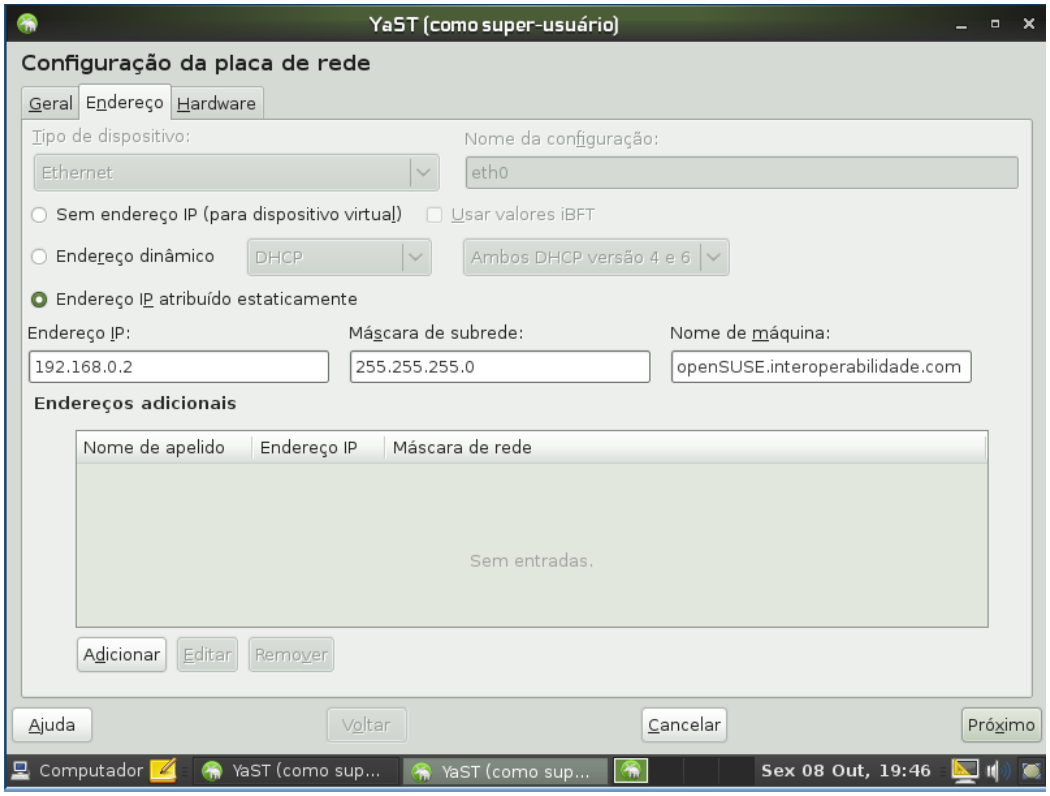

Figura 5: Configuração IP *openSUSE 11.3*

4.1.2 Instalação do Windows Server 2008 Enterprise

Assim como na instalação do *openSUSE 11.3*, as configurações podem permanecer como sugeridas pelo instalador. Apenas duas exceções a essa regra:

- Devido ao fato de possuir a certificação de instrutor oficial *Microsoft (Microsoft Certified Trainer)* e ter acesso aos softwares e chaves dos produtos comercializados pela mesma, ao ser questionado pelo instalador sobre o serial foi informada uma chave original adquirida diretamente no site http://technet.microsoft.com/pt-br/subscriptions/default.aspx, voltada justa-

mente para criação de ambientes de testes e projetos sem a necessidade de aquisição de licenças;

- Nas configurações da placa de rede foi optado por definir um endereço IP fixo como mostra a figura 5, de forma que ambos os sistemas estejam na mesma rede, pois a comunicação entre as máquinas será necessária no futuro para configuração do ambiente proposto.

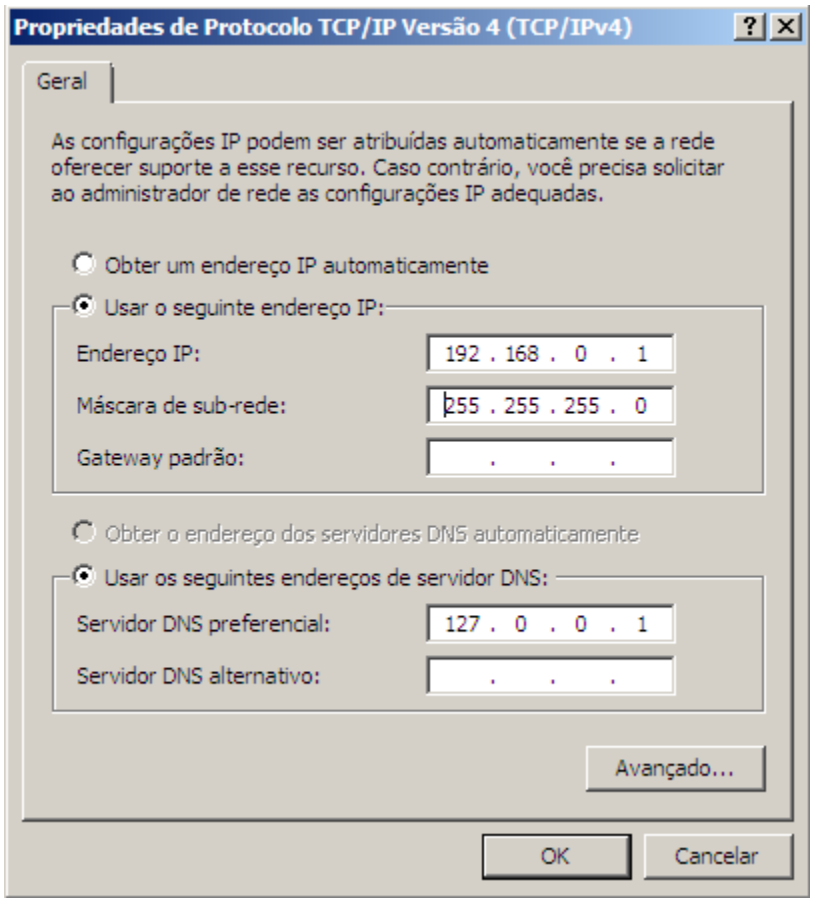

Figura 6: Configuração IP *Windows Server 2008 Enterprise*®

4.2 Instalações dos Sistemas Operacionais Clientes

Nessa parte, destacamos alguns pontos referentes as instalações dos sistemas operacionais clientes que serão usados para testes de autenticação cruzada na rede através do ambiente heterogêneo *Linux* x *Windows* que será implantado. Os sistemas operacionais clientes a serem instalados serão o *Windows 7* e o *Ubuntu 10.04 LTS*. Nessas instalações novamente não há segredos, sendo que todas as opções padrões sugeridas pelo instalador são adequadas para uso com o cenário proposto.

Da mesma forma que foi feito com o *Windows Server 2008 Enterprise* e o *openSUSE 11.3*, no momento de alteração das propriedades da placa de rede deve-se definir um endereço IP fixo de forma que essas máquinas estejam na mesma rede que as instalações dos sistemas operacionais de servidores acima mencionados.

Nas configurações das placas de rede das estações clientes que vão se autenticar usando o *Active Directory* deve-se informar na área específica do servidor DNS (*Domain Name System*) o endereço IP do servidor *Windows Server 2008 Enterprise*, do contrário essas estações não conseguirão ser inseridas no domínio do *Active Directory* a ser criado e o acesso aos recursos dos servidores *Windows* não será permitido.

Ainda nas propriedades da placa de rede, é recomendável usar um nome de computador com no máximo 15 caracteres. Isso se faz necessário para a correta integração e acesso entre ambientes *Linux* e *Windows*, visto que se trata de uma restrição de nomes *NetBios* de computadores na rede. Para *hosts* de outras plataformas que não a *Microsoft* o nome de *host* deverá ser limitado a 15 caracteres [Blair, 1998].

A licença para o *Windows 7* assim como para o *Windows Server 2008 Enterprise* foi adquirida através do site http://technet.microsoft.com entrando com as credenciais de instrutor *Microsoft*.

4.3 Instalação dos Serviços de Diretório

Conforme descrito no referencial teórico, faz-se necessário, após a instalação dos sistemas operacionais de rede, a instalação dos serviços de diretório em ambas as plataformas, *Active Directory* para *Windows* e *OpenLDAP* para *Linux*. Segue nos próximos tópicos a documentação das instalações desses serviços.

4.3.1 Instalação do *Active Directory*

Nesta documentação será demonstrada a instalação do *Active Directory*, a implementação do protocolo *LDAP* da *Microsoft*.

Nesta primeira foram instalados apenas os binários do *Active Directory*, para no próximo capítulo ser realizada a sua configuração. Primeiramente foi acessado o *Server Manager* e selecionada a opção *Add Roles* como mostra a figura 6.

Na sequência apenas foi verificado se todas recomendações foram atendidas. Na etapa seguinte selecionou-se a *role Active Directory Domain Services* e clicou-se em *Next* como aparece na figura 7.

Os passos seguintes são apenas informativos e devem ser seguidos clicando em *Next* até chegar a tela final de confirmação de instalação, aonde é informado que a mesma foi realizada com sucesso, então clica-se em close como é exibido na figura 8.

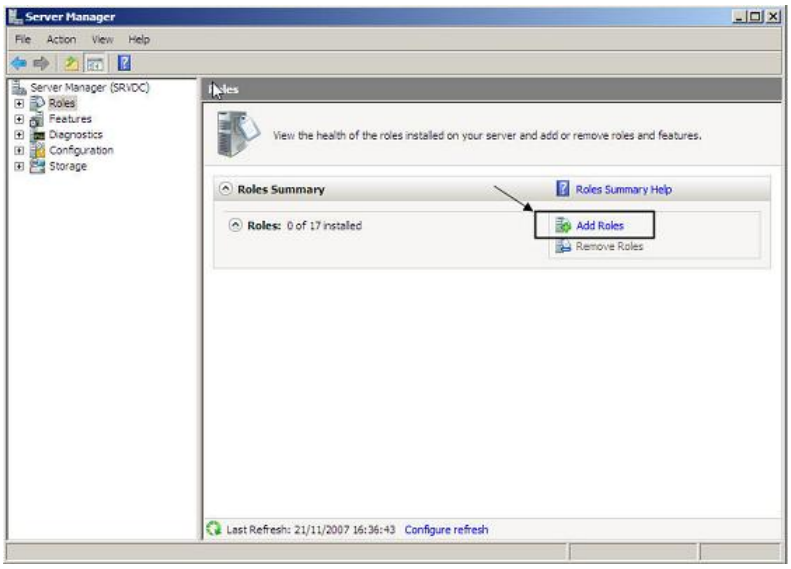

Figura 7: Tela do *Server Manager*

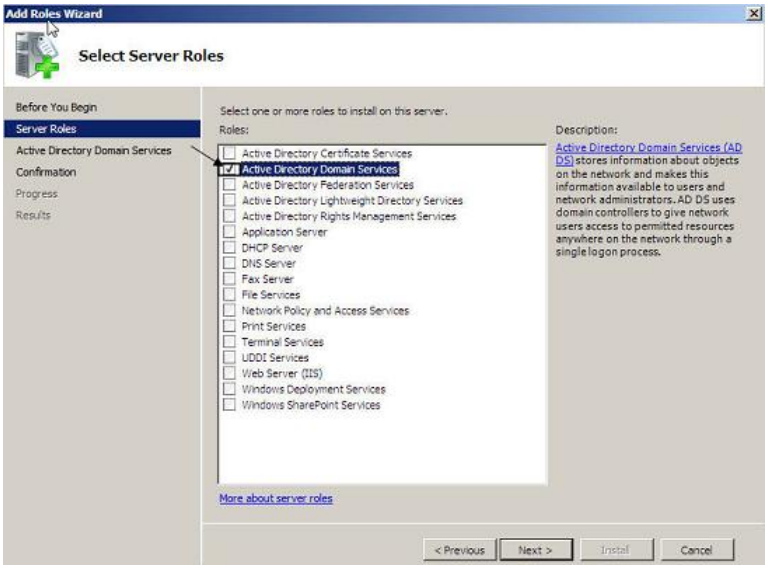

Figura 8: Selecionando a opção *Active Directory Domain Services*

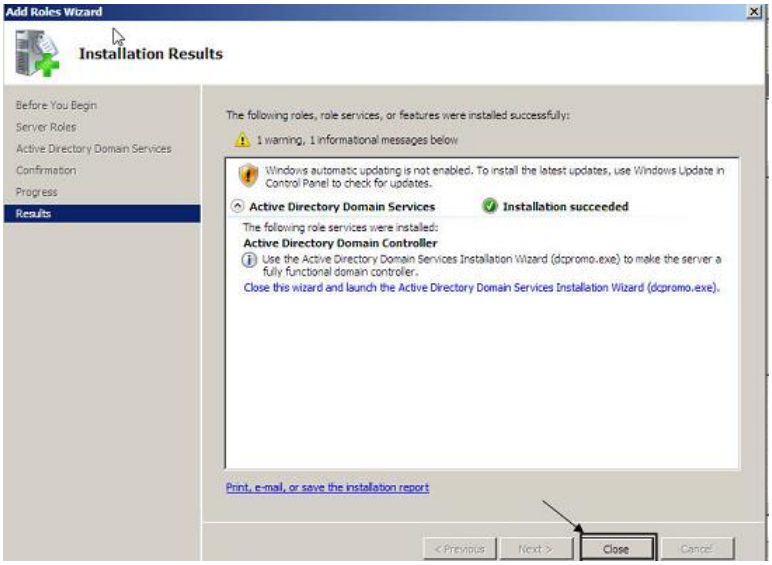

Figura 9: Instalação realizada com sucesso

4.3.2 Instalação do *OpenLDAP*

O OpenLDAP é um serviço de diretório *open source* disponível nas distribuições *Linux*, como por exemplo o *openSUSE 11.3*.

Sua instalação é realizada usando-se o *YasT*, cujo procedimento será demonstrado a seguir. No servidor *openSUSE 11.3*, é necessário logar com o usuário *root* e abrir o *YasT*. Na tela que surge, após selecionar o grupo *software* e depois gerenciamento de *software*, deverá aparecer um assistente.

No campo de pesquisa ao digitar *LDAP* será exibida uma tela como mostra a figura 9 onde deverá ser selecionado o pacote *yast2-ldap-server* e aceitas as instalações das dependências. É necessário clicar em aceitar para concluir.

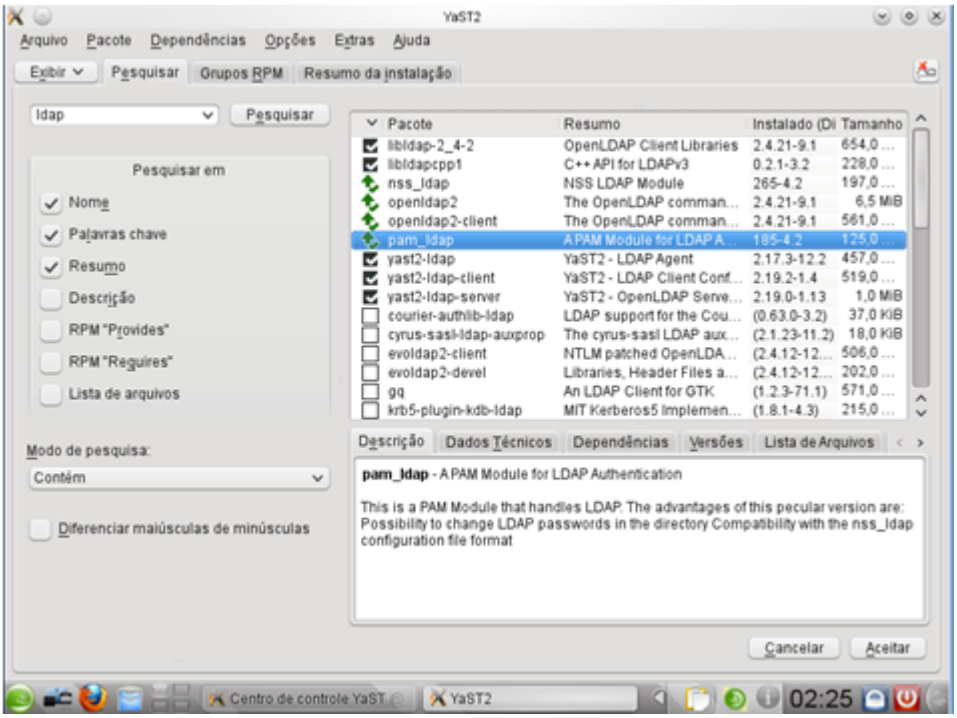

Figura 10: Instalação *OpenLDAP*

5 CONFIGURAÇÕES NECESSÁRIAS PARA A AUTENTICAÇÃO CRUZADA

Este capítulo tem como objetivo demonstrar as configurações necessárias para que o ambiente de autenticação cruzada possa ser implantado e opere de maneira correta e eficiente. Esses procedimentos incluem:

- Configuração do *Active Directory*®;
- Configuração do *OpenLDAP*;
- Configurações dos clientes (*Windows 7*®, *Ubuntu 10.04 LTS*);
- Configurações das ferramentas adotadas (*Likewise Open*, *pGina*).

5.1 Autenticação Cruzada Cliente x Servidor (*Ubuntu 10.04 LTS* x *Windows Server 2008 Enterprise*)

Nesta etapa serão dadas as diretrizes para a autenticação cruzada entre a estação cliente *Ubuntu 10.04 LTS* e o servidor *Windows Server 2008 Enterprise*®, com o serviço de diretório *Active Directory*® instalado.

5.1.1 Configurando o *Active Directory*

A configuração do *Active Directory* requer uma série de passos e opções. Devido a esse motivo e para proporcionar uma melhor sequência na leitura a documentação de sua configuração foi colocada como apêndice, denominado: APÊNDICE A - Configuração do Active Directory.

5.1.2 Configuração da estação cliente *Ubuntu 10.04 LTS*

Após a criação e configuração do domínio no *Active Directory*®, temos agora que configurar o cliente *Ubuntu 10.04 LTS* para que o mesmo possa ingressar no domínio e usar o mecanismo de autenticação da Microsoft®, assim teremos o logon de uma máquina cliente *Linux* em um servidor *Windows*®.

Antes de inserirmos o *Ubuntu 10.04 LTS* no domíno do *Active Directory*® alguns pontos devem ser analisados, como:

- ***Domain Name System*** **(DNS)**

Primeiramente, para ingressar o cliente *Linux* no domínio do *Active Directory*®, precisamos garantir que o mesmo seja configurado com o endereço IP do *Windows Server 2008 Enterprise*® como seu servidor DNS primário, em seguida devemos verificar se a estação cliente *Linux* que desejamos ingressar no domínio está cadastrada no serviço DNS com seu respectivo registro de recurso do tipo A, como mostra a figura 21.

Usando a linha de comando no *Ubuntu 10.04 LTS* podemos verificar facilmente se o registro dessa máquina está cadastrada no servidor de DNS, bastanto para isso emitir o comando host seguido do FQDN (*Fully Qualified Domain Name*) da máquina em um terminal como é demonstrado a seguir:

ubuntu@ubuntu: host ubuntu.interoperabilidade.com
ubuntu.interoperabilidade.com has address 192.168.0.3

Outro ponto referente ao DNS é a criação de uma zona reversa já que muitos serviços na plataforma *Linux* usam esse tipo de zona para resolução de nomes. Com o mesmo comando exibido acima podemos verificar se um registro

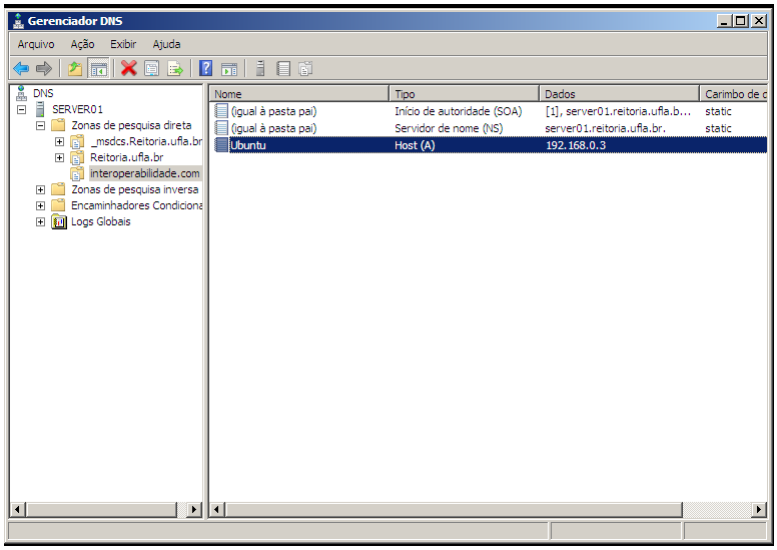

Figura 11: Registro de recurso do *Ubuntu 10.04 LTS* no DNS

reverso foi criado no servidor de DNS bastando apenas trocar o nome dá máquina pelo seu endereço IP, no nosso caso ficaria da seguinte forma:

ubuntu@ubuntu: host 192.168.0.3

3.0.168.192.in-addr.arpa domain name pointer ubuntu.interoperabilidade.com

- **Hostname**

É importante garantir também que FQDN (Fully Qualified Domain Name) da máquina cliente que irá engressar no domínio tenha correspondência com registro criado no servidor DNS. Essa informação é armazenada no arquivo de configuração hostname que se encontra em /etc/hostname no *Ubuntu 10.04 LTS*, e deve corresponder também a entrada armazenada no arquivo *hosts* em /etc/hosts. Você pode verificar o FQDN na máquina Ubuntu 10.04 LTS pela linha de comando usando o comando hostname, por exemplo:

ubuntu@ubuntu: hostname -f
ubuntu.interoperabilidade.com

- **Sincronização de Tempo**

O protocolo *Kerberos* usado internamente pelo *Active Directory*® para a autenticação é sensível ao tempo entre os computadores que desejam ingressar no domínio. A tolerância por padrão é 300 segundos de diferença entre o servidor e o cliente, no nosso caso entre o *Windows Server 2008 Enterprise*® e o *Ubuntu 10.04 LTS*. Se a máquina cliente e o servidor diverem uma diferença maior do que 5 minutos entre seus relógios a autenticação através do *Active Directory*® irá falhar. Podemos sincronizar o cliente *Ubuntu 10.04 LTS* com o servidor *Windows Server 2008 Enterprise*® através do comando *ntpdate* seguido do IP do *Windows Server 2008 Enterprise*®, como segue:

ubuntu@ubuntu:sudo ntpdate 192.168.0.1
14 Out 20:19:50 ntpdate[4358]: step time server 192.168.0.1 offset -1.457341 sec

Uma vez que todas as condições acima foram atentidas, a máquina cliente estará pronta para ingressar no domínio do *Active Directory*®. Para isso iremos utilizar o software *Likewise Open*.

5.1.2.1 Instalando o *Likewise Open*

A instalação é bem prática e pode ser feita tanto pela linha de comando digitando:

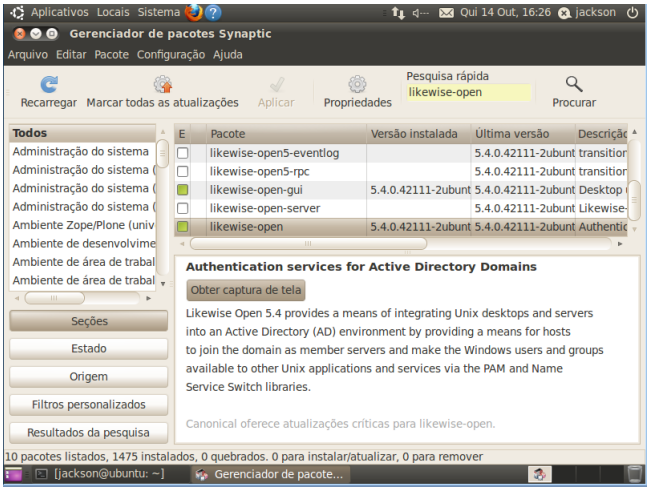

Figura 12: Instalação do *Likewise Open*

ubuntu@ubuntu: sudo apt-get install likewise-open

, ou pela interface gráfica seguindo o caminho Sistema > Administração > Gerenciador de pacotes *Synaptic* e no campo de pesquisa digitar *Likewise Open* como mostra a figura 22. Com isso será realizado o *download* dos pacotes necessários e sua instalação irá prosseguir automaticamente.

Figura 13: Ingressando o *Ubuntu 10.04 LTS* no *Active Directory*

5.1.2.2 Ingressando no Domínio do *Active Directory*

Após a instalação, podemos iniciar a ferramenta *Likewise Open* seguindo o caminho Sistema -> Administração -> *Active Directory Membership*. A janela *Active Directory Membership* será aberta aonde devemos configurar o nome da máquina e o nome do domínio que queremos ingressar como mostra a figura 23. Também temos a opção de selecionarmos em qual Unidade Organizacional desejamos adicionar a estação cliente. Por padrão todas as máquinas são acopladas no contêiner *computers*.

Após preenchermos com as informações necessárias serão solicitadas as credenciais de administrador do domínio, como é exbido na figura 24. E em alguns instantes podemos visualizar o ingresso com sucesso no domínio do *Active Directory*®. A constatação se a operação foi realizada com sucesso, pode ser

Figura 14: Tela credenciais de Administrador

verificada através da criação do ícone computador no contêiner *computers* da ferramenta *Active Directory Users and Computers*, como mostra a figura 25.

5.2 Autenticação Cruzada Cliente x Servidor (*Windows 7* x *openSUSE 11.3*)

Nesta etapa apresentaremos os passos para a autenticação cruzada entre a estação cliente *Windows 7*® e o servidor *openSUSE 11.3*, que possui o serviço de diretório *OpenLDAP* instalado.

5.2.1 Configurando o *OpenLDAP*

Primeiramente iremos realizar as configurações no servidor *Linux* no que diz respeito ao serviço de diretório que foi instalado anteriormente, a saber o *OpenLDAP*.

Iniciamos a configuração do serviço de diretório do *OpenLDAP* com o módulo servidor. Neste módulo configuramos o servidor LDAP. Para isso clique em Network Services, no menu do *YaST*, e depois em LDAP Server. Na tela inicial

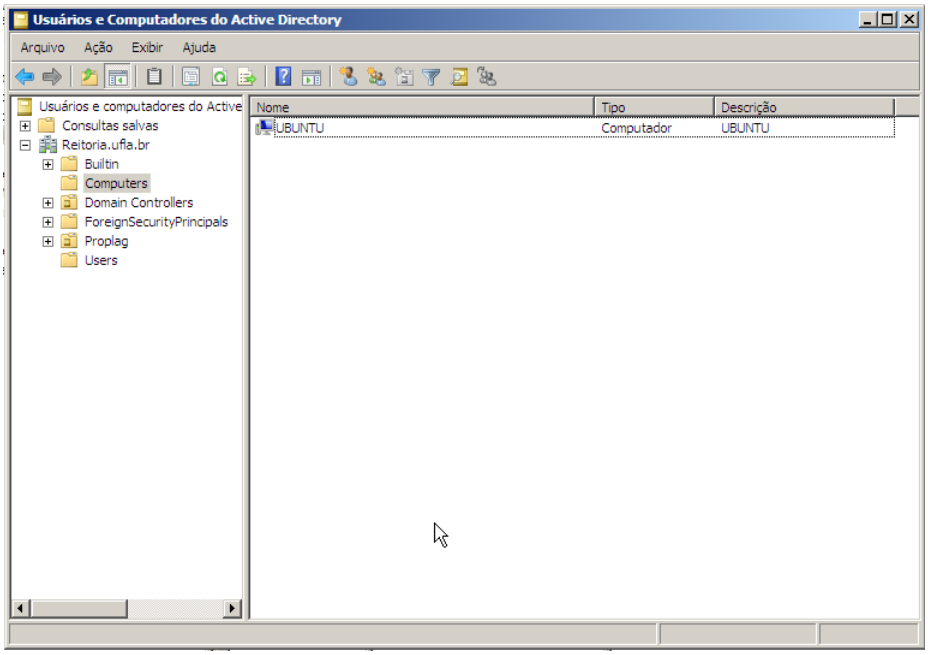

Figura 15: Estação cliente Ubuntu 10.04 LTS adicionada ao Active Directory

que é exibida marcamos como sim a opção *Start LDAP Server* e selecionamos a caixa *Open Port in Firewall* como é exibido na figura 26.

clicando em *Next* seguimos para próxima etapa aonde devemos escolher o tipo de servidor LDAP que queremos configurar, temos três opções:

- *Standalone Server*: Um cenário sem replicação, onde contamos com apenas um único servidor LDAP;
- *Master Server*: Ambientes onde temos mais de um servidor LDAP e a replicação acontece a partir do *Master Server* para o *Slave Server*, constituindo assim bases redundantes;
- *Slave Server*: Basicamente consiste de uma réplica de um *Master Server*, atuando como uma base de *backup*.

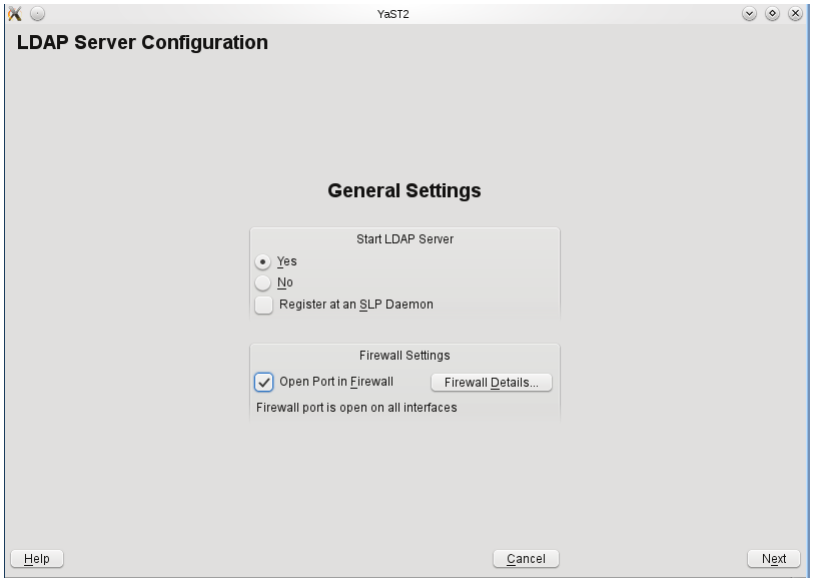

Figura 16: Tela Inicial LDAP *Server Configuration*

Em nosso cenário foi selecionado a opção *Standalone Server*, como podemos observar na figura 27.

Após selecionada a opção clicamos em *Next* e seguimos para a tela *TLS Settings*, aqui não foi alterado nenhuma opção, permanecendo como se encontra por padrão, apenas selecione *Next* e siga para a próxima tela. Em *Basic Database Settings* certifique-se de que *Database Type* esteja selecionado com o tipo hdb, no campo base DN preenchemos com o nome do domínio que no nosso caso é dc=INTEROPERABILIDADE, dc=COM. O campo *Administrator* DN deve estar como cn=*Administrator* e o *chekbox Append* Base DN marcado. Na sequência coloque a senha LDAP no campo LDAP *Administrator Password* e confirme em *Validate Password*. Em *Database Directory* deixamos o caminho que foi especificado por padrão e por último marcamos a opção *Use this Database as the default for OpenLDAP clients*, assim todos os clientes LDAP que estabelecerem conexões

Figura 17: *Select Server Type*

com esse servidor irão conectar a essa base por padrão. Isso cria um servidor LDAP com a seguinte configuração como exibida na figura 28.

Dando conclusão ao processo teremos a tela do sumário aonde temos um resumo de todas as opções que foram adotadas, aqui devemos revisar cada uma delas e confirmar clicando em *Finish* caso estejam corretas, do contrário devemos usar o botão *back* e retornar até o ponto que diverge das diretrizes passadas. Com isso finalizamos a configuração do módulo servidor.

Com o módulo servidor configurado passamos em seguida para o módulo cliente acessando *Yast* > *Network Services* > LDAP *Client*. A janela LDAP *Client Configuration* é exibida como mostra a figura 29.

Aqui é aonde definimos a primeira fonte de autenticação. Marcamos a caixa de seleção *Use* LDAP. Note que os campos *Adresses of LDAP Servers* e LDAP Base DN já aparecem preenchidos com seus respectivos valores. Sele-

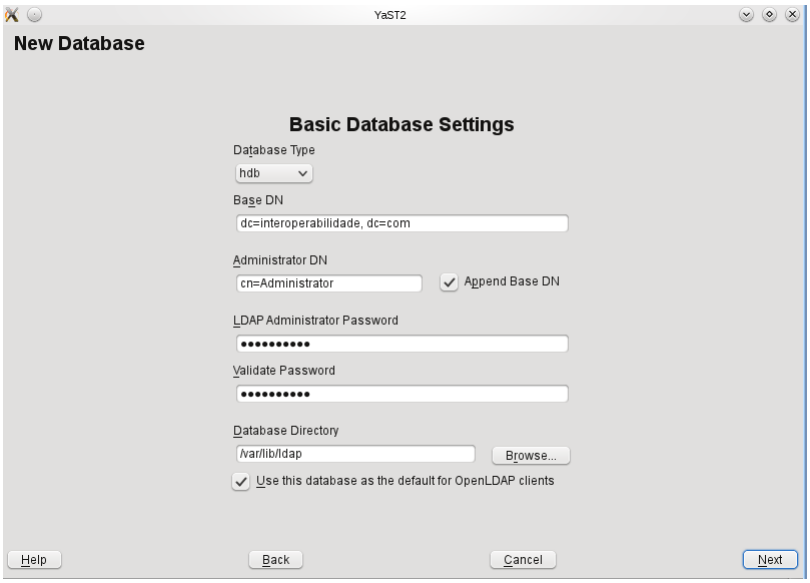

Figura 18: Tela *New Database*

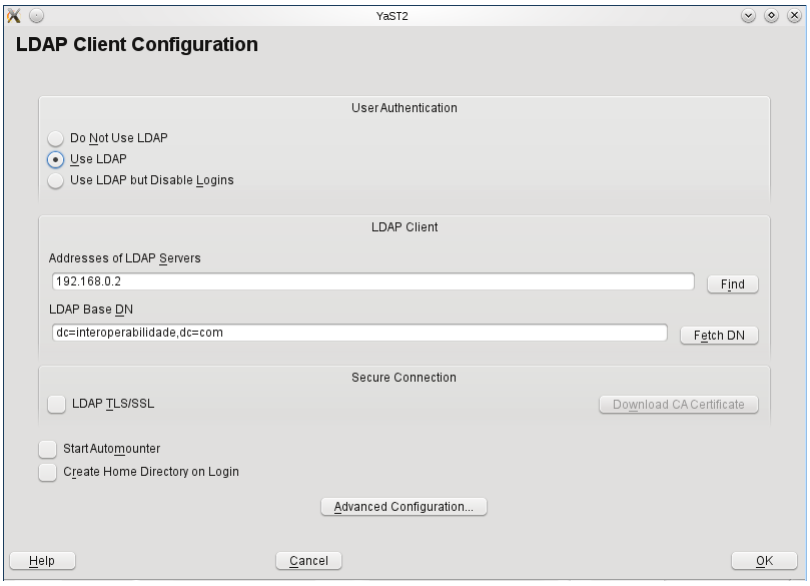

Figura 19: LDAP *Client Configuration*

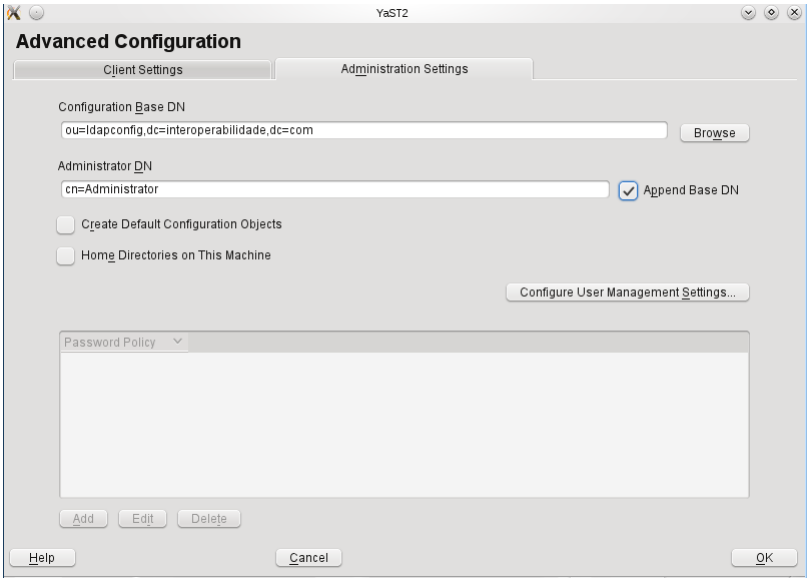

Figura 20: *Advanced Configuration OpenLDAP*

cione *Advanced Configuration*. Vá na aba *Administration Settings*, e perceba que o campo *Configuration* Base DN está como na figura 30,

enquanto o campo *Administrator* DN pode ou não estar vazio. Se estiver, preencha o *Administrator* DN com cn=*Administrator* e selecione *Append* Base DN e clique em *ok* para finalizar.

Agora é importante salientarmos a questão de criação de usuários e grupos no *OpenLDAP* e suas peculiaridades. No *Linux*, a cada usuário é dado um User ID (UID) que o identifica unicamente. Na maioria dos sistemas o usuário *root* têm seu UID (*User ID*) menor que 1000, e o primeiro usuário real é o 1000. Usuários LDAP podem ser autenticados em qualquer cliente Linux. Por isso os UIDs dos usuários LDAP devem, para não correr o risco de haver conflitos, começar em 10.000. Além disso os usuários podem pertencer a mais de um grupo, cada um com seu GID (Group ID), para evitar o mesmo problema por motivos de conflito.

Para a criação dos usuários e grupos devemos acesssar o *YaST -> Security and Users -> User and Group Management* e então digitar a senha do usuário administrator. Clique no botão LDAP *Options* -> LDAP *User and Group Configuration*, a seguir adicione um novo objeto de configuração de grupo clicando em *New* e digite, configuração de grupo por exemplo e clique em OK. As configurações de grupo são então mostradas. Note que o primeiro GID é 1000, o que é bom pois não entrará em conflito com grupos comuns que na maioria dos sistemas começam em 100. Clique em *new* novamente e então adicione um objeto de configuração de usuário chamando-o, por exemplo, de configuração de usuário, quando suas opções são mostradas note que o UID começa em 1000.

Com isso temos a seguinte configuração de diretório que contém:

- Uma base DN (dc=interoperabilidade,dc=com)
- Uma unidade organizacional *ldapconfig* (ou=*ldapconfig*,dc=interoperabilidade,dc=com)
- Os objetos de configuração dos usuários e grupos (configuração de usuário,configuração de grupo).

5.2.2 Configuração da estação cliente *Windows 7*

Após a criação e configuração do domínio no *OpenLDAP*, temos agora que configurar a estação cliente *Windows 7*® para que a mesma possa efetuar logon no servidor *openSUSE 11.3* e usar o seu mecanismo de autenticação.

Para autenticar um sistema *Windows*® em um serviço de diretório LDAP instalado em uma plataforma *open source* como o *Linux*, precisamos fazer uso de uma biblioteca denominada *pGina*, a qual nos da suporte para que a autenticação seja efetuada.

O software *pGina* é um módulo cujo propósito é substituir de forma parcial a biblioteca *GINA* (*Graphical Identification and Authentication*). A biblioteca GINA é um módulo que está presente na plataforma Windows®, este módulo é carregado pelo processo *winlogon* ficando assim responsável pelos processos de *login*, *logout* e bloqueio de tela nos sistemas operacionais.

A instalação do *pGina* no sistema implica que este novo módulo seja carregado pelo processo *winlogon* ao invés de carregar diretamente a biblioteca *GINA*, padrão dos sistemas *Windows*®. O propósito principal dessa modificação é possibilitar que uma máquina *Windows*® seja capaz de realizar a autenticação através de um servidor LDAP em plataforma *Linux*.

A biblioteca *pGina* foi concebida para funcionar através de módulos. Uma vez instalada essa biblioteca, pode-se configurá-la para que, no processo de *login* seja utilizado um módulo para que a autenticação aconteça em um servidor LDAP por exemplo, ou alternativamente em um servidor MySQL, POP3, ou qualquer outro mecanismo que possa lidar com a verificação de credenciais.

5.2.2.1 Utilizando o *pGina*

A instalação da biblioteca *pGina* deve ser realizada de forma muito cuidadosa já que, tratando-se do processo de autenticação da máquina, um erro de instalação, ou do próprio *pGina*, pode tornar a máquina inacessível. Por esta razão, é importante ter uma cópia de backup do sistema, ou a possibilidade de poder iniciar no modo de segurança, para poder retroceder este processo de forma que o encarregado da autenticação de usuários volte a ser o próprio GINA, o padrão do sistemas *Windows*®.

A página *web* do projeto é *http://www.pgina.org*. Nela você encontra os arquivos para *download* e a documentação dos pacotes e *plugins* existentes. Em

nosso cenário utilizamos a versão 2.1.0 do *pGina* que é destinada a versões mais recentes dos sistemas da *Microsoft*® como é o caso do *Windows 7*®.

A instalação do módulo *pGina* 2.1.0 é bem simples e não requer nenhuma opção além das selecionadas por padrão para seu correto funcionamento. Uma vez instalado é necessário a adição de um *plugin* para que a autenticação ocorra através de um servidor LDAP, esse *plugin* é denominado *LDAPAuth 1.5.3* e pode ser encontrado através do endereço *http://www.pgina.org/index.php/Plugins:LDAP_Auth*, baixe o *plugin* e copie ele para a pasta *plugins* que foi criada na instalação do *pGina*.

Uma vez baixado e transferido para a pasta mencionada, devemos abrir o local onde a instalação foi realizada e clicarmos em configure *pGina*, na opção *plugin*, carregamos o *LDAPAuth 1.5.3* como mostra a figura 31.

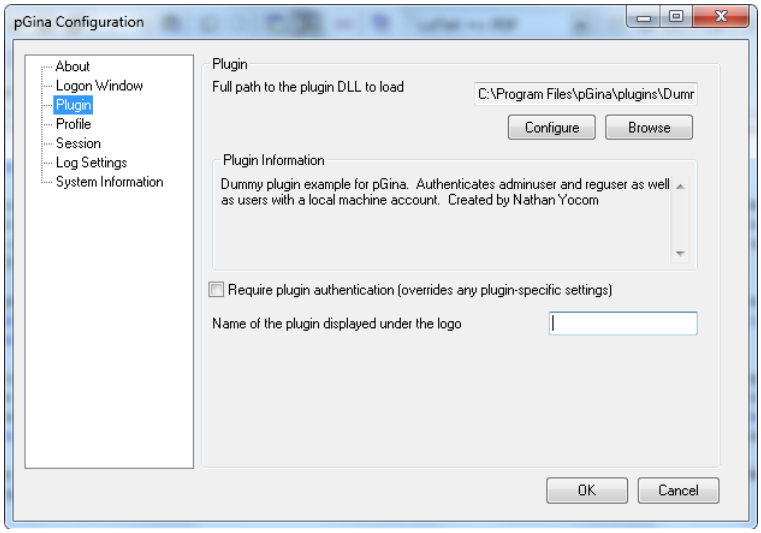

Figura 21: Configuração pGina

Ao selecionarmos a opção configure será exibida uma janela como a apresentada na figura 32, onde teremos que preencher com os valores corretos para que

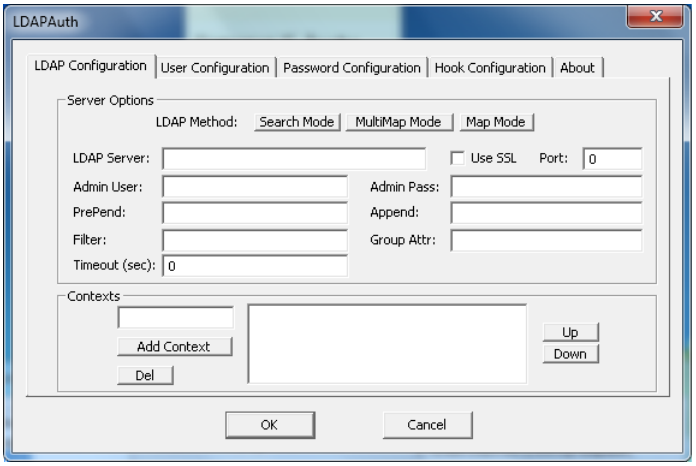

Figura 22: Configuração do Plugin

a comunicação do *plugin* com o servidor LDAP que no nosso caso é o *openSUSE 11.3* ocorra sem problemas. As opções configuradas em nosso ambiente ficaram como segue:

- LDAP Server: 192.168.0.2 (IP do *openSUSE 11.3*)
- Port: 389 (Porta de comunicação usada pelo LDAP)
- LDAP Method: Map Mode
- PrePend: uid=
- Append: ou=people, dc=interoperabilidade, dc=com

Com isso a estação cliente está preparada para ser autenticada pelo nosso servidor LDAP. A figura 33 mostra a nova janela que será exibida no *Windows 7*® para que a autenticação possa ser realizada através do servidor *openSUSE 11.3*.

Figura 23: Nova Tela de Logon do *Windows 7*®

6 RESULTADOS E DISCUSSÃO

Este capítulo irá abordar os resultados alcançados no trabalho, ou seja, se a autenticação cruzada foi realizada com sucesso e qual o comportamento dos sistemas frente à interoperabilidade, e em seguida as dificuldades encontradas.

6.1 Autenticação Cruzada

A autenticação cruzada pode ser realizada com sucesso, tanto na plataforma *Windows*® com a utilização do serviço de diretório *Active Directory*® e sistemas clientes *Linux*, quanto em servidores *open source* com o *OpenLDAP* e estações clientes *Windows*®.

A associação entre servidores e clientes ocorreu em níveis diferentes de interoperabilidade, com uma integração maior entre o *Ubuntu 10.04 LTS* e *Windows Server 2008 Enterprise*®, em parte pela grande diferença de recursos disponíveis entre *Active Directory*® e *OpenLDAP* e com isso a possibilidade de testes para aplicação de diretivas nas estações clientes.

Como exemplo de algumas diretivas configuradas no *Active Directory*® e que foram processadas e "entendidas"no cliente *Ubuntu 10.04 LTS* pode-se citar:

- O usuário deve alterar a senha no próximo *logon*;
- Horários de *Logon*;
- Fazer *logon* em (configuração que determina em qual estação cliente o usuário pode efetuar logon);
- Conta desabilitada;
- O usuário não pode alterar a senha.

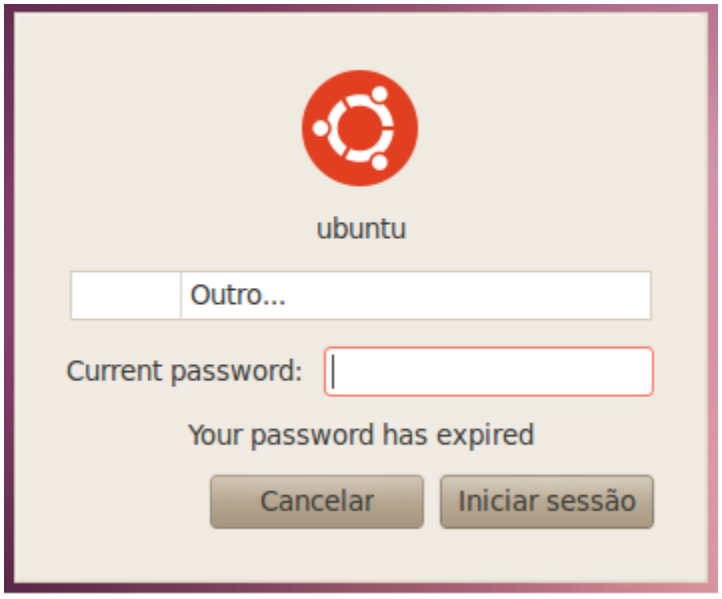

Figura 24: Tela com a mensagem de senha expirada

Entre as diretivas citadas, uma deles merece um adendo, a "O usuário deve alterar a senha no próximo *logon*". Quando configura-se essa diretiva em um determinado usuário do *Active Directory*® e tenta-se iniciar o processo de *logon* na estação *Ubuntu 10.04 LTS* digitando usuário e senha, o mesmo primeiramente informa que sua senha expirou como exibido na figura 34.

Em seguida é iniciado um processo onde primeiro solicita-se que o usuário entre com a senha atual, na tela seguinte é exibida a mensagem para inserir a nova senha desejada e depois confirmar novamente a mesma. Após feito isso, a seguinte mensagem é mostrada na tela "nenhuma conta de usuário disponível"como podemos visualizar na figura 35.

O que acontece na realidade, é que o *Ubuntu 10.04 LTS* primeiramente envia uma diretiva ao servidor *Windows Server 2008 Enterprise*® e altera a senha no *Active Directory*®. Sendo assim, precisa-se após esse processo entrar nova-

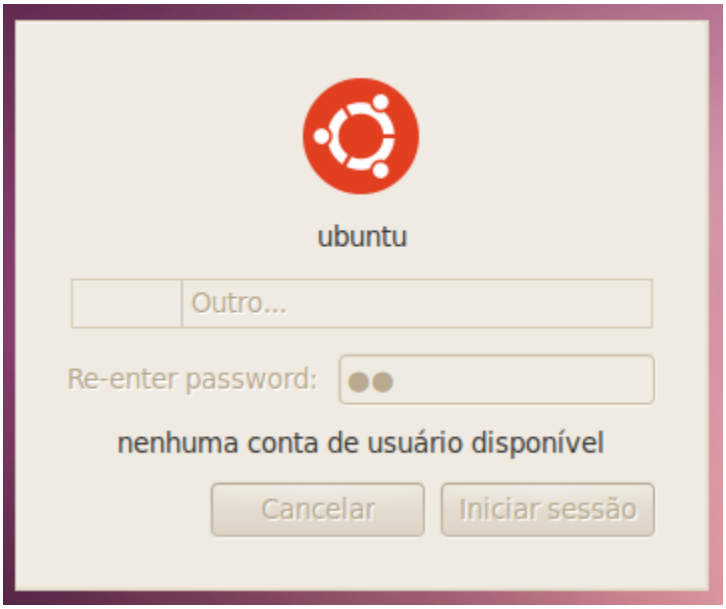

Figura 25: Tela nenhuma conta de usuário disponível

mente com as credenciais do usuário, agora já com a nova senha e efetua-se a autenticação com sucesso.

Com isso, observa-se que o cliente *Ubuntu 10.04 LTS* usa a primeira tentativa de *logon* para na verdade realizar a troca da senha quando esta diretiva está habilitada no servidor *Windows*® e após isso pode-se efetuar o *logon* normalmente.

A ferramenta *Likewise Open* utilizada neste trabalho para o ingresso de estações *Ubuntu 10.04 LTS* ao domínio do *Active Directory*®, demonstrou-se bastante prática e eficiente, alcançando de forma rápida e objetiva o seu propósito. Diferentemente do software *pGina*, o *Likewise Open* não mantem um *cache* das credenciais dos usuários. Assim, a alteração de uma senha no serviço de diretório tem efeito imediato no *logon* seguinte.

É importante resaltar também que as contas de usuários e grupos criados no *Active Directory*® e utilizados para efetuar *logon* em estações clientes *Linux*, não possuem os atributos que por padrão estariam presentes em uma conta criada nessa plataforma. Para contornar tal fato e estender o *schema* do *Active Directory*® para que o mesmo suporte tais características e assim esteja em conformidade com a RFC 2307, a qual define quais atributos LDAP são necessários para sistemas Unix e Unix-like, como o Ubuntu 10.04 LTS, deve-se instalar o recurso presente no *Windows Server 2008 Enterprise*®, denominado *Identity Management for UNIX*.

Com isso pode-se observar uma maior integração entre os objetos criados no *Active Directory*® e seu posterior uso no *Ubuntu 10.04 LTS*, uma vez que atributos *Unix* passam agora a fazer parte das classes de usuários e grupos presentes no *Active Directory*®. A figura 36 exibe a forma como deve-se entrar com as informações para realizar a autenticação entre a estação cliente *Ubuntu 10.04* e o servidor *Windows Server 2008 Enterprise*®. No campo nome do usuário deve-se inserir primeiro o nome do domínio seguido de uma barra invertida e o nome do usuário a ser utilizado.

Figura 26: Autenticando no Domínio

Da mesma forma, a autenticação entre o servidor *Linux openSUSE 11.3* e a estação cliente *Windows 7*® no serviço de diretório do *OpenLDAP*, aconteceu de forma satisfatória e eficiente, tendo alguns pontos de dificuldades como:

- Falta de documentação sobre o assunto e direcionamento para resoluçao de problemas.
- Conhecimento de ambas as plataformas (*Windows*/*Linux*) para a configuração correta do ambiente.
- Dificuldades na configuração adequada tanto do software *pGina* quanto no plugin *LDAPAuth 1.5.3*, pois fontes distintas não possuiam um consenso sobre os parametros a serem setados.
- Configuração do serviço de diretório *OpenLDAP*.

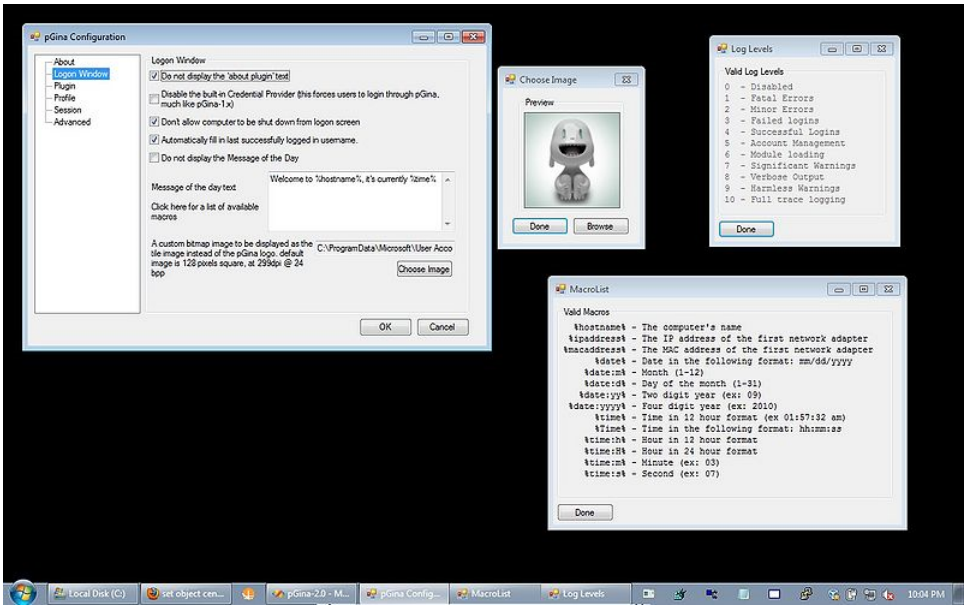

Figura 27: Estação cliente Windows autenticada no OpenLDAP

Ao longo do tempo essas dificuldades foram sendo sanadas com consultas a livros, monografias e artigos da área. A ferramente *pGina 2.0* juntamente com o plugin *LDAPAuth 1.5.3* permite uma série de configurações nas contas de usuários, o que permite também uma flexibilidade maior em escolher e definir o ambiente de trabalho, dando assim maior liberdade ao utilizador. A figura 37 exibi a tela da estação cliente Windows 7® após ter sido autenticado com uma conta *Linux* criada no *OpenLDAP* e as diversas opções de configurações do *software pGina 2.0*.

7 CONCLUSÕES E TRABALHOS FUTUROS

7.1 Conclusões

A implementação de um ambiente de rede heterogêneo com as plataformas *Windows* e *Linux* para a autenticação cruzada demonstrou-se extremamente viável e benéfica. Como primeiro resultado teve-se a geração de uma documentação onde diretrizes e ressalvas estão documentadas como forma de orientar futuros leitores que tenham a necessidade de implementar um ambiente misto e precisem de orientações para alcançar tais objetivos.

A autenticação cruzada entre as estações clientes (*Ubuntu 10.04 LTS*, *Windows 7*®) e os servidores (*Windows Server 2008 Enterprise*®, *openSUSE 11.3*) foi realizada com sucesso, e com isso tem-se novas potencialidades que podem ser exploradas como, centralizar a autenticação das estações de trabalho independente do sistema operacional cliente adotado, *Linux* ou *Windows*. Isso gera uma série de benefícios como:

- Redução no número de senhas para gerenciar e administrar. Pesquisas indicam que 35% das chamadas ao *helpdesk* são para resetar senhas, aumentando os custos da organização de TI na medida em que o número de repositórios de usuários cresce. Uma grande organização tem mais de vinte repositórios de usuários, resultando numa média de mais de cinco pares de *logins* e senhas por usuário final caso as integrações não estejam configuradas;

- Possibilidade de um ponto único de manipulação dos objetos que servem a diversos sistemas, plataformas ou ambientes. Esse ponto central pode ser tanto um servidor *Windows* com o serviço de diretório do *Active Directory*, ou um servidor *Linux* com o *OpenLDAP*.

- Ambientes integrados requerem um número menor de servidores, diminuindo por conseqüência a necessidade de aquisição de novas licenças, realização de configurações e manutenção;

- A integração proposta mantém na rede da empresa a solução do serviço de diretório do *Active Directory*, que já foi um investimento absorvido pela empresa, visto que o serviço de diretório da *Microsoft* é o líder de instalações no mercado. A solução configurada mantém esse legado da empresa;

- A integração permite ao administrador a flexibilidade do uso de qualquer plataforma tanto para servidores quanto para estações de trabalho, aumentando assim as soluções possíveis de serem instaladas na empresa, dando maior flexibilidade ao ambiente.

Em linhas gerais, o desenvolvimento do trabalho e as pesquisas na área de interoperabilidade demonstram que a opção por soluções em plataforma livre gera um custo menor devido a não aquisições de licenças, que pode chegar a zero, mas por outro lado temos um custo de mão de obra na instalação e configuração desse sistema, uma vez que há uma escassez maior de profissionais especialistas. Já para a plataforma proprietária pode-se considerar o inverso.

Com isso, concluído o objetivo do trabalho gera-se um leque maior de opções, onde possíveis soluções de problemas na área de gerenciamento de identidades podem agora ser analisadas com uma visão maior levando em conta ambas as plataformas, *Window*® e *Linux*.

7.2 Trabalhos Futuros

Como trabalho futuro pode-se apontar a criação de um mecanismo de replicação entre as bases do servidor LDAP no *Linux* com o serviço de diretório

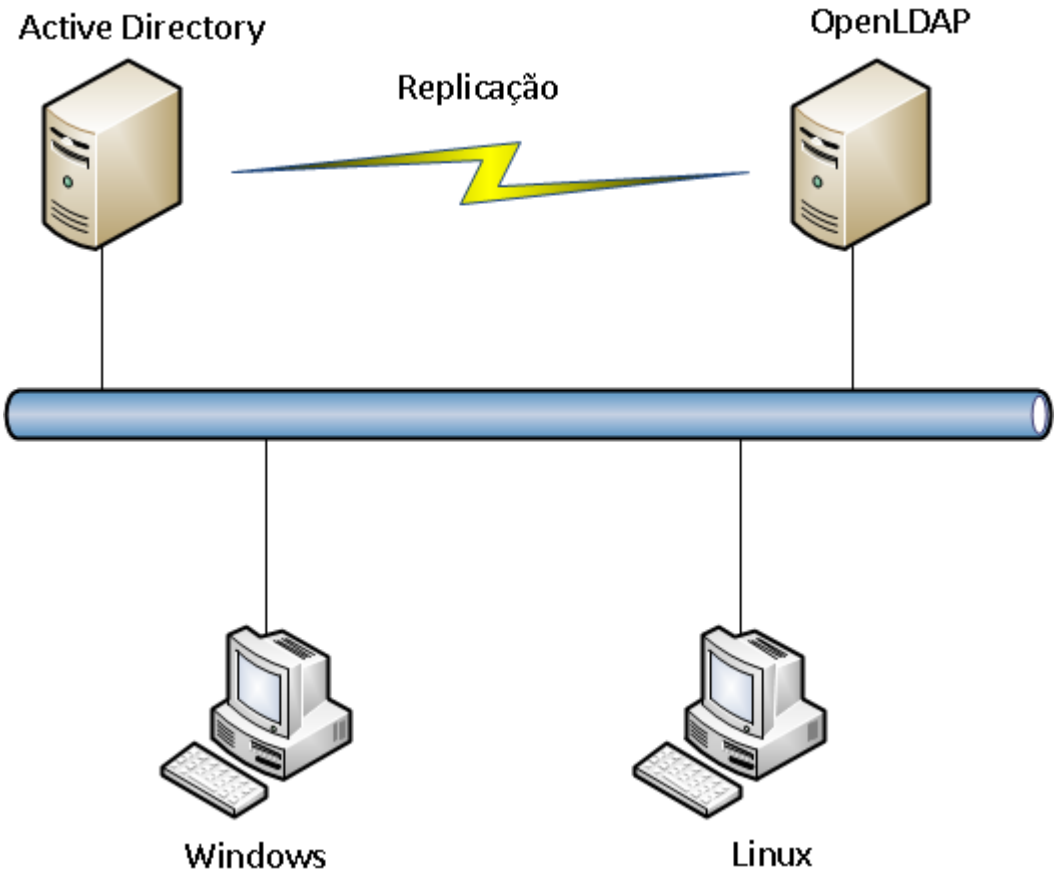

Figura 28: Sincronização entre Active Directory e OpenLDAP

da *Microsoft*® o *Active Directory*®. Assim torna-se possível a sincronização de senhas, usuários e grupos, e com isso uma maior integração e interoperabilidade entre a plataforma proprietária e *open source*. Introduzindo um ambiente com tolerância a falhas onde ambos servidores poderão responder a pedidos de autenticação e suas bases estarão consistentes devido à replicação. A figura 38 exibi uma possível topologia para esse cenário.

8 REFERÊNCIAS

- BATTISTI, J. **Windows Server 2003 Curso Completo**. 1. ed. 2003. 1568 p. Axcel Books.

- BLAIR, J. D. **SAMBA: Integrating UNIX and Windows**. 1. ed. 1998. 298 p.

- BOSQUE, L.; MACEDO, G. **Active Directory e OpenLdap handbook** Disponível em: http://ndos.codeplex.com. Acesso em: 20 set. 2010.

- COOMBS, K. **An Introduction to LDAP: Part 1-LDAP Primer**. Disponível em http://www.novell.com/coolsolutions/feature/15359.html. Consultado em 01/10/2010.

- DESMOND, B.; RICHARDS, J.; ALLEN, R.; NORRIS, A. G. L. **Designing, Deploying, and Running Active Directory**. 4. ed. 2009. 791 p.

- FIGUEIREDO, A. **Integrando Windows NT e UNIX**. Disponível em http://www.revista.unicamp.br/infotec/admsis/admsis2-1.html#ref1. Consultado em 01/09/2010.

- GEYER, C.; KELLERMANN, G. A.; SILVELLO, J. C. **Manual OpenLDAP**. Disponível em http://www.inf.ufrgs.br/gppd/disc/inf01008/trabalhos/sem01-1/t1/openldap/. Consultado em 10/09/2010.

- GOMES, C. L.; ARRUDA, F. M. J.; WATTER, L. H.; SZTOLTZ, L; TEIXERA, R. S. **Guia do Servidor da Conectiva, Editora Conectiva SA**. 2001.

- JUNIOR, C. H. F. G. **GERI Gerenciamento de Identidade** Monografia (Graduação em Sistemas de Informação) - Faculdade Salesiana Maria Auxiliadora, Macaé, 2009.

- KOUTSONIKOLA, V.; VAKALI, A. **LDAP: Framework, Practices, and Trends. IEEE Internet Computing**, v. 8, n. 5, p. 66-72, 2004.

- LAUREANO, M. A. P. **Uma Abordagem para a Proteção de Detectores de Intrusão Baseada em Máquinas Virtuais**. Ph. D. Thesis, Pontifícia Universidade Católica do Paraná, 2004.

- MACHADO, E. S.; JUNIOR, F. S. M. **Autenticação Integrada Baseada em Serviço de Diretório LDAP** Monografia (Graduação em Sistemas de Informação) - Universidade de São Paulo, São Paulo, 2006.

- MINASI, M. **Dominando O Windows Server 2003 - A Biblia**. 1. ed. 2003. 1408 p.

- MEIRELLES, F. S. 21ª Mercado Brasileiro de Informática e Uso nas Empresas. **21ª Pesquisa Anual da FGV-EAESP-CIA**, São Paulo, maio 2010. Disponível em: <http://www.eaesp.fgvsp.br/subportais/interna/relacionad/GVciaPesqResumoNoticias2010.pdf>. Acesso em: 19 ago. 2009.

- MICROSOFT, C. **Introdução à infra-estrutura do Active Directory**. 1. ed. 2003. 44 p.

- NAGUEL, F. F.; FERNANDES, E. C. **LDAP - Lightweight Directory Access Protocol**

- PEREIRA, E. D. V. **Integração dos Sistemas Operativos Windows e Linux Análise e Descrição dos Mecanismos de Integração**. Monografia (Bacharel em Engenharia de Sistemas e Informática) - Universidade Jean Piaget de Cabo Verde, Cabo Verde, 2005.

- POPEK, G. J.; GOLDBERG, R. P. **Formal requirements for virtualizable third generation architectures**. Communications of the ACM, v. 17, n. 7, p. 412, julho 1974.

- QUERINO, F. S.; JUNIOR, H. S. F. **Autenticação distribuída de sistemas híbridos e serviços de rede baseadas em serviços de directórios** Disponível em: https://www.redes.unb.br/PFG.202004.pdf. Acesso em: 19 ago. 2009.

- REINHARDT, A.; MELLO, D.; MARTINS, F.; MACHADO, M.**Gerenciamento Integrado de Identidade em Ambientes Corporativos, s.d.**. Disponível em http://www.inf.unisinos.br/p̃aschoal/arqs_gerencia_redes/trabs/grad/Apres Ger_Identidade.pdf. Consultado em 01/09/2010.

- RIGOLETO, F. **Implementação de Ambientes Mistos Linux Windows para Compartilhamento de Recursos e Autenticação de Usuários** Monografia (Graduação em Análise de Sistemas) - Universidade São Francisco, Itatiba, 2006.

- SENA, C. **LDAP Um Guia Prático**. 1. ed. 2005. 168 p.

- SHERESH, B.; SHERESH, D. **Understanding Directory Services**. 2. ed. 2002. 567 p.

- SMITH, M. C.; HOWES, T. A.; GOOD, G. S. **Understanding and Deploying LDAP Directory Services.**. 2. ed. 2004.

- WILKINS, D.; DONALD, C.; MICHAEL, N. **Windows Interoperability With Linux in the Enterprise (WINWILE): A Solution to the High Cost of Licensing, Downtime, and Security Problems. Journal of Computing Sciences in Colleges**, v. 20, n. 2, p. 260-266, 2004.

- ZAMBALDE, A. L.; PADUA, C.I.P.S.; ALVES, R. M. **O documento científico em Ciência da Computação e Sistemas de Informação**. Lavras, Minas Gerais, Departamento de Ciência da Computação, UFLA, 2008. 74 p.

APÊNDICES

APÊNDICE A - Configuração do Active Directory

Inicialmente será demonstrada a configuração do *Active Directory* no servidor *Windows Server 2008 Enterprise* instalado anteriormente.

Para que o *Active Directory* possa ser configurado corretamente o serviço de DNS (*Domain Name System*) para resolução de nomes deve estar disponível na rede ou então deve-se configurá-lo durante a criação do domínio, do contrário o serviço de diretório da *Microsoft* não funcionará adequadamente.

Para iniciar o processo de configuração obrigatoriamente deve-se efetuar o logon no *Windows Server 2008 Enterprise* com as credenciais de administrador. Em seguida seleciona-se o *menu start* e a opção *run*. Na tela que se abre digita-se o comando *dcpromo* e pressiona-se enter. Será então carregado o *Active Directory Domain Service Installation Wizard* conforme mostra a figura 10 onde há uma breve explicação sobre a instalação do *Active Directory*. Para dar continuidade clica-se em *Next* e segue-se para a próxima etapa.

Na tela *Operating System Compatibility* é exibido um alerta sobre o novo padrão de segurança do *Windows Server 2008*, o qual informa que ele poderá causar um impacto em clientes *Windows NT 4.0*, clientes não *Microsoft* e dispositivos NAS (*Network Attached Storage*) que não suportam algoritmo de criptografia forte. Caso esteja sendo instalando em um ambiente de produção é preciso avaliar os impactos antes de prosseguir, verificando se possui alguns dos dispositivos mencionados. Na sequência será carregada a janela conforme mostra a figura 11.

Figura 29: Tela inicial de Configuração do *Active Directory*®

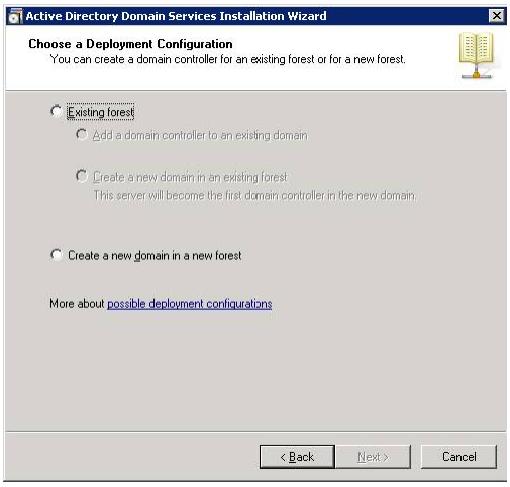

Figura 30: *Choose a Deployment Configuration*

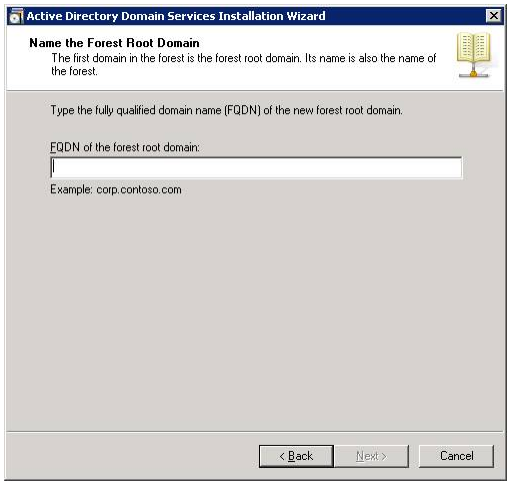

Figura 31: Tela *Name the Forest Root Domain*

Em *Choose a Deployment Configuration* há a opção de criar um *Domain Controller* para uma floresta existente (*Existing forest*) ou criar um novo *Domain Controller* para uma nova floresta (*Create a new domain in a new forest*). Como no cenário utilizado está sendo criado o primeiro domínio da floresta, denominado INTEROPERABILIDADE.COM, é necessário selecionar a opção *Create a new domain in a new forest* e seguir para a próxima etapa. A janela conforme mostra a figura 12 será exibida.

Nesta etapa, denominada *Name the Forest Root Domain*, é definido o nome do domínio raiz da floresta. Esse nome também será o nome da floresta. Ao digitar um nome FQDN (*Fully Qualified Name*), como por exemplo, INTEROPERABILIDADE.COM e em seguida clicado em *Next*, será carregada a janela conforme mostra a figura 13.

A tela *Set Forest Functional Level* permite selecionar o nível funcional da floresta. O nível funcional da floresta irá fornecer os recursos disponíveis conforme o nível selecionado, por exemplo, se for selecionado

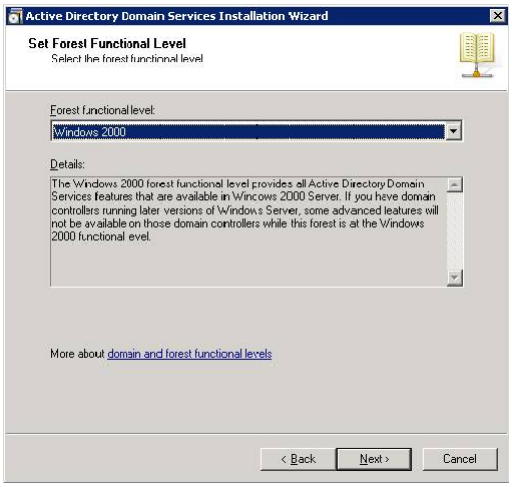

Figura 32: Tela *Set Forest Functional Level*

o nível funcional *Windows 2000* terá compatibilidade com *Domain Controllers* com *Windows 2000*, porém alguns novos recursos do *Windows Server 2008 Entreprise* não estarão disponíveis. Os níveis de florestas disponíveis são:

- Windows 2000
- Windows Server 2003
- Windows Server 2008

No exemplo apresentado será selecionado o nível de floresta Windows Server 2008 para que se tenha todas as funcionalidades mais recentes disponíveis e não haver limitação de não ingresso de sistemas legados (Windows server 2000/2003) no domínio, pois em nosso cenário não se faz necessário. Após selecionar o nível da floresta e clicar em *Next*, será carregada a janela conforme mostra a figura 14.

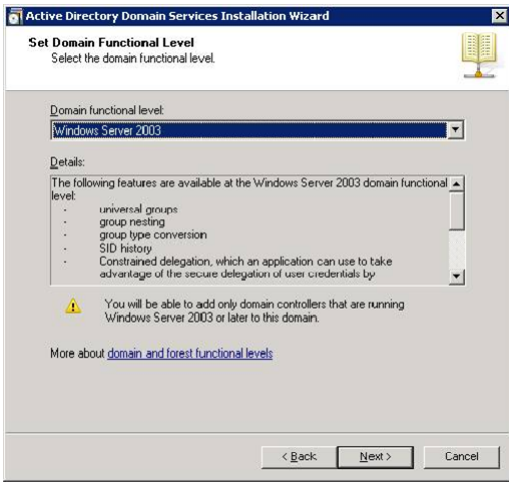

Figura 33: Tela *Set Domain Functional Level*

Na opção *Set Domain Functional Level* é necessário selecionar o nível funcional do domínio. O nível funcional da floresta configurado anteriormente engloba vários domínios dentro de uma mesma floresta, já o nível funcional de domínio irá fornecer os recursos disponíveis somente a esse domínio configurado em específico. Os níveis de domínio são:

- Windows 2000
- Windows Server 2003
- Windows Server 2008

Para o ambiente utilizado neste trabalho foi selecionado o nível do domínio *Windows Server 2008*. Selecionando-se o nível do domínio e em seguida clicando em *Next* será carregada a janela conforme mostra a figura 15.

A tela *Additional Domain Controller Options* permite incluir opções adicionais no *Domain Controller*. Ao instalar o primeiro *Domain Con-*

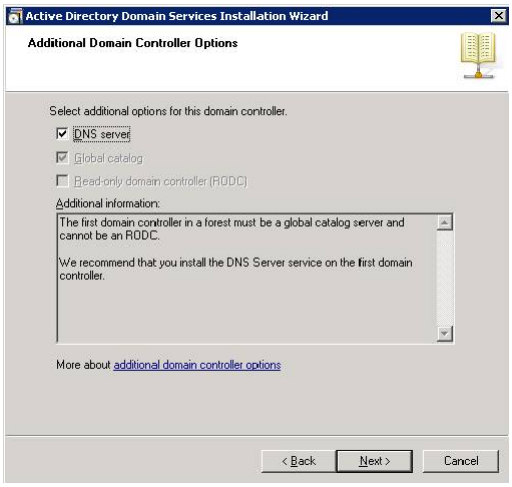

Figura 34: Tela *Additional Domain Controller Options*

troller da floresta o assistente de instalação automaticamente seleciona a opção *Glogal Catalog*, permitindo assim que esse *Domain Controller* atue como repositório central para todos os objetos de todos os domínios dessa floresta. O *Glogal Catalog* tem a função de armazenar todos os objetos dos domínios de uma mesma floresta, atuando como um local central para realizar pesquisas sobre esses mesmos objetos.

O assistente recomenda que o serviço de DNS seja instalado, como comentado anteriormente é extremamente recomendável instalar o serviço de resolução de nomes (DNS) ao configurar o *Active Directory*, uma vez que ao adotar essa abordagem todos os registros de recursos necessários ao correto funcionamento do *Active Directory* serão criados automaticamente no DNS.

No ambiente utilizado será instalado o serviço de DNS nesse *Domain Controller*. É necessário escolher a opção e em seguida clicar em *Next*. Se houver um ou mais adaptadores de rede que recebe o endereço IP

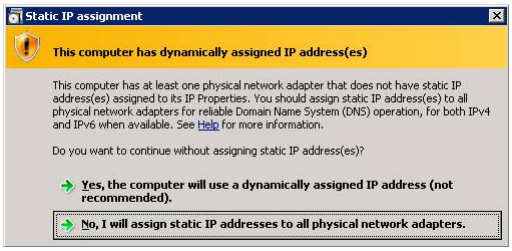

Figura 35: Tela Alerta Configuração IP

dinamicamente ou se tiver somente um adaptador configurado com IPv4 e IPv6, em que um deles receba o endereço IP dinamicamente, provavelmente será exibido um alerta conforme mostra a figura 16.

A opção *No, I will assign static IP addresses to all physical network adapters* deve ser selecionada acessando o *Control Panel* e seguido pelo *Network and Sharing Center*. Em *Tasks* na opção *Manage network connections* deve ser selecionado *Local Area Connection* e em seguida *Properties*, onde o *Internet Protocol Version* 6 (TCP/IPv6) deve ser desmarcado.

Em *Additional Domain Controller Options* escolhendo-se *Next* para continuar, será exibido um alerta informando que a delegação para o DNS não pode ser criada como mostra a figura 17. Isso ocorre devido a ainda não existir uma zona de DNS criada no servidor, para que isso não ocorresse, uma zona direta de nome INTEROPERABILIDADE.COM teria que ser criada previamente no servidor de DNS, não exibindo assim essa mensagem.

Neste caso essa mensagem pode ser ignorada, porque o serviço de DNS ainda não está instalado e configurado no *Domain Controller*, o qual será feito pelo assistente de instalação do *Active Directory* automaticamente. Será carregada então a janela conforme mostra a figura 18.

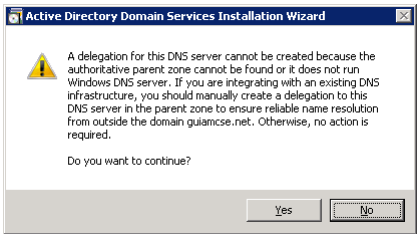

Figura 36: Tela Delegação para o DNS

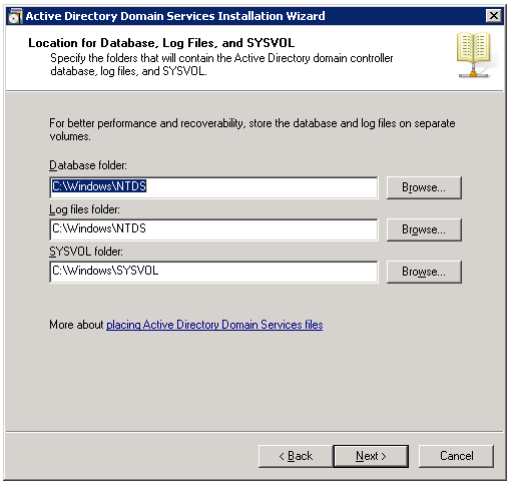

Figura 37: Tela *Location for Database, Log Files, and SYSVOL*

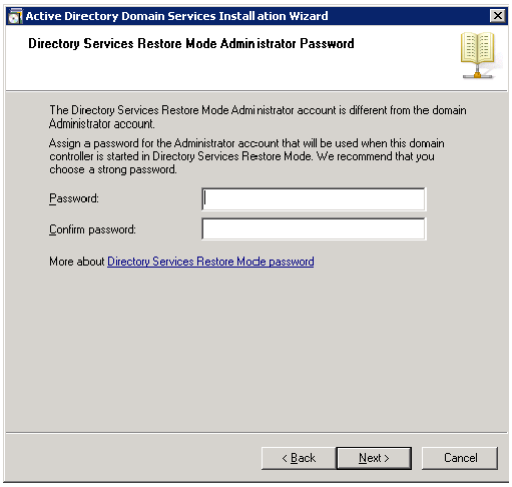

Figura 38: *Directory Services Restore Mode Administrator Password*

Em *Location for Database, Log Files, and SYSVOL* defini-se onde será armazenado o banco de dados do Active Directory, os arquivos de *log* e a pasta *SYSVOL*. Como boa prática para uma performance melhor recomenda-se colocar tais arquivos em discos separados. Neste ambiente tem-se somente um volume, portanto deixa-se o caminho padrão e em seguida siga para a próxima etapa. A janela conforme mostra a figura 19 será carregada.

Em *Directory Services Restore Mode Administrator Password* entre com uma senha, a qual será utilizada quando esse *Domain Controller* for iniciado em *Restore Mode*, ou seja quando for necessário realizar algum reparo ou recuperação no *Active Directory* é obrigatório que se entre com a senha setada neste passo.

Dando sequência tem-se o *Summary* onde visualiza-se todas as opções escolhidas com o assistente de instalação.Onde também se encontra a opção de exportar as configurações para serem utilizadas em um arquivo de

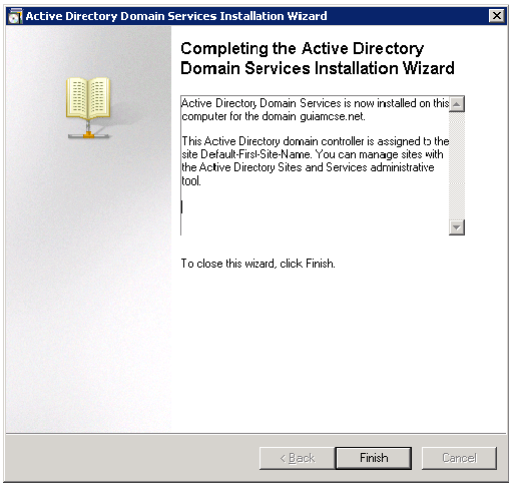

Figura 39: Termino da Configuração

resposta em uma futura instalação, sendo necessário somente clicar no botão *Export settings* e salvar o arquivo em um local seguro.

Nesse momento o assistente de instalação do *Active Directory* irá instalar e configurar o serviço de DNS, o próprio Active Directory e todas as demais opções selecionadas e necessárias. Espere até o termino da instalação. Quando for exibida a tela conforme a figura 20 a configuração terá sido completada com êxito.