INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA SUL-RIO-GRANDENSE - IFSUL, CÂMPUS PASSO FUNDO
CURSO DE TECNOLOGIA EM SISTEMAS PARA INTERNET

MARCELO LUIS GROSS

ACTIVE DIRECTORY SOBRE SAMBA

Prof. José Antônio Oliveira de Figueiredo

PASSO FUNDO, 2015

MARCELO LUIS GROSS

ACTIVE DIRECTORY SOBRE SAMBA

Monografia apresentada ao Curso de Tecnologia em Sistemas para Internet do Instituto Federal Sul-Rio-Grandense, Câmpus Passo Fundo, como requisito parcial para a obtenção do título de Tecnólogo em Sistemas para Internet.

Orientador: Prof. José Antônio Oliveira de Figueiredo

PASSO FUNDO, 2015

MARCELO LUIS GROSS

ACTIVE DIRECTORY SOBRE SAMBA

Trabalho de Conclusão de Curso aprovado em ____/____/____ como requisito parcial para a obtenção do título de Tecnólogo em Sistemas para Internet

Banca Examinadora:

_____

Prof. José Antônio Oliveira de Figueiredo (Orientador)

_____

Prof. Thiago dos Santos Marini (Convidado)

_____

Prof. Lisandro Lemos Machado (Convidado)

_____

Prof. Alexandre Tagliari Lazzaretti

Coordenador do Curso

PASSO FUNDO, 2015

A minha família
pela compreensão e o estímulo
em todos os momentos.

RESUMO

Este trabalho implementou o Active Directory em Windows e em Linux usando SAMBA 4, visando a resolução das dificuldades práticas e a criação de um tutorial. Após serem obtidos os resultados funcionais, foi feito uma comparação direta de desempenho destas implementações simples para verificar suas equivalências e suas diferenças.

Palavras-chave: Redes, SAMBA, Active Directory, Windows, Linux Debian, Comparação, Tutorial

ABSTRACT

This work is the implementation of Active Directory, in Windows and Linux using SAMBA, aimed at resolving the practical difficulties and the creation of a howto. After being obtained functional outcomes, was made a performance benchmark of these simple implementations to verify equivalences and differences.

Key words: Network, SAMBA, Active Directory, Windows, Linux Debian, Benchmark, Howto

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

LDAP: *Lightweight Directory Access Protocol* (ou Protocolo Leve de Acesso a Diretórios)

AD: *Active Directory* (ou Diretório Ativo)

RFC: *Request for Comments* (ou Pedido para Comentários)

DFS: *Distributed File System* (ou Sistema de Arquivo Distribuído)

DNS: Domain Name System (ou Sistema de Nomes de Domínio)

NetBIOS: Network Basic Input/Output System (ou Sistema Básico de Entrada/Saída de Rede)

UCL: User Account Control (ou Controle de Conta de Usuário)

PDC: Primary Domain Controller (ou Controlador Primário de Domínio)

SUMÁRIO

1 INTRODUÇÃO

A implementação de sistemas para internet, em muitos casos, implica na necessidade do conhecimento de tecnologias de rede correlacionadas e a ausência deste conhecimento pode implicar na inoperância das comunicações, que é um dos requerimentos mais básicos de um sistema informático.

Das muitas tecnologias de redes, uma das mais conhecidas para redes de computadores, especialmente aquelas que usam de forma homogênea o sistema operacional Windows, é o Active Directory.

O controle de domínio LDAP é implementado nos sistemas operacionais Windows como Active Directory (AD). Por questões de praticidade e segurança, muitas redes de computadores Windows são configuradas com AD, mas isso originalmente implicava na utilização única e exclusiva de sistemas operacionais em toda a rede envolvida, ou pelo menos no servidor, cujas licenças sempre foram muito mais onerosas do que as versões de Windows para estações de trabalho.

O SAMBA sempre buscou a interoperabilidade na comunicação entre sistemas heterogêneos. Em sua versão 4, ganhou uma reimplementação em software livre do protocolo Active Directory, sendo desenvolvido por Andrew Tridgell, em conjunto com toda a comunidade de software livre. Esta inovação que permitiu que uma máquina com sistema operacional Unix possa cumprir o mesmo papel de um servidor Windows, no que se refere as funções de diretório ativo.

Este trabalho irá explorar as questões correlacionadas a este recurso em um ambiente heterogêneo, com a utilização de um cliente Windows 8, que poderá trabalhar com um servidor Windows ou trabalhar junto a um servidor Linux.

1.1 MOTIVAÇÃO

Este trabalho foi motivado pela curiosidade de testar as novas funcionalidades do SAMBA 4 e verificar suas potencialidades.

O domínio da tecnologia Active Directory é importante devido à popularidade do sistema operacional Windows.

Nesta área específica, o mercado encontra uma quantidade relativamente escassa de profissionais que atuam no segmento e é cada vez mais comum que o gerenciamento de redes

de computadores, de segurança corporativa e até de equipamentos de impressão, tem sido feito por empresas terceirizadas (COMPUTERWORLD, 2014).

Como principal atrativo para o gerenciamento da segurança no AD, o administrador da rede tem acesso a todos os recursos (objetos) do diretório por meio de um único logon (usuário e senha).

A partir do domínio da tecnologia AD sobre o servidor SAMBA, é possível usufruir de todas as vantagens das aplicações software livre, como a gratuidade e a possibilidade de auditoria do código fonte.

Também seria de grande importância a criação de uma apostila didática de Active Directory sobre SAMBA, que poderia estar à disposição dos outros alunos do curso de TSPI e se tornar em um material de estudo complementar do aluno, já que a apostila traria alguns tutoriais práticos e descritivos das operações, tornando o aprendizado mais direto e simples, caso o aluno se interessar pelo assunto e procurar pelo material.

1.2 OBJETIVOS

Demonstrar o Active Directory sobre o SAMBA.

1.2.1 Objetivo Geral

Implementar Active Directory tanto no SAMBA como no Windows, criando um tutorial para ambos e fazer uma comparação simples de ambas implementações.

1.2.2 Objetivos Específicos

- Implementar Active Directory em um laboratório com sistemas Windows.
- Implementar a rede usando SAMBA.
- Desenvolver um tutorial de implementação do SAMBA.
- Estudar e implementar um sistema de métricas.
- Comparar o desempenho de sistemas Windows e Linux.

2 O ACTIVE DIRECTORY

Segundo a Microsoft, o Active Directory (AD) é um serviço de diretório desenvolvido pela empresa para o domínio das redes Windows e está incluído na maioria dos sistemas operacionais Windows Server como um conjunto de processos e serviços (MICROSOFT DEVELOPMENT NETWORK, 2010).

Esta tecnologia permite aos usuários de uma rede de computadores trabalharem usando entradas personalizadas de usuário e senha, não importando se o usuário decidir usar outro computador, suas configurações e arquivos pessoais poderão ser acessados, desde que tais máquinas estejam dentro de um mesmo domínio controlado por um servidor.

Segundo a Microsoft (How Active Directory Searches Work, 2010), o Active Directory é uma tecnologia de controle de domínio tradicionalmente implementada pela Microsoft nos sistemas operacionais Windows, baseada essencialmente na personalização do protocolo LDAP feito pela empresa.

2.1 Usos Do Active Directory

AD é um controlador de domínio que autentica e autoriza todos os usuários e computadores em uma rede de tipo domínio do Windows, atribui e aplica as políticas de segurança para todos os computadores autenticados, como instalação e atualizações de software.

O AD é usado em empresas com redes Windows, nas quais os administradores de redes escolheram utilizar este recurso como forma de centralizar a administração dos recursos, bem como da segurança.

Como facilidade, ele armazena centralmente os dados de usuários e computadores, permitindo que os usuários tenham apenas uma senha para acessar todos os recursos disponíveis na rede.

O diretório também pode ser utilizado para compartilhamento de arquivos, impressoras, gerenciamento de atualizações de estações de trabalho através do WSUS (*Windows Server Update Services*), tudo em um console simples e gerenciável. (LDC SOLUÇÕES, 2014)

2.2 Funcionamento Básico Do Active Directory

Quando um usuário faz *logon* em um computador que faz parte de um domínio de rede, o AD verifica a senha apresentada e determina se o usuário é um administrador de sistema ou um utilizador normal. (TECHNET, 2011)

Uma instância do AD consiste em um banco de dados e o correspondente código executável responsável pelo atendimento de pedidos e a manutenção do banco de dados.

A parte executável é chamada de Directory System Agent (DSA), que é uma coleção de serviços do Windows e processos que são executados no Windows 2000 e versões posteriores. (MICROSOFT DEVELOPMENT NETWORK, 2010)

Os objetos no bancos de dados do AD podem ser acessados através do protocolo LDAP, o ADSI (interface dos COMs (*Component Object Model*)) e dos serviços da APIs de mensagens e o Gerenciador de Contas de Segurança. (RUSSINOVICH, SOLOMON e ALLCHIN, 2004, p. 840)

2.3 Estrutura E Hierarquia Lógica Do Active Directory

No Active Directory são encontrados objetos, florestas, arvores, domínios, partiçoes, esquemas e unidades organizacionais (similares a pastas), que são explicados a seguir.

2.3.1 Objetos

Uma estrutura de AD é um arranjo de informações sobre objetos. Os objetos se dividem em duas categorias principais (TECHNET ARTICLES, 2013):

- Recursos: Hardware em uma rede ex.: Impressoras
- Entidades de segurança: Entidades puramente lógicas ex.: Contas de usuário ou grupos.

Para cada entidade de segurança são atribuídos *security identifiers* (SIDs) únicos. Cada objeto representa uma única entidade: um usuário, um computador, uma impressora ou um grupo e seus atributos, e certos objetos podem conter outros objetos. (TECHNET, 2011)

2.3.2 Florestas, Árvores e Domínios

Dentro de uma implantação, os objetos são agrupados em domínios. Os objetos para um único domínio são armazenados em uma única base de dados (que podem ser replicados). Os domínios são identificados pelo seu o *namespace* (nome no DNS).

Um domínio é definido como um grupo lógico de objetos de rede (usuários, dispositivos) que compartilham o mesmo banco de dados AD.

Uma árvore é uma coleção de um ou mais domínios, e árvores de domínio em um *namespace* contínuo, vinculados em uma hierarquia de confiança transitiva.

Uma floresta é uma coleção de árvores que compartilham um catálogo global comum, esquemas de diretório, estruturas lógicas e a configuração do diretório. A floresta representa o limite de segurança dentro do qual os usuários, computadores, grupos e outros objetos são acessíveis. (SUPORTE DA MICROSOFT, 2009)

2.3.3 Partições (Contextos De Nome)

O banco de dados do AD está organizado em partições, cada um armazenando tipos de objetos específicos e seguindo um padrão de replicação.

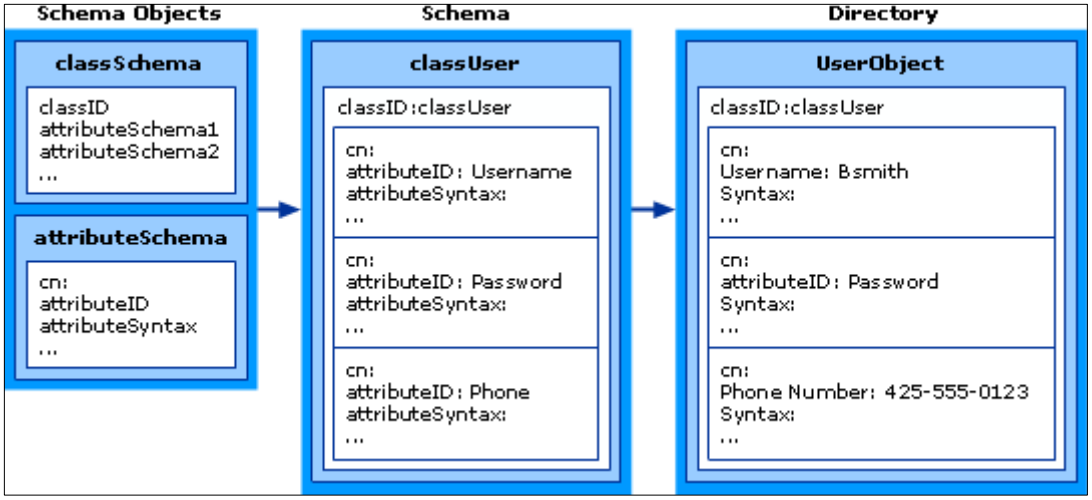
A partição *schema* contém a definição de classes de objetos e atributos dentro da Floresta. A partição *Configuration* contém informações sobre a estrutura física e de configuração da floresta (como a topologia física). Ambos replicam para todos os domínios da floresta. A partição do domínio detém todos os objetos criados nesse domínio e replica somente dentro de seu próprio domínio. (TECHNET, 2007)

2.3.4 Esquemas

Um objeto é identificado exclusivamente por seu nome.

Possui um conjunto de atributos das características e das informações que o objeto representa - Definido pelo *schema* (esquema de banco de dados) do Active Directory, que determina os tipos de objetos que podem ser armazenados no banco.

Figura 1 - Esquema como herança de objetos e instanciação



Fonte: *Schema of Active Directory* **(TECHNET, 2011)**

O objeto *schema* permite que os administradores estendam ou modifiquem o esquema quando necessário. No entanto, cada objeto de esquema é essencial para a definição de objetos do Active Directory, desativar ou alterar esses objetos pode mudar radicalmente ou interromper o funcionamento de toda implementação de rede. (Windows Server 2003: Active Directory Infrastructure, p. 8-9)

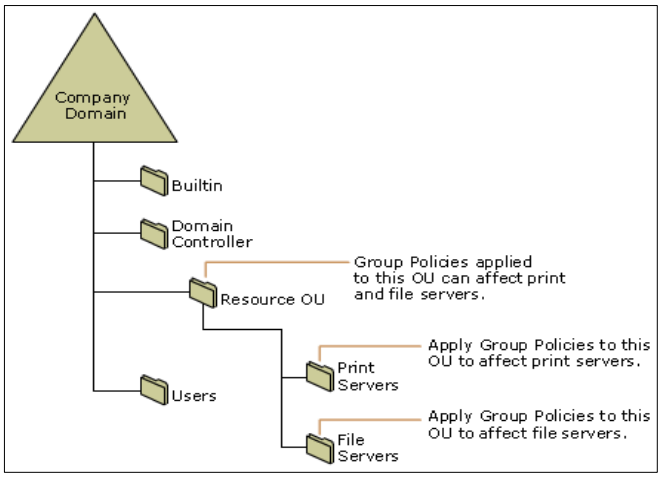
Como pode ser visto nas heranças de objeto na Figura 1, as alterações de esquema se propagam automaticamente por todo o sistema. Uma vez criado, um objeto só pode ser desativado, mas não excluído. Alterar o *schema* geralmente requer planejamento.

2.3.5 Unidades Organizacionais

Os objetos mantidos dentro de um domínio podem ser agrupados em Organizational Units (OUs). OUs pode fornecer hierarquia dentro de um domínio, facilitar a sua administração. OUs pode conter outras OUs, e os domínios são os recipientes neste sentido, como pode ser visto na Figura 2.

OUs é o nível recomendado de a aplicação de políticas de grupo, que são objetos do AD chamados formalmente Group Policy Objects (GPOs), embora as políticas também podem ser aplicadas a domínios ou sites. A UO é o nível em que os poderes administrativos são comumente delegados, mas a delegação pode ser executada com os objetos individuais ou com os atributos também (TECHNET, Organizational Units, 2010).

Figura 2 - Criando uma sub-árvore OU com dois recursos, em uma diretiva de grupo



Fonte: *OU Design Concepts* **(TECHNET, 2014)**

Por fim, as OUs são um arranjo para o administrador e não funcionam como recipientes; o domínio subjacente é o verdadeiro recipiente. Não é possível, criar contas de usuários com um nome de usuário idêntico em OUs separadas. (TECHNET, 2010)

Isto é assim porque o atributo de objeto de usuário (sAMAccountName), deve ser exclusivo dentro do domínio.

Dois usuários em diferentes OUs podem ter o mesmo Common Name (o nome sob o qual eles são armazenados no próprio diretório)

A razão para este problema de nomes duplicados através de diretórios hierárquicos, é que a Microsoft baseia-se nos princípios do NetBIOS, que é um método de gerenciamento de objetos de redes de arquivos simples, que vem desde o Windows NT 3.1 e MS-DOS LAN Manager.

Permitir a duplicação de nomes de objetos no diretório, ou remover completamente o uso de nomes de NetBIOS, impediria a compatibilidade com softwares e equipamentos legados (MICROSOFT DEVELOPER NETWORK, SAM-Account-Name attribute, 2010).

2.4 O Volume De Sistema (Sysvol)

O Volume de Sistema (SYSVOL) que é um diretório compartilhado (MICROSOFT SUPPORT KB 324175), que armazena a cópia do servidor de arquivos de domínio público, que deve ser compartilhado para acesso e replicação em domínios comuns.

Ela contém:

a) O Logon de rede compartilhado. Hospedam scripts de logon e objetos de diretiva dos computadores clientes.
b) Scripts de logon de usuário, para os domínios em que o administrador usa as opções “Usuários e Computadores” do Active Directory.
c) Diretivas de grupo do Windows.
d) Os arquivos de transferências, das pastas e arquivos que devem estar disponíveis e sincronizados entre os controladores dos domínios de serviço de replicação (FRS).
e) Junções de sistema de arquivo.

Segundo a Microsoft (ASK THE DIRECTORY SERVICES TEAM, 2011), o recomendável é instalar esses 3 em locais distintos, preferencialmente em HDs separados, para facilitar a recuperação do sistema em caso de falha de hardware.

Se a floresta está no nível de funcionalidade do Windows Server 2008 ou Windows Server 2008 R2, o sistema de replicação de SYSVOL deixa de ser o NT File Replication Service (NTFRS) e passa a ser o Distributed File System Replication (DFSR), o que termina criando uma dependência de uma versão específica de sistema operacional Windows.

2.5 Desenvolvimento Histórico

O AD faz uso do protocolo Lightweight Directory Access (LDAP) versão 2 e 3, da implementação da Microsoft do Kerberos, do serviço de DNS e também são usados os conceitos similares aos dos diretórios X.500 e das Organizational Unit (OU).

As seguintes RFCs contribuíram diretamente para a criação do LDAP:

- RFC 1823 (IETF, 1995)
- RFC 2307 (IETF, 1998)
- RFC 3062 (IETF, 2001)

2.5.1 Windows 2000 Nativo

O Microsoft Active Directory foi lançado em 1999 com o Windows 2000 Server Edition. Segundo a Microsoft (WINDOWS SERVER, 2014), historicamente, os seus principais recursos eram:

- Grupos universais: Tanto para grupos de segurança e distribuição.
- Aninhamento de grupos
- Conversão de grupos: Permite a conversão entre grupos de segurança e de distribuição
- Identificadores de segurança (SID)

Se uma floresta tiver o nível funcional do Windows 2000, esses recursos estarão disponíveis e se forem criados na rede outros domínios, os recursos mais avançados não estarão disponíveis nesses domínios, mesmo sendo versões mais recentes.

2.5.2 Windows 2003 Nativo

O AD teve uma revisão para estender as funcionalidades e melhorar a administração no Windows Server 2003, quando ocorreu a sua maior mudança. Segundo a Microsoft (WINDOWS SERVER, 2014), além das funcionalidade anteriores, foram adicionadas outras, como:

- Uma ferramenta de gerenciamento de domínio (Netdom.exe), que permite renomear controladores de domínio.
- Atualizações de data e hora, no início de sessão: O atributo lastLogonTimestamp é atualizado com o último horário do logon de um cliente. Esse atributo é replicado no domínio.
- A capacidade de definir o atributo userPassword como a senha efetiva em inetOrgPerson e objetos de usuário
- A capacidade de redirecionar contêineres de Usuários e Máquinas: Por padrão, dois contêineres conhecidos são fornecidos para computadores habitação e contas de usuário, ou seja, cn = Computadores, <domínio raiz> e cn = Usuários, < domínio raiz > permitindo a definição de um novo local para essas contas.
- Gerenciador de autorização que armazena as políticas de autorização no AD
- A delegação restrita: Torna possível que aplicativos tirem proveito da delegação segura de credenciais de usuário por meio da autenticação baseada

em Kerberos. Também permite restringir a delegação apenas para serviços de destino específicos.

- Autenticação seletiva: Permite especificar os usuários e grupos em uma floresta confiável que terá permissão para autenticar servidores de recursos em uma floresta confiante.

Os domínios criados em uma floresta no nível funcional de domínio do Windows Server 2003 vão oferecer todos os recursos do Windows 2000, além dos seguintes recursos adicionais:

- Replicação de valor vinculado, que melhora a replicação das alterações em associações de grupo.
- Geração mais eficiente de topologias de replicação complexas pelo *Knowledge Consistency Checker* (KCC, verificador da consistência dos conhecimentos)
- Confiança a nível de floresta, permitindo compartilhamento fácil de organizações
- Recursos internos em múltiplas florestas.

2.5.3 Windows 2008 Nativo

Melhorias adicionais foram incluídas com o Windows Server 2008. Além das funções já existentes no Windows Server 2003, foram adicionadas:

- DFS (*Distributed File System*) com apoio para replicação de volume do SYSVOL (*Windows Server System Volume*);
- Para os domínios baseados em *namespaces* do tipo DFS, incluiu-se um suporte para enumeração baseada em acesso, garantindo maior escalabilidade. (WINDOWS SERVER, 2008);
- Criptografia AES 128 e AES 256 na autenticação Kerberos;
- *Logon* Interativo: Mostra a hora do último *logon* bem sucedido e do número de tentativas falhas;
- Regras refinadas de senhas: Permite regras sejam determinadas para usuários e grupos de segurança, dentro de um domínio (WINDOWS SERVER, 2009).

2.5.4 Windows 2008 R2

Esta versão de Windows 2008, além de possuir todos os recursos nativos, possui uma garantia extra do mecanismo de autenticação, que funciona agrupando as informações sobre o tipo do método de *logon*, permitindo que as informações possam ser extraídas sempre que um usuário tentar acessar quaisquer aplicativos que reconheçam a autorização com base no método de *logon* de um usuário (WINDOWS SERVER, 2012).

Florestas com esse nível de operação oferecerão todos os recursos da opção anterior e mais o recurso de lixeira, que quando for ativado, fornece a capacidade de restaurar objetos excluídos em sua totalidade, enquanto os serviços do AD estiverem em execução.

2.5.5 Windows 2012 Nativo

Esta versão possui todos os recursos anteriores, mas acrescenta melhorias na autenticação Kerberos, como a compressão da base de dados. (WINDOWS SERVER, 2012)

2.5.6 Windows 2012 R2

Esta versão criou a política de autenticação em silos na floresta, permitindo criar uma relação entre usuário, serviços e computador, para fins de classificação das contas ou isolamento da autenticação. (WINDOWS SERVER, 2014)

2.5.7 As Diferenças De Versões, Níveis, E Mudanças De Nível

Após a instalação, as florestas ou domínios criados podem ter seus níveis funcionais aumentados para versões mais novas, mas, após o aumento, eles não podem mais ser diminuídos, com exceção do Windows Server 2008 R2 para Windows Server 2008.

Conforme a Microsoft (ASK THE DIRECTORY SERVICES TEAM, 2011), uma mudança mal pensada de nível funcional, de uma floresta ou mesmo de um domínio, pode fazer máquinas antigas da rede envolvidas em AD pararem de funcionar de forma irreversível.

Neste caso, é necessária a restauração de backup prévio para que o funcionamento retorne ao normal. Se não houver backup, é necessária a desinstalação e reimplantação a partir do zero de todas as configurações AD no Servidor.

O Windows XP ainda detém quase 20% do mercado mundial de desktops (TREND MICRO, 2015), uma taxa que é ainda mais elevada dentro das empresas do Brasil.

A poucos dias, o Google estendeu o suporte ao Chrome para Windows XP (OLHAR DIGITAL, 2015), portanto, considerando um parque de máquinas comum no Brasil atual, que executa majoritariamente Windows XP e Windows 7, ao se constituir um AD, pode ser interessante ficar somente com as funcionalidades do Windows Server 2003, que são bastante similares as do Windows 2008 e mais próximos em compatibilidade.

A Microsoft cortou oficialmente o suporte a clientes Windows XP no Windows Server 2012. (TECHNET MICROSOFT LIBRARY WINDOWS SERVER 2012)

Administradores de Windows Server 2012 reportaram a Microsoft (SOCIAL TECHNET FORUM, 2013) e sem respostas funcionais, que o Windows XP não consegue autenticar em domínios do Windows Server 2012. Mesmo quando este tenta operar no nível funcional de Windows Server 2003, devido a problemas nos protocolos de comunicação em TLS, e mesmo tentando fazer alterações no registro, o problema não pode ser resolvido.

Por isso, a escolha do nível funcional de floresta da instalação neste trabalho será do Windows Server 2003, e para evitar possíveis problemas e choques de compatibilidade, também foi escolhido o nível funcional Windows Server 2003.

3 O SAMBA

Samba é uma re-implementação livre do protocolo de rede SMB/CIFS, e foi originalmente desenvolvido por Andrew Tridgell.

Seu nome vem de SMB (Server Message Block), o nome do protocolo padrão usado pelo sistema de arquivos de rede Microsoft Windows.

O Samba fornece serviços de arquivo e impressão para vários clientes Windows e pode integrar-se com um domínio do Windows Server, ou como um controlador de domínio (DC) ou como um membro do domínio.

O Samba é distribuído segundo a licença GPLv3, vem junto em quase todas as distribuições de Linux e é geralmente incluída como um serviço básico de sistema, rodando na maioria dos sistemas Unix, como Solaris, AIX, BSD, Linux e o OS X da Apple.

Tridgell explica como é o seu desenvolvimento:

> "Imagine que você queria aprender francês, e não havia livros, cursos, etc... disponíveis para te ensinar. Você pode optar por aprender, voando para a França e se sentando em um café francês, e apenas escutar as conversas ao seu redor. Você toma notas copiosas sobre o que os clientes dizem para o garçom e quais comidas chegam. Dessa forma, você finalmente aprende as palavras para pão, café etc.. Usamos a mesma técnica para aprender sobre as adições de protocolo que Microsoft faz." (How Samba was written, 2003)

3.1 SAMBA 1 e 2

As versões até 1.9 foram seguidas de forma muito rápida, com esta última sendo lançada em janeiro de 1995.

Tridgell considera que a adoção do CVS em maio 1996 marcou o nascimento da equipe do Samba. O principal foco da equipe era na simulação do protocolo NETBIOS.

A versão 2 foi lançada em janeiro de 1999, e a versão 2.2 em Abril de 2001.

3.2 SAMBA 3

Segundo Bartlett (2005, p. 57), o SAMBA 3.0 possuía a capacidade de entrar como usuário em uma rede operando com Active Directory. Esta funcionalidade foi o início dos trabalhos com Active Directory, que vieram a tona de forma mais convincente no SAMBA 4.

3.3 SAMBA 4

Em sua versão 4, o SAMBA suporta domínios do Windows e Active Directory, recursos que foram explorados neste trabalho, principalmente a possibilidade da utilização de ferramentas gráficas Windows para o controle do AD existente no SAMBA.

4 METODOLOGIA DO TRABALHO

O trabalho foi conduzido no intuito da construção do conhecimento e na sua posterior difusão, sob a forma de tutorial. As atuais tecnologias de virtualização são de grande proveito e foram utilizadas para acelerar os processos. A virtualização oferece praticidade de gerenciamento e permite testes não destrutivos sobre o software da máquina local, isto é, não é necessário formatar e perder temporariamente uma máquina produtiva.

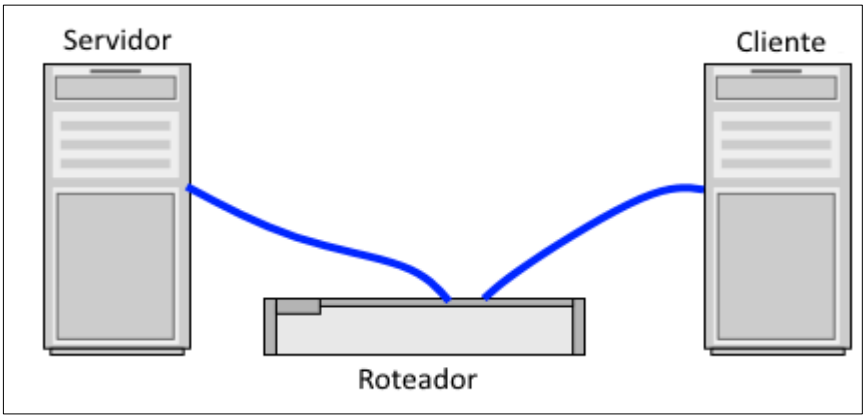
Nas métricas, se buscou sempre avaliações idôneas, já que o hardware utilizado para testar as máquinas virtuais foi essencialmente o mesmo, por tanto, a informação mais importante é a porcentagem de variação entre o desempenho de ambos servidores.

A todo momento e em todas as fases de ação, sempre serão observadas e respeitadas todas as questões legais envolvidas, de forma que nenhum ato implique em qualquer tipo de ilícito.

4.1 ESCOPO DO TESTE

O teste realizado foi do tipo *stress*, cujo objetivo é avaliar o desempenho de instalações simplistas de Active Directory no Windows Server e no SAMBA, comparando o desempenho de ambas, que a priori, deverá ser revelador quanto ao desempenho dos mesmos, já que pouco ou nenhum ajuste de afinamento foi feito em ambos, já que ajustes de afinamento extremamente complexos poderiam modificar de forma decisiva o comportamento dos sistemas, os que não é desejado para um teste padrão.

Figura 3 - Exemplo de topologia de rede proposta



Fonte: Do autor

Foi implementada uma rede Windows e o controle do Active Directory foi feito com um servidor Windows Server 2008, e depois o controle foi substituído por um servidor Debian rodando SAMBA, utilizando uma topologia de rede cliente-servidor como pode ser vista na Figura 3.

Todas as máquinas foram virtuais e estavam sendo executandas no VirtualBox, que e hipervisores *open-source* e gratuito.

A máquina com Windows Server 2008 R2 usada neste teste possui apenas um processador, simulando a licença padrão simples do Windows Server (Foundation), ao passo que a máquina Debian tinha dois processadores.

Considerando que o SAMBA faz uma emulação das funções do Windows Server, desde o princípio fica implícito que seu desempenho será inferior a um Windows Server, que é a plataforma nativa.

A grande questão é "quanto" exatamente seria essa diferença.

4.2 ESTRATÉGIAS E FERRAMENTAS DE TESTE

Existem empresas que vendem software para efetuar a medição de desempenho de um Active Directory, e esta venda implica também em serviços de consultoria (X9000.COM, 2014), o que não é desejado neste caso.

A própria Microsoft disponibiliza gratuitamente um software de avaliação de desempenho, o Active Directory Performance Testing Tool (MICROSOFT DOWNLOAD CENTER, 2012), que se trata de uma ferramenta de geração de carga do tipo Active Directory, que simula as operações do cliente para fazer os testes de tempo envolvido nas operações.

Neste tipo de teste, o cliente Windows irá efetuar o teste de stress pela rede sobre o servidor de Active Directory, que pode ser tanto o Windows Server quanto o SAMBA.

A ferramenta utilizada será a da própria Microsoft para testes de performance em AD, pois mesmo se o servidor for um Linux rodando SAMBA, o cliente Windows vai enxergar um Windows Server, já que as ferramentas do SAMBA incluem até um registro virtual.

O Active Directory Performance Test Tool (ADTest) é baixado diretamente do site da Microsoft, e possui tanto a versão 32bits como a versão 64 bits (Active Directory Performance Testing Tool, 2012).

4.3 CALCULO DAS MÉTRICAS

O ADTest efetua testes, exibindo na tela com regularidade:

- O número de loops de testes executados;
- O número instruções que redundaram em falhas;
- A velocidade em operações por segundo que o teste está rodando;
- O tempo de Kernel;
- O tempo de usuário;

A informação mais importante para a métrica do desempenho, sem dúvida, é o número de operações por segundo (Op/Sec) na qual o teste está se desenrolando.

Como se trata de várias amostragens, o ideal é fazer a média das amostragens obtidas, registrando o desvio padrão dessas amostragens para saber qual é a estabilidade destas medições.

A média, representada na fórmula abaixo pela letra grega *Chi* acentuada com *Macron*, é a somatória de todas as amostragens, dividido pelo número das amostragens.

$$\overline{\chi} = \frac{(\sum \chi)}{N}$$

O desvio padrão, representado na fórmula abaixo pela letra grega *Sigma* minúsculo, é a raiz quadrada da variância, que por sua vez, é a média da soma dos quadrados das variações de cada elemento em relação a média.

$$\sigma = \sqrt{\sum [(X - \mu)^2]}$$

4.4 REQUISITOS A SEREM TESTADOS

No arquivo com as diretivas de teste que é distribuído pela Microsoft, há diversos tipos de teste, inclusive o usuário pode criar seus próprios testes, mas optou-se usar somente os testes já existentes, cujos mais interessantes foram:

- Teste de autenticação no Kerberos: São as autenticações com AD propriamente dito, e impactará no tempo de entrada do usuário no domínio

- Teste de autenticação NT Logon: O tempo desta autenticação sempre será menor do que a anterior, por que é incompleta, e poderia ser dito que se trata da autenticação feita em compartilhamentos PDC. (Domain Controller Roles, 2014)

- Teste de pesquisa de atributos: Todas as vezes que uma máquina está na rede, existe alta possibilidade de ocorrer a busca de recursos. Por tanto, foi escolhido o teste mais estressante, o da busca de 10 atributos simultâneos.

- Teste de atualização de atributos: Este verificará a velocidade que eventuais mudanças ocorrem dentro de um domínio AD. Foi escolhido teste mais estressante, a atualização de 10 atributos simultâneos.

- Teste de criação de usuários: Os testes serão feitos para uma massa de usuários, sendo repetidos várias vezes. Para que todos esses testes possam ser feitos, é necessário uma grande massa de usuários que deverão ser criados em algum momento, e devem estar no banco de dados do AD.

- Teste de criação de grupos: Os usuários deverão estar dentro de múltiplos grupos para simular a complexidade de uma instalação real.
-
- Teste da adição dos usuários nos grupos: Complementa o teste de criação dos grupos.

- Teste de criação de raízes: Se todos os usuários estiverem em uma só estrutura, isso poderia tornar o processo mais rápido. Então devem ser criadas dezenas de unidades organizacionais, com pelo menos 3 níveis, para tornar o teste mais realista, simulando a complexidade de um sistema cheio.

Haverá 8 testes no total, que vão desde criação de estruturas básicas de usuários, até testes de simulação de carga.

4.5 QUESTÕES LEGAIS, LICENSAS E OBTENÇÃO DE SOFTWARES

Os sistemas operacionais foram baixados todos da internet.

O sistemas Windows utilizados foram versões *trial*, obtidas diretamente do website da empresa Microsoft, e a versão de Linux Debian foi baixada diretamente do repositório oficial.

Para o servidor Windows, será utilizado uma versão *trial* 180 dias do Windows Server 2008 R2 pode ser obtido via download no site da Microsoft (MICROSOFT DOWNLOAD CENTER, 2015).

A versão 2003 do Windows Server não terá mais suporte da Microsoft em breve, e versões *trial* não podem mais serem obtidas. (MICROSOFT CLUD PLATAFORM, 2015)

Windows Server 2008 R2 com a licença *trial* de 180 dias, que é disponibilizado no site da Microsoft. (MICROSOFT.COM, Windows Server Evaluations, 2008), sendo que os 180 dias dados é o tempo equivalente a 1 semestre de curso superior, tempo mais do que suficiente para fazer as configurações e os testes.

Como clientes, foi usado o sistema Windows 8 Enterprise, que da mesma forma que os Windows 8.1 Enterprise, Windows 10 Enterprise, todos contam com uma licença *trial* de 90 dias, e estão disponíveis para download no site da Microsoft. (MICROSOFT.COM, Windows Evaluations, 2014).

O *download* de todas as versões *trial*, estão condicionadas mediante a criação de uma conta gratuita de e-mail da Microsoft (SIGNUP LIVE, 2014).

Dos sistemas Unix que serão utilizados, se buscará sistemas gratuitos e *open-source*, havendo muitas distribuições de Linux.

Para evitar quaisquer possíveis entraves legais, optaremos pela distribuição de Linux Debian, por ser uma distribuição 100% software livre (DEBIAN.ORG, 2004).

O VirtualBox também é *open-source*, e a ferramenta de teste ADTest da Microsoft é gratuita.

5 TESTE DE DESEMPENHO SIMPLES DE ACTIVE DIRECTORY ENTRE MÁQUINAS WINDOWS

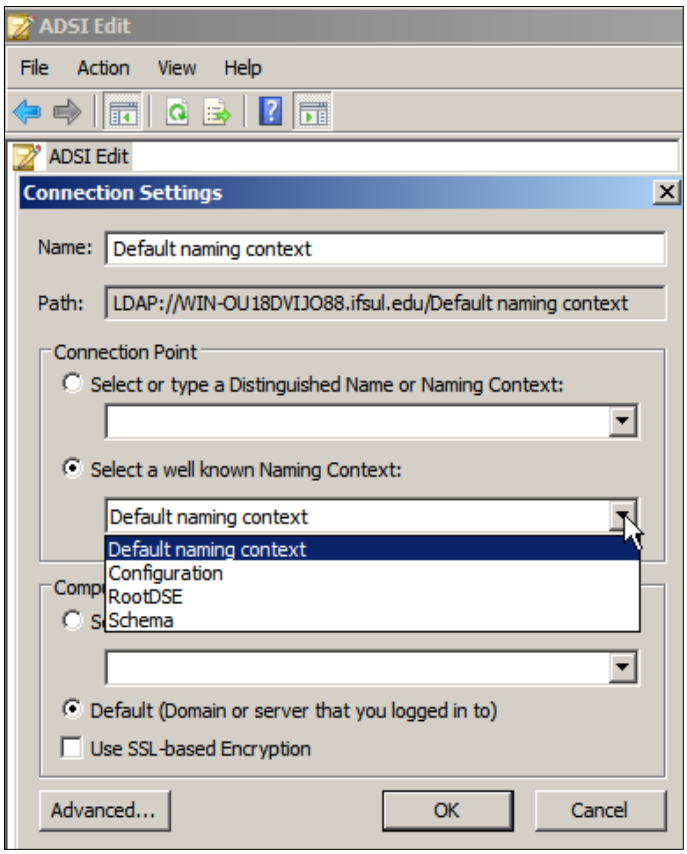
O desenvolvimento foi feito pela parte mais simples, que são as configurações de AD entre máquinas Windows, passando para a criação do servidor Linux com SAMBA, e por fim, efetuando o teste em ambos os sistemas implementados.

Ambas as implementações simples de AD constam nos dois apêndices A e B. Em posse desses servidores com instalação simples de AD, foi feito o teste sobre ambos.

5.1 PREPARAÇÃO DO WINDOWS SERVER

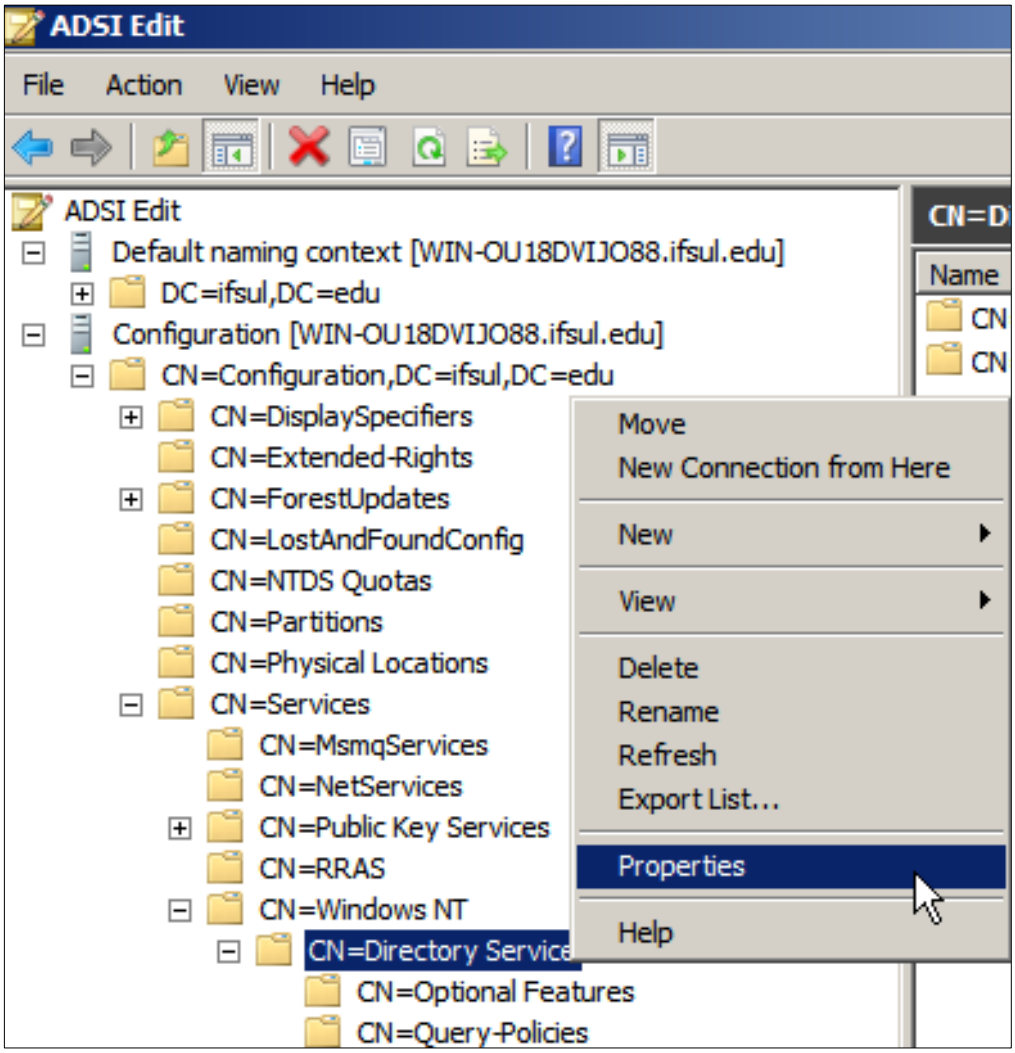
Passo 1: Modificar dSHeuristics, e isso é feito executando adsiedit.msc e se conectando no domínio local, clicando com o botão direito sobre a raiz, conforme demostrado na Figura 4.

Figura 4: Janela de conexão com domínios



Após conectar nas configurações do domínio, o usuário deve ir para a subpasta CN=Configuration/CN=Services/CN=Windows NT/CN=Directory Service, e clicar com o botão direito sobre ela para exibir as propriedades.

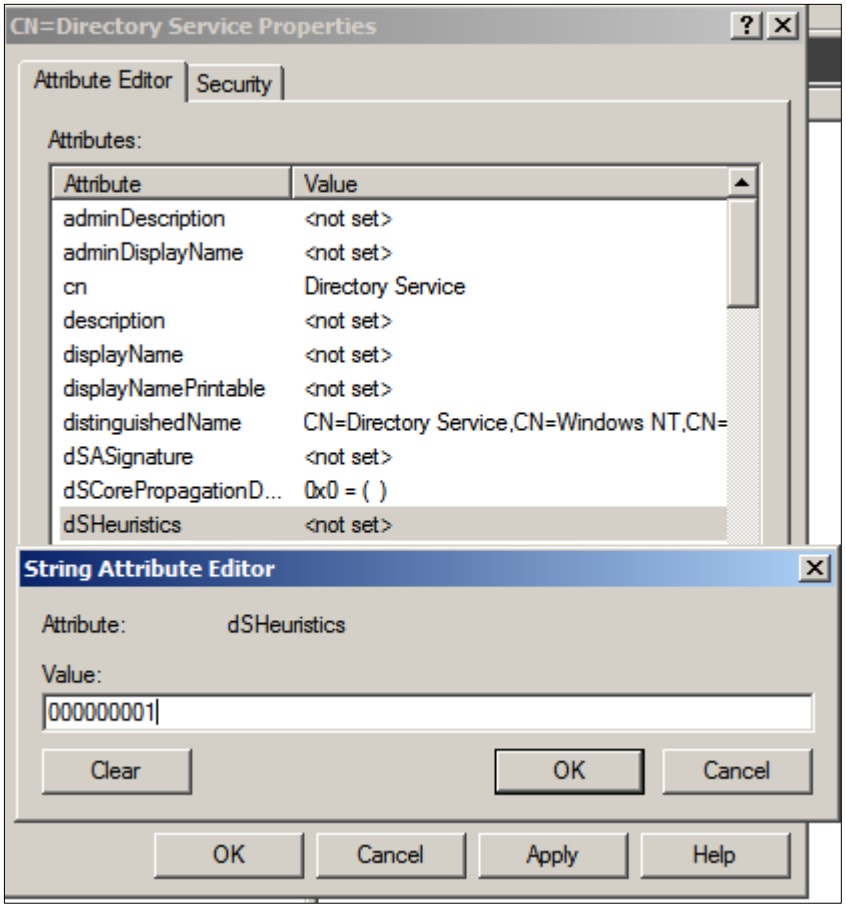
Figura 5: Local da propriedade que será modificada



Dentro das propriedades, modificar o atributo dSHeuristics para 1, dentro de uma cadeia de 9 bits, isto é, 000000001, conforme demonstrados nas figuras 5 e 6.

Quando o atributo dSHeuristics é habilitado para 1, isso serve como flag para ativar o recurso ANR (Ambiguous Name Resolution), o que na prática, tornará as pesquisas LDAP anônimas para aumentar a velocidade das mesmas (Suporte Microsoft Windows Server 2003 Operações LDAP anônimas, 2007).

Figura 6: Modificando o atributo dSHeuristics



Passo 2: Aumentar o número de conexões permitidas para um usuário, modificando o MaxUserPort que controla o número máximo de portas usadas, quando um aplicativo solicita abertura de portas para um usuário do sistema, usando o comando.

set ipv4 dynamicport TCP start = 1025 num = 64510

Não será necessário modificar TcpWindowSize, pois o atributo é ignorado em Windows Servers superiores a versão 2003 (Microsoft Technet Windows Server 2000).

Passo3: Criar um usuário de teste. Neste caso, o usuário criado se chama “testar”, com o password “Senha-12345”, o que é feito no menu dos usuários e computadores do Active Directory, que está nas ferramentas administrativas do Windows Server.

A criação e suas opções são demonstradas nas figuras 7, 8 e 9.

Figura 7: Criando usuário de teste

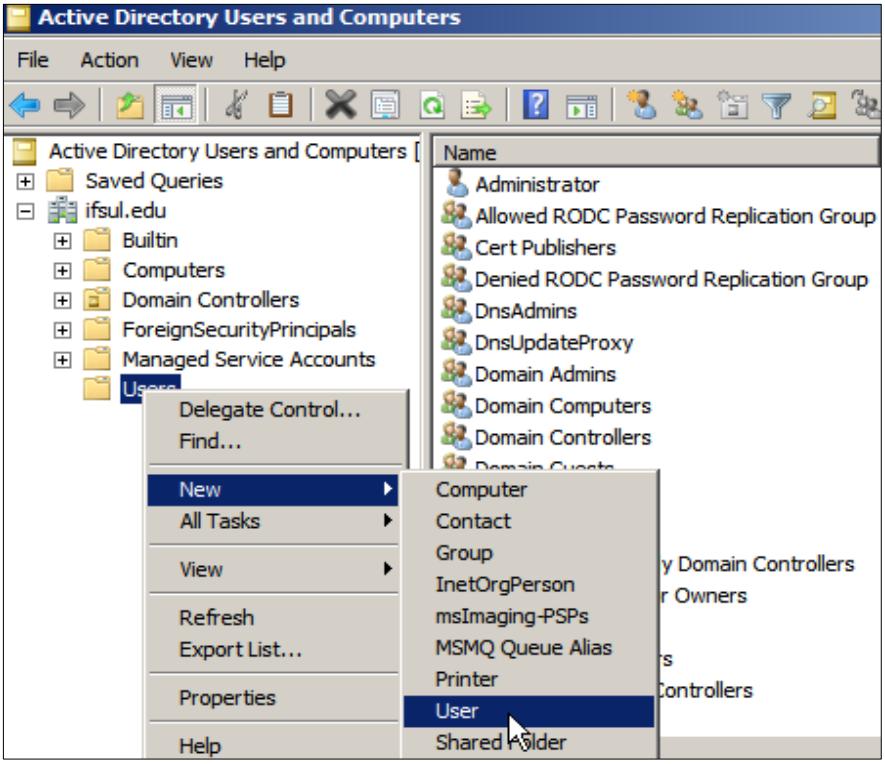


Figura 8: Cadastrando novo usuário

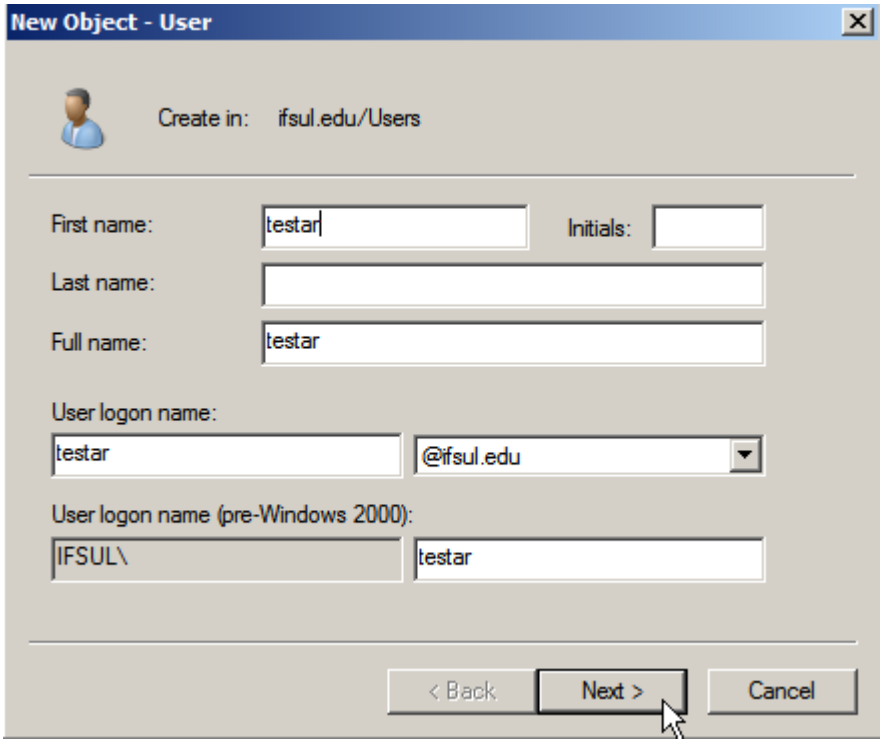
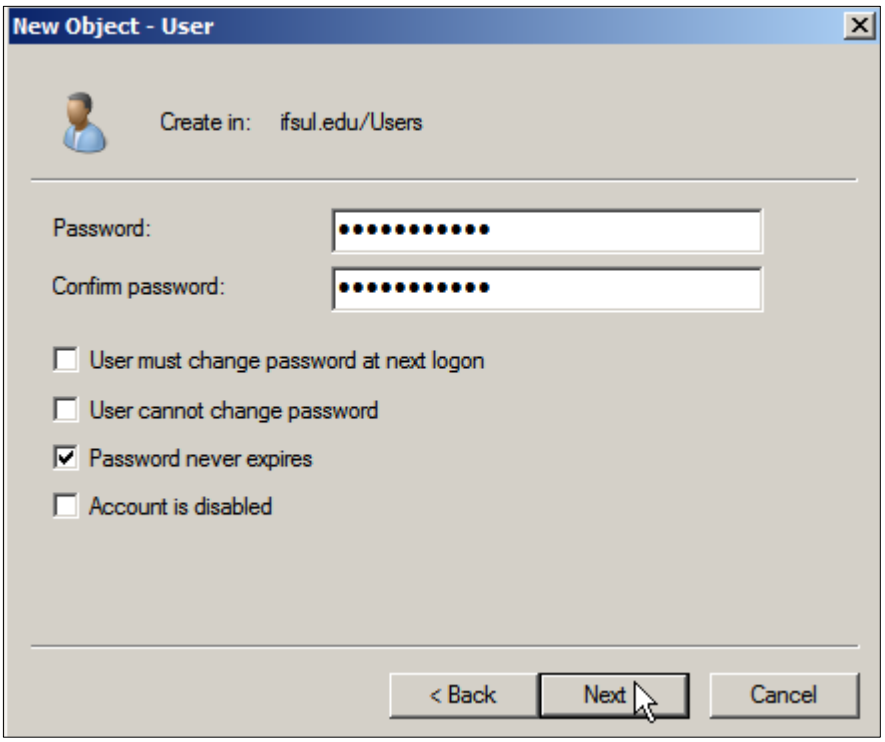


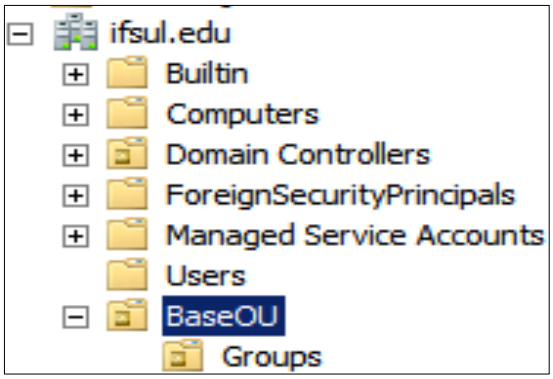
Figura 9: Confirmando senha sem expiração



5.1.1 Preparação Do Ambiente

Na raiz do domínio principal, criaremos uma unidade organizacional chamada "BaseOU", que será a base dos testes, e dentro desta, criaremos outra uma unidade organizacional chamada "Groups", bastando clicar com o botão direito sobre os alvos e escolher a opção "novo", e "Organizacional Unit", como demonstrado na Figura 10.

Figura 10: Domínio com a OU de teste criada



Também deve ser dado permissão para que o usuário de teste possa escrever no disco.

5.2 PREPARAÇÃO DO SERVIDOR SAMBA NO DEBIAN

Basta criar um usuário qualquer, e se o usuário não tiver permissão para efetuar operações, basta adicionar ele no grupo “Domain Administrators” que ele obterá por herança as permissões

samba-tool user add teste

samba-tool group add “Domain Administrators” teste

Para agilizar as operações, a estrutura de Active Directory do SAMBA foi manipulado usando ferramentas instaladas no cliente Windows (Remote Server Administration Tools for Windows 8), desta maneira, o servidor SAMBA permaneceu sem interface gráfica.

O kit traz aplicações que existem por padrão no Windows Server, e a interface gráfica das aplicações é idêntica.

As operações que devem ser feitas sobre a estrutura AD do SAMBA são as mesmas a serem efetuadas nas estruturas AD do Windows Server 2008, como apresentado nas figuras anteriores da preparação do Windows Server.

As configurações de portas do Debian foram modificadas alterando os seguintes parâmetros no arquivo sysctl.conf:

net.core.rmem_default = 262144

net.core.rmem_max = 33554432

net.core.wmem_default = 262144

net.core.wmem_max = 33554432

net.core.optmem_max = 40960

net.core.netdev_max_backlog = 5000

net.ipv4.ip_local_port_range = 2048 65000

net.ipv4.tcp_no_metrics_save = 1

net.ipv4.tcp_rmem = 4096 16777216 33554432

net.ipv4.tcp_wmem = 4096 16777216 33554432

5.3 PORTAS DO CLIENTE WINDOWS

Da mesma maneira que a limitação de portas precisou ser aumentada no Windows Server. O comando precisa ser feito como administrador, e isso pode ser feito invocando taskmanager por meio das teclas de atalho ctrl+shift+esc e ir no menu “arquivo” e depois “executar nova tarefa”, e executar o “cmd” marcando a opção “Criar esta tarefa com privilégios administrativos”.

Na nova janela cmd, dar o comando:

netsh int ipv4 set dynamicport tcp start=1025 num=64510

Se o comando funcionou, a resposta no terminal será “OK.”

5.4 AS DIRETIVAS DE TESTE

A aplicação ADTest possui sua própria especificação de diretivas, cujo principal exemplo pode ser visto num documento publicado pela Microsoft, fazendo a comparação entre Windows Server 2003 SP1 64 bits e Windows Server 2003 SP1 32 bits (Active Directory Performance for 64-bit Versions of Windows Server 2003)

A aplicação deve ser baixada do site da Microsoft e instalada na máquina local, e as diretivas utilizadas neste teste foram salvas no arquivo “teste.ats” e constam no Apêndice C desde documento, e foi modificado conforme os casos de teste criados.

Desabilitar o UAC (Controle de Conta de Usuário) do cliente Windows pode agilizar as operações de teste, já que estamos trabalhando com várias contas, mas não é recomendado a máquina cliente está em um ambiente com múltiplos usuários.

Como o usuário criado “testar” opera normalmente como um outro usuário na máquina, para agilizar as operações de teste, o ideal é o administrador compartilhar o acesso do HD para este usuário. Isso é feito se autenticando como o usuário “testar”, e pedindo para modificar as diretivas de segurança do HD, e inserindo usuário e senha do Administrator do Windows Server para modificar as permissões.

As diretivas de teste usadas no teste foi uma pequena variação simplificada das diretivas usadas pela própria Microsoft em seu documento.

5.5 EFETUANDO OS TESTES

A máquina cliente que efetuará os testes deve se juntar ao domínio que será testado. No caso deste teste, como a máquina com Windows 8 é a mesma utilizada para a implementação anterior do AD, já havia um usuário cadastrado, o nome da maquina teve de ser alterado.

Em cada teste, deve-se apontar para o controlador de rede como sendo o DNS da conexão, pois ele quem fará a resolução dos nomes.

O principal valor disponibilizado pelo aplicativo ADTest é o desempenho em operações por segundo (Op/Sec).

Os 3 primeiros testes efetuam a criação de estruturas preparatórias para os 5 testes mais decisivos.

5.5.1 Teste De Criação De Unidades Organizacionais

Cria 100 estruturas OU aninhadas de 3 níveis dentro de BaseOU.

Esse teste efetua 3 operações sobre a raiz do Active Directory:

- Cria uma OU com nome ou??_division[1]

- Dentro da nova ou??_division, cria uma OU com nome ou??_unit

- Dentro da nova ou??_ unit, cria uma OU com nome ou??_team

Sendo que o os dois caracteres representados com interrogação são numéricos e variam de 00 a 99.

Tabela 1: Resultado do primeiro teste

Servidor	**Velocidade média (Op/Sec)**
Windows Server 2008	49,63
Debian com SAMBA	36,17

[1] Em todos os casos, os dois caracteres representados com interrogação são numéricos de dois dígitos, e variam de 00 a 99.

Neste pequeno teste, o SAMBA foi 27% mais lento, mas este teste é muito pequeno para quaisquer conclusões.

5.5.2 Teste De Criação De Grupos

Cria 100 grupos de segurança global dentro da OU Groups que foi criado previamente.

Esses grupos terão permissão total por que serão usados nos próximos testes, e seguirão o nomes GrpAcc_0000??, sendo os dois últimos caracteres numéricos variando entre 00 e 99.

Tabela 2: Resultado do segundo teste

Servidor	**Velocidade média (Op/Sec)**
Windows Server 2008	49,63
Debian com SAMBA	45,6

A diferença entre os dois sistemas foi de 8%, pode se dizer que o desempenho foi quase igual, embora esse teste seja muito pequeno.

5.5.3 Teste De Criação De Usuários

Cria 10.000 usuários, 100 dentro de cada uma das 100 estruturas criadas durante o teste de criação das OUs.

Os usuários criados seguirão o nome u??_0000??, sendo os dois primeiros caracteres relativos a OU na qual o usuário faz parte (00 a 99), e os dois últimos caracteres variam de 00 a 99.

O Windows Server apresentou uma média de 48,03 Op/Sec, com um desvio padrão principal de 5,11 Op/Sec entre as medições. O desempenho foi baixo apenas na medição do início do teste (18,78 Op/Sec), mas as próximas medições apresentaram uma boa estabilidade até o final do teste, apresentado um desvio padrão de 2,33 Op/Sec até o final.

O Debian com SAMBA apresentou um desempenho médio de 14,48 Op/Sec, com um desvio padrão principal de 4,12 Op/Sec entre as medições. O início teve bom desempenho (25,14 Op/Sec) mas o desempenho foi caindo até chegar em 9,4 Op/Sec.

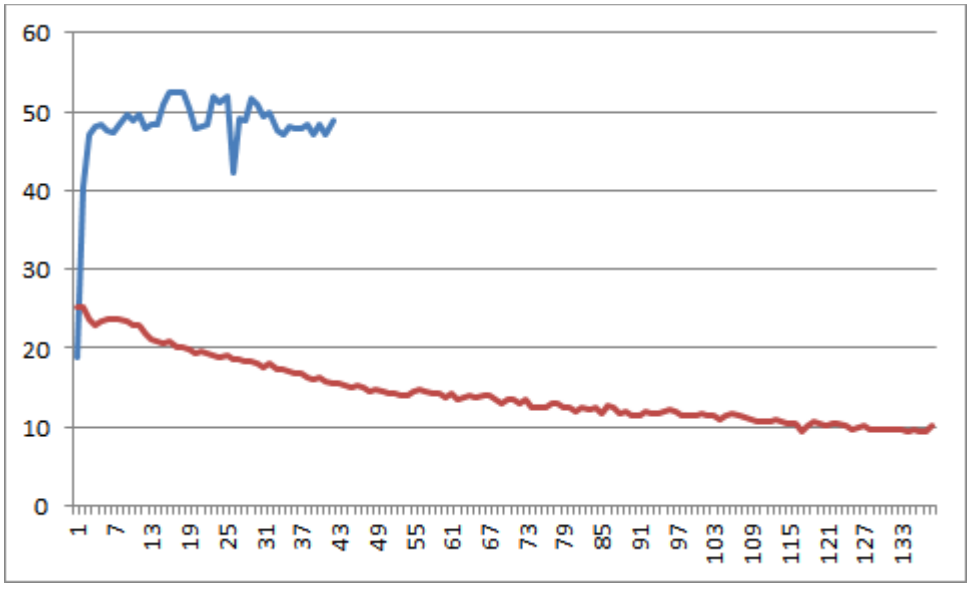
Ao se verificar os motivos da queda de desempenho do SAMBA, foi verificada que se trata por problemas de I/O, com o software chegando a pedir 130MB/s da máquina física.

Neste teste, o Windows Server apresentou 100% de uso do CPU e um uso de disco da ordem de 3MB/s. O Linux apresentou a velocidade máxima de uso do disco, com 20MB/s (o limite da máquina física) e um processamento baixo de 8%.

Essa carga maior no HD terminou por se tornar em um gargalo, que deixou o desempenho do SAMBA muito abaixo do Windows Server.

Portanto, na criação dos primeiros 170 usuários o SAMBA foi 34% mais rápido que o Windows Server (25,14 Op/Sec vs 18,78 Op/Sec), mas se apresentou 3,3 vezes mais lento até o final do teste (48,03 Op/Sec vs 14,48 Op/Sec), conforme gráfico apresentado na Figura 11.

Figura 11: Op/Sec por amostra temporal - Windows em azul e Debian em vermelho



Fonte: Do Autor

Esse problema pode estar vinculado a forma de uso da partição pelo SAMBA, já que é necessário adicionar argumentos de segurança no fstab. De qualquer maneira, não foi testado o que aconteceria com o Windows Server se ocorresse uma súbita falta de energia durante esse teste.

Em situações do cotidiano, como a criação de um ou poucos usuários em um servidor em um ambiente de produção, poderia ser dito que ambos são equivalentes.

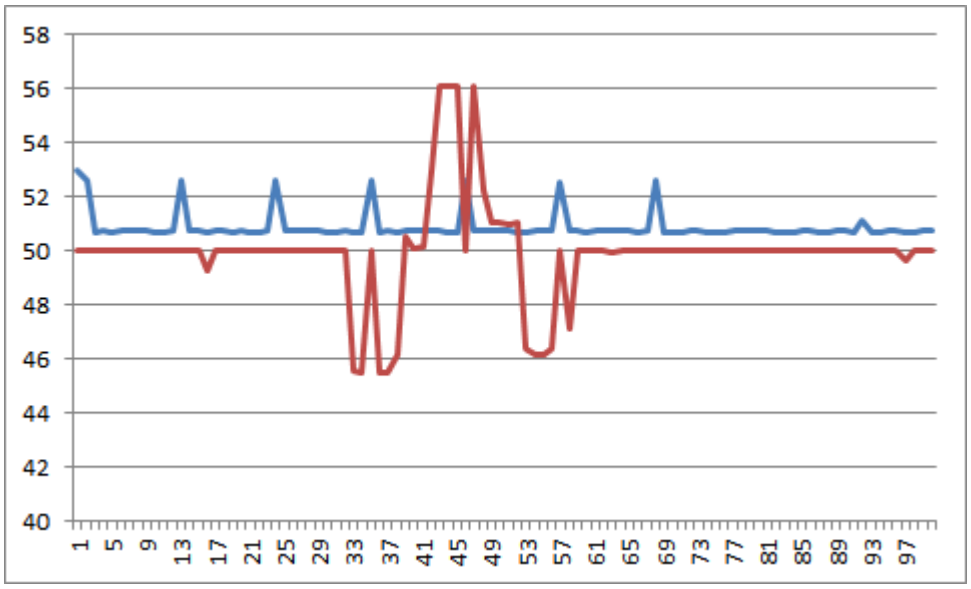
5.5.4 Teste De Manipulação De Grupos

Adiciona os 10000 usuários criados no teste anterior, de 100 em 100, em cada um dos 100 grupos globais criados no teste anterior da criação dos usuários.

Tabela 3: Resultado do quarto teste

Sistema	Velocidade média (Op/Sec)	Desvio padrão
Windows Server 2008	50,88	0,51
Debian com SAMBA	49,93	1,81

Figura 12: Op/Sec em amostras temporais - Windows em azul e Debian em vermelho



Do Autor

Como mostrado na Figura 12, ambos cumpriram a mesma tarefa no mesmo tempo, em uma velocidade praticamente igual.

5.5.5 Teste De Logon NT

Efetua o logon do tipo Windows NT em 100 usuários, e repete a operação por uma quantidade indefinida de vezes.

Neste teste, o Windows Server foi quase 10 vezes mais rápido (9,44x), o que não é surpresa, pois é uma plataforma nativa.

Tabela 4: Resultado do quinto teste

Sistema	**Velocidade média (Op/Sec)**
Windows Server 2008	1369
Debian com SAMBA	144,87

5.5.6 Teste De Atualização De Atributos

Atualiza 10 atributos de 100 usuários, repetindo a operação por uma quantidade indefinida de vezes.

Tabela 5: Resultado do sexto teste

Sistema	**Velocidade média (Op/Sec)**	**Desvio padrão**	**Estabilidade (σ/x̄)**
Windows Server 2008	2337,3	245,7	10,5%
Debian com SAMBA	153,05	5,26	3,4%

O Debian com SAMBA foi quase três vezes mais estável do que o Windows Server 2008, mas o Windows Server 2008 foi mais de 15 vezes mais rápido em desempenho.

5.5.7 Teste De Pesquisa De Atributos

Faz uma pesquisa 100 vezes por 10 atributos de usuários, e repete a operação por uma quantidade indefinida de vezes.

Tabela 6: Resultado do sétimo teste

Sistema	Velocidade média (Op/Sec)	Desvio padrão
Windows Server 2008	9162,2	103,61
Debian com SAMBA	1313,5	45,9

O Windows Server se saiu quase 7 vezes mais rápido neste teste.

5.5.8 Teste De Logon Kerberos

Efetua o logon com Kerberos em 100 usuários, e repete a operação por uma quantidade indefinida de vezes.

Tabela 7: Resultado do oitavo teste

Sistema	Velocidade média (Op/Sec)	Desvio Padrão
Windows Server 2008	47,24	0,95
Debian com SAMBA	45,06	1,3

O desempenho dentro das margens de desvio padrão ficou em 0,15% de distância entre ambos (46,36 vs 46,29), e pode ser afirmado que o desempenho de ambos foi praticamente igual neste teste.

5.6 AVALIAÇÃO DOS RESULTADOS

Em algumas atividades o Windows Server se saiu um desempenho muito melhor, 7, 10 ou até 15 vezes mais, dando a ideia de que se tratam de atividades nativas de fato, e que o SAMBA só consegue atingir as tais por meio de emulação, sendo mais mais lento.

Algumas dessas atividades dependem de um grande tráfego de rede, as vezes na casa de 65Mbps, por tanto, em uma situação de rede real, com a presença de um ou dois switches entre servidor e cliente, as diferenças entre Windows e Linux tendem a cair significativamente.

Se a máquina Debian possuísse 4 processadores, boa parte dos resultados do SAMBA seriam melhores, pois dependem de processamento. Neste aspectos, o Linux tem uma grande vantagem – Os processadores mais poderosos, que geralmente serão utilizados em servidores, possuem uma grande quantidade de núcleos, e como o SAMBA não possui custos de licença, e poderia ser interessante usar o dinheiro das licenças para investir em hardware.

Os detalhes mais interessantes deste teste:

1) Ambos os servidores foram testados pelo mesmo cliente Windows
2) A ferramenta de teste foi desenvolvida pela Microsoft

3) As diretivas de teste foram baseadas no “teste padrão” que é distribuído pela Microsoft, e que compõe o documento onde a empresa compara as versões 32 bits e 64 bits do Windows Server 2003
4) O gerenciamento do AD no SAMBA foi feito remotamente, usando ferramentas gráficas da Microsoft, a partir de um cliente Windows, demonstrando uma compatibilidade impressionante.

6 CONSIDERAÇÕES FINAIS

A curva de aprendizado do SAMBA é bastante lenta, pode se dizer que um usuário que não tem conhecimento no assunto, precise de uns 60 dias de envolvimento (teoria + prática), para conseguir absorver os conhecimentos, resolver erros com uma maior naturalidade, e conseguir resultados de forma mais rápida e eficiente.

Tabela 8: Comparativo Windows Server x Linux SAMBA

	Pontos Positivos	**Pontos Negativos**
Windows Server 2008 R2	Melhor Desempenho Plataforma Nativa	Alto Custo
Debian Jessie + SAMBA 4.2	Gratuito Compatibilidade Superior	Exige conhecimentos em Linux e Windows

Sobre a compatibilidade do SAMBA, vale lembrar que o AD com Windows Server 2012 não funciona para máquinas que operem com o Windows XP, enquanto o SAMBA funcionará com o mesmo.

Neste sentido, pode ser dito que a interoperabilidade oferecida pelo SAMBA é superior as soluções oferecidas pela Microsoft, por que atende sistemas Windows que não possuem mais suporte oficial, além de toda a vasta gama de SOs do tipo Unix, como o OS X da Apple.

É possível rodar aplicações Unix no Windows Server, mas isso pode terminar deixando as operações mais complexas, e é muito mais simples (e barato) usar Linux nativo.

Desde o início deste trabalho, do ano passado até agora, o SAMBA demonstrou grandes evoluções, com a instalação mais simplificada nas distribuições Debian Jessie[2].

Outro recurso impactante é a operação do AD no SAMBA com uso de ferramentas da Microsoft, fazendo com que o administrador visualize praticamente a mesma interface gráfica que veria se estivesse operando um Windows Server, diminuindo a curva de aprendizado necessária para a operação do sistema.

7 TRABALHOS FUTUROS

Tanto o Debian quanto o SAMBA possuem código fonte aberto e configurações abertas, e poderia ser feito diversos ajustes (*tunning*) de configurações que poderiam implicar em diferentes desempenhos. O mesmo se aplicaria ao Windows Server de uma forma mais estrita, pois, embora o mesmo não possua código fonte aberto, possui dezenas de configurações que podem ser modificadas.

Os testes seriam feitos, e os métodos de tunning poderiam ser registrados em um documento que possa ajudar a administradores a melhorar o desempenho de suas redes.

[2] Disponível em https://www.debian.org/releases/stable/ acessado em 18/06/2015

REFERÊNCIAS

ANDREW TRIDGELL. How Samba was written. **SAMBA**, set. 2003. Disponivel em: <https://www.samba.org/ftp/tridge/misc/french_cafe.txt>. Acesso em: 14 jul. 2015.

ASK THE DIRECTORY SERVICES TEAM. What is the Impact of Upgrading the Domain or Forest Functional Level? **Microsoft's official enterprise support blog for AD DS and more**, 2011. Disponivel em: <http://blogs.technet.com/b/askds/archive/2011/06/14/what-is-the-impact-of-upgrading-the-domain-or-forest-functional-level.aspx>. Acesso em: 06 abr. 2015.

BARTLETT, A. **Samba 4 - Active Directory**. Samba.Org. [S.l.], p. 78. 2005.

CHRISTIAS , P. Iptables. **Unix Help**, 1994. Disponivel em: <http://unixhelp.ed.ac.uk/CGI/man-cgi?iptables>. Acesso em: 12 mar. 2015.

COMPUTERWORLD. Empresas sofrem com a falta de profissionais de segurança. **ComputerWorld**, 2014. Disponivel em: <http://computerworld.com.br/carreira/2014/02/07/empresas-sofrem-com-a-falta-de-profissionais-de-seguranca/>. Acesso em: 13 nov. 2014.

DEBIAN.ORG. Contrato Social Debian. **Debian.org**, 2004. Disponivel em: <https://www.debian.org/social_contract>. Acesso em: 18 nov. 2014.

GIBSON, D. et al. **MCSA Microsoft Windows 8.1 Complete Study Guide:** Exams 70-687, 70-688, and 70-689. Indianápolis: John Wiley & Sons, 2015.

HANSELMAN, S. How to sign into Windows 8 or 8.1 without a Microsoft account. **Scott Hanselman**, 2013. Disponivel em: <http://www.hanselman.com/blog/HowToSignIntoWindows8Or81WithoutAMicrosoftAccountMakeALocalUser.aspx>. Acesso em: 01 abr. 2015.

IETF. Reference 1823. **IETF**, 1995. Disponivel em: <https://www.ietf.org/rfc/rfc1823.txt>. Acesso em: 09 set. 2014.

IETF. Reference 2307. **IETF**, 1998. Disponivel em: <https://www.ietf.org/rfc/rfc2307.txt>. Acesso em: 09 set. 2014.

IETF. Reference 3062. **IETF**, 2001. Disponivel em: <https://www.ietf.org/rfc/rfc3062.txt>. Acesso em: 09 set. 2014.

LDC SOLUÇÕES. Active Directory. **LDC Soluções**, 2014. Disponivel em: <http://www.ldc.com.br/produto/33/active-directory>. Acesso em: 09 set. 2014.

MICROSOFT. Active Directory Performance for 64-bit Versions of Windows Server 2003. **Microsoft Download Center**, 2006. Disponivel em: <http://www.microsoft.com/en-us/download/details.aspx?id=4948>. Acesso em: 01 jun. 2015.

MICROSOFT. Suporte Microsoft Windows Server 2003 Operações LDAP anônimas. **Operações LDAP anônimas ao Active Directory estão desativadas nos controladores de domínio do Windows Server 2003**, 2007. Disponivel em: <https://support.microsoft.com/pt-br/kb/326690>. Acesso em: 01 jun. 2015.

MICROSOFT. How Active Directory Searches Work. **TechNet**, 2010. Disponivel em: <http://technet.microsoft.com/en-us/library/cc755809%28v=WS.10%29.aspx>. Acesso em: 17 set 2014.

MICROSOFT. Active Directory Performance Testing Tool. **Download Center**, 2012. Disponivel em: <http://www.microsoft.com/en-us/download/details.aspx?id=15275>. Acesso em: 01 jun. 2015.

MICROSOFT. Remote Server Administration Tools for Windows 8. **Windows Download Center**, 2012. Disponivel em: <https://www.microsoft.com/en-us/download/details.aspx?id=28972>. Acesso em: 06 jun. 2015.

MICROSOFT. Windows Server 2008 R2 and Windows 7 evaluation version. **Microsoft Support Article ID:** 2021579, 2012. Disponivel em: <https://support.microsoft.com/en-us/kb/2021579>. Acesso em: 01 jun. 2015.

MICROSOFT. Domain Controller Roles. **Technet Microsoft Library**, 2014. Disponivel em: <https://technet.microsoft.com/en-us/library/cc786438%28WS.10%29.aspx>. Acesso em: 14 jul. 2015.

MICROSOFT CLUD PLATAFORM. Microsoft Cloud Plataform. **Fim do suporte para o Windows Server 2003**, 2015. Disponivel em: <http://www.microsoft.com/pt-br/server-cloud/products/windows-server-2003/>. Acesso em: 01 mar. 2015.

MICROSOFT COMMUNITY. Microsoft Community. **Questions**, 2012. Disponivel em: <http://answers.microsoft.com/en-us/windows/forum/windows_8-networking/what-is-the-purpose-of-livecommexe-and-skydriveexe/d3ca910c-43dd-462d-870d-f72c365f3320?page=1>. Acesso em: 08 mar. 2015.

MICROSOFT CORPORATION. **Windows Server 2003:** Active Directory Infrastructure. [S.l.]: Microsoft Press, 2003.

MICROSOFT DEVELOPER NETWORK. Ambiguous Name Resolution. **Microsoft Developer Network**, 2015. Disponivel em: <https://msdn.microsoft.com/en-us/library/cc223243.aspx>. Acesso em: 01 jun. 2015.

MICROSOFT DEVELOPMENT NETWORK. Directory System Agent. **Microsoft Development Network**, 2010. Disponivel em: <http://msdn.microsoft.com/en-us/library/ms675902%28v=vs.85%29.aspx>. Acesso em: 09 set. 2014.

MICROSOFT DOWNLOAD CENTER. Active Directory Performance Testing Tool. **Microsoft Download Center**, 2012. Disponivel em: <http://www.microsoft.com/en-us/download/details.aspx?id=15275>. Acesso em: 11 nov. 2014.

MICROSOFT DOWNLOAD CENTER. Windows Server 2008 R2 Evaluation (180 days). **Download Center**, 2015. Disponivel em: <http://www.microsoft.com/en-us/download/details.aspx?id=11093>. Acesso em: 01 mar. 2015.

MICROSOFT SCRITP CENTER. New-NetIPAddress. **Scritp Center**, 2015. Disponivel em: <https://technet.microsoft.com/en-us/library/hh826150.aspx>. Acesso em: 20 mar. 2015.

MICROSOFT SOFTWARE RECOVERY. Windows 7. **Software Recovery**, 2015. Disponivel em: <http://www.microsoft.com/en-us/software-recovery>. Acesso em: 01 mar. 2015.

MICROSOFT SUPPORT KB 324175. Práticas recomendadas para manutenção de Sysvol. **Microsoft Support kb 324175**, 2007. Disponivel em: <https://support.microsoft.com/pt-br/kb/324175/pt-br>. Acesso em: 01 maio 2015.

MICROSOFT TECHNET. Microsoft Technet Windows Server 2000. **Windows Server 2000 TcpWindowSize**, 2000. Disponivel em: <https://technet.microsoft.com/en-us/library/cc938219.aspx>. Acesso em: 01 jun. 2015.

MICROSOFT WINDOWS. Windows 8. **Synchronising settings between PCs with OneDrive**, 2015. Disponivel em: <http://windows.microsoft.com/en-gb/windows-8/sync-settings-pcs>. Acesso em: 01 mar. 2015.

OLHAR DIGITAL. Google estende suporte ao Chrome para Windows XP. **Olhar Digital**, 2015. Disponivel em: <http://olhardigital.uol.com.br/noticia/google-estende-suporte-ao-chrome-para-windows-xp/48032>. Acesso em: 01 maio 2015.

RUSSINOVICH, M. E.; SOLOMON, D. A.; ALLCHIN, J. F. **Microsoft Windows Server 2003, Windows XP, and Windows 2000**. IV. ed. [S.l.]: [s.n.], 2004.

SAMBA TEAM. SAMBA XP 2015. **SAMBA XP 2015**, 2015. Disponivel em: <http://www.sambaxp.org/>. Acesso em: 14 jul. 2015.

SIGNUP LIVE. Criar uma conta. **SignUp Live**, 2014. Disponivel em: <https://signup.live.com/signup.aspx?wa=wsignin1.0&rpsnv=12&ct=1416013656&rver=6.0.5276.0&wp=MCMBI&wreply=https%3a%2f%2fprofile.microsoft.com%2fRegSysProfileCenter%2fwizard.aspx%3fwizid%3db93a84f8-62e4-4ab6-8335-cc4c0e07abcb%26lcid%3d1033%26fu%3dhttp%253a%>. Acesso em: 2014 nov. 14.

SIMO SOURCE. SAMBAXP 2014. **Simo Source**, 2014. Disponivel em: <https://ssimo.org/slides/sambaxp2014-openstack-and-samba.pdf>. Acesso em: 14 jul. 2015.

SOCIAL TECHNET FORUM. Windows XP can't join Windows Server 2012 R2 DC. **Social TechNet Forum**, 2013. Disponivel em: <https://social.technet.microsoft.com/Forums/pt-BR/bc5eddeb-dd85-458d-bbb9-3fa723ce943b/windows-xp-cant-join-windows-server-2012-r2-dc?forum=windowsserverpreview>. Acesso em: 01 maio 2015.

SUPORTE DA MICROSOFT. Serviços do Active Directory e Windows 2000 ou domínios do Windows Server 2003 (parte 1). **Suporte da Microsoft**, 2009. Disponivel em: <http://support.microsoft.com/kb/310996/pt-br>. Acesso em: 09 set. 2014.

SUPORTE MICROSOFT. O serviço de Logon de rede no Windows Server 2008. **Suporte Microsoft kb 942564**, 2008. Disponivel em: <http://go.microsoft.com/fwlink/?LinkId=104751>. Acesso em: 10 maio 2015.

TECHNET. Active Directory Replication Traffic. **TechNet**, 2007. Disponivel em: <http://technet.microsoft.com/en-us/library/bb742457.aspx>. Acesso em: 09 set. 2014.

TECHNET. Organizational Units. **TechNet**, 2010. Disponivel em: <http://technet.microsoft.com/en-us/library/cc978003.aspx>. Acesso em: 09 set. 2014.

TECHNET. AD DS on a Windows Server Network. **TechNet**, 2011. Disponivel em: <http://technet.microsoft.com/en-us/library/cc780036%28WS.10%29.aspx#w2k3tr_ad_over_qbjd>. Acesso em: 09 set. 2014.

TECHNET. How Security Identifiers Work. **TECHNET**, 2011. Disponivel em: <http://technet.microsoft.com/en-us/library/cc778824%28v=ws.10%29.aspx>. Acesso em: 11 nov. 2014.

TECHNET. How the Active Directory Schema Works. **Technet**, 2011. Disponivel em: <http://technet.microsoft.com/en-us/library/cc773309%28v=ws.10%29.aspx>. Acesso em: 14 nov. 2014.

TECHNET. Reviewing Organizational Unit Design Concepts. **Technet**, 2014. Disponivel em: <http://technet.microsoft.com/pt-br/library/cc758466%28v=ws.10%29.aspx>. Acesso em: 13 nov. 2014.

TECHNET ARTICLES. Active Directory: Concepts Part 1. **TechNet Articles**, 2013. Disponivel em: <http://social.technet.microsoft.com/wiki/contents/articles/16968.active-directory-concepts-part-1.aspx>. Acesso em: 13 nov. 2014.

TECHNET EVALUATION CENTER. TechNet Evaluation Center. **Windows Evaluations**, 2015. Disponivel em: <http://www.microsoft.com/en-us/evalcenter/evaluate-windows-8-1-enterprise>. Acesso em: 01 mar. 2015.

TECHNET MICROSOFT LIBRARY WINDOWS SERVER 2012. Get Connected in Windows Server Essentials. **TechNet Microsoft Library Windows Server 2012**, 2012. Disponivel em: <https://technet.microsoft.com/en-us/library/jj713510.aspx>. Acesso em: 01 maio 2015.

TECHNET MICROSOFT WINDOWS SERVER. Selecting the Forest Root Domain. **TechNet Microsoft Windows Server**, 2012. Disponivel em: <https://technet.microsoft.com/en-us/library/cc726016%28v=ws.10%29.aspx>. Acesso em: 10 maio 2015.

TREND MICRO. O Windows XP não está morto! **Trend Micro**, 2015. Disponivel em: <http://blog.trendmicro.com.br/o-windows-xp-nao-esta-morto/#.VVBpPJO-Dcs>. Acesso em: 06 maio 2015.

UNIVERSIDADE FEDERAL DO PARANÁ. Debian Repository. **Universidade Federal do Paraná**, 2015. Disponivel em: <http://debian.c3sl.ufpr.br/debian-cd/7.8.0/i386/iso-cd/debian-7.8.0-i386-CD-1.iso>. Acesso em: 05 mar. 2015.

VIRTUALBOX. VirtualBox. **Download VirtualBox**, 2015. Disponivel em: <https://www.virtualbox.org/wiki/Downloads>. Acesso em: 01 mar. 2015.

WINDOWS SERVER. Choose a Namespace Type. **Windows Server**, 2008. Disponivel em: <http://technet.microsoft.com/en-us/library/cc770287.aspx>. Acesso em: 13 nov. 2014.

WINDOWS SERVER. Guia passo a passo para configuração da diretiva de bloqueio de senhas e contas refinadas. **Windows Server**, 2009. Disponivel em: <http://technet.microsoft.com/pt-BR/library/2199dcf7-68fd-4315-87cc-ade35f8978ea>. Acesso em: 13 nov. 2014.

WINDOWS SERVER. Service Accounts Step-by-Step Guide. **Windows Server**, 2012. Disponivel em: <http://technet.microsoft.com/en-us/library/dd548356%28WS.10%29.aspx>. Acesso em: 13 nov. 2014.

WINDOWS SERVER. What's New in Kerberos Authentication. **Windows Server**, 2012. Disponivel em: <http://technet.microsoft.com/en-us/library/hh831747.aspx>. Acesso em: 13 nov. 2014.

WINDOWS SERVER. Understanding Active Directory Domain Services (AD DS) Functional Levels. **Windows Server**, 2014. Disponivel em: <http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels%28v=ws.10%29.aspx>. Acesso em: 13 nov. 2014.

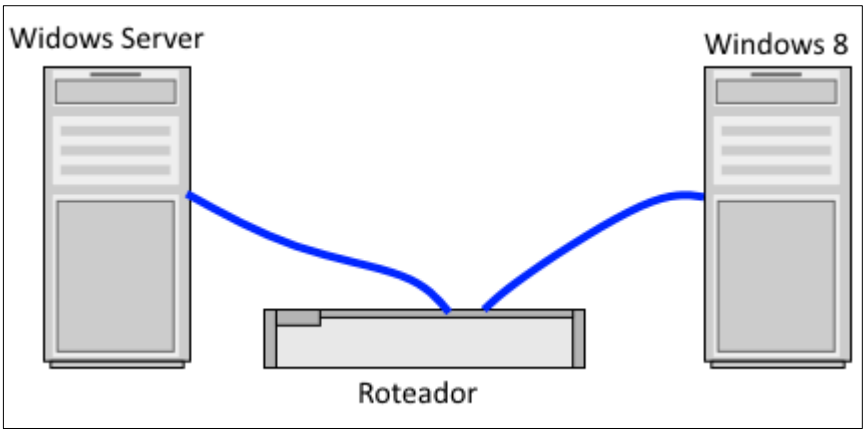
WINDOWS SERVER TECHCENTER. Windows Server. **Windows Server 2008 System Requirements**, 2012. Disponivel em: <https://technet.microsoft.com/en-us/windowsserver/bb414778.aspx>. Acesso em: 01 mar. 2015.

X9000.COM. Active Directory Benchmarking Tool. **x9000.com Consulting Services Limit**, 2014. Disponivel em: <http://www.x9000.com/Downloads/ADBenchmark.aspx>. Acesso em: 11 nov. 2014.

APÊNDICES

APÊNDICE A – TUTORIAL EXPLICATIVO DE IMPLEMENTAÇÃO SIMPLES DO ACTIVE DIRECTORY ENTRE MÁQUINAS WINDOWS

Figura 1 – Topologia de rede a ser emulada



Na emulação foi usada o aplicativo open-source VirtualBox versão 4.3.26.r98988 (VIRTUALBOX, 2015), na topologia especifica como na Figura 1, com Windows Server 2008.

1 WINDOWS SERVER

Segundo a Microsoft (WINDOWS SERVER TECHCENTER, 2012) as recomendações mínimas de hardware da instalação são: “Processador 1GHz x86, Memória RAM de 512MB, espaço em disco de 4GB, Drive de CD-Rom, monitor resolução 800x600, teclado e mouse”.

Por isso, a máquina virtual criada tem 512 MB de RAM, espaço em disco de 16GB, pois a instalação padrão consome mais de 8GB (menos do que 4GB, só a instalação Server Core).

O adaptador de Rede foi IntelPro/1000 MT Destop (82540EM) no modo "Rede Interna"

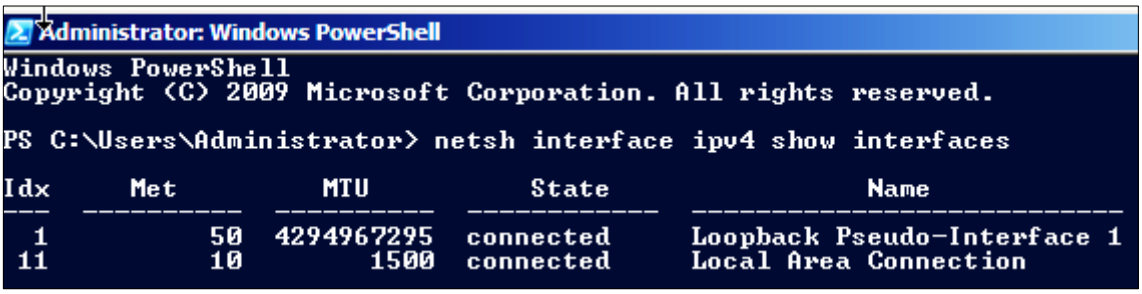
1.1 INSTALAÇÃO E CONFIGURAÇÃO BÁSICA

Após escolher a instalação padrão (Standard Full), adotar para o administrador uma senha complexa (mais de 6 caracteres, números e maiúsculas e minúsculas), a rede foi configurada, pela interface de comando.

Primeiro, deve se descobrir qual é o número da interface de rede.

netsh interface ipv4 show interfaces

Figura 2: Identificando a interface de rede via PowerShell



Na Figura 2 é possível ver que a interface de rede está identificada sob o número “11”. Este número é a referência que deve ser usada nos comandos de configuração. Será configurada um ip estático 10.0.0.1/24 usando a máquina roteador como gateway

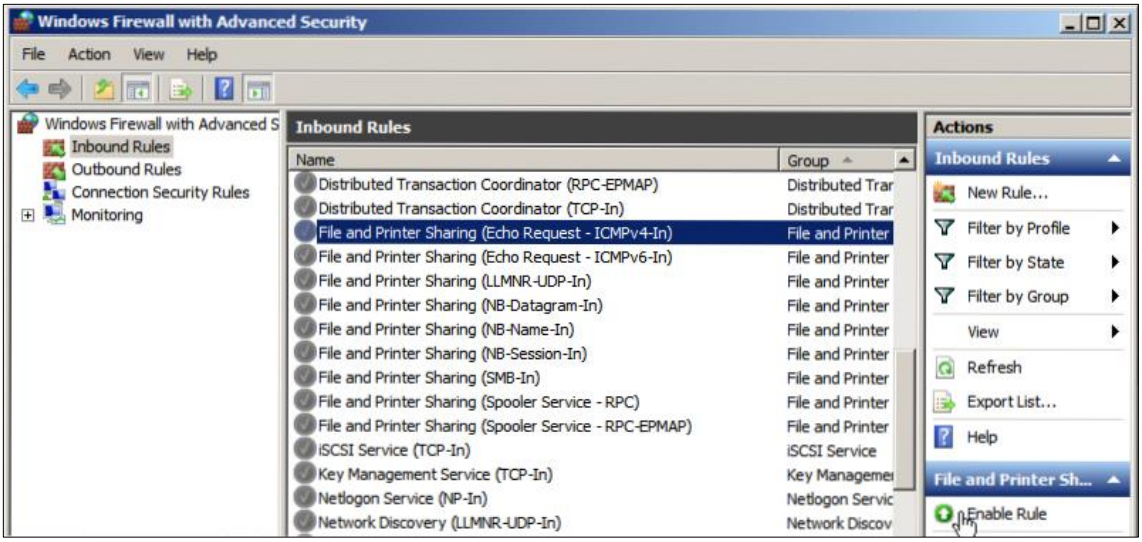
netsh interface ipv4 set address name=11 source=static address=10.0.0.1 mask=255.255.255.0 gateway=10.0.0.254

Depois basta configurar o DNS, que vamos usar o próprio gateway

netsh interface ipv4 add dnsserver name=11 address=10.0.0.254 index=1

O shell de rede (netsh) funciona tanto no Windows PowerShell, como no Command Shell, que é o terminal padrão das versões antigas do Windows, como 2000/XP/Server 2003/Vista/7.

Figura 3: Firewall do Windows Server 2008



Para fazer os testes de rede, pode ser necessário habilitar temporariamente o recurso de Ping, cuja maneira mais simples de fazer é por meio do Firewall do Windows, como pode ser visto na Figura 3, nas opções Inbound Rules, para a regra “File and Printer Sharing (Echo Request – ICMPv4-In)”

A interface de comando até funciona, mas apresenta alerta de que está caindo em desuso (deprecated), e foi substituído por opções mais avançadas

netsh firewall set icmpsetting 8 enable

netsh firewall set icmpsetting 8 disable

A nova sintaxe recomendada de netsh pede para que o usuário crie uma regra no firewall com nome qualquer, que vai habilitar o protocolo, e depois desligar o ping apagando a regra pelo nome

netsh advfirewall firewall add rule name="Habilita Ping" protocol=icmpv4:8,any dir=in action=allow

netsh advfirewall delete rule “Habilita Ping”

Esses comandos terminam por ser mais trabalhosos e demorados do que usar a interface gráfica, a menos que se esteja operando um Server Core ou o administrador crie um script com esses comandos, para automatizar o trabalho.

1.2 INSTALANDO O ACTIVE DIRECTORY

A instalação do Active Directory ocorre executando dcpromo.exe

O objetivo essencial deste facilitador (Wizard) é colocar as diretivas certas nos locais certos. Em uma instalação Server Core, sem interface gráfica, as diretivas deveriam ter sido organizadas em um arquivo de entrada, desta maneira:

[DCINSTALL]

InstallDNS = yes

NewDomain = florest

NewDomainDNSName =ifsul

DomainNetBiosName = marcelo

E o arquivo oferecido ao instalador usando o comando:

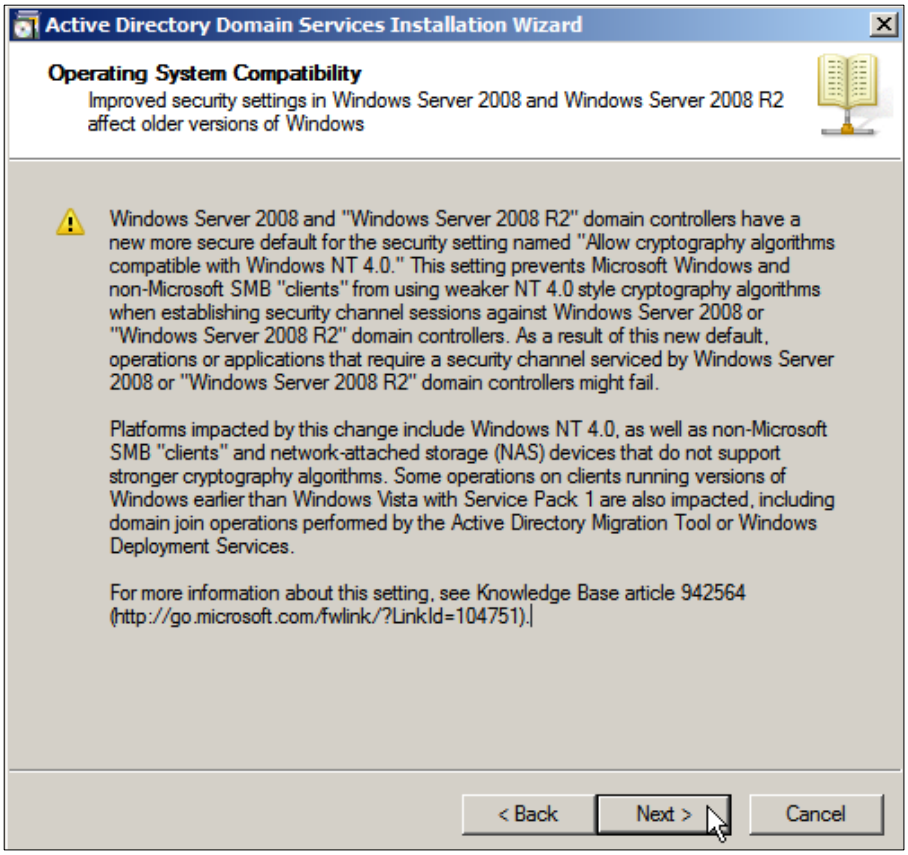
dcpromo.exe / unattend:diretivas.txt

Como pode ser visto na Figura 4, se preferiu uma instalação padrão tradicional.

Figura 4: Tela inicial do dcpromo

O primeiro alerta informa que esta versão de AD pode causar problemas de compatibilidade com versões de AD anteriores, e com clientes não-Windows, já que houve mudança na criptografia em relações a versões anteriores, como pode ser visto na Figura 5.

Figura 5: Alerta de eventuais problemas de compatibilidade



O link exibido na Figura 5 (SUPORTE MICROSOFT, 2008) menciona problemas de autenticação com o erro 0x4Fh1 com a mensagem “ERROR_DOWNGRADE_DETECTED” em clientes SAMBA antigos, que também é o mesmo erro apresentado em Windows versões 2000/XP/Server 2003/Vista.

Se trata de um erro de compatibilidade entre criptografias de autenticação, pois o Windows NT 4.0 não possui mais suporte da Microsoft, e sua autenticação é considerada por padrão como “de segurança comprometida” pelo Windows Server 2008.

Se caso o problema surgir, ele é contornado habilitando a criptografia compatível com NT4, por meio do Group Policy Management (gpmc.msc) no Windows 2008 Server.

O próximo passo é escolher se deseja usar uma floresta já existente ou criar uma nova. Como mostra a Figura 6, estamos criando uma nova.

Figura 6: Instalação da Floresta

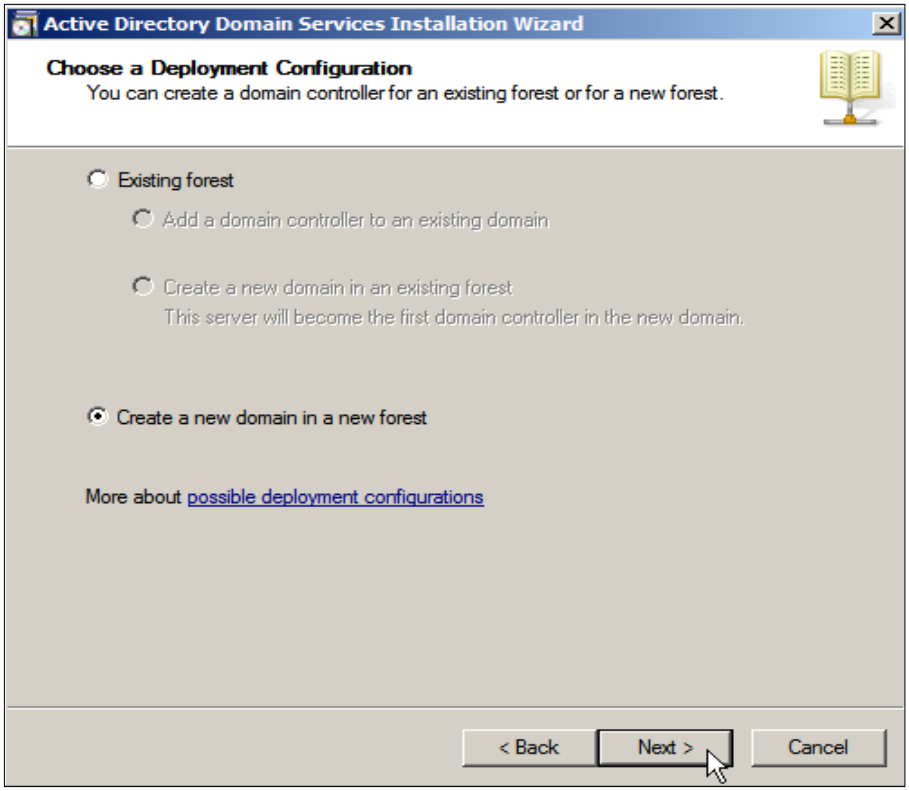
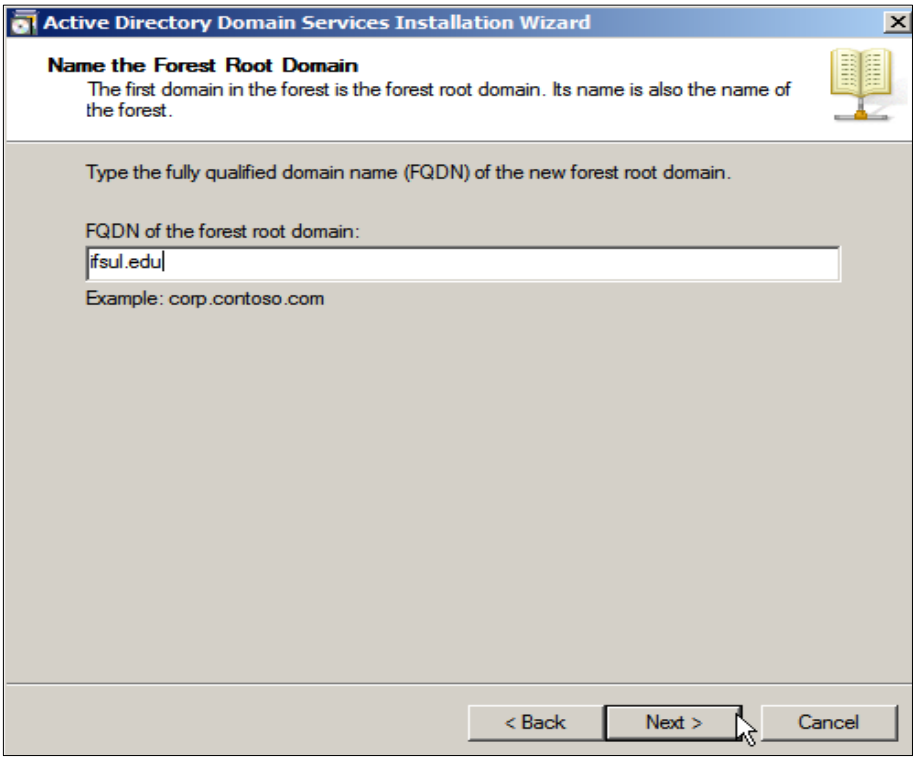


Figura 7: Inserção do nome e domínio

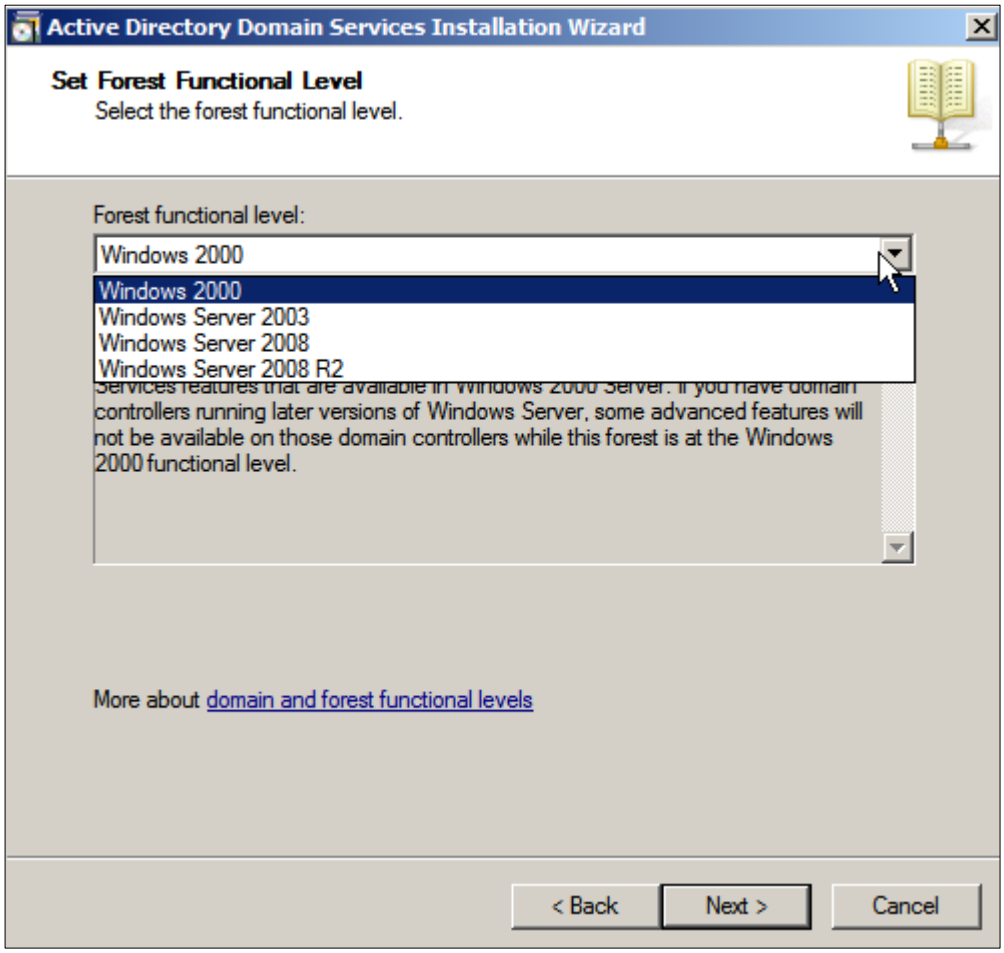


As recomendações padrão (TECHNET MICROSOFT WINDOWS SERVER, 2012) para os domínios totalmente qualificados, é que sejam nomes menos propensos a mudanças, como nomes de corporações, como mostrado na Figura 7, em que o nome do domínio raiz é “ifsul.edu”.

Os nomes são case-sensitive, podem possuir hífen (-) e aceitam dígitos numéricos, mas não podem ser formados exclusivamente por dígitos (ex: ifsul.123).

Estes nomes não podem ultrapassar 15 caracteres, ou haverá problemas de interpretações pelo NetBios, que passará interpretar o nome como sendo igual ao prefixo.

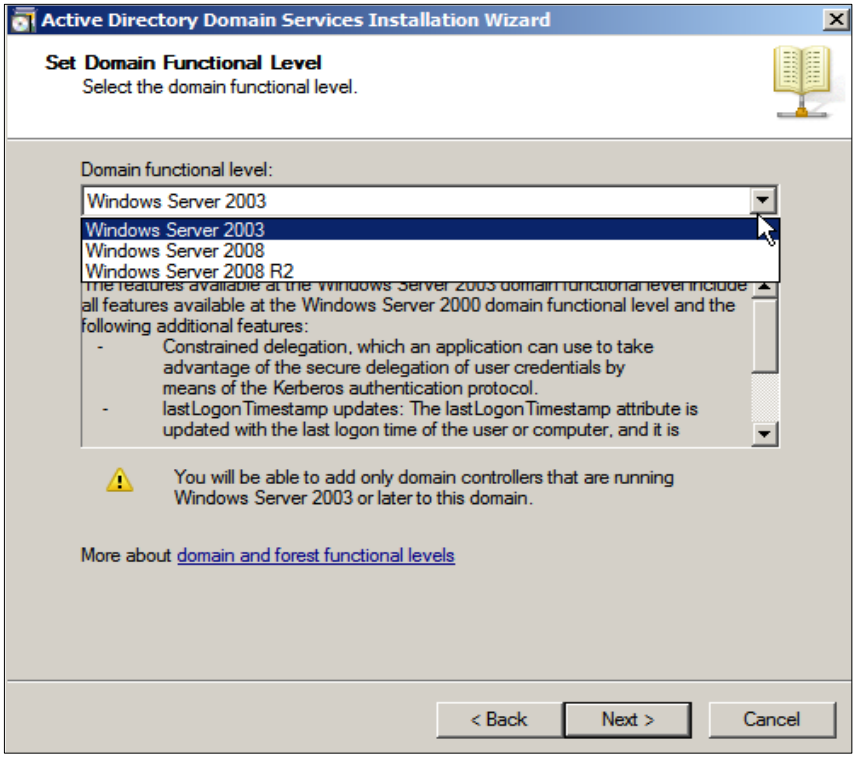
Figura 8: Tipos de funcionalidades de Active Diretory



São oferecidos 4 tipos de níveis funcionais floresta, como compatibilidade com versões anteriores do AD para Windows Server, como mostra a Figura 8.

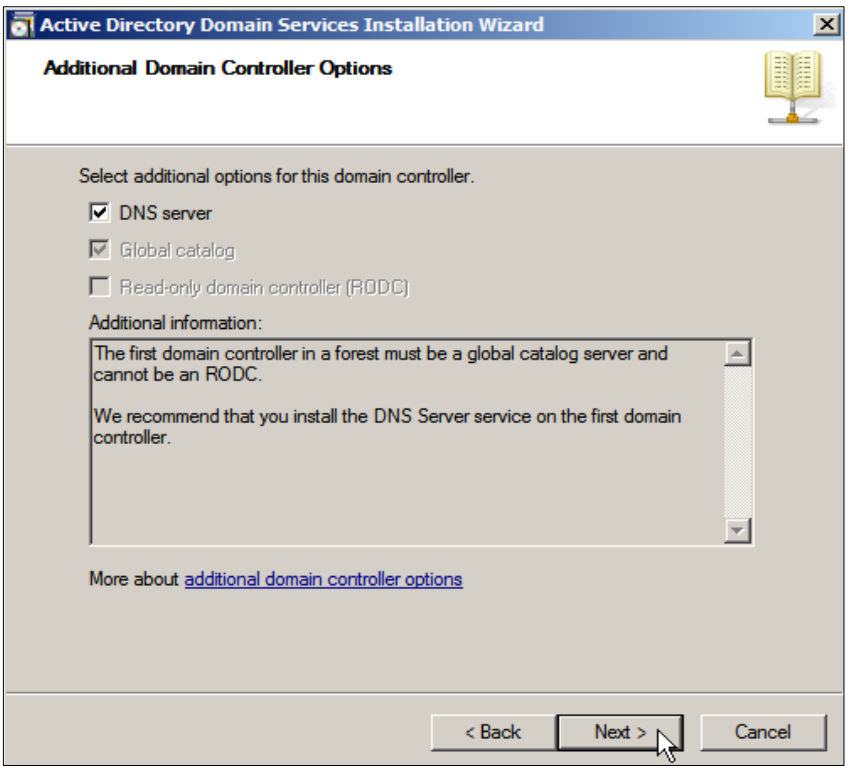
Como pode ser visto na Figura 9, o próximo passo da instalação também pede pelo nível funcional desejado para os domínios.

Figura 9: Seleção do nível funcional dos domínios



1.3 CONFIGURAÇÕES DO SISTEMA

Figura 10: Instalação do DNS e do Catálogo Global



Como este é o primeiro controlador de domínio que está sendo instalado, a opção de catálogo global vem habilitada por padrão.

O DNS é necessário, mas poderia vir de uma outra máquina, um controlador de domínio apenas-leitura (RODC) se esta instalação de controlador de domínio não fosse a primeira da floresta. Como pode ser visto na Figura 10, se trata do primeiro controlador de domínio, a recomendação é instalar o serviço DNS na máquina local.

O IPs desta máquina deve ser estático, pois se for IPs dinâmicos, haverá erro, e a instalação vai pedir para o usuário mudar o IP para estático. Se os IPs estiverem totalmente dinâmicos, e o usuário não souber configurar, pode ser mais rápido desabilitar o IPv6 da máquina, e resolver a questão posteriormente.

Figura 11: A instalação não encontrou um Windows DNS Server

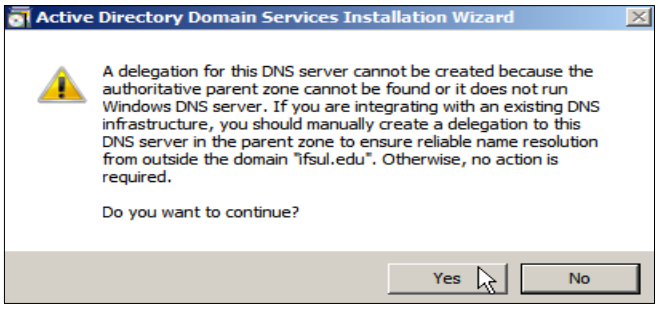
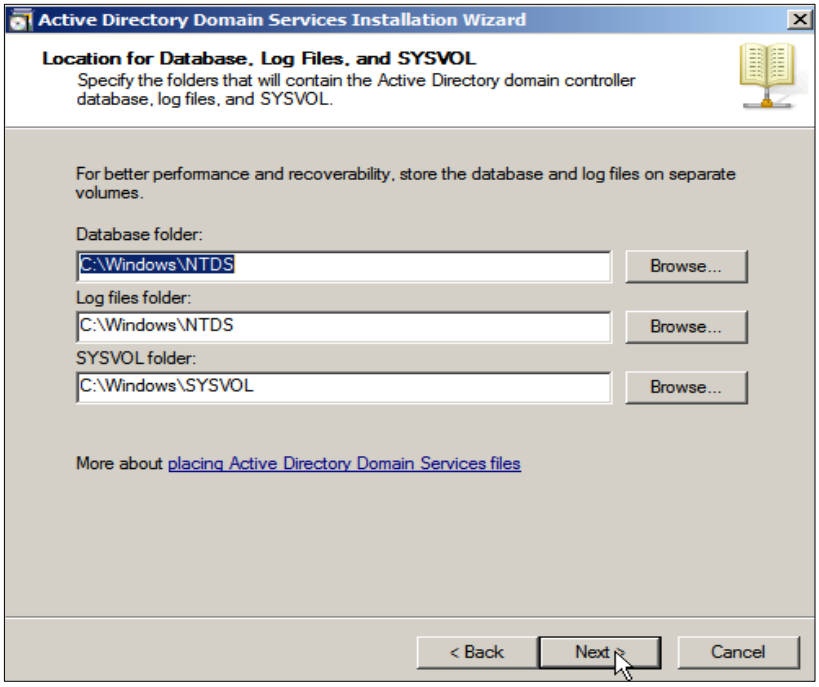


Figura 12: Localização do armazenamento dos arquivos



Como apresentado na Figura 11, a instalação do DNS apresenta um alerta por não ter encontrado um outro Windows DNS Server.

É um erro padrão que ocorre na instalação do primeiro controlador de domínio, basta ignorar e confirmar para efetuar a instalação do DNS.

Posteriormente a instalação pede pelos caminhos onde vão ficar armazenados os banco de dados, os logs, e o Volume de Sistema (SYSVOL), como pode ser visto na Figura 12.

No próximo passo, como pode ser visto na Figura 13, o instalador pede uma senha para quando for efetuada uma possível restauração dos diretórios.

Depois a instalação apresentará um sumário com todas as configurações escolhidas. Basta clicar em “Next” e a instalação ocorre, como pode ser visto na Figura 14, e depois, basta reiniciar.

Figura 13: Senha para restauração

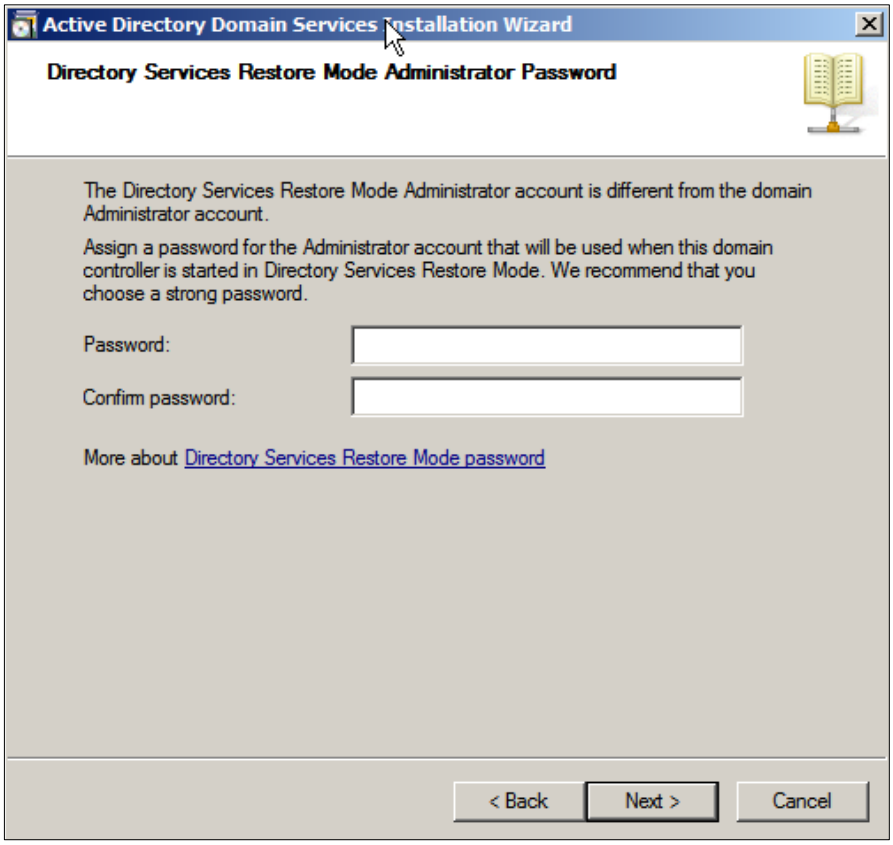
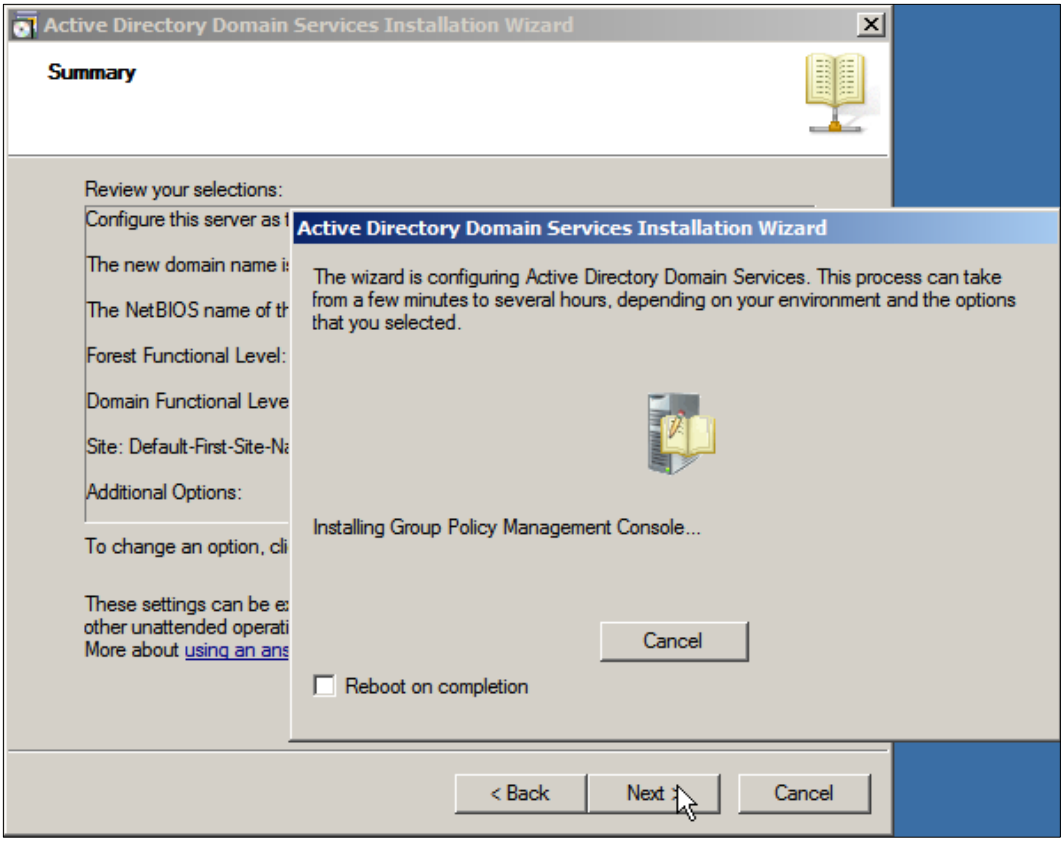


Figura14: Instalação ocorrendo



Depois de tudo instalado, basta usar a interface gráfica do Active Directory, como mostrado nas Figuras 15 e 16.

Figura15: Inserir um usuário no AD

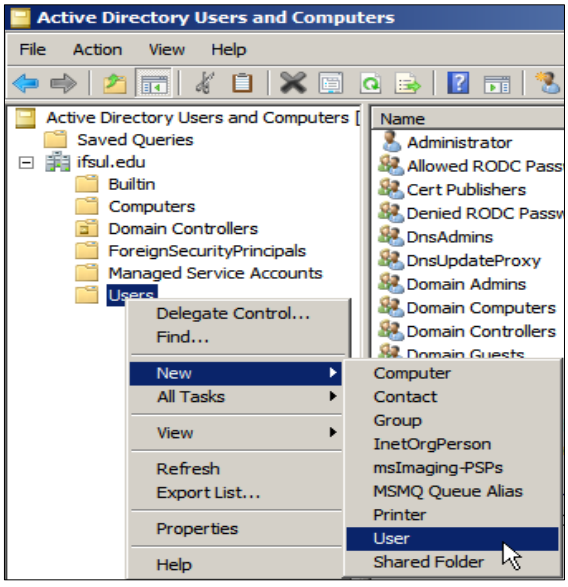
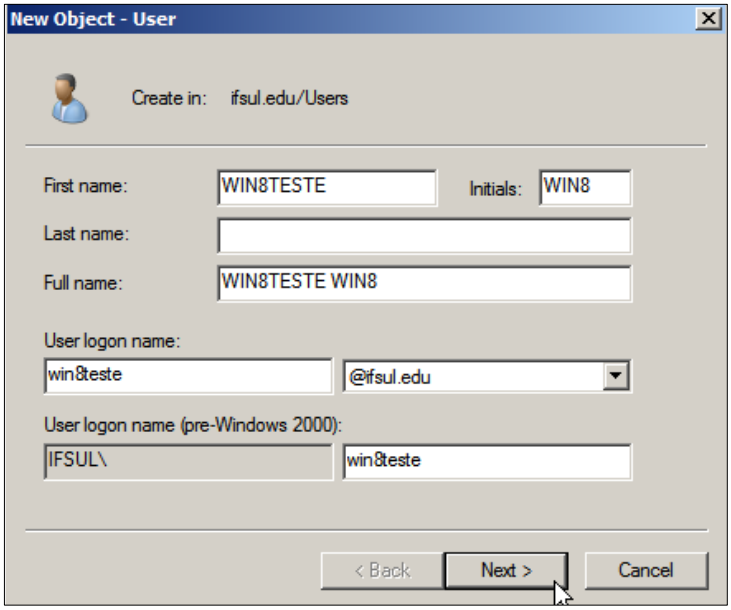


Figura 16: Dados do usuário



2 ROTEADOR USANDO LINUX

A distribuição de sistema Linux escolhida foi Debian, que está na versão 7.8, e foi baixado o primeiro CD da versão 32bits. A máquina virtual foi configurado com dois adaptadores de redes

Adaptador1: Rede IntelPro/1000 MT Destop (82540EM) no Modo Bridge, para que a máquina ganhasse um IP real na minha rede pessoal.

Adaptador2: Rede IntelPro/1000 MT Destop (82540EM) no modo "Rede Interna"

Na instalação foi escolhido 512 MB de RAM, para evitar gargalos de desempenho, e espaço em disco de 4GB.

Durante a instalação a máquina foi nomeada “roteador”, e o usuário foi chamado “marcelo”. Foi escolhido apenas utilitários padrões do sistema, sem interface gráfica. O gateway da rede local onde foi feito os testes é o IP 192.168.1.1

3 WINDOWS 8

Uma versão trial 90 dias do Windows 8 foi obtida via download no site da Microsoft (TECHNET EVALUATION CENTER, 2015).

Versões anteriores do sistema Windows não são disponibilizadas para testes, apenas o Windows 7 é disponibilizado no modo backup de CD, sendo necessário o usuário possuir um Windows licenciado para conseguir baixar o arquivo ISO de instalação (MICROSOFT SOFTWARE RECOVERY, 2015).

3.1 ENTRANDO NO DIRETÓRIO

Depois que o Windows Server 2008 estiver configurado, basta coloca-lo como sendo o DNS desta máquina cliente, e se fazer o login no domínio, como pode ser visto nas Figuras 17 e 18. Lembrar que o nome do usuário e a senha devem ser os mesmos dos definidos pelo administrador de rede.

Figura 17: Entrando no domínio do Active Directory

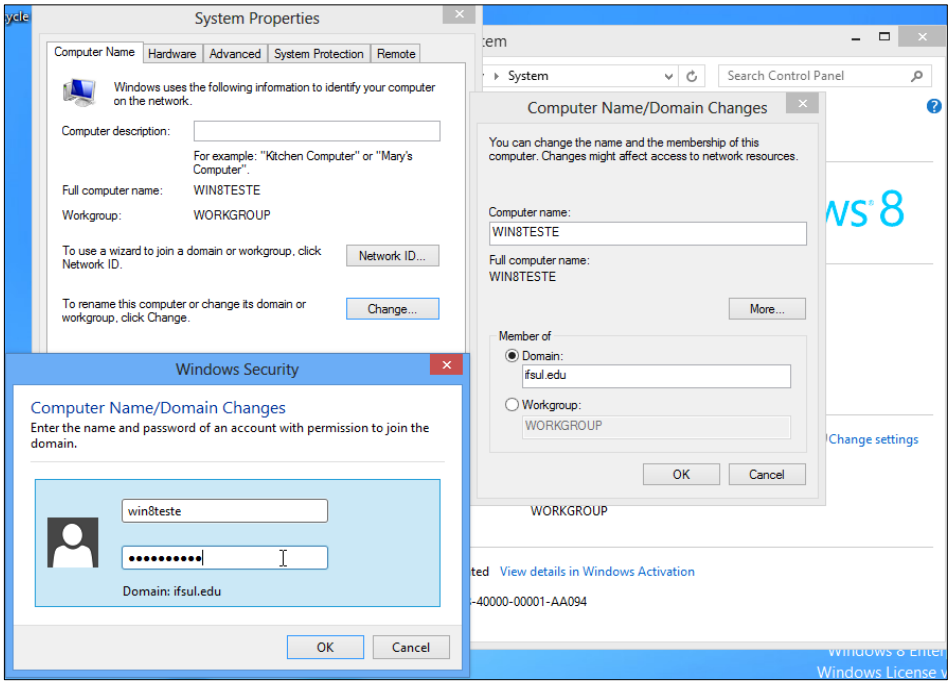
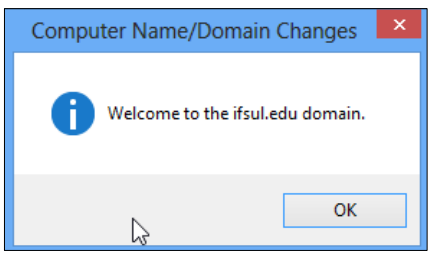


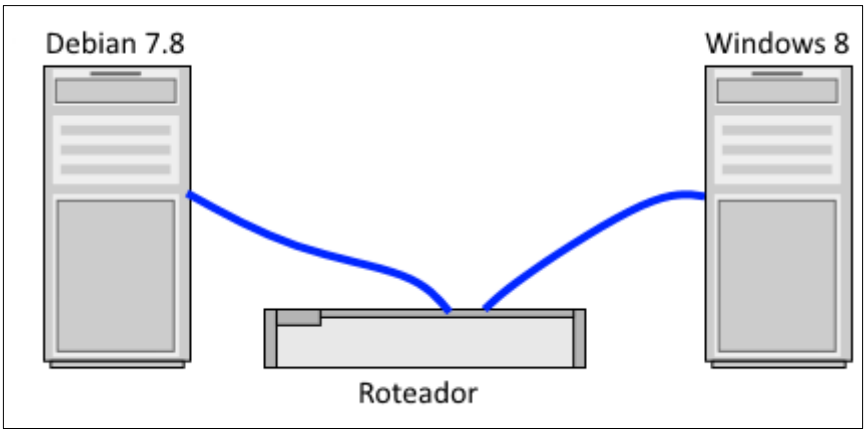
Figura 18: Entrada no AD feita com sucesso



APÊNDICE B – TUTORIAL EXPLICATIVO DE IMPLEMENTAÇÃO SIMPLES DO ACTIVE DIRECTORY SOBRE SAMBA

Esse tutorial não se deterá em explicar a implementação do roteador com Linux e nem do cliente Windows, pois podem ser usadas as mesmas máquinas criadas no tutorial anterior.

Figura 1 – Topologia de rede a ser emulada



Na emulação foi usada o aplicativo open-source VirtualBox versão 4.3.26.r98988 (VIRTUALBOX, 2015), na topologia especifica como na Figura 1.

1. SERVIDOR DEBIAN COM SAMBA

A distribuição de sistema Linux escolhida foi Debian, que está na versão 7.8, e foi baixado o primeiro CD da versão 32bits

A máquina virtual foi configurado com um adaptador de rede Rede IntelPro/1000 MT Destop (82540EM) no modo "Rede Interna"

Na instalação, foram escolhidas as mesmas configurações do Windows Server que já havia sido implementado anteriormente, isto é, 512 MB de RAM espaço em disco de 16GB.

Durante a instalação a máquina foi nomeada “**sambaserver**”, e o usuário foi chamado “**marcelo**”

Foi escolhido a apenas utilitários padrões do sistema, sem interface gráfica. O gateway da rede local onde foi feito os testes é o IP 192.168.1.1

1.1. DEPENDÊNCIAS DO SAMBA

Primeiro, será necessário instalar os pacotes de dependências do Active Directory para o SAMBA.

aptitude install build-essential

Não aceite a sugestão da remoção em massa de pacotes. Negue, e depois aceite a segunda opção, de remover apenas o gcc. Na próxima janela, selecione "Yes" para interromper os serviços durante a atualização, sem perguntar. Ao terminar a atualização, reinicie.

aptitude install libacl1-dev libblkid-dev

Biblioteca de controle de listas estáticas, e identificação de dispositivos

aptitude install libgnutls-dev

Não aceite instalar sem resolver as pendências, aceite a segunda opção, de fazer a instalação resolvendo as dependências.

aptitude install python-dev python-dnspython

Biblioteca de desenvolvimento na linguagem Python e Kit de utilitários DNS

aptitude install gdb pkg-config libreadline-dev

Debuguer GNU e gerenciador de flags de compilação e ligação, e históricos do GNU

aptitude install libpopt-dev docbook-xsl

Efetua o parsing dos parâmetros de linhas de comando, folha de estilos para processamento de documentos XML.

aptitude install libldap2-dev libbsd-dev

Bibliotecas de desenvolvimento do OpenLDAP, funções utilitárias de serviços BSD

aptitude install attr gnutls-bin gnutls-dev

Utilitário para manipulação de atributos, utilitário TLS de linha de comando

aptitude install krb5-user

Programas para autenticação kerberos.

Na janela de configuração do domínio, deixar a opção vazia e confirmar.

aptitude upgrade

Atualiza os pacotes. Se a instalação parar, exibindo dados sobre o certificado do Mozilla, pressione “q” para dar sair e continuar a instalação.

No caso da instalação ser feita com a distribuição Jessie, as dependências que não resolvidas serão: build-essential, libacl1-dev, libblkid-dev, libreadline-dev, python-dev , libpam0g-dev, gdb , pkg-config, libpopt-dev, libldap2-dev, libbsd-dev, krb5-user, docbook-xsl, libcups2-dev, assim como o próprio smbclient que deverá ser instalado separadamente.

Se for instalado um controlador de domínio na distribuição Jessie, ao se consultar o status do serviço SAMBA, a resposta será que o serviço está mascarado e morto.

service samba status

- samba.service
  Loaded: masked (/dev/null)
  Active: inactive (dead)

Isso ocorre por que o serviço que administra o domínio se chama samba-ad-dc (samba active directory domain control).

1.2. CONFIGURANDO O SISTEMA DE ARQUIVOS

O SAMBA possui dependência primária nos sistemas de arquivos, tanto ext3, ext4, ou xfs, pois o sistema deve ter suporte a recursos de namespaces xattr, por causa da pasta

/usr/local/samba/var/locks/sysvol/

Este recurso é baseado no utilitário de manipulação de atributos attr, e é sobre essa pasta **sysvol** que ocorre o funcionamento do Active Diretory, pelo compartilhamento da

mesma, segundo o Sistema de Arquivos Distribuídos (DFS, Distributed File System) que funciona nos servidores que executam Windows Server.

Para adicionar esses recursos no Linux, primeiro é necessário descobrir o tipo do sistema de arquivos da máquina Linux local, com o comando **blkid.** Nesta instalação, como é a padrão, o sistema é ext4.

Para conseguir os recursos mais avançados do Active Directory, o sistema de arquivos deve também ter suporte a Listas de Controle de Acesso (ACL, Access Control List).

Assim, devemos modificar a partição onde o sistema efetua a montagem da pasta dos usuários, no caminho /home, não errando o tipo de sistema de arquivos já existente.

/dev/sdb1 /home ext4 user_xattr,acl,barrier=1 1 1

Se caso sua instalação Linux foi de uma única partição, então aplique as configurações em todo a raiz

/dev/sda1 / ext4 user_xattr,acl,barrier=1 1 1

Qualquer erro neste processo pode deixar a máquina não iniciável, por isso, se estiver em uma máquina virtual, crie um instantâneo da máquina, que poderá vir a ser restaurado se houver problemas.

Observe que ao invés do UUID da partição, foi colocado o caminho do dispositivo, pois o sistema sabe interpretar o fstab ambos os modos, embora o uso de UUIDs seja mais robusto pois não haverá problemas, se caso houver trocas de discos na máquina.

A última diretiva “barrier=1” serve para tentar ativar a proteção contra falta de energia, conhecida como Enfileiramento de Comandos Nativo (NCQ, Native command queuing) existente no hardware dos HDs modernos. Para descobrir se o HD da máquina possui esse recurso, seria necessário instalar o pacote hdparm, e efetuar o comando:

hdparm -I /dev/sda (caminho do HD)

Se a saída do comando não apresentar nada sobre NCQ, então o HD não possui esse recurso. No caso das máquinas virtuais do VirtualBox 4.3.26 (e posteriores) os HDs virtuais possuem esse recurso.

Nesta instalação de SAMBA, o objetivo de se habilitar esse recurso, é para que haja segurança, evitando uma eventual corrupção dos dados caso ocorra qualquer interrupção

subida de energia, durante as transações do banco de dados LDB (LDAP-like embedded DataBase).

O LBD que se trata de um banco de dados simples do tipo TDB (Trival Data Base) que possui internamente uma API (application programming interface) do tipo LDAP (Lightweight Directory Access Protocol) e é o motor principal de funcionamento do SAMBA.

1.3. TESTANDO O SISTEMA DE ARQUIVOS

Para testar, basta reiniciar a máquinas com as novas alterações do fstab, ou remontar a unidade que foi modificada.

mount -o remount,rw /home

É necessário testar se os novos recursos da partição estão funcionando:

Criar um arquivo

touch x.txt

Criando atributos e os atribuindo ao arquivo

setfattr -n user.aluno -v tema x.txt

setfattr -n security.reitor -v licitação x.txt

Ler os atributos criados

getfattr -d x.txt

getfattr -n security.reitor -d x.txt

A resposta dos comandos deve ser respectivamente:

file: x.txt

user.aluno=”tema”

file: x.txt

security.reitor=”licitação”

1.4. DOWNLOAD E COMPILAÇÃO DO SAMBA

Primeiro é necessário verificar a versão mais recente do SAMBA em seu website. Nesta situação foi utilizado a versão 4.1.8 que pode ser baixada pelo comando:

wget https://download.samba.org/pub/samba/stable/samba-4.1.8.tar.gz

Essa versão do SAMBA foi utilizada, por que versões mais novas ainda estão em fase beta e são instáveis, além de precisar que várias dependências de pacotes sejam resolvidas manualmente (como o gnutls 3.4.1, que depende do nettle 3.1), cada uma sendo baixada de seu site específico e instalada manualmente, o que aumenta exponencialmente o grau de dificuldade da operação.

Descompactar, entrar na pasta, verificar dependências, compilar e instalar.

tar -zxvf samba-4.1.8.tar.gz

cd samba-4.1.8

./configure

make

make install

Se durante o comando **./configure** houver erros, certamente haverá avisos envolvendo ausência dos pacotes de dependências.

Após esse processo, o SAMBA estará instalado na pasta **/usr/local**

Para facilitar os outros passos, e melhor colocar o SAMBA no PATH

export PATH=$PATH:/usr/local/samba/bin:/usr/local/samba/sbin

A instalação foi feita na distribuição Jessie por meio de apt-get ou aptitude, o instalador já fez esse trabalho de corrigir o path.

1.5. INSTALAÇÃO DO ACTIVE DIRECTORY COM SAMBA

A instalação é iniciada com a ferramenta samba-tool, com o comando:

/usr/local/samba/bin/samba-tool domain provision

Passo 1: A instalação inicia perguntando o FQDN a ser criada, que é chamado de “reino” (Realm). Nesta instalação, foi escolhida ifsul.edu.

Passo 2: É perguntado o domínio, é só confirmar a primeira palavra antes do ponto, que neste caso foi ifsul.

Passo 3: É perguntado qual será a regra do servidor:

a) Domain Controller: Controlador de domínios
b) Member: Se fará parte de um domínio já existente.
c) Standalone: Controlador isolado, com nível de segurança mais baixa

Nesta instalação foi utilizada a opção Domain Controler “dc”

Passo 4: Qual o tipo de DNS será utilizado

a) DNS interno do SAMBA: DNS baseado em Python
b) BIND9 com arquivo puro: DNS clássico padrão
c) BIND9 com Zonas Dinâmicas (DLZ, Dynamically Loadable Zones)

Para simplificar a instalação, foi escolhido o DNS dinâmico, com a opção SAMBA_INTERNAL

Passo 5: Qual o DNS externo para redirecionamento das requisições?
Foi escolhido o IP da máquina roteador, 10.0.0.254

Passo 6: Qual a senha do Administrador. No nosso caso, foi colocado Ifsul123!

A instalação criará todos os arquivos, e já está funcionando. A existência de um arquivo smb.conf anterior vai impedir essa criação de domínio, e precisará ser apagado.

1.6. TESTANDO O ACTIVE DIRECTORY NO SAMBA

Subir o SAMBA no servidor, testar a conexão de um cliente com o AD na própria máquina, e testar autenticação NetLogon do administrador com a senha que criamos, listando os diretórios compartilhados.

/usr/local/samba/sbin/samba

/usr/local/samba/bin/smbclient -L localhost -U%

/usr/local/samba/bin/smbclient //localhost/netlogon-UAdministrator%'Ifsul123!' -c 'ls'

Os resultados são apresentados na tela, como podem ser vistos na Figura 2

Figura 2: Teste de conexão e teste de autenticação

A máquina que oferece o serviço DNS deve ter IP fixo, e o nome do domínio que criamos deve constar na resolução de nomes. Portanto, devemos editar o arquivo **/etc/resolv.conf** para conter o seguinte texto.

domain ifsul.edu

nameserver: 10.0.0.1

Devemos testar se o DNS automático do SAMBA está funcionando, verificando os registro de serviço (SRV record) ldap e kerberos e o próprio nome do servidor.

host -t SRV _ldap._tcp.ifsul.edu

host -t SRV _kerberos._udp.ifsul.edu

host -t A sambaserver.ifsul.edu

Como pode ser visto na Figura 3, o servidor se identificou com o seu próprio IP, o ldap escuta a porta 389 e kerberos escuta a porta 88, a prioridade de ambos é zero, e o peso atribuído é 100.

Figura 3: Resultados dos Testes no DNS

```
root@sambaserver:/# host -t SRV _ldap._tcp.ifsul.edu
_ldap._tcp.ifsul.edu has SRV record 0 100 389 sambaserver.ifsul.edu.
root@sambaserver:/# host -t SRV _kerberos._udp.ifsul.edu
_kerberos._udp.ifsul.edu has SRV record 0 100 88 sambaserver.ifsul.edu.
root@sambaserver:/# host -t A sambaserver.ifsul.edu
sambaserver.ifsul.edu has address 10.0.0.1
```

A prioridade e peso implicam na divisão de trabalho que será feito na rede, os serviços com prioridade de valor baixo serão procurados muito mais do que os serviços de valor alto. Se a prioridade de um serviço for 200, ele praticamente só será procurado se for o único na rede.

Com relação ao peso, se trata da demanda de clientes atendidos na rede, o valor adotado será uma parte, dentro da soma aritmética de todos os mesmos serviços presentes na rede.

Por exemplo, se houver um serviço com peso 50 e um segundo sendo disponibilizado com peso 100, então, a demanda pelo primeiro será de um terço do total (50/150), enquanto o segundo terá uma demanda de dois terços do total (100/150).

1.7. CONFIGURANDO O KERBEROS

Para que o protocolo de comunicação segura Kerberos funcione, é necessário fazer uma substituição nos arquivos da instalação.

cp –a /usr/local/samba/share/setup/krb5.conf /etc/

E editar o arquivo krb5.conf, escrevendo o nome do reino que criamos, em caixa alta, no lugar do texto “${REALM}” existente, como está sendo apresentado na figura 4.

Se a instalação ocorreu na distribuição Jessie, ao final da instalação do domain o samba tool irá gerar o arquivo correto na pasta /var/lib/samba/private/krb5.conf para ser copiado manualmente para a pasta /etc/.

Após isso, basta iniciar o Kerberos como o administrador no domínio, e entrar com a senha **Ifsul123!** que criamos na instalação do SAMBA.

kinit administrator@IFSUL.EDU

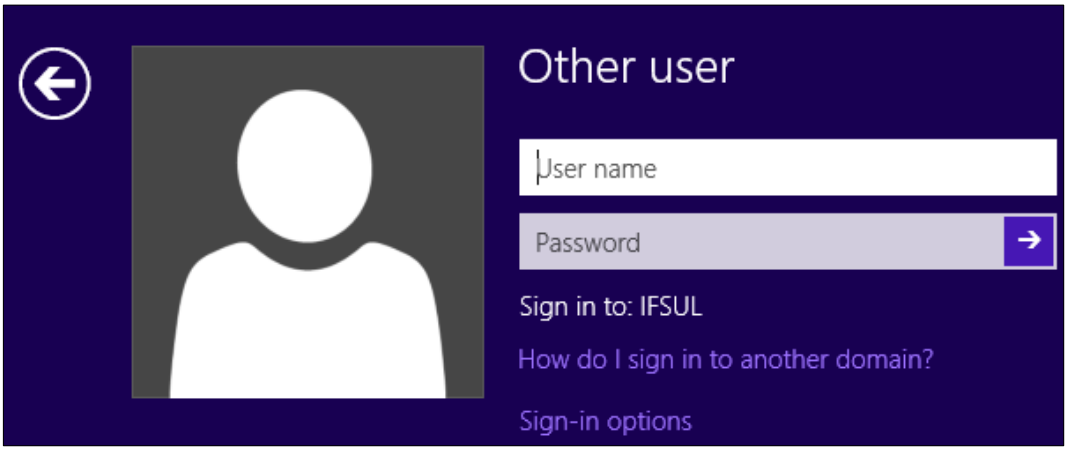
Se funcionou, o comando **klist** vai retornar a existência de um ticket para o administrador.

Figura 4: Após a alteração, foi exibido o arquivo krb5.conf na tela, para fins de demonstração

```
root@sambaserver:/etc# kinit administrator@IFSUL.EDU
Password for administrator@IFSUL.EDU:
Warning: Your password will expire in 41 days on Qua 24 Jun 2015 17:23:55 BRT
root@sambaserver:/etc# cat krb5.conf
[libdefaults]
        default_realm = IFSUL.EDU
        dns_lookup_realm = false
        dns_lookup_kdc = true
root@sambaserver:/etc# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: administrator@IFSUL.EDU

Valid starting       Expires              Service principal
13-05-2015 20:11:38  14-05-2015 06:11:38  krbtgt/IFSUL.EDU@IFSUL.EDU
        renew until 14-05-2015 20:11:32
```

Figura 5: Login do Windows 8 identificando o domínio



Na Figura 5, o Windows 8 identificou o domínio IFSUL que está sendo disponibilizado via AD pelo servidor SAMBA.

No servidor samba foi criado um usuário “teste” com a senha “teste1230” com o comando

samba-tool user add teste

Ao testar o login “teste” com a senha “teste1230” no Windows 8, um usuário foi criado na máquina local Windows, e pode usar o computador normalmente.

Como pode ser visto na Figura 6, foi verificado os processos e a lista de usuários no SAMBA

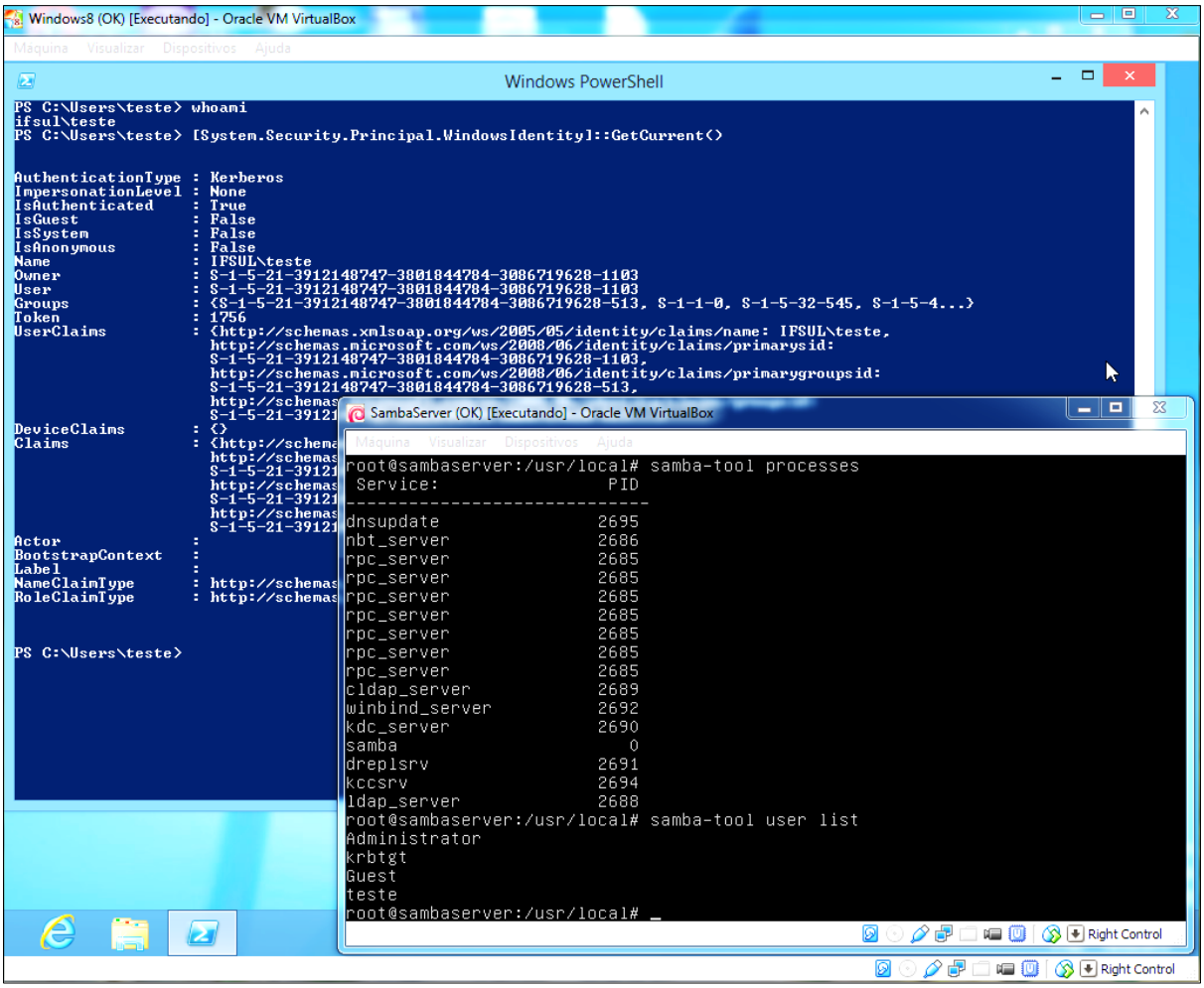
Samba-tool processes

Samba-tool user list

No Windows 8 foi verificado o AD no PowerShell com o comando

[System.Security.Principal.WindowsIdentity]::GetCurrent()

Figura 6: Máquinas Virtuais - Windows 8 sob AD do Samba 4.1 em Debian 7.8



APÊNDICE C – ARTEFATOS DE TESTE

Conteúdo dos arquivos bath utilizados para efetuar os testes, que foram criados no cliente Windows 8.

Teste de criação de OUs
adtest -r NewRoot -f teste.ats -user teste -password Teste123 -root 0 -t 100 -sf -e -o newroot.log

Teste de criação de usuários
adtest -r AddUser -f teste.ats -user teste -password Teste123 -root 0 -t 100 -sf -e -o adduser.log

Teste da criação de Grupos
adtest -r AddGlobalSecurityGroup -f teste.ats -user teste -password Teste123 -root 0 -t 1 -sf -e -o creategroups.log >> test3.txt

Teste de adição dos usuários nos grupos
for /l %%i in (0,1,99) do adtest -r AddMembers -f teste.ats -user teste -password Teste123 -root 0 -t 1 -sf -e -set GROUP=%%i -o temp%%i.log
copy/b temp*.log addmembers.log
del/q temp*.log

Teste de NT Logon
adtest -r NTLM_Logon -f teste.ats -user teste -password Teste123 -root 0 -t 6 -sf -e -o LogonNT.log

Teste de atualização de atributos
adtest -r Update_10Attr -f teste.ats -user teste -password Teste123 -root 0 -t 6 -sf -e -o updateattr.log

Teste de pesquisa de atributos
adtest -r Search_Base_10Attr -f teste.ats -user teste -password Teste123 -root 0 -t 6 -sf -e -o searchattr.log

Teste de Logon com Kerberos
adtest -r Kerberos_Logon -f teste.ats -user teste -password Teste123 -root 0 -t 6 -sf -e -o kerberos.log

Os resultados dos testes foram disponibilizados on-line[3]

[3] Disponível em https://goo.gl/XWwVij

Arquivo teste.ats com as diretivas de teste, fortemente baseado no documento distribuído pela Microsoft, conforme pode ser visto no quadro abaixo.

```
001 //---------------- DEFINIÇÕES ----------------------//
002 // [ROOT] é especificamente uma linha de comando(e.g. -r 32 for [ROOT] = 32)
003 //Numero de Usuários na Unidade Organizacional
004 #define $DefaultRange #(0-99)
005 //Usuários são formatados como u0001_0001
006 #define $Padding ######
007 #define $UserName u##([ROOT])_$Padding(*)
008 //Hierarquia da Unidade Organizacional
009 #define $Division ou##([ROOT])_division
010 #define $Unit ou##([ROOT])_unit
011 #define $Team ou##([ROOT])_team
012 #define $DivisionBranch ou=$Division,ou=BaseOU,[DOMAIN]
013 #define $UnitBranch ou=$Unit,ou=$Division,ou=BaseOU,[DOMAIN]
014 #define $TeamBranch ou=$Team,ou=$Unit,ou=$Division,ou=BaseOU,[DOMAIN]
015 #define $FQDN
cn=$UserName,ou=$Team,ou=$Unit,ou=$Division,ou=BaseOU,[DOMAIN]
016 #define $BaseOU ou=BaseOU,[DOMAIN]
017 #define $GroupOU ou=Groups,ou=BaseOU,[DOMAIN]
018 //---------------- TESTES ----------------------//
019 //---------------- AUTENTICAÇÕES -------------//
020 NTLM_Logon
021 {
022    TEST [LOGON]
023    LOOP RAND
024    RANGE $DefaultRange
025    DN $UserName
026    PWD ss-123456!T
027    OP LOGON32_LOGON_NETWORK
028    SCOPE LOGON32_PROVIDER_WINNT40
029 }
030 Kerberos_Logon
031 {
032    TEST [LOGON]
033    LOOP RAND
034    RANGE $DefaultRange
035    DN $UserName
036    PWD ss-123456!T
037    OP LOGON32_LOGON_INTERACTIVE
038    SCOPE LOGON32_PROVIDER_DEFAULT
039 }
040 //-------------------- ATUALIZAÇÕES -------------------------//
041 Update_10Attr
042 {
```

```
043    TEST [MODIFY]
044    LOOP RAND
045    OP LDAP_MOD_REPLACE
046    RANGE $DefaultRange
047    DN $FQDN
048    ATTR homePhone:###(0-999)-###(0-999)-####(0-9999)
049    ATTR pager:###(0-999)-###(0-999)-####(0-9999)
050    ATTR mobile:###(0-999)-###(0-999)-####(0-9999)
051    ATTR facsimileTelephoneNumber:###(0-999)-###(0-999)-####(0-9999)
052    ATTR ipPhone:###(0-999)-###(0-999)-####(0-9999)
053    ATTR company:Microsoft
054    ATTR title:Program Manager
055    ATTR postOfficeBox:101010
056    ATTR streetAddress:1 Microsoft Way
057    ATTR postalCode:98052
058 }
059 //-------------------- BUSCA ----------------------//
060 Search_Base_10Attr
061 {
062    TEST [SEARCH]
063    LOOP RAND
064    RANGE $DefaultRange
065    DN $FQDN
066    FILTER (objectClass=*)
067    SCOPE LDAP_SCOPE_BASE
068    ATTR postalCode;postOfficeBox;preferredLanguage;roomnumber;streetAddress
069    ATTR homePhone;ipPhone;telephonenumber;title;wWWHomePage
070 }
071 //-------------------- CONFIGURAÇÃO -------------------------//
072 // A ordem desses testes não é importante, mas são processados mais
073 // rapidamente no tempo de inicialização se você definir primeiro os
074 // os testes internos (ex: AddDivision) e depois os tests externos (ex: NewRoot).
075 // Usando NewRoot para executar AddDivision, AddUnit e AddTeam de uma só vez
076 AddDivision
077 {
078    TEST [ADD]
079    LOOP SEQ | ONCE
080    OP LDAP_MOD_ADD
081    DN $DivisionBranch
082    ATTR ObjectClass:organizationalUnit
083    ATTR name:$Division
084    ATTR instanceType:4
085 }
086 AddUnit
087 {
088    TEST [ADD]
089    LOOP SEQ | ONCE
090    OP LDAP_MOD_ADD
```

```
091     DN $UnitBranch
092     ATTR ObjectClass:organizationalUnit
093     ATTR name:$Unit
094     ATTR instanceType:4
095 }
096 AddTeam
097 {
098     TEST [ADD]
099     LOOP SEQ | ONCE
100     OP LDAP_MOD_ADD
101     DN $TeamBranch
102     ATTR ObjectClass:organizationalUnit
103     ATTR name:$Team
104     ATTR instanceType:4
105 }
106 NewRoot
107 {
108     RANGE #(1)
109     LOOP SEQ | ONCE
110     TEST AddDivision
111     TEST AddUnit
112     TEST AddTeam
113 }
114 AddUser
115 {
116     TEST [ADD]
117     LOOP SEQ | ONCE
118     OP LDAP_MOD_ADD
119     RANGE $DefaultRange
120     DN $FQDN
121     ATTR ObjectClass:user
122     ATTR userAccountControl:66048
123     ATTR cn:$UserName
124     ATTR SAMAccountName:$UserName
125     ATTR userPrincipalName:$UserName
126     ATTR aCSPolicyName:UnicodeString
127     ATTR adminCount:1
128     ATTR adminDescription:Uni
129     ATTR adminDisplayName:Uni
130     ATTR comment:Uni
131     ATTR company:Microsoft
132     ATTR CountryCode:8
133     ATTR department:Windows2003CapacityPlanning-$Padding(*)
134     ATTR description:Uni
135     ATTR desktopProfile:UnicodeString
136     ATTR destinationIndicator:PrintableString
137     ATTR displayName:$UserName
138     ATTR displayNamePrintable:UniP
```

```
139     ATTR division:Uni
140     ATTR employeeID:Uni
141     ATTR extensionName:23456
142     ATTR facsimileTelephoneNumber:425-555-1227
143     ATTR givenName:$UserName
144     ATTR groupPriority:UnicodeString
145     ATTR homeDirectory:UnicodeString
146     ATTR homeDrive:Uni
147     ATTR homePhone:425-555-1218
148     ATTR ipPhone:425-555-1217
149     ATTR initials:Uni
150     ATTR maxStorage:3
151     ATTR mhsORAddress:Uni
152     ATTR mobile:425-555-1216
153     ATTR otherHomePhone:425-555-1215
154     ATTR otherIpPhone:Uni
155     ATTR otherMailbox:Uni
156     ATTR otherMobile:425-555-1213
157     ATTR otherPager:425-555-1214
158     ATTR otherTelephone:425-555-1220
159     ATTR pager:425-555-1219
160     ATTR personalTitle:PM
161     ATTR physicalDeliveryOfficeName:Uni
162     ATTR postalAddress:Uni
163     ATTR postalCode:Uni
164     ATTR postOfficeBox:Uni
165     ATTR preferredLanguage:English
166     ATTR roomnumber:1326
167     ATTR streetAddress:Uni
168     ATTR telephonenumber:425-555-1212
169     ATTR title:SDE
170     ATTR wWWHomePage:www.microsoft.com
171     ATTR userPassword:ss-123456!T
172 }
173 AddGlobalSecurityGroup
174 {
175     TEST [ADD]
176     LOOP SEQ | ONCE
177     OP LDAP_MOD_ADD
178     RANGE #(0-99)
179     DN cn=GrpAcc_$Padding(*),$GroupOU
180     ATTR ObjectClass:group
181     ATTR groupType:-2147483646
182     ATTR name:GrpAcc_$Padding(*)
183     ATTR sAMAccountName:GrpAcc_$Padding(*)
184     ATTR instanceType:4
185 }
186 AddMembers
```

```
187 {
188    TEST [MODIFY]
189    LOOP SEQ | ONCE
190    OP LDAP_MOD_ADD
191    RANGE $DefaultRange
192    DN cn=GrpAcc_$Padding([GROUP]),$GroupOU
193    ATTR member:$FQDN
194 }
```