

Centro Universitário de Brasília Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

LEONARDO COSTA LIMA SILVA

UM ESTUDO SOBRE SERVIÇO DE DIRETÓRIO E FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO

Brasília 2015

LEONARDO COSTA LIMA SILVA

UM ESTUDO SOBRE SERVIÇO DE DIRETÓRIO E FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como prérequisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança da Informação.

2015

LEONARDO COSTA LIMA SILVA

UM ESTUDO SOBRE SERVIÇO DE DIRETÓRIO E FERRAMENTAS DE SEGURANÇADA INFORMAÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Redes de Computadores com Ênfase em Segurança da Informação.

Brasília, ____ de _____ de 2015.

.

Banca Examinadora

Prof. Dr.

Prof. Dr. Nome completo

AGRADECIMENTO(S)

Agradeço todo o apoio, compreensão e paciência, em tempos muitos difíceis, a minha namorada Natássia Caroline e ao meu chefe Romulo Rosa.

"Que homem é o homem que não torna o mundo melhor". Frase retirada do filme Cruzadas.

RESUMO

Este trabalho tem por objetivo abordar o serviço de diretório e a sua importância tanto na operação, manutenção e controle de redes como na segurança dos dados de empresas de todos os portes, bem como mostrar diferentes ferramentas de gerenciamento de diretório, abordando com mais perícia o funcionamento, as diferenças e dificuldades entre ferramentas muito conhecidas no mercado: O Active Directory e o OpenLDAP. Para mostrar as diferenças entre essas ferramentas em termos de segurança, foram usadas, como parâmetro, três regras básicas de segurança conforme padronização internacional ISO 27001, a autenticação de usuários, a administração de políticas de segurança e a segurança no compartilhamento de arquivos, além do próprio processo de instalação e configuração de cada ferramenta. O presente trabalho mostra os detalhes de configuração e de funcionamento dessas ferramentas, concluindo que as ferramentas são eficazes guando testadas, porem a complexidade de configuração e nível de conhecimento necessários para realizar os testes são diferentes, sugerindo que a ferramenta Active Directory é mais amigável, facilitando para o administrador de uma rede realizar sua instalação e configuração com uma interface interativa e acesso fácil à tutorias completos tanto de sítios especializados como do sítio do fabricante. Já a ferramenta de distribuição gratuita, o OpenLDAP, exige conhecimento avancado a nível de linha de comando com interface pouco amigável com acesso a tutoriais diversos de vários sítios para distribuições, o que faz com que muitas vezes seja necessário complementar informações de configuração com aquelas obtidas em fóruns de comunidade de pesquisa.

Palavras-chave: Serviço de Diretório. Active Directory. OpenLDAP. ISO 27001. Segurança.

ABSTRACT

This paper aims to introduce on the directory service and its importance in both the operation, maintenance and network control as well in security of all sizes of enterprises, over all, as showing different directory management tools with more precise focus on the distinct operation, differences and difficulties between two wellknown tools on the market, the Active Directory and OpenLDAP. To show the differences between these tools were used as parameter three basic security rules imposed by the international standard ISO 27001, user authentication, administration of security policies and security in file sharing, in addition to the installation process itself and configuration of each tool. This study shows the configuration and operating details of these tools. Concluding that the tools are effective when tested, however the complexity of configuration and level of knowledge required to perform the tests are different, suggesting that the Active Directory tool is more user friendly and interactive, making it easier for the administrator to perform a network installation and configuration, an interactive interface and easy access to complete tutorials from both specialized websites and manufacturer website. Already tool free distribution, OpenLDAP, requires advanced knowledge level of the command line with unfriendly interface with access to numerous tutorials from various sites for various distributions and who are not always applicable, in addition the support is based on forums searches.

Key words: Directory Service. Active Directory. OpenLDAP. ISO 27001. Segurança.

SUMÁRIO

INTRODUÇÃO	10
1 O SURGIMENTO DO SERVIÇO DE DIRETÓRIO	12
1.1 Serviço de Diretório	12
1.1.1 OpenLDAP	13
1.1.2 Edirectory	13
1.1.3 Microsoft Active Directory	14
1.2 Autenticação	14
2 MICROSOFT ACTIVE DIRECTORY	16
2.1 Identidade e Acesso	16
2.2 Domínio do Active Directory	17
2.3 Infraestrutura IDA	18
2.4 Componentes do Active Directory	20
2.4.1 Armazenamento de Dados	<u>21</u>
2.4.2 Controladores de Domínio	21
2.4.3 Unidades Organizacionais	22
2.4.4 Domínio	23
2.4.5 Floresta	23
2.4.6 Árvore	24
2.4.7 Replicação	<u>24</u>
2.4.8 Sites	25
2.4.9 Relação de Confiança	25
3 OpenLDAP	27
3.1 Identidade Única	28
3.2 Entrada LDAP	29
3.3 Árvore de Informações do Diretório	30
3.4 Componentes do OpenLDAP	30
3.4.1 Servidores	31
3.4.2 Clientes	32
3.4.3 Utilitários	32
3.4.4 Bibliotecas	32
4 ISO 27001	33
4.1 Objetivos de Controle	34

4.2 Objetivos de Controle Aplicados aos Sistemas de Serviço de			
Diretório	35		
5 ISO 27001 APLICADA AO ACTIVE DIRECTORY E AO OPENLDAP E	M		
AMBIENTE DE TESTE PARA FINS COMPARATIVOS EM PARAMETR	OS		
EQUIPARADOS	37		
5.1 Testes com o Microsoft Active Directory	37		
5.1.1 Configurar IP Estático	37		
5.1.2 Verificação do Nome do Servidor	40		
5.1.3 Instalação do Serviço de Diretório	<u>41</u>		
5.1.4 Desafio ao Active Directory	56		
5.1.5 Criação de Usuários	56		
5.1.6 Criação dos Grupos	58		
5.1.7 Inclusão de Servidores e Clientes no Domínio	<u>61</u>		
5.1.8 Experimento 1 – Criação de Políticas de Segurança e Verificação d	los		
resultados	67		
5.1.8.1 Editar	73		
5.1.8.2 Verificar a Política Aplicada	76		
5.1.9 Experimento 2 - Criação de Política de Acesso em Pastas de Serv	idor de		
Arquivos e Verificar os Resultados	81		
5.1.9.1 Criação de Pastas no Servidor de Arquivos	81		
5.1.9.2 Criação da Política de Acesso ás Pastas de Armazenamento de A	Arquivos		
	82		
5.1.9.3 Verificação da Eficácia da Política de Acesso as Pastas	85		
5.2 Testes com o OpenLDAP	88		
5.2.1 Criar um domínio com um banco de usuários	91		
5.2.2 Por que SAMBA?	93		
5.2.3 Testes Samba	94		
5.2.3.1 Instalação do Ubuntu Server 14.04	94		
5.2.3.2 Configuração do Controlador de Domínio	108		
5.2.3.3 Configurar IP Estático	110		
5.2.3.4 Modificar o Nome do Computador	112		
5.2.3.5 Atualizar o Sistema	114		
5.2.3.6 Pré-requisitos	115		
5.2.3.7 Instalação do SAMBA	118		

5.2.3.8 Criação do Domínio	120
5.2.3.9 Configuração do DNS	121
5.2.3.10 Configurar o Kerberos	123
5.2.3.11 Pastas para Usuários	126
5.2.3.12 Senha de Administrador	128
5.2.3.13 Configurar IP da Máquina Cliente	129
5.2.3.14 Adicionar Computador Cliente no Domínio	133
5.2.3.15 Instalar as Ferramentas de Gerencia do Domínio	136
5.2.3.16 Autenticação no Domínio	141
CONCLUSÃO	150
REFERÊNCIAS	152

INTRODUÇÃO

É possível observar que ferramentas básicas de segurança de tecnologia da informação nos dias de hoje são montadas sobre sistemas de diretório. Os sistemas de diretório armazenam informações de pessoas, objetos ou qualquer matéria que possa ser catalogada em um banco de dados que permita consulta a qualquer momento. Porém, a consulta às informações armazenadas no banco de diretórios podem ser controladas de várias formas, com ferramentas distintas. Essas ferramentas garantem a segurança da informação.

O presente estudo apresenta uma introdução aos serviços de diretório e às ferramentas de gerenciamento de serviços de diretório Microsoft Active Directory e OpenLDAP para Linux. Propõe uma comparação de esforço e acesso ao conhecimento para instalar e configurar sistemas de diretório com uma segurança baseada na ISO 27001, utilizando ambiente virtualizado.

O objetivo do presente trabalho é comparar duas ferramentas muito utilizadas de gerenciamento de diretório, no caso o Active Directory e OpenLDAP, capazes de aplicar segurança de acesso a informação nos quesitos: praticidade, compatibilidade, esforço, acesso ao conhecimento, eficácia e eficiência, além de, mostrar uma configuração possível em laboratório onde o Linux e o Windows coexistem em um ambiente com serviço de diretório.

Para alcançar esse objetivo, procedeu-se da seguinte maneira, foi feita a instalação dos sistemas operacionais Windows Server e Ubuntu Server, ambos capazes de suportar o Active Directory e o OpenLDAP respectivamente. Em seguida a instalação e configuração do Active Directory e do OpenLDAP com os serviços de autenticação e controle de usuário a partir de um domínio, aplicação de política de segurança quanto à complexidade de senhas e o compartilhamento com controle de acesso a arquivos e pastas. Um servidor Linux foi montado como servidor de diretórios e uma máquina Windows como interface gráfica para manipulação do diretório.

Espera-se demonstrar com este estudo a importância da segurança aplicada ao serviço de diretório e principalmente a formação de opinião quanto às necessidades em torno das ferramentas apresentadas neste trabalho e ainda apresentar uma solução para que essas ferramentas coexistam para funcionamento de um serviço de diretório.

O presente trabalho foi então estruturado em 5 capítulos, como a seguir.

No primeiro capítulo, apresentam-se uma introdução ao sistema de diretório. O que é, para que serve e como funciona alguns tipos de gerenciadores de sistemas de diretório. O segundo capítulo é focado no funcionamento do básico do Microsoft Active Diretory. O terceiro capítulo, apresenta o foco no gerente de sistema de diretório OpenLDAP. No quarto é apresentado a ISO 27001 e os parâmetros nela contidos que serão usados nos testes dos programas. O quinto e último capítulo é apresentado como foram feitos os testes com as duas ferramentas nas mesmas condições de ambiente com os mesmos parâmetros de segurança além da solução para coexistência das ferramentas.

1 O SURGIMENTO DO SERVIÇO DE DIRETÓRIO

Sabemos que no início da humanidade a comunicação era limitada somente a gestos e grunhidos. Com o crescimento da humanidade a comunicação sofreu vários avanços ganhando forma e sofisticação. Fica perceptível que com o passar dos anos a comunicação passou a ter um valor comercial, dependendo do seu conteúdo. Cada Informação trocada passou a ter um grau importância.

Na época em que começaram a haver guerras por exemplo, a informação passada entre os comandantes precisava ser protegida. E muitos morreram para proteger esse tipo de informação por tentar protege-la.

Após o advento do micro computador percebeu-se a necessidade de continuar protegendo a informação, principalmente com o surgimento das redes de comunicação de computadores.

Em 1967 a primeira rede de comunicação de computadores de diferentes fabricantes estava pronta. Através de um IMP (*Interface Message Processor*), máquina ao qual vários computadores eram interligados, foi feita a comunicação entre máquinas de diferentes fabricantes por meio de tradução. (FOROUZAN; FEGAN, 2008).

Quando computadores passaram a ter acesso a outros computadores foi preciso fazer planos para proteger a informação: políticas de segurança; antivírus; departamentos de segurança da informação; entre outros.

Foi a partir dessa ideia de controle de acesso a informação que várias corporações que primam por segurança da informação desenvolveram sistemas para controlar esse acesso, entre esses sistemas está o sistema de serviço de diretório.

1.1 Serviço de Diretório

O serviço de diretório de rede é um serviço que gerencia objetos de uma rede de forma a fazer o controle de acessibilidade, protocolos de comunicação,

certificação digital entre outros, em recursos da rede como usuários, computadores, pastas, documentos e aplicações utilizando o método de autenticação. Alguns conceituam o serviço de diretório como sendo apenas uma comparação com o serviço prestado por uma lista telefônica que armazena dados para busca. No entanto o serviço de diretório engloba tanto o armazenamento de informações como o gerenciamento das mesmas através de ações específicas.

Hoje no mercado, as aplicações de serviço de diretório que estão entre as mais conhecidas e implantadas são: (MARINHO, 2013)

- OpenLdap para sistemas open source;
- Edirectory para sistemas Novell;
- Active Directory para sistemas Microsoft com suporte aos acima sitados.

1.1.1 OpenLDAP

O Open Ldap (*Lightweight Directory Access Protocol*) é um serviço de diretório aberto, ou seja, seu código fonte pode ser modificado, permitindo dessa forma a incorporação completa de serviços que são realizados por sistemas operacionais de rede. É bastante utilizada em plataforma Linux para construção de serviços de diretório distribuídos. Em comparação com outras soluções de diretórios, o Open Ldap apresenta um bom grau de tolerância a falhas e bom desempenho. (RIBEIRO et al., 2004)

1.1.2 Edirectory

O Edirectory foi desenvolvido pela Novell, que criou um serviço de diretório *standalone* e *cross-plataform* para suportar *e-commerce*, relacionamento B2B e aplicações em *internet*, também trabalhando com o FSD (*Full Service Directory*), um banco de dados genérico que gerencia busca, descoberta,

segurança, armazenamento e relacionamentos de objetos. (SHERESH; SHERESH, 2002)

1.1.3 Microsoft Active Directory

O Active Directory (AD) é o sistema operacional de diretório de rede da *Microsoft*, construído sobre o *Windows* 2000 e o *Windows Server* 2003. Esse sistema operacional habilita administradores de redes gerenciar quase toda a informação da rede eficientemente de um repositório central que pode ser globalmente distribuído. Uma vez que informações sobre usuários e grupos, computadores e impressoras, aplicações e serviços são adicionadas ao *Active Directory* também se tornam disponíveis para uso em toda a rede para todos os objetos da rede que os administradores do sistema derem autorização de acesso. (RICHARDS et al., 2006)

1.2 Autenticação

Em sua essência autenticação significa o que o próprio nome diz, processo de verificação de autenticidade. O processo da autenticação é encontrado em praticamente todos os serviços de diretório. Mas o propósito principal de se ter o um processo de autenticação em um serviço de diretório é de verificar se objetos que estão fora de uma rede pertencem ou não aquela rede e se devem ou não ter acesso a outros objetos dentro da mesma. A autenticação é feita quase da mesma forma na maioria dos serviços de diretório.

Existem dois tipos de autenticação:

- Local ou interativa: O usuário faz uma autenticação diretamente a um computador, assim camo quando é feito o acesso a um *laptop*.
- Remoto ou de rede: O usuário que está em seu laptop faz uma autenticação em outro computador para ter acesso a outros

recursos da rede como em um servidor de arquivos ou de email para acessar recursos específicos dos mesmos.

2 MICROSOFT ACTIVE DIRECTORY

Faz parte do trabalho de um profissional de TI, conectar usuários de uma rede com a informação necessária para que eles façam seu trabalho. Devido aos usuários precisarem de diferentes níveis de acesso e diferentes classes de informação é preciso associar o usuário correto à um nível de acesso específico para proteger a informação.

Existem várias formas de proteger e classificar uma informação:

- Identidade e Acesso (IDA): Usuários e outros ativos de segurança, que pode incluir também computadores, serviços e grupos são chamados de identidades ou contas aos quais é dado acesso (permissões) a informações, recursos, ou sistemas.
- Autenticação, Autorização, Identificação (AAA):Usuários fornecem um nome de usuário e uma senha que são autenticadas quando suas credenciais são validas. Os usuários recebem permissões (controle de acesso) que são usados para autorizar as requisições de acesso. O acesso é monitorado, provendo identificação de audição.
- Confidencialidade, Integridade e Disponibilidade (CIA): A informação é protegida para garantir que não é acessível para usuários não autorizados (confidencialidade), não é modificada incorretamente (integridade) intencionalmente ou acidentalmente, e disponível sempre que necessário (disponibilidade).

2.1 Identidade e Acesso

O Active Directory é o serviço de diretório fabricado pela Microsoft e feito para funcionar em um ambiente de redes com Windows. Em um sistema protegido cada usuário é representado por um uma identificação. Nos sistemas Windows, a identidade é a conta do usuário. As contas de um ou mais usuários são colocadas em um armazenamento de identidades, que também é conhecido como banco de dados de diretório. Uma identidade é chamada de objeto de segurança nos sistemas Windows. Os objetos de segurança são unicamente identificados por um atributo chamado de identidade de segurança (SID).

Do outro lado do sistema está o recurso o qual o usuário requer acesso. O recurso está segurado com permissões, e cada permissão tem um nível de acesso específico. Muitos recursos do Windows são segurados por um descritor de segurança que contém uma lista de controle de acesso discricionária (DACL) em que cada permissão tem a forma de uma entrada de controle de acesso (ACE).

O sistema tem um funcionamento simples, é preciso apenas mapear o SID de um usuário a seu ACE apropriado de um recurso. (MICROSOFT, 2011)

2.2 Domínio do Active Directory

Quando um usuário precisa fazer acesso a sua máquina ele é questionado quanto suas credencias armazenadas dentro computador. Cada computador mantem somente um único armazenamento confiável: uma lista local de usuários e grupos armazenados em um registro, o banco de dados Gerente de Contas de Segurança (SAM).

Se o usuário precisar acessar uma pasta compartilhada em um servidor através de seu computador, não será bem sucedido. Isso devido a que cada computador confia no seu próprio banco de credencias SAM. Se por acaso o usuário tiver suas credencias catalogadas no SAM do servidor em que se encontra a pasta compartilhada identicamente às credenciais do SAM em seu computador, o acesso será permitido sem problemas. Mas se alguém trocar qualquer detalhe nas credenciais tanto do servidor como do computador do usuário, as credencias do SAM das duas maquinas não estarão mais sincronizadas, por tanto não será possível fazer o acesso conforme desejado. Se mais usuários forem adicionados no SAM dos servidores de pastas compartilhadas a probabilidade de algum usuário não estar sincronizado é muito grande.

Para resolver esse problema a Microsoft criou um SAM centralizado, onde nenhum usuário precisa ter um cadastro idêntico em cada computador da rede, mas

sim cada usuário tem apenas um cadastro em um banco de identidades confiável para todos os computadores. Esse banco de credenciais centralizado faz parte da infraestrutura de domínio e florestas do Active Directory.

Um domínio do Active Directory provê um armazenamento de identidades centralizado e confiável para todos os computadores que fazem parte do domínio. Um domínio também fornece um serviço de autenticação centralizada. Tanto o armazenamento de identidades como os serviços de autenticação centralizados, junto com outros serviços e componentes, são armazenados em um servidor fazendo o papel de um controlador de domínio.

2.3 Infraestrutura IDA

Uma infraestrutura de identidade de acesso ou IDA é necessária para manter a segurança de recursos de uma empresa como arquivos, e-mails, aplicações e banco de dados. Seu funcionamento se caracteriza da seguinte forma:

> • Armazenar informações de usuários, grupos, computadores e outras identidades. Uma identidade é uma representação de uma entidade que tomará ações dentro de uma rede empresarial. Por exemplo um usuário abre documentos dentro de uma pasta compartilhada. Quando esse usuário acessa um documento dentro da rede ele passará por uma lista de controle de acesso ou ACL. O acesso a documentos dentro da rede é gerenciado pelo subsistema de segurança do servidor que compara a identidade do usuário com as identidades dentro da ACL para determinar se a solicitação do usuário de acessar o documento é permitida ou negada. Computadores, grupos, serviços e outros objetos também têm uma identificação. Junto com cada identificação de objeto estão as propriedades desse objeto formando uma identificação única, como um nome de usuário ou um SID e o password da identidade. O armazenamento de identidades é um componente da infraestrutura IDA. O armazenamento de dados do Active Directory também conhecido como diretório é um armazenamento

de identidades. O diretório é localizado dentro de um controlador de domínio, um servidor fazendo papel de AD DS, que também faz seu gerenciamento.

- Autenticar uma identidade. O servidor não vai assegurar acesso a um usuário a não ser que o servidor verifique que a identidade apresentada na solicitação de acesso seja válida. Para validar a identidade o usuário fornece um segredos apenas conhecidas pelo próprio usuário e pela infraestrutura IDA. Esses segredos são comparados com a informação no armazenamento de identidades em processo chamado de autenticação.
- Em domínio do Active Directory, um protocolo chamado Kerberos é usado para autenticar identidades. Quando um usuário ou um computador faz um *login* (acesso) no domínio, o Kerberos autentica as credenciais e verifica um pacote de informações chamado TGT (ticket granting ticket). Antes do usuário se conectar ao servidor para requisitar um documento, uma solicitação Kerberos é enviada para o controlador de domínio junto com o TGT que serve para identificar o usuário autenticado. O controlador de domínio verifica outro pacote de informação do usuário chamado ticket de serviço que identifica o usuário autenticado ao servidor. O usuário apresenta o ticket de serviço ao servidor, que aceita o ticket de serviço como prova que o usuário foi autenticado.
- Essas transações Kerberos resultam em um acesso único na rede ou single sign-on. Após o usuário ou computador ter inicialmente acessado a rede e tenha coletado um TGT, o usuário está autenticado dentro de todo o domínio e pode estar conseguindo tickets de serviço que identificam o usuário a qualquer serviço. Toda essa atividade com tickets é gerenciada pelos clientes Kerberos e serviços construídos no Windows, é transparente para o usuário.

- Controle de acesso. A infraestrutura IDA é responsável por proteger informações confidenciais como informações armazenadas em um documento. Acesso a documentos confidenciais precisam ser gerenciados de acordo com as políticas de segurança da empresa. Uma ACL para um documento reflete uma política de segurança que contem permissões que especificam níveis de acesso a identidades específicas. O subsistema do servidor neste exemplo está realizando a funcionalidade de controle de acesso em uma infraestrutura IDA.
- Prover uma trilha de auditoria. Uma empresa deve querer monitorar as mudanças e atividades dentro da infraestrutura IDA, então é preciso fornecer um mecanismo para gerenciar auditoria.

2.4 Componentes do Active Directory

Abaixo estão os componentes que estão entre os principais do Active Directory:

- Armazenamento de Dados;
- Controladores de Domínio;
- Unidades Organizacionais:
- Domínio;
- Floresta;
- Arvore;
- Replicação;
- Sites;
- Relações de Confiança.

2.4.1 Armazenamento de Dados

O serviço de domínio do *Active Directory* armazena as identidades em um diretório que fica dentro de um controlador de domínio. O diretório é um arquivo único chamado de ntds.dit, e seu local padrão é na pasta %systemroot%\ntds dentro de um controlador de domínio.

O banco de dados é dividido em algumas partições:

- Schema: Define o atributo e os tipos dos objetos que podem ser armazenados no diretório.
- Contexto de Nomeação do Domínio (NC do Domínio): Contém dados sobre os objetos do domínio como, usuários, grupos e computadores. Quando é feita uma alteração no índice usuários e computadores do Active Directory, como adicionar um usuário ou computador, o conteúdo do NC do domínio é modificado.
- Configuração: Contém informações sobre domínios, serviços e topologia.
- DNS: Contém informações e recursos do DNS.
- Configuração de Atributos Parcial (PAS): É a partição usada pelo catálogo global.

O Active Directory também armazena informações em uma pasta chamada SYSVOL. Por padrão esta pasta é localizada em %systemroot%\SYSVOL. Contém itens como *scripts* de *logon* e arquivos relacionados a políticas de grupo (GPOs). (MICROSOFT, 2011)

2.4.2 Controladores de Domínio

Controladores de domínio também conhecidos como DCs tem a função de serviço de domínio. Parte dessa função dessa função é reter e replicar o banco de dados do Active Directory (NTDS.DIT) e SYSVOL. Os DCs também executam o Centro de Distribuição de Chaves Kerberos (KDC) que realiza autenticação e outros serviços do Active Directory.

Devido a autenticação ser crítica para uma empresa a melhor pratica é sempre ter a disposição dois DCs, pois se usuários tiverem problemas de acesso a um deles podem ser autenticas no outro disponível. (MICROSOFT, 2011)

2.4.3 Unidades Organizacionais

Uma unidade organizacional (OU) é um objeto do serviço de domínio do AD (AD DS) dentro do domínio que pode ser usado para tarefas específicas como:

- Organizar objetos dentro de um domínio. OUs contém objetos do domínio, como contas de usuários e computadores, e grupos. Compartilhamento de arquivos e impressoras que são publicados para o AD DS também são encontrados nas OUs.
- Delegar controle administrativo. Pode-se designar até controle administrativo completo, como a permissão de controle total, sobre todos os objetos na OU ou designar controle administrativo limitado, como a habilidade de modificar informações de email de objetos dentro da OU. Para delegar controle administrativo é preciso designar permissões especificas em uma OU e objetos que estão contidos na OU para um ou mais usuários e grupos.
- Simplificar o gerenciamento de recursos agrupados comumente. Usando OUs, podem-se criar containers que representam estruturas lógicas ou hierárquicas, na organização. Desta forma pode-se usar uma política de grupo para gerenciar a configuração das definições de usuário e computador baseado no modelo organizacional da empresa.

2.4.4 Domínio

Um ou mais controladores de domínio são necessários para criar um domínio do Active Directory. Um domínio é uma unidade administrativa onde certas capacidades e características são compartilhadas. Todos os controladores de domínio replicam a partição de armazenamento de dados do domínio, que contem, entre outras coisas, os dados de identidade dos usuários, grupos, e computadores do domínio. Desta forma todas os DCs mantem o mesmo armazenamento de identidade, ou seja, qualquer DC pode realizar a autenticação de uma identidade no domínio.

Um domínio é um escopo de políticas administrativas como complexidade de senha e políticas de bloqueio de senha. Essas políticas que são configuradas no domínio afetam todas as contas do domínio e não afetam as contas de outro domínio. (MICROSOFT, 2011)

2.4.5 Floresta

Uma floresta é uma coleção de um ou mais domínios do Active Directory. O primeiro domínio instalado em uma arvore é chamado de domínio raiz da floresta. Uma floresta tem uma definição única da configuração da rede e uma única instancia do schema do diretório. Cada controlador de domínio na floresta replica a partição da configuração e do schema, e essas duas partições são as mesmas para cada domínio da floresta, ou seja, não se pode ter mais de uma configuração e um schema em uma floresta. O domínio raiz da floresta contem contas administrativas de toda a floresta como a Enterprise Admin e Schema Admin. A conta Enterprise Admin tem privilégios administrativos em todos os dominós da floresta, podendo editar a estrutura da floresta adicionando ou removendo domínios, estendendo schema entre outros.

Uma floresta é uma instancia única no diretório, nenhuma informação do diretório é replicada para fora das barreiras da árvore. Porem a floresta define os limites de replicação e segurança. (MICROSOFT, 2011)

2.4.6 Árvore

A configuração de nome do Domain Name System (DNS) do domínio dentro de uma floresta pode criar árvores. Se um domínio é um subdomínio de outro domínio, esses domínios são considerados juntos uma árvore. Por exemplo se a floresta trayresearch.net contém dois domínios traysearch.net е antártica.traysearch.net, os domínios constituem uma porção contígua da configuração de nome do DNS portanto são considerados uma árvore. Se por ventura houver mais um domínio chamado proseware.com, que não é contíguo aos outros dois domínios então tem-se duas árvores na floresta. As árvores são resultados diretos dos nomes DNS escolhidos para os domínios em uma floresta.

2.4.7 Replicação

Os Serviços de replicação distribuem dados do diretório por toda a rede. Isso inclui armazenamento de dados e dados requeridos para implementar políticas e configuração, incluindo *scripts* de *logon*. O Active Directory matem uma partição separada dos dados armazenados chamados do configuração, que matem informações sobre a configuração da rede, a topologia e serviços.

O Active Directory também usa uma replicação multimaster para sincronizar as informações do diretório. A verdadeira replicação multimaster pode ser contrastada com outros serviços de diretório que utilizam a abordagem mestreescravo para as atualizações onde todas as atualizações precisam ser feitas no mestre depois copiadas para os escravos. A abordagem mestre-escravo é adequada para organizações com um números pequenos de cópias e onde as modificações podem ser feitas centralizadamente. No Active Directory nenhum DC é um mestre, ao invés disso, todos os DCs dentro de um domínio são equivalentes. Mudanças podem ser feitas em um DC que todos os outros serão sincronizados periodicamente. Na replicação multimaster não é necessário replicar para cada DC, o sistema implementa um robusto conjunto de conexões que determina que DC deve sincronizar informações com que outro DC. Isso garante que a rede não ficará sobrecarregada com trafego de replicações desta forma a latência de replicações não fica longa de forma a causar inconveniência a usuários. O conjunto de conexões por onde as modificações são replicadas para os DCs dentro de uma empresa é chamada de topologia de replicação. (MICROSOFT, 2011)

2.4.8 Sites

No Active Directory os sítios ou *sites* têm um significado especifico devido a uma classe de objeto especifica no AD chamada *site*.

Um site do Active Directory é um objeto que representa uma porção da empresa onde a conectividade de rede é boa. Um site cria um limite de replicação e utilização de serviços. Também é considerado um interpretação logica da rede física.

Controladores de domínio replicam mudanças dentro de um site em segundos. Mudanças são replicadas entre sites em uma base controlada assumindo que as conexões entre sites são lentas, caras ou não confiáveis. Ao criar um site é o mesmo que dizer ao Active Directory que existem vários controladores de domínio em lugares físicos na rede e que a conexão entre esses lugares é lenta. (MICROSOFT, 2011)

2.4.9 Relação de Confiança

Para um novo computador ser adicionado no domínio do Active Directory primeiro é preciso ter um usuário confiável, ou seja que tenha suas credenciais armazenadas no banco de dados do domínio, uma vez que esse usuário é autenticado no domínio estabelece-se uma relação de confiança entre o novo computador adicionado e o AD. O mesmo conceito pode ser estendido entre domínios. Um domínio pode autenticar usuários de outro domínio e ter permissão para esses usuários acessarem recursos do outro domínio. Isso é possível quando se estabelece uma relação de confiança entre domínios. (MICROSOFT, 2011)

3 OPENLDAP

OpenLDAP é um programa que utiliza o protocolo LDAP (*Lightweight Directory Access Protocol*) para fazer centralização de autenticação e banco de dados oferecendo um serviço de diretório.

O modelo geral do protocolo LDAP baseia-se em operações de protocolo realizadas entre um cliente e um servidor. Neste modelo, o cliente transmite uma solicitação de protocolo descrevendo a operação que será feita para um servidor. O servidor então é o responsável por realizar as operações necessárias no diretório. Uma vez completada as operações, o servidor então retorna uma resposta contendo o resultado ou erro ao cliente solicitante. (RFC 2251)

O protocolo LDAP é padronizado e assim como protocolos de rede, a estrutura de diretório e serviços providos por um servidor LDAP estão todos disponíveis em RFCs (*Requests for Comments*).

A versão mais atual do LDAP é a v.3 (versão 3), um padrão desenvolvido em 1997 na RFC 2251. A especificação original foi atualizada em 2006, e RFCs de 4510 a 4519 fornecem especificações mais claras e coesivas para o LDAP.

Alguns tipos de serviços de diretório apenas fornecem um serviço limitado e especifico. Um servidor de diretório com propósito único, assim com um dicionário de endereços, deve armazenar apenas um tipo especifico de dado, como números de telefone, endereços e informações de *e-mail* de algumas pessoas. Esses tipos de diretórios não são extensíveis, apenas tem um propósito único.

O LDAP foi desenvolvido para ser servidor de diretório com propósito geral ou seja, foi desenvolvido para que os administradores dos servidores possam definir que tipo de informação deve ser armazenado pelo servidor, com clareza e cuidado.

Um diretório genérico permite armazenar muitos tipos de informação, desta forma deve armazenar muitos tipos de informação sobre vários diferentes tipos de entidades. Por exemplo, um diretório de propósito geral deve armazenar informações sobre entidades como pessoas além de informações sobre amostras de pedras por exemplo. Mas as informações que serão armazenadas de pessoas não são as mesmas que seriam armazenadas sobre pedras.

Uma pessoa deve ter um nome de usuário, um telefone ou um e-mail, já uma pedra deve ter um número de identificação, informações sobre sua origem geográfica ou sua classificação de solidez.

O protocolo LDAP torna possível definir como uma entrada sobre pessoas deve parecer e como uma entrada sobre rochas deve parecer. Essa arquitetura geral fornece as capacidades necessárias para o gerenciamento de grandes quantidades de diversas entradas de diretório.

3.1 Identidade Única

A melhor forma de distinguir entre duas entradas muito similares é criar uma identidade única para cada entrada, cada dado, armazenado no diretório. Essa é a estratégia adotada pelo LDAP. Cada entrada de armazenamento no diretório tem um *distighished name* (nome distinguido) abreviado como DN.

Em um diretório LDAP, o criador do diretório é quem decide que componentes vão fazer parte do DN, mas tipicamente o DN reflete à sua localidade dentro do diretório, assim como algumas informações que distinguem essa entrada das outras semelhantes.

Uma DN então, é composta de uma combinação de informação de diretório por exemplo:

dn: o=Acme Services, l=Chicago, st=Illinois, c=US (BUTCHER, 2007)

Este único identificador é suficiente para distinguir entre uma empresa da cidade de *Springfield* com o mesmo nome. A DN da empresa de *Springfield* seguindo o mesmo raciocínio seria:

dn: o=Acme Services, l=Springfield, st=Illinois, c=US (BUTCHER, 2007)

Quando definindo que campos farão parte da DN, é necessário ter certeza de que os campos escolhidos serão suficientes para separar e distinguir entre duas diferentes entradas. Em outras palavras tudo que é preciso para quebrar a sintaxe da DN criada para o exemplo, é o surgimento de outra empresa, chamada *Acme Services* em Chicago.

3.2 Entrada LDAP

Uma entrada LDAP ou uma gravação LDAP, é a unidade do diretório que armazena a informação sobre um item individual dentro do diretório e essa entrada contém informações sobre uma unidade específica porem o alvo exato dessa unidades não é específico. Pode ser uma pessoa, uma rocha, uma empresa ou alguma entidade virtual como um objeto Java.

Uma entrada LDAP é composta de um DN e um ou mais atributos. O DN serve como um identificador único dentro da árvore de informação do diretório LDAP. Os atributos fornecem informações sobre a entrada.

A primeira linha é o DN e as outras linhas representam os atributos. Esse é um formato de entrada simples que será interpretada pelo diretório.

Existem muitas variações e regras que diferenciam um atributo do outro e essas regras são gravadas dentro de um *schema* (esquema) compacto, que o servidor de diretório mantém armazenado para consulta.

Os atributos não são sensíveis a caixa alta ou baixa. O atributo com nome o é tratado como sinônimo com nome O. Assim como, *GivenName*, *givenname* e *givenName* são todos avaliados como sendo o nome do mesmo atributo.

3.3 Árvore de Informações do Diretório

A informação em um diretório telefônico é tipicamente armazenado em uma lista alfabética. A informação em um diretório LDAP é organizado em uma ou mais hierarquias, onde no topo da hierarquia, existe uma entrada base e as outras entradas são organizadas abaixo como uma árvore que tem como base a entrada base. Cada nó na hierarquia é uma entrada, com uma DN e mais de um atributos.

Essa coleção de entradas organizadas hierarquicamente é chamada de Árvore de Informações do Diretório, também sendo referido como Árvore do Diretório ou DIT (*Directory Information Tree*).

Aplicações de dentro de uma organização podem fazer conexão com o diretório LDAP, autenticando seus usuários no diretório.

3.4 Componentes do OpenLDAP

O pacote Open LDAP é composto por quatro componentes principais:

- Servidores: Fornecem os serviços LDAP;
- Clientes: Manipulam os dados LDAP;
- Utilitários: Servidores LDAP de suporte;
- Bibliotecas: Fornecem interfaces de programação para o LDAP.

Esses quatro componentes funcionam conforme a figura 1 abaixo:



Figura 1 - Comunicação dos componentes do Open LDAP

Fonte - Adaptado de Butcher (2007)

3.4.1 Servidores

O Servidor principal do pacote LDAP é SLAPD (Stand-Alone LDAP Daemon). Este servidor fornece acesso a uma ou mais árvores de diretório. Os clientes conectam-se ao servidor através do protocolo LDAP, normalmente usando conexão de rede.

Um servidor pode armazenar dados de diretório localmente, ou acesso simples (ou acesso proxy) a fontes externas. Tipicamente, fornece autenticação e serviços de busca e também pode suportar adição, remoção e modificação de dados do diretório. Isso fornece controle de acesso ao diretório.

3.4.2 Clientes

Clientes acessam os servidores LDAP através do protocolo de rede LDAP. Seu funcionamento se caracteriza por requisitar que o servidor realize operações especificas. Tipicamente o cliente primeiro irá se conectar as servidor de diretório, fazer autenticação e então realizar nenhuma ou alguma operação (pesquisa, modificação, adição, deleção, assim por diante), fazer o operação reversa da autenticação e desconectar.

3.4.3 Utilitários

Ao contrário dos clientes, os utilitários não realizam operações usando o protocolo LDAP. Os dados são manipulados em camadas mais baixas e sem mediação pelo servidor. São usados principalmente para manutenção do servidor.

3.4.4 Bibliotecas

Existem várias bibliotecas *Open* LDAP que são compartilhadas entre aplicações LDAP. As bibliotecas fornecem funções LDAP para essas aplicações. Os clientes, utilitários e servidores compartilham acesso a algumas dessas bibliotecas.

Interfaces de Programação de Aplicação (APIs) são fornecidas para permitir que desenvolvedores de *software* escrevam suas próprias aplicações LDAP sem ter que reescrever o código fundamental LDAP.

Enquanto as APIs fornecidas com o Open LDAP são escritas em C, o projeto do Open LDAP também duas APIs Java. Essas bibliotecas em Java não são incluídas no pacote do OpenLDAP. Mas essas APIs podem ser encontradas no site da aplicação (www.openIdap.org). A partir do momento em que se deve proteger um sistema de informações é preciso que se estabeleça um conjunto de regras para acesso e distribuição da informação. Setores específicos tem acesso apenas aos documentos que lhes têm interesse, o funcionário não deve explicitar a sua senha de acesso, a senha de acesso deve ter um nível de complexidade que dificulte quem tentar adivinhar essas senhas, ou seja, um conjunto de regras criadas para garantir a segurança da informação e esse conjunto de regras também é conhecido como política de segurança da informação.

Porém, para a construção de uma política de segurança é preciso seguir algumas normas de segurança padronizadas, que são definidas pela ISO (International Organization for Standardization).

A ISO responsável por padronizar a segurança da informação é a 27001.

A ISO 27001 adota um modelo de controle para criação, implantação e verificação de normas de segurança de informação, o PDCA (*Plan-Do-Check-Act*), é utilizado para estruturar todos os processos do Sistema de Gestão de Segurança da Informação (SGSI). (ISO 27001)

<i>Plan</i> (planejar) (estabelecer o SGSI)	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
<i>D</i> o (fazer) (implementar e operar o SGSI)	Implementar e operar a política, controles, processos e procedimentos do SGSI.
<i>Check</i> (checar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
Act (agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

Quadro 1 – Modelo PDCA aplicado aos processos do SGSI

Fonte- ISO 27001

4.1 Objetivos de Controle

Os objetivos de controle são aqueles que estão listados no anexo A da ISO 27001 para definir especificidades que devem ser asseguradas com a norma para determinados objetos de tecnologia da informação.

A primeira parte da ISO 27001 explica como as partes atuantes dentro de uma empresa devem se portar e ações que devem ser tomadas por cada parte para que um planejamento estratégico seja aplicado.

O anexo A contém tópicos que especificam detalhes de como uma ação deve ser tomada para um determinado objetivo de controle, por exemplo, o tópico Política de Segurança está definido com o seguinte objetivo:

> Prover uma orientação e apoio da direção para segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

Após a definição do objetivo de controle ser definido para a política de segurança da informação, subtópicos apresentam objetos que são relacionados ao objetivo de controle e como realizar o controle sobre ele. Por exemplo, a política de segurança precisa de uma documentação, essa documentação deve ser tratada conforme controle estabelecido nesse subtópico.

 Um documento de política de segurança da informação deve ser aprovado pela direção, publicada e comunicada para todos os funcionários e partes externas relevantes.

O quadro abaixo exemplifica a organização da ISO 27001.

A.5 Política de segurança					
A.5.1 Po	A.5.1 Política de segurança da informação				
<i>Objetivo:</i> Pr requisitos d	<i>Objetivo</i> : Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.				
		Controle			
A.5.1.1	Documento da política de segurança da informação	Um documento da política de segurança da informação deve ser aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.			
		Controle			
A.5.1.2	Análise crítica da política de segurança da informação	A política de segurança da informação deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.			

	Quadro 2 –	Objetivos	de controle	e controles
--	------------	-----------	-------------	-------------

4.2 Objetivos de Controle Aplicados aos Sistemas de Serviço de Diretório

Para fazer os testes com os sistemas de serviço de diretório e então compara-los, foram escolhidos objetivos da ISO 27001 que são normalmente adotados em políticas de segurança da informação, são eles, a autenticação de usuário, acesso a caminhos de rede bloqueados devido a restrições de acesso e a atribuição de senhas apropriadas para controle de acesso.

O quadro três define o controle de acesso a caminhos de rede e autenticação de usuários nos itens A.11.4.1 e A.11.4.2 respectivamente. O quadro quatro define a autenticação para o sistema operacional que é instalado em uma máquina e a senha que deve ser usada para controlar esse acesso nos itens A.11.5.2 e A.11.5.3 respectivamente.
	Quadro 3 –	Controle de	acesso a	rede e	autenticad	:ão de	usuários
--	------------	-------------	----------	--------	------------	--------	----------

A.11.4 Controle de acesso à rede				
Objetivo: Pr	evenir acesso não autorizado ao	s serviços de rede.		
	Delítico de uno des comuises	Controle		
A.11.4.1	de rede	Os usuários devem receber acesso somente aos serviços que tenham sido especificamente autorizados a usar.		
	Autoptigação para conovão	Controle		
A.11.4.2	externa do usuário	Métodos apropriados de autenticação devem ser usados para controlar o acesso de usuários remotos.		
		Controle		
A.11.4.3	Identificação de equipamento em redes	Devem ser consideradas as identificações automáticas de equipamentos como um meio de autenticar conexões vindas de localizações e equipamentos específicos.		
	Protosão o configuração do	Controle		
A.11.4.4	portas de diagnóstico remotas	Deve ser controlado o acesso físico e lógico para diagnosticar e configurar portas.		

Quadro 4 – Controle de senhas

A.11.5 Controle de acesso ao sistema operacional						
Objetivo: Pr	Objetivo: Prevenir acesso não autorizado aos sistemas operacionais.					
	Propodimentos seguros de	Controle				
A.11.5.1	entrada no sistema (<i>log-on</i>)	O acesso aos sistemas operacionais deve ser controlado por um procedimento seguro de entrada no sistema (<i>log-on</i>).				
		Controle				
A.11.5.2	Identificação e autenticação de usuário	Todos os usuários devem ter um identificador único (ID de usuário), para uso pessoal e exclusivo, e uma técnica adequada de autenticação deve ser escolhida para validar a identidade alegada por um usuário.				
	Cistama da garansismento da	Controle				
A.11.5.3 Sistema de gerenciamento de senha		Sistemas para gerenciamento de senhas devem ser interativos e assegurar senhas de qualidade.				
		Controle				
A.11.5.4	Uso de utilitários de sistema	O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações deve ser restrito e estritamente controlado.				

5 ISO 27001 APLICADA AO ACTIVE DIRECTORY E AO OPENLDAP EM AMBIENTE DE TESTE PARA FINS COMPARATIVOS EM PARAMETROS EQUIPARADOS.

5.1 Testes com o Microsoft Active Directory

Para iniciar um serviço de diretório usando o Active Directory Domain Services (ADDS) da Microsoft é preciso ter um IP estático para que sempre que o IP for consultado ele tenha um dono. Nesse experimento o IP do ADDS é 10.0.0.11 em um Windows Server 2012, o IP de outro servidor fazendo papel de Controlador de Domínio é 10.0.0.12 em um Windows Server 2008 R2 e o IP de uma estação de trabalho é 10.0.0.13 usando o Windows 8.

Também é preciso ter certeza de que o nome do servidor está correto porque após a instalação do serviço de diretório não será mais possível modifica-lo.

Ao fazer o primeiro acesso à um Windows server 2012 uma janela para gerenciamento do servidor é automaticamente aberta chamada de Server Manager. Pode-se verificar de imediato que todos os detalhes do servidor estão resumidos nessa janela.

5.1.1 Configurar IP Estático

Para configurar o IP é preciso abrir o painel de controle e abrir o centro de compartilhamento e redes.

Figura 2 – Acesso ao Network and Sharing Center



Após isso clicar em Ethernet, que é o nome dado por padrão a um adaptador de rede, e em seguida em propriedades:

Figura 3 – Propriedades do Adaptador de Rede

Ethernet Properties	x		
Networking			
Connect using:			
Microsoft Hyper-V Network Adapter	1		
<u>C</u> onfigure			
This connection uses the following items:			
Gent for Microsoft Networks GoS Packet Scheduler GoS Packet Scheduler GoS Packet Scheduler GoS Retwork Adapter Multiplexor Protocol d. Link-Layer Topology Discovery Mapper I/O Driver d. Link-Layer Topology Discovery Responder d. Internet Protocol Version 6 (TCP/IPv6) d. Internet Protocol Version 4 (TCP/IPv4)			
Install Uninstall Properties			
Allows your computer to access resources on a Microsoft network.			
OK Cancel			

Para configurar o IP estático conforme já apresentado é preciso selecionar o protocolo de internet versão 4 (TCP/IPv4) e clicar em propriedades:

Internet Protocol Version 4 (TC	P/IPv4) Properties ? X				
General					
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.					
O <u>O</u> btain an IP address automatical	у				
• Use the following IP address:					
IP address:	10 . 0 . 0 . 11				
S <u>u</u> bnet mask:	255 . 255 . 255 . 0				
Default gateway:					
○ Obtain DNS server address automatically					
• Use the following DNS server addresses:					
Preferred DNS server:	10 . 0 . 0 . 11				
<u>A</u> lternate DNS server:					
Vaļidate settings upon exit	Ad <u>v</u> anced				
	OK Cancel				

Ao iniciar o servidor com Server 2012 é observado uma interface gráfica praticamente auto explicativa. Conforme imagem abaixo:



Figura 5 – Gerenciador do Servidor no Windows Server 2012 R2

Dashboard é a tela em que são apresentados os serviços ou roles em caráter de resumo, apresentando se a alguma anormalidade.

5.1.2 Verificação do Nome do Servidor

Para verificação do nome do servidor é preciso clicar em Local Server. O Local Server é onde podem ser encontrado todos os detalhes sobre o servidor que está sendo configurado.

h.	Server Manager - 🖬 🗙				x			
Server M	lanager 🕨 Local S	erver			② 🚩 Manage	<u>T</u> ools <u>\</u>	(iew	<u>H</u> elp
🗰 Dashboard	PROPERTIES For DC01-W2012					Т	ASKS 🔻	•
Local Server All Servers File and Storage Services ▷	Computer name Workgroup	DC01-W2012 WORKGROUP		Last installed updates Windows Update Last checked for updates	Never Not configured Never			Ξ
	Windows Firewall Remote management Remote Desktop NIC Teaming Ethernet	Public: Off Enabled Enabled Disabled 10.0.0.11, IPv6 enabled		Windows Error Reporting Customer Experience Improvement Program IE Enhanced Security Configuration Time zone Product ID	Off Not participating On (UTC-03:00) Brasilia 00184-20405-00319-AA77	6 (activated)		
	Operating system versior Hardware information	Microsoft Windows Server 2012 Standard Microsoft Corporation Virtual Machine		Processors Installed memory (RAM) Total disk space	Intel(R) Core(TM) i5 CPU 1.5 GB 29.66 GB	M 560 @ 2.6	7GHz	
	EVENTS All events 11 total	→ (ii) → (ii) →				Т	isks 🔹	
	Server Name ID	Severity Source	Log	Date and Time				
	DC01-W2012 111 DC01-W2012 111 DC01-W2012 111	Error Microsoft-Windows-TerminalServices-Printers Error Microsoft-Windows-TerminalServices-Printers Error Microsoft-Windows-TerminalServices-Printers Error Microsoft-Windows-TerminalServices-Printers	System System System	14/02/2014 16:10:27 14/02/2014 16:10:27 14/02/2014 16:10:21				

Figura 6 - Detalhes do Servidor no Gerenciador do Servidor

Uma vez na tela do Local Server, observa-se que a primeira propriedade do computador é o nome do mesmo. Para altera-lo basta clicar no nome e altera-lo colocando a credencial administrativa do servidor. Essa credencial é criada para acesso ao servidor no momento da instalação do sistema operacional.

Nesse experimento o nome do servidor é DC01-W2012.

5.1.3 Instalação do Serviço de Diretório

Para ativar o serviço de diretório do Windows server 2012 é preciso ativar a função ADDS, ao clicar em Add roles and features (Adicionar funções e características) na tela Dashboard é aberto um Wizard, assistente de instalação, para facilitar o acesso as opções de configuração do servidor, conforme figura abaixo:



Figura 7 – Assistente para Adicionar Funcionalidades ao Servidor

Nesse *Wizard* o Windows faz sugestões baseadas nas configurações já realizadas para melhorar o desempenho das funções escolhidas e sugere algumas features (características) que são necessárias para que as funções escolhidos correspondam as expectativas do administrador.

Logo em seguida o Windows oferece duas opções de instalação para as novas funções, uma em que funções serão instaladas no servidor local e outra para criar uma função em outro servidor virtual via rede conforme figura a baixo:



Figura 8 – Tela do Assistente para Escolha do Tipo de Instalação

Nesse experimento será feita a instalação no servidor local.

O Windows em seguida pergunta se existe um pool de servidores onde é possível escolher um servidor na rede que não seja o local para fazer a instalação do serviço. Porem nesse experimento esse servidor é o primeiro da rede e só ele poderá ser escolhido.

Figura 9 – Tela do Assistente para Escolha do Disco Virtual para Instalação de Funções

🚡 Add Roles and Features Wizard 💶 🗖 🗙				
Select destinatior	Server Destination server DC01-W2012			
Before You Begin	Select a server or a virtual hard disk on which to install roles and features.			
Installation Type	Select a server from the server pool			
Server Selection	O Select a virtual hard disk			
Server Roles	Server Pool			
Features				
Confirmation	Filter:			
Results	Name IP Address Operating System			
	DC01-W2012 10.0.0.11 Microsoft Windows Server 2012 Standard			
	1 Computer(s) found This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.			
	< Previous Next > Install Cancel			

Como próximo passo, é aberta no wizard a tela para escolha dos serviços a serem instalados. Nessa tela além de terem vários serviços como opção para instalação ainda existe uma breve descrição sobre o que cada serviço pode proporcionar, conforme abaixo:

a	Add Roles and Features Wizard	_ D X
Select server roles	5	DESTINATION SERVER DC01-W2012
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection	Active Directory Certificate Services	 Active Directory Certificate Services
Server Roles	Active Directory Domain Services	(AD CS) is used to create
Features	Active Directory Federation Services	role services that allow you to issue
Confirmation	Active Directory Lightweight Directory Services	and manage certificates used in a
Results	Active Directory Rights Management Services	variety of applications.
	Application Server	
	DHCP Server	=
	DNS Server	
	Fax Server	
	File And Storage Services (Installed)	
	Hyper-V	
	Network Policy and Access Services	
	Print and Document Services	
	Remote Access	
	Remote Desktop Services	~
	< Previous	lext > Install Cancel

Figura 10 – Tela do Assistente para Escolha das Funções do Servidor

Ao clicar em Active Directory Domain Services (ADDS), é aberta uma janela de sugestões para instalações de características (features), que vão permitir o funcionamento por completo da função escolhida. Se essas features não forem instaladas o Windows impedirá a instalação do serviço.





Ao clicar em Add Features, o administrador aceita a instalação dos prérequisitos.

O Windows server também possibilita a instalação do de outros serviços simultaneamente. A Microsoft faz a recomendação de sempre instalar no servidor que terá o ADDS o serviço DNS. O DNS é o serviço que dá nome aos computadores e servidores participantes do domínio. Ao invés de procurar um computador pelo IP para armazenar documentos pode-se ter o catálogo de nome dos computadores para facilitar os acessos.

Nesse experimento o DNS se faz necessário devido a necessidade de toda organização ter um serviço DNS e a motivação deste trabalho é de simular a realidade empresarial.

Para instalar o DNS basta clicar também no serviço DNS que apresentado no wizard para seleção de funções. Da mesma forma que quando o serviço de ADDS é selecionado o wizard apresenta as features necessárias para o correto funcionamento do serviço.

Figura 12 - Tela do Assistente Questionando a Instalação do Serviço DNS



Figura 13 - Tela do Assistente Adicionando a Função de DNS

2	Add Roles and Features Wizard	_ D X
Select server roles	5	DESTINATION SERVER DC01-W2012
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection Server Roles Features AD DS DNS Server Confirmation Results	 Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server DHCP Server ✓ DNS Server Fax Server File And Storage Services (Installed) Hyper-V Network Policy and Access Services Print and Document Services Remote Access Remote Desktop Services 	Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
	< <u>P</u> revious <u>N</u> ext	> Install Cancel

Agora que os dois serviços principais estão selecionados basta clicar em next. Em seguida o wizard leva o administrador para a seleção de features, onde é visível que algumas delas já estão marcadas para serem instaladas, essas são as que o wizard sugeriu como pré-requisito para o correto funcionamento dos serviços escolhidos.

2	Add Roles and Features Wizard	
Select features		DESTINATION SERVER DC01-W2012
Before You Begin	Select one or more features to install on the selected server.	
Installation Type	Features	Description
Server Selection		.NET Framework 3.5 combines the
Server Roles	NET Framework 4.5 Features (Installed)	power of the .NET Framework 2.0
Features	Background Intelligent Transfer Service (BITS)	building applications that offer
AD DS	BitLocker Drive Encryption	appealing user interfaces, protect
DNS Server	BitLocker Network Unlock	your customers' personal identity
Confirmation	BranchCache	secure communication, and provide
Results	Client for NFS	the ability to model a range of
Results	Data Center Bridging	business processes.
	Enhanced Storage	
	Failover Clustering	
	✓ Group Policy Management	
	Ink and Handwriting Services	
	Internet Printing Client	
	IP Address Management (IPAM) Server	
	< <u>P</u> revious <u>N</u> ext	> Install Cancel

Figura 14 - Tela do Assistente Adicionando o Group Policy Manager

Ao clicar em next, o wizard mostra algumas recomendações da Microsoft para o melhor funcionamento do sistema, e ainda faz a descrição de algumas features que são instaladas junto com o ADDS.



Figura 15 – Tela do Assistente Alertando Sobre o Serviço ADDS



Continuando adiante o wizard mostra por fim o resumo de todos os serviços e features que serão instalados enquanto questiona se deve instalar os mesmos, conforme figura abaixo:

Figura 17 – Tela do Assistente Resumindo Todas as Funções

a	Add Roles and Features Wizard	_ 🗆 🗙
Confirm installat	on selections	DESTINATION SERVER DC01-W2012
Before You Begin	To install the following roles, role services, or features on selected server,	click Install.
Installation Type	Restart the destination server automatically if required	
Server Selection	Optional features (such as administration tools) might be displayed on th	is page because they have
Server Roles	been selected automatically. If you do not want to install these optional f their check boxes.	eatures, click Previous to clear
Features		
AD DS	Active Directory Domain Services	^
DNS Server	DNS Server	
Confirmation	Group Policy Management	
Results	Remote Server Administration Tools	
	AD DS and AD LDS Tools	=
	Active Directory module for Windows PowerShell	
	AD DS Tools	
	Active Directory Administrative Center	
	AD DS Snap-Ins and Command-Line Tools	~
	Export configuration settings Specify an alternate source path	
	< <u>P</u> revious <u>N</u> ext >	Install Cancel

Depois da Instalação outros serviços são mostrados na tela de resumo de serviços do Dashboard, são eles o ADDS, o DNS, Todos os Servidores, Serviço de armazenamento e Servidor Local conforme figura abaixo:



Figura 18 - Tela da Gerencia do Servidor com Serviços Instalados

Em um segundo momento, em seguida da instalação dos serviços do ADDS e DNS, um sinal de exclamação fica visível na parte superior da janela server manager. Esse sinal de exclamação significa que o servidor precisa avisar algo para o administrador e neste caso específico avisa ao administrador que deve ser feita continuação da instalação dos serviços recém instalados.

A primeira ação que deve ser tomada após a instalação do ADDS é promover o servidor e torna-lo um Controlador de Domínio, basta acessar o link Promete this server to a domain controler, conforme figura abaixo.

Figura 19 – Gerenciador do Servidor Apresentando a Opção de Controlador de Domínio

<u>a</u>		Server Manager		
Server Ma	anager • Dashboard		• @ M	Manage Tools View Help
Dashboard Local Server All Server All Servers AD DS DNS File and Storage Services	Add WHAT'S NEW A Cree LEARN MORE ROLES AND SERVER GROUPS Roles 3 Server groups Server total:	I other servers to manage ate a server group	Post-deployment Configura TASKS Y X Configuration required for Active Directory Domain Services at DC01-W2012 Promote this server to a domain controller Task Details	Hide
	AD DS 1 Manageability Events Services Performance BPA results	DNS 1 ① Manageability ① Events Services Performance BPA results	File and Storage 1 Services 1 Manageability Imageability Events Events Performance Services BPA results Performance BPA results BPA results	1
	All Servers 1 Manageability Events Services			

Logo após acessar o link do domain controler (DC), outro wizard é iniciado para auxiliar na configuração do novo controlador de domínio.

Figura 20 – Assistente para Configuração do ADDS

B	Active Directory Domain Services (Configuration Wizard	_ 🗆 X
Deployment Configuration Deployment Configuration Domain Controller Options Additional Options Paths Review Options Prerequisites Check Installation Results	Active Directory Domain Services (iguration Select the deployment operation Add a gomain controller to an existi Add a new domain to an existing for Add a new forest Specify the domain information for this Root domain name:	TARGET SERVER DC01-W2012	
	More about deployment configurations	evious <u>N</u> ext >	Install Cancel

Conforme pode ser observado na figura acima, o wizard traz uma série de etapas que devem ser cumpridas para que o novo serviço fique com funcionamento correto. A primeira etapa é escolher a operação de instalação e como esse é o primeiro DC deve-se adicionar uma nova floresta. Um conjunto de domínios é uma

floresta, dessa forma para começar uma floresta é preciso então configurar o primeiro domínio que terá o nome de MONOGRAFIA.LOCAL.

Após iniciar uma nova floresta é preciso definir o nível funcional. O nível funcional determina o nível de funções que farão parte do domínio e de todos os servidores do domínio. Se no domínio houver um servidor com Windows Inferior ao 2012 então o 2012 se comunicará com esse servidor no nível de sua capacidade. No caso desse experimento um outro controlador de domínio será inserido no domínio e seu Windows é o Server 2008 R2, portanto, o nível funcional desse domínio será Windows Server 2008 R2.

B	Active Directory Domain Services	Configuration Wizard	_
Domain Controlle	r Options		TARGET SERVER DC01-W2012
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Select functional level of the new forest Forest functional level: Domain functional level: Specify domain controller capabilities Ogmain Name System (DNS) server Solobal Catalog (GC) Read only domain controller (RODC) Type the Directory Services Restore Mo Passworg: Confirm password:	and root domain Windows Server 2008 R2 • Windows Server 2008 R2 • de (DSRM) password • •••••••• •	
	< <u>P</u>	revious <u>N</u> ext > <u>I</u> nstall	Cancel

Ainda nesta etapa é preciso definir uma senha para que em caso de ser necessário restaurar serviços ser possível resgata-los.

No próxima etapa não é possível delegar nenhuma opção do serviço a nenhum outro servidor no momento devido a este servidor ser o primeiro do domínio.

Figura 21 – Assistente para Configuração de Nível Funcional do ADDS

Ъ	Active Directory Domain Services Configuration Wizard	_ □	x
DNS Options		TARGET SER DC01-W	RVER 2012
A delegation for this DNS	server cannot be created because the authoritative parent zone cannot be found	Show more	×
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Specify DNS delegation options		
	More about DNS delegation		
	<pre></pre>	Cance	:I

Figura 22 – Erro Relacionado ao DNS na Configuração do ADDS

Ne etapa subsequente o nome Netbios já vem preenchido com o nome principal do domínio, neste caso é preciso aceitar a opção e continuar com a configuração.

— • • • • •	~~	A '			~	- L -	NI.		
FIGUID	·)·2	Accietanta	nara	CONTINU	racan	AO.	NIAMA		
i iuuia	20 -		Dala	Comuuu	lacau	uu	INCINC	INCLDICO	

b	s Configuration Wizard	_ 🗆 X	
Additional Option	TARGET SERVER DC01-W2012		
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Verify the NetBIOS name assigned to The NetBIOS domain name:	the domain and change it if necessary MONOGRAFIA	
	More about additional options	Previous Next > Install	Cancel

No próximo passo, o wizard questiona quanto o local do armazenamento do banco de dados com a pasta NTDS e o local para armazenamento dos scripts e políticas com a pasta SYSVOL, no caso do experimento essas pastas serão armazenadas no próprio servidor.

🚡 Active Directory Domain Services Configuration Wizard 📃 🗖 🗙							
Paths			TARGET SERVER DC01-W2012				
Deployment Configuration Domain Controller Options DNS Options Additional Options Paths Review Options Prerequisites Check Installation Results	Specify the location of the AD DS datal <u>D</u> atabase folder: <u>Log</u> files folder: <u>SY</u> SVOL folder:	aase, log files, and SYSVOL C:\Windows\NTDS C:\Windows\NTDS C:\Windows\SYSVOL					
More about Active Directory paths							
	< <u>P</u>	revious <u>N</u> ext >	Install Cancel				

Figura 24 – Assistente para Localização da Base de Dados do ADDS

Em Seguida o wizard apresenta um resumo das configurações que serão instalados e em seguida verifica se os arquivos pré-requisitos estão instalados e tem o início da instalação.



Figura 25 – Resumo da Configuração do ADDS

Figura 26 – Checagem de Pré-requisitos do ADDS



5.1.4 Desafio ao Active Directory

Uma vez criado o domínio, inicia-se a fase de aplicação do planejamento da infraestrutura do domínio.

Esse experimento tem o foco de acompanhar algumas exigências comuns das políticas de segurança mais utilizadas pela maioria das empresas de grande porte, incluindo governo federal e simula-las em laboratório conforme o capítulo quatro lista nas tabelas da ISO 27001

Entre as exigências de segurança mais conhecida pela tecnologia da informação estão, a autenticação de usuários, ou seja, cada funcionário de uma empresa deve ter um usuário cadastrado para fazer acesso aos recursos de tecnologia da empresa, o acesso restrito a pastas e documentos, somente pessoas autorizadas podem ter acesso a pastas especificas, e senhas para acesso do usuário ao domínio com nível de dificuldade especifico para cada grupo de usuários que impeçam acesso não autorizado de funcionários aos equipamentos da empresa.

Para que seja possível simular esse ambiente é preciso cadastrar novos usuários, cadastrar novos grupos de usuários, incluir computadores no domínio, criar pastas para cada departamento no servidor de arquivos e aplicar políticas de gerenciamento para controle de acesso às pastas por grupos de usuários.

5.1.5 Criação de Usuários

Para adicionar usuários no domínio é preciso acessar as ferramentas no link tools da tela do server manager. A primeira ferramenta usada é a usuários e computadores do Active Directory (Active Directory Users and Computers).



Figura 27 – Usuários e Computadores do Active Directory

Ao selecionar o novo domínio são abertas as pastas para gerenciamento de computadores e usuários do domínio. Para esse experimento serão criados duas novas pastas do domínio, também chamadas de Unidades Organizacionais (OU), uma para usuários e outra para grupos de usuários. A pasta Users traz usuários padrão do domínio como o usuário administrador usado para acessas o servidor do ADDS.



Figura 28 - Criação das Unidades Organizacionais

O padrão de usuários é usuárioXX e senha 123456 conforme figuras

abaixo:

	New Object - User						
Create in: monografia Jocal/Usuários Monografia							
<u>F</u> irst name:	Usuario01 <u>I</u> nitials:						
Last name:	Mono						
Full n <u>a</u> me:	Usuario01 Mono						
User logon name:							
ukuario01 @monografia.local V							
User logon name (pre- <u>W</u> indows 2000):							
MONOGRAFIA	usuario01						
	< Back Next > Cancel						

Figura 29 – Assistente para Criação de Novo Usuário

Figura 30 – Assistente para Criação de Senha para Novo Usuário

New Object - User
Create in: monografia Jocal/Usuários Monografia
Password: •••••• Confirm password: •••••••
User must change password at next logon User cannot change password Password never expires Account is disabled
< Back Next > Cancel

Foram criados 6 usuários para este experimento.

•	Active Directory Users and Compute	ers	_ _ X
<u>File Action View H</u> elp			
	🖬 🖏 🐮 🝸 🖉 💐	_	
 Active Directory Users and Computers [Saved Queries Saved Queries Builtin Computers Domain Controllers ForeignSecurityPrincipals Grupos Monografia Managed Service Accounts Users Usuários Monografia 	Name Usuario01 Mono Usuario02 Mono Usuario03 Mono Usuario04 Mono Usuario05 Mono Usuario06 Mono	Type User User User User User	Description

Figura 31 – Novos Usuários Criados na OU

5.1.6 Criação dos Grupos

Para criar os grupos basta clicar na nova OU grupos e cria-los, porém, é importante separar o tipo do grupo a ser criado neste experimento será usado somente o grupo local, devido a ser apenar um DC.

Figura 32 – Container de Grupos do Domínio



Figura 33 – Assistente para Criação de Novo Grupo

	New Object - Group	x					
Create in: monografia.local/Grupos/Grupos Locais							
Group name:							
Marketing							
Group name (pre-Windows	3 2000):						
Marketing							
Group scope	Group type						
O Domain local	● <u>S</u> ecurity						
<u>G</u> lobal	○ <u>D</u> istribution						
○ <u>U</u> niversal							
	OK Cano	el					

Figura 34 – Grupos Novos Criados no Container de Grupos

Active Directory Users and Computers					x
Eile Action ⊻iew Help ← ⇒	TT 💈 🐮 📷 🔻 🗾 🐮				
 Active Directory Users and Computers [Saved Queries Builtin Computers Domain Controllers ForeignSecurityPrincipals Grupos Grupos Globais Grupos Universais Managed Service Accounts Users Servidores Servidores 	Name Marketing Recursos Humanos Suporte Técnico	Type Security Group - Global Security Group - Global Security Group - Global	Descrip	tion	
< III >	٢	I			>

Foram criados os grupos de Marketing, Recursos Humanos e Suporte Técnico. De acordo com a uma política de segurança comum, cada departamento da empresa acessa somente os arquivos e pastas respectivos e tem acesso restrito ao dos outros departamentos. No caso deste experimento o grupo Marketing irá acessar somente a pasta Marketing, o grupo Recursos Humanos irá acessar somente a pasta Recursos Humanos e o grupo suporte acessará todas as pastas incluindo a pasta Suporte Técnico. Os usuários 01 e 02 serão do departamento de Marketing, os usuários 03 e 04 serão do departamento de Recursos Humanos e os usuários 05 e 06 serão do suporte técnico.

Suporte Técnico Properties
General Members Member Of Managed By
Members:
Name Active Directory Domain Services Folder
Usuario 05 Mono monografia.local/Usuários
👗 Usuario 06 Mono monografia.local/Usuários
< III >
Add <u>R</u> emove
OK Cancel Apply

Figura 35 – Propriedades do Grupo Suporte Técnico

5.1.7 Inclusão de Servidores e Clientes no Domínio

Para incluir os servidores e estações de trabalho no domínio é preciso entrar nas propriedades dos computadores e modificar o nome. Para este experimento utilizando o ADDS será usado um servidor de arquivo Windows Server 2008 R2 e uma estação de trabalho Windows 8.

Para incluir a estação de trabalho no domínio é preciso modificar as configuração da estação acessando o link Change Settings.



Neste caso será preciso acessar o link Change do janela de propriedades

do computador.

Figura 37 – Propriedades do Sitema



Para este experimento a estação de trabalho terá o nome de cliente01 e fará parte do domínio monografia.local.

Figura 38 – Modificando o Nome e o Domínio

Computer Name/Domain Changes
You can change the name and the membership of this computer. Changes might affect access to network resources.
Computer name:
Cliente))1
Full computer name: Cliente01
<u>M</u> ore
Member of
<u>D</u> omain:
monografia.local
○ Workgroup:
WORKGROUP
OK Cancel

Figura 39 – Confirmação de Alteração de Domínio para Monografia.local



Figura 40 - Requisição para Reiniciar o Computador



Agora que a estação de trabalho está no domínio é preciso fazer o acesso com algum usuário criado no ADDS para fazer a verificação do ingresso no domínio. Para este caso o acesso pode ser feito com o usuario01 porém, para que o usuário possa fazer acesso remoto a máquina virtual é preciso adicionar o usuário no grupo padrão do ADDS de acesso remoto WinRMRemoteWMIUsers_.

Figura 41 – Grupo para Acesso Remoto

2		Active Directory Users and	d Computers	_ 0	x
Eile Action View Help					
◆ ⇒ 2 🗊 🖌 🗎 🗙 🖬 🧔	🗟 🛛 🖬 🔧 📚 🗑 🍸 🖻 🛠				
Active Directory Users and Computers [Name	Туре	Description		
Saved Queries	& Administrator	User	Built-in account for ad		
⊿ 🏥 monografia.local	& Allowed RODC Password Replication Group	Security Group - Domain	Members in this group c		_
Builtin	& Cert Publishers	Security Group - Domain	Members of this group		_
Computadores	& Cloneable Domain Controllers	Security Group - Global	Members of this group t		_
Computers	& Denied RODC Password Replication Group	Security Group - Domain	Members in this group c		_
Domain Controllers	& DnsAdmins	Security Group - Domain	DNS Administrators Gro		_
ForeignSecurityPrincipals	& DnsUpdateProxy	Security Group - Global	DNS clients who are per		_
⊿ ⊆ Grupos	& Domain Admins	Security Group - Global	Designated administrato		_
Crupos Giobais	& Domain Computers	Security Group - Global	All workstations and ser		_
Grupos Locais	& Domain Controllers	Security Group - Global	All domain controllers i		_
Managed Service Accounts	& Domain Guests	Security Group - Global	All domain guests		_
Servidores	A Domain Users	Security Group - Global	All domain users		_
Users	& Enterprise Admins	Security Group - Universal	Designated administrato		_
Usuários	& Enterprise Read-only Domain Controllers	Security Group - Universal	Members of this group		_
	Stroup Policy Creator Owners	Security Group - Global	Members in this group c		_
	🛃 Guest	User	Built-in account for gue		_
	AS and IAS Servers	Security Group - Domain	Servers in this group can		_
	A Read-only Domain Controllers	Security Group - Global	Members of this group		_
	💐 Schema Admins	Security Group - Universal	Designated administrato		_
	KinRMRemoteWMIUsers_	Security Group - Domain	Members of this group		
					_
					_
					_
					_
					_
					_
					_
					_
					_
					_
< 111 >					_
1					

Figura 42 – Membros Pertencentes ao Grupo de Acesso Remoto

WinRMRemo	oteWMIUsers_ Properties	
General Members	Member Of Managed By	
Members:		
Name	Active Directory Domain Services Folder	
👃 Usuario01 Mo	monografia.local/Usuários	
Usuario02 Mo	monografia.local/Usuários	
S Usuario03 Mo	monografia local/Usuários	
SUSUANOU4 Mo	monografia.local/Usuarios	
Usuario06 Mo	monografia local/Usuários	
Add	Remove	
	OK Cancel Apply	

No cliente acessar com o usuário do domínio.

Figura 42 – Autenticação do Usuário no Domínio

Segurança do Windows
Digite suas credenciais Essas credenciais serão usadas para a conexão com 10.0.0.14.
suporte
monografia.local\usuario01 Domínio: monografia.local
Lembrar minhas credenciais
OK Cancelar

Figura 43 – Usuário Logado no Computador Cliente



Para incluir o servidor Windows Server 2008 R2 é preciso acessar com o usuário de administrador local, e abrir o gerenciador do servidor ou Server Manager e marcar o servidor local conforme abaixo:

er Manager (WIN-805J3PUOR3T)	Server Manager (WIN-805J3PL	IOR3T)	
eatures lagnostics fonfiguration ltorage	Get an overview of the features.	e status of this server, perform top managen	ent tasks, and add or remove server roles and
	Server Summary		Server Summary Help
	Computer Information		🕅 Activate Windows
	Full Computer Name:	WIN-805J3PUOR3T.monografia.com	Change System Properties
	Workgroup:	WORKGROUP	Configure Remote Desktop
	Local Area Connection:	10.0.0.12, IPv6 enabled	Configure Server Manager Remote Management
	Remote Desktop:	Enabled	
	Server Manager Remote Management:	Disabled	
	Product ID:	Not activated	
	Do not show me this con	sole at logon	
	Security Information		😭 Go to Windows Firewall
	Windows Firewall:	Public: On	Configure Updates
	Windows Updates:	Not configured	Run Security Configuration Wizard
	Last checked for updates:	Never	% Configure IE ESC
	Last installed updates:	Never	
	IE Enhanced Security Configuration (ESC):	On for Administrators On for Users	

Figura 44 – Gerencia do Servidor 2008 R2 para Arquivos

Depois de marcar o servidor local é preciso modificar as propriedades do sistema acessando o link Change System Properties.

Figura 45 – Propriedades do Sistema do Servidor de Arquivos

System Properties		×
Computer Name Hardwa	re Advanced Remote	
Windows uses on the network	the following information to identify your computer	
Computer description:		
	For example: "IIS Production Server" or "Accounting Server".	
Full computer name:	WIN-80SJ3PUOR3T.monografia.com	
Workgroup:	WORKGROUP	
To rename this computer workgroup, click Change	or change its domain or <u>C</u> hange	
	OK Cancel Apply	

Figura 46 – Troca de Nome e Domínio do Servidor

Computer Name/Domain Changes 🛛 🗙
You can change the name and the membership of this computer. Changes might affect access to network resources. <u>More information</u>
Computer name:
Servidor01
Full computer name: Servidor01.monografia.com
More
Member of
• Domain:
monografia.loca
C Workgroup:
Jwonkanoon
OK Cancel

Figura 47 – Confirmação de Alteração de Domínio para Monografia.local



5.1.8 Experimento 1 – Criação de Políticas de Segurança e Verificação dos resultados

As políticas de segurança que serão adotadas para experimento seguem algumas regras de segurança estabelecidas por políticas de segurança usadas em empresas de grande porte incluindo governo federal.

Os parâmetros de segurança usados neste experimento são:

Senha com complexidade

Acesso restrito a pastas

Existem duas procedimentos para definir a senha de segurança como complexa só para o grupo de suporte técnico. A primeira é modificando a politica padrão do AD, que determina que todas as senhas tenham complexidade para que não seja mais uma exigência em seguido acessando criando uma politica só para o

grupo de suporte técnico exigindo a complexidade de senha forçadamente. A Segunda opção é criar uma política que não exige senha complexa e atrelar a cada grupo criado menos aquele que terá a exigência mantendo a política padrão do AD. A primeira forma foi escolhida para o experimento devido ao menor esforço.



Figura 48 – Gerência de Política de Grupo

Figura 49 – Grupos Locais – GPO

📓 Group Poli	cy Management	_ D X
<u>Eile Action View Window H</u> elp		_ 8 ×
Group Policy Management	Grupos Locais	
⊿ ▲ Forest: monografia.local	Linked Group Policy Objects Group Policy Inheritance	Delegation
⊿ 🛃 Domains	Link Deter GPO	
⊿ monografia.local I Default Descrip Deling		
Derault Domain Policy Computadores		
 Domain Controllers 		
⊿ 🖬 Grupos	∇	
Grupos Globais	\Box	
📴 Grupos Locais		
Grupos Universais		
Servidores		
Scoup Policy Objects		
WMI Filters		
Starter GPOs		
Sites		
🔯 Group Policy Modeling		
🔀 Group Policy Results		
	< 111	>
	J	
7		

Figura 50 – GPO Senha Complexa

	New GPO	x
<u>N</u> ame: Senha Complexa		
<u>S</u> ource Starter GPO: (none)	OK Can	 cel

Figura 51 - GPOs no Grupo Local



Figura 52 – Escopo da GPO Senha Complexa

<u>R</u>	Group Policy Management	_ 0 ×
<u> F</u> ile Action <u>V</u> iew <u>W</u> indow <u>H</u> elp		_ # ×
🗢 🔿 📶 🗙 🖸 📓 🖬		
Group Policy Management Group Policy Management Group Policy Management Group Policy Management Group Policy Group Second Group Sec	Senha Complexa Scope Details Settings Delegation Links Display links in this location: monografia.local The following stes, domains, and OUs are linked to this GPO: Location Enforced Link Enabled Image: Complex Comp	V Path monografia local/Grupos/Grupos Locais
Group Policy Objects		>
General Filters Group Policy Modeling Group Policy Results	Security Filtering The gettings in this GPO can only apply to the following groups, users, and computers: Name Authenticated Users Add Remove Properties WMI Effection	
	This GPO is linked to the following WMI filter:	



Figura 53 – Aba para Atribuir Permissão no Grupo

Figura 54 – Permissão para o Grupo Suporte Técnico

📓 Gro	up Policy Management				i x
<u> F</u> ile <u>A</u> ction <u>V</u> iew <u>W</u> indow <u>H</u> elp					_ & ×
Image: The Action View Window Help Image: The Action View Window Window Help Image: The Action View Window Window Window Image: The Action View Side View View View Side View View View View View View View Vie	Jexa Settings Delegation dusers have the specified permission for th s: ed Users mins (MONOGRAFIA\Domain Admins) Admins (MONOGRAFIA\Domain Admins) SE DOMAIN CONTROLLERS creico (MONOGRAFIA\Supote Técnico)	is GPO Allowed Permissions Read (from Security Filtering) Edit settings, delete, modify sec Read Flead Edit settings, delete, modify sec	Inherited No No No No No		
A <u>d</u> d	Remove Prop	perties		Adva <u>n</u> ce	d
Senha Complexa Security Settings					
--					
Security					
<u>G</u> roup or user names:					
Suporte Técnico (MONOGRAFIA\Suporte Técnico)					
Somain Admins (MONOGRAFIA\Domain Admins)					
Enterprise Admins (MONOGRAFIA\Enterprise Admins)					
M ENTERPRISE DOMAIN CONTROLLERS					
< III >					
Add Remove					
Permissions for Suporte Técnico Allow Deny					
Write					
Create all child objects					
Delete all child objects					
Apply group policy					
Special permissions					
For special permissions or advanced settings, Advanced Advanced.					
Learn about access control and permissions					
OK Cancel <u>A</u> pply					

Figura 55 – Configurações de Segurança da GPO de Senha Complexa

Figura 56 – Filtro de Segurança para Suporte Técnico

<u>R</u>	Group Policy Management	_ 0 ×
😹 File Action View Window Help		_ & ×
Image: Second Secon	Scope Details Settings Delegation Unks Display links in this location: monografia.local The following sites, domains, and OUs are linked to this GPO: Location Cocation Cocati	/Grupos Locais
 ▶ Stater GPOs ▶ State Broup Policy Modeling ▲ Group Policy Results ▲ usuario05 on CLIENTE01 	Security Filtering The settings in this GPO can only apply to the following groups, users, and computers: Name Image: Support Técnico (MONOGRAFIA\Support Técnico) Add Remove Properties WMI Filtering This GPO is Inked to the following WMI filter: (none> Vopen	
		14:45 18/03/2014

Ao editar a política de segurança padrão, todos os objetos do domínio são submetidos a nova regra geral. Permitindo que novas regras sejam criadas. Após a modificação da política padrão do AD foi criada a política de complexidade para o grupo alvo de experimento.





Figura 58 – Editor de Políticas de Contas

🧾 Group P	olicy Management Editor	_ 0 ×
<u>File Action View Help</u>		
🗢 🔿 📶 🗶 🗟 🔢 🖬		
File Action View Help Image: Software Settings Image: Software Settings Image: Software Resettings	Name Account Policies Local Policies Local Policies Restricted Groups System Services Registry File System Windows Firewall with Advanced Security Windows Firewall with Advanced Security Windows Firewall with Advanced Security Wineless Network (IEEE 802.3) Policies Wineless Network (IEEE 802.1) Policies Wineless Network (IEEE 802.1) Policies Public Key Policies Software Restriction Policies Software Restriction Policies Polication Control Policies P Security Policies on Active Directory (M Advanced Audit Policy Configuration	Description Password and account lockout policies Auditing, use rights and security options polici Even Log Restricted Groups System service settings Registry security settings File system security settings Wired Network Policy Administration. Manage Wired Network Policy Administration. Manage Wiredses Network Policy Administration. Manage Wireless Network Policy Administration. Mana Network Access Protection Application Control Policies Internet Protocol Security (IPsec) Administration Advanced Audit Policy Configuration
< III >		

Figura 59 – Acesso à Política de Senhas da GPO

🧾 Group P	olicy Management Editor		- 0	x
<u>File Action View H</u> elp				
◆ ⇒ 2 🚾 🗙 🗟 🖬				
Senha Complexa [DC01-W2012.MONOGRAFIA.LOCAL] Policy	Name	Description		
🔺 👰 Computer Configuration	Password Policy	Password Policy		
⊿ 🧮 Policies	Account Lockout Policy	Account Lockout Policy		
Software Settings	Herberos Policy	Kerberos Policy		
⊿ 🚞 Windows Settings		÷		
Name Resolution Policy				
Scripts (Startup/Shutdown)				
A here security Settings				
Account Policies				
Local Policies				
Event Log				
Restricted Groups				
System Services				
Registry				
File System				
Wired Network (IEEE 802.3) Policies				
Windows Firewall with Advanced Security				
Network List Manager Policies				
Wireless Network (IEEE 802.11) Policies				
Public Key Policies				
Software Restriction Policies				
Network Access Protection				
Application Control Policies				
Security Policies on Active Directory (MONOGRAFIA.EOCAL)				
Advanced Addit Policy Configuration				
Directory and the provided of the provided				
P Preferencer				
Ilser Configuration				
Policies				
< III >				

J Group	Policy Management Editor	_ 0 X
File Action View Help		
← → 2 🚾 🗙 🗉 🕞 🛛 🖬		
Senha Complexa [DC01-W2012.MONOGRAFIA.LOCAL] Policy	Policy ^	Policy Setting
Computer Configuration	Enforce password history	Not Defined
a 🧰 Policies	🔯 Maximum password age	Not Defined
Software Settings	Minimum password age	Not Defined
⊿ 🧮 Windows Settings	Minimum password length	Not Defined
Name Resolution Policy	Password must meet complexity requirements	Not Defined
Scripts (Startup/Shutdown)	Store passwords using reversible encryption	Not Defined
A Becurity Settings	s s s s s s s s s s s s s s s s s s s	
⊿ Account Policies		
Password Policy		
Account Lockout Policy		
Kerberos Policy		
Local Policies		
Event Log		
Restricted Groups		
System Services		
Registry		
File System		
Wired Network (IEEE 802.3) Policies		
Windows Firewall with Advanced Security		
Network List Manager Policies		
Wireless Network (IEEE 802.11) Policies		
Public Key Policies		
Software Restriction Policies		
Intervork Access Protection		
Application Control Policies		
Security Policies on Active Directory (MONOGRAFIA.LOC)		
Advanced Addic Policy Configuration		
Administrative Templates: Policy definitions (ADMX files) retrieved:		
Preferences		
4 Suser Configuration		
b Policies		
Preferences		
< III >		
	P	

Figura 60 – Editando a Regra de Complexidade de Senhas

Figura 61 – Habilitando a Política de Complexidade de Senhas

Password must meet complexity requirements Pro	?	x
Security Policy Setting Explain		
Password must meet complexity requirements		
Define this policy setting:		
Enabled		
⊖ Di <u>s</u> abled		
OK Cancel	Ap	ply

5.1.8.2 Verificar a Política Aplicada

Ao utilizar um usuário que não faz parte do grupo suporte técnico, a política permitiu que o usuário trocasse a senha por uma sem complexidade com sucesso. O usuário usuario04 fez acesso a máquina Cliente01 com a senha sem complexidade 123456 quando questionado para modificar, a senha nova foi coloca sem complexidade, 654321 e Windows permitiu a mudança com sucesso.

Quando o usuario5 que faz parte do grupo de suporte foi questionado a modificar a senha, foi feito o teste de colocar uma senha sem complexidade, o Windows retornou a necessidade de colocar uma nova senha respeitando a política de complexidade. O teste foi realizado com sucesso provando a eficácia da política aplicada.

Abaixe segue as imagens das respostas do Windows durante os testes:







Figura 63 – A Senha Deve Ser Modificada

Figura 64 – Troca de Senha

	©	Other user usuario04 Sign in to: MONOGRAFIA How do I sign in to another domain?
ભ		



Figura 65 – Senha foi Modificada para Uma de Baixa Complexidade

Figura 66 - Acesso do Usuário no Cliente





Figura 67 – A Senha deve Ser Modificada

Figura 68 – Troca de Senha





Figura 69 - Senha não Foi Modificada por ter Baixa Complexidade

Figura 70 - Senha Modificada com Por Complexidade Alta



5.1.9 Experimento 2 – Criação de Política de Acesso em Pastas de Servidor de Arquivos e Verificar os Resultados.

Neste experimento foi usado um servidor de arquivos off-site, ou seja, o armazenamento de arquivos está localizado em outro servidor que não o AD. O

servidor usado neste experimento é um Windows Server 2008 R2 nomeado de Server01.

5.1.9.1 Criação de Pastas no Servidor de Arquivos

Para criar as pastas no servidor de arquivos basta acessar o servidor Server01 entrar em documentos e criar a pastas para salvar arquivos.

Para experimento foram criadas três pastas, Marketing, Recursos Humanos e Suporte Técnico, conforme figura abaixo.

Documents						_ 8 ×
💽 🕞 🗸 Libraries 🔹	Documents *			•	Search Documents	2
Organize Share with	New folder					• 🔟 😧
🔆 Favorites	Documents library Includes: 2 locations				Arrange by:	Folder 🔻
Downloads Recent Places	Name *	Date modified	Туре	Size		
Marcon Proces	🕌 Marketing	24/02/2014 11:45	File folder			
🥽 Libraries	🁪 Recursos Humanos	24/02/2014 11:46	File folder			
Documents	鷆 Suporte Técnico	24/02/2014 11:46	File folder			
J Music						
Pictures						
La nacos						
🜉 Computer						
🙀 Network						
3 items						
灯 Start 🛛 🕌 🔰					PT 🕞 🙀 👍	18:08 24/02/2014 💻

Figura 71 – Pastas Criadas em Documentos

5.1.9.2 Criação da Política de Acesso ás Pastas de Armazenamento de Arquivos

A política de acesso às pastas é feita através do compartilhamento na rede das mesmas, atribuindo permissões conforme o desejado pelo administrador.

No caso do experimento será dada permissão de acesso a pasta Marketing aos usuários pertencentes ao grupo Marketing, a pasta Recursos Humanos ao grupo Recursos Humanos e a pasta Suporte Técnico ao grupo Suporte Técnico.

Para isso é preciso acessar a máquina Server01 e modificar as permissões de compartilhamento. O mesmo procedimento foi feito para todas as pastas e grupos respectivos.

Figura 72 – Acessando as Propriedades da Pasta

Documents						E ×
🚱 🗇 🖻 🔹 Libraries	× Documents ×				 Search Documents 	2
Organize 🔻 🎇 Open	Share with 🔻 New folder				III 👻 🗖	0
Favorites	Documents library Includes: 2 locations				Arrange by: Folder	•
Downloads Recent Places	Name *	Date modified	Туре	Size		
	📕 Marketing	24/02/2014 11:45	File folder			
Conjunctions Music Music Futures Computer Computer Network	Acursos Humanos	24/02/0014 11:46 24/02/0014 11:46	File folder File folder			
Marketing Dat File folder	te modified: 24/02/2014 11:45					

Figura 73 - Propriedades da Pasta

📜 Marketing P	roperties	×
General Shari	ng Security Previous Versions	
	Marketing	
Туре:	File folder	
Location:	C:\Users\administrator.MONOGRAFIA\Documents	
Size:	9 bytes (9 bytes)	
Size on disk:	4,00 KB (4.096 bytes)	
Contains:	1 Files, 0 Folders	
Created:	segunda-feira, 24 de fevereiro de 2014, 11:45:16	
Attributes:	Read-only (Only applies to files in folder)	
	Hidden Advanced	
	OK Cancel Apply	

Figura 74 – Aba de Compartilhamento da Pasta

📕 Marketing Properties 🛛 🗙 🗙
General Sharing Security Previous Versions
Network File and Folder Sharing
Marketing Not Shared
Network Path: Not Shared
[]
Advanced Sharing Set custom permissions, create multiple shares, and set other advanced sharing options.

Figura 75 – Compartilhamento Avançado

dvanced Sharing	×
Share this folder	
Settings	
S <u>h</u> are name:	
Marketing	
Add Remove	
Limit the number of simultaneous users to:	
Comments:	
OK Cancel Apply	

Figura 76 – Permissões de Acesso na Pasta

📜 Permissions for Marketing		×
Share Permissions		
<u>G</u> roup or user names:		
Susario01 Mono (usuario01 & Usuario02 & Usuario02 & Usuario02 Mono (usuario02 & Usuario02	Qmonografia.local) Qmonografia.local)	
	A <u>d</u> d	<u>R</u> emove
Permissions for Usuario01 Mono	Allow	Deny
Full Control Change Read	য য	
Learn about access control and p	ermissions	
ОК	Cancel	

Figura 77 – Aba de Segurança de Acesso a Pasta

📕 Marketing Propertie	:5			×
General Sharing Sec	urity Previous Ver	sions		_,
Objectiname: C:\Use	ers\administrator.MI	DNOGR.	AFIA\Documents	;
Group or user names:				
AN SYSTEM				
administrator (MON	NOGRAFIA\adminis	strator)		
Administrators (SE	RVIDOR01\Admini	strators)		
To change permissions	oliok Edit			
r o change permissions,	, CIICK L'UIC	_	<u>E</u> dit	
Permissions for SYSTEI	м	Allow	Deny	
Full control		~		
Modify		~		
Read & execute		~		
List folder contents		\sim		
Read		\sim		11
Write		~	-	
For special permissions click Advanced.	or advanced settin	gs,	Advanced	
Learn about access co	ntrol and permission	<u>15</u>		
	Close	Cancel	Apply	

Figura 78 – Grupo com Acesso a Pasta

🕌 Permissions for Marketing		X
Security		
Object name: C:\Users\adminis	trator.MONOGRA	FIA\Documents
Group or user names:		
administrator (MONOGBAEIA	(administrator)	
Administrators (SEBVIDOB01	(Administrators)	
Marketing (MONOGRAFIA\M	larketing)	
	-4	
,	1	
	A <u>d</u> d	<u><u>H</u>emove</u>
Permissions for Marketing	Allow	Deny
Full control		
Modify		
Read & execute		
List folder contents		
Read		
Learn about access control and pe	ermissions	
ОК	Cancel	

5.1.9.3 Verificação da Eficácia da Política de Acesso as Pastas

Verificação e teste da regra de segregação de pastas do servidor de arquivos.

Para fazer o teste é preciso acessar o computador cliente01, acessar a pasta correspondente ao grupo do usuário com sucesso e receber uma mensagem de acesso negado ao tentar acessar a pasta não correspondente ao grupo do usuário.

Acesso do usuário 1 a pasta correspondente:

Figura 79 – Credencias de Acesso

Segurança do Windows
Digite suas credenciais Essas credenciais serão usadas para a conexão com cliente01.
monografia\administrator
usuario01 Senha Domínio: monografia
Lembrar minhas credenciais
OK Cancelar

Figura 80 – Desktop do Cliente

Sta	rt					Usu	ario01
Mail		Calendar	Internet Explorer	Store	Bing		
People	**	Photos	Maps	SkyDrive			
Messagin	g	Finance	Sports		Games	Camera	
Desktop	***	Weather	News		Music	Video	
]/>				=

Para acessar a pasta compartilhada com a segurança é preciso acessar o servidor em que ela se encontra. No caso desse experimento o servidor de arquivos é o servidor01.

💭 📑 🔁 =	٤	ervidor01 -	. 🗆 🗙
F Home Share	View		~ e
	etwork > SERVIDOR01 >	✓ C Search servidor01	Q
 ★ Favorites ■ Desktop ֎ Downloads 2 Recent places ⇒ Libraries >> Documents → Music >> Pictures 	Marketing Share Share Share	Recursos Humanos Share Users Share	
Videos			
🗣 Network			
4 items			

Figura 81 – Janela no Cliente, do Servidor, com as Pastas Criadas

Ao acessar a pasta de Marketing, o usuário 1 tem acesso de controle

total.

🪇 🔒 🔁 =	M	arketing		-	×
F Home Share	View				~ 📍
€ ∋ - ↑ 🎍 ► N	etwork → servidor01 → Marketing		✓ C Searce	h Marketing	, P
	Name	Date modified	Type	Size	
Y Favorites			T ID I	1 1/0	
Desktop	MARKETING	2/24/2014 0:40 AIVI	Text Document	I KB	
Recent places					
🥽 Libraries					
Documents					
J Music					
Pictures					
Videos					
🎘 Computer					
👊 Network					
I CLIENTE01					
👰 DC01-W2012					
1 NBSB7925					
I SERVIDOR01					
🖳 tsclient					
1 item					

Ao tentar acessar a pasta de Recursos Humanos o usuário 1 recebe a seguinte mensagem:

Figura 83 – Acesso Negado ao Usuário na Pasta



E ao tentar acessar a pasta de suporte técnico o usuário 1 recebe a

mesma mensagem:

Figura 84 – Acesso Negado ao Usuário na Pasta



O mesmo acontece com o usuário 2. Para os usuários 3 e 4 o mesmo acontece quando acessam a pasta de Recursos humanos e para os usuários 5 e 6 ao tentarem acesso à pasta Suporte Técnico.

5.2 Testes com o OpenLDAP

Para instalar o OpenLDAP é preciso ter um sistema operacional Linux instalado em uma máquina física ou virtual. Como o Linux tem um código de programação aberto, foram identificados vários tipos diferentes de Linux cada um deles descendente de um código fonte diferente com diferentes comandos, porem grande parte deles tem quase os mesmos comandos para operações simples.

Para este experimento foi escolhido por sua popularidade o sistema operacional Linux distribuição Ubuntu.

Inicialmente foi criada uma máquina virtual com parâmetros prédeterminados, para este teste especifico com um ambiente relativamente pequeno, onde existe um servidor de serviço de diretório responsável por fazer a autenticação centralizada para poucas maquinas no caso um máximo de duas máquinas.

O hardware-virtual da máquina foi configurado com os seguintes parâmetros:

- Processamento da máquina hospedeira no caso um CORE i5;
- 1024 Mb de memória RAM dinâmica, ou seja, é possível balancear o uso da memória do computador hospedeiro com outras aplicações, disponibilizando mais ou menos memória conforme necessário;
- 16 Gb de Armazenamento em disco rígido virtual;

Após a criação da máquina virtual foi obtido o programa do sistema operacional em que será instalado o programa OpenLDAP, neste caso, a distribuição Linux Ubuntu versão 13.10. Além de estar sendo indicado o uso pelo livro Mastering OpenLDAP de Matt Butcher.

É preciso fazer a atualização do sistema após a instalação usando os comandos:

Apt-get update Apt-get dist-upgrade Apt-get upgrade Apt-get autoremove

Informação retirado do sítio: http://www.ubuntubrsc.com/13-principaiscomandos-do-ubuntu.html.

Para transformar a distribuição Ubuntu, sistema Linux com base Debian, em um servidor de serviço de diretório é preciso instalar o OpenLDAP e o pacote slapd. Os clientes estão no pacote Idap-utils, e as bibliotecas estão empacotadas na versão mais nova do libldap. Quando o pacote libldap está desatualizado e uma instalação é feita, o próprio Linux sugere uma biblioteca mais nova, como na imagem abaixo: Figura 85 – Falha na Instalação dos Pacotes



Neste caso o comando teve que ser modificado para apt-get install libldap-2.4-2 slapd ldap-utils.

Figura 86 – Instalação do Pacote



Figura 87 - Pacotes Instalados



Durante a instalação dos pacotes o usuário é questionado quanto a senha do usuário que será o administrador do serviço de diretório, em seguida o OpenLDAP está instalado. De acordo com o livro Mastering OpenLDAP de Matt Butcher é preciso fazer o backup do slapd.conf, arquivo de configuração do diretório que vem préconfigurado e criar um novo arquivo com o mesmo nome, porem, ao tentar localizar o arquivo, o Ubuntu informa que o arquivo não pode ser localizado.

Após esse erro, que de acordo com alguns sites está com o nome do arquivo desatualizado, foi feita a instalação do OpenLdap usando as informações do site oficial do OpenLDAP, porém, um erro de configuração de pré-requisitos para instalação é apresentado. Após varias tentavas de criar um laboratório com o OpenLDAP sem sucesso. Foi decidido então procurar um ambiente que já tem o sistema configurado para fazer os testes propostos nesse trabalho.

O primeiro desafio proposto tanto para o sistema Windows como para o sistema Linux é criar um banco de dados de usuários que possam ser consultados oferecendo o serviço de diretório.

O segundo desafio é restringir acesso de usuários a um arquivo ou pasta, levando em conta a segurança.

O terceiro desafio é forçar que cada usuário, para fazer acesso no domínio criado, tenha senha com nível de complexidade específico dependendo do privilegio do usuário.

5.2.1 Criar um domínio com um banco de usuários

De acordo com o *site* oficial do OpenLDAP para instalar o software é preciso primeiro fazer o *download* no próprio *site* da ultima versão e descompacta-lo usando o seguinte comando:

gunzip -c openIdap-VERSION.tgz | tar xvfB -

Onde openIdap-VERSION.tgz deve ser substituído pelo nome da ultima versão do programa. Em é necessário entrar no diretório criado com a descompactação, usando o comando:

cd openIdap-VERSION

Em seguida de entrar no diretório é preciso rodar o *script configure* que é fornecido no pacote OpenLDAP para construir a distribuição na máquina. O *script*

configure suporta vários outros comandos que habilitam ou desabilitam outras funcionalidades do sistema. O comando abaixo deve ser usado:

./configure (O comando "./configure --help" mostra outras funcionalidades que podem ser configuradas com outros comandos)

Para de construir o software é precisa usar dois comandos:

make depend

make

O passo seguinte é instalar o programa, usando o comando:

su root -c 'make install'

O comando "su" é usado para aumentar os privilégios do administrador.

Para criar o domínio é preciso editar o arquivo de configuração usando qualquer editor de arquivos para editar o arquivo slapd.conf para conter uma definição de banco de dados "BDB" no seguinte formato:

database bdb

suffix "dc=<MY-DOMAIN>,dc=<COM>" rootdn "cn=Manager,dc=<MY-DOMAIN>,dc=<COM>" rootpw secret directory /usr/local/var/openIdap-data

Neste caso é preciso substituir o "MY-DOMAIN" pelo nome do novo domínio, o domínio sugerido pelo site é *exemple.com*. A edição ficaria:

database bdb suffix "dc=exemple,dc=COM" rootdn "cn=Manager,dc=exemple,dc=com" rootpw secret directory /usr/local/var/openIdap-data

Para iniciar o servidor é preciso iniciar o Standalone LDAP Daemon, slapd, usando o comando:

su root -c /usr/local/libexec/slapd

De acordo com o site nesse momento o serviço de diretório está funcional, o próximo passo é adicionar novas entradas no diretório.

Para adicionar novas entradas no diretório é preciso criar um arquivo com extensão LDIF e rodar o comando "Idapadd".

Para criar a nova entrada é preciso abrir o arquivo LDIF com o editor de texto e completa-lo com alguns detalhes principais:

dn: dc=<MY-DOMAIN>,dc=<COM> objectclass: dcObject objectclass: organization o: <MY ORGANIZATION> dc: <MY-DOMAIN>

dn: cn=Manager,dc=<MY-DOMAIN>,dc=<COM> objectclass: organizationalRole cn: Manager

Após mudar os valores que estão entre os símbolos "<" e ">" o banco de dados do diretório tem o primeiro membro.

Com esses usuários no domínio pode-se acessar a maquina fazendo uma autenticação no banco de dados do diretório.

Porém o OpenLDAP é uma ferramenta que controla somente a autenticação de usuários, podendo fazer o controle dos usuários para acessar serviços usando listas de controle de acesso. Para fazer o controle de acesso a pastas e arquivos é preciso usar outro programa chamado SAMBA.

5.2.2 Por que SAMBA?

Em um ambiente de redes ideal, todos os computadores deveriam ser do mesmo fabricante, ter o mesmo sistema operacional, usar o mesmo protocolo de comunicação, ou seja, todos os equipamentos deveriam ser preparados pela mesma empresa para se comunicarem perfeitamente uns com os outros. Isso não é o que acontece. Hoje existem centenas de equipamentos que fazem a mesma coisa, que se comunicam por protocolos diferentes, tem fabricantes diferentes, formas diferentes, quase tudo diferente, porém, todos eles se comunicam entre si e realizam as funções que foram criados para realizar.

Usando esse pensamento e trazendo para a realidade, quase todas as empresas tem ambientes mistos, com equipamentos de diferentes fabricantes, sistemas operacionais diversos, e milhões de ferramentas de operação. O Samba é uma ferramenta que que consegue fazer o gerenciamento de diretório, compartilhamento de arquivos, entre outra várias funcionalidades, entre a maioria, quase totalidade, dos sistemas operacionais do mundo.

O Samba implementa o protocolo de rede CIFS (Common Internet File System). Usando esse protocolo, o Samba permite que computadores com sistemas operacionais baseados no UNIX como, Linux, FreeBSD, CentOS, Solaris e OS X, se comuniquem com o Windows da Microsoft ou qualquer outro sistema que utilize o protocolo CIFS, seja ele um cliente ou um servidor. (CARTER, 2007)

Para este trabalho a forma genérica é a melhor opção, devido os ambientes de rede terem maquinas Microsoft e Unix.

5.2.3 Testes Samba

Para iniciar um serviço de diretório usando o SAMBA é preciso ter um IP estático para que sempre que o IP for consultado ele tenha um dono. Nesse experimento o IP do SAMBA é 192.168.1.100 em um Ubuntu Server 14.04 e o IP de uma estação de trabalho é 192.168.1.110 usando o Windows 8.1.

Também é preciso ter certeza de que o nome do servidor está correto porque após a instalação do serviço de diretório não será mais possível modifica-lo, nesse caso o servidor se chamará *ubuntuserver*.

5.2.3.1 Instalação do Ubuntu Server 14.04

Para fazer a instalação do Ubuntu Server foi criada uma máquina virtual no Hyper-V, ferramenta de virtualização do Windows para simular um rede. É preciso entrar no site oficial do Ubuntu, http://www.ubuntu.com/download/server, para fazer o download do sistema operacional.

Uma vez com o sistema operacional é preciso inicia-lo na máquina virtual.

Em um primeiro momento é preciso escolher a língua que terá o servidor Ubuntu.

Language				
Amharic	Français	Македонски	Tamil	
Arabic	Gaeilge	Malayalam	తెలుగు	
Asturianu	Galego	Marathi	Thai	
Беларуская	Gujarati	Burmese	Tagalog	
Български	עברית	Nepali	Türkçe	
Bengali	Hindi	Nederlands	Uyghur	
Tibetan	Hrvatski	Norsk bokmål	Українська	
Bosanski	Magyar	Norsk nynorsk	Tiếng Việt	
Català	Bahasa Indonesia	Punjabi(Gurmukhi)	中文(简体)	
Čeština	Íslenska	Polski	中文(繁體)	
Dansk	Italiano	Português do Brasil		
Deutsch	日本語	Português		
Dzongkha	ქართული	Română		
Ελληνικά	Қазақ	Русский		
English	Khmer	Sámegillii		
Esperanto	ಕನ್ನಡ	ເ ພິ∘ກ⊚		
Español	한국어	Slovenčina		
Eesti	Kurdî	Slovenščina		
Euskara	Lao	Shqip		
ىسراف	Lietuviškai	Српски		
Suomi	Latviski	Svenska		
Help F2 Language F3	Keymap F4 Modes	F5 Accessibility F6 O [.]	ther Options	

Figura 88 – Idioma do Sistema

Após a escolha de língua o Ubuntu se apresenta interativo, questionando quanto as ações a serem tomadas, por exemplo questionando se o disco do sistema deve ser usado para criar um novo servidor. Em seguida questionando quanto a língua do sistema e a língua padrão do teclado.



Figura 89 – Aviso de Instalação do Sistema Operacional

Figura 90 - Idioma para a Instalação

[!!] Sele Choose the language to be used for the inst also be the default language for the instal Language: C Albanian Arabic Asturian Basque Belarusian Bosnian Bulgarian	ct a language allation process. The selected language will led system. - No localization * - Shqip - چربي - Asturianu - Euskara - Беларуская - Bosanski - Български
Catalan Chinese (Simplified) Chinese (Traditional) Croatian Czech Danish Dutch Codlick	- Català - 中文(简体) - 中文(衛體) - Hrvatski - Čeština - Dansk - Nederlands
Engeranto Esperanto Estonian Finnish French Galician German Greek	- Engrish - Esperanto - Eesti - Suomi - Français - Galego - Deutsch - Ελληνικά ≁
<go back=""></go>	
rab> moves; ≺Space> selects; ≺Enter> activates	; buttons

Figura 91 - Configuração de Localidade

Country to base default	e used is listed in the ilocale settings on: Antigua and Barbuda Australia Botswana Canada Hong Kong India Ireland New Zealand Nigeria Philippines Singapore Couth Ofeice	- en. - en. - en. - en. - en. - en. - en. - en. - en. - en.	Column. _AG _AU.UTF-8 _BW.UTF-8 _CA.UTF-8 _IK.UTF-8 _IN _IE.UTF-8 _NZ.UTF-8 _NG _PH.UTF-8 _SG.UTF-8 _SG.UTF-8	
	United Kingdom United States Zambia Zimbabwe	- en, - en, - en, - en,	8.UTF-8 _US.UTF-8 _ZM _ZW.UTF-8	
<go back=""></go>				

Figura 92 – Detecção de Teclado

[!] Configure the keyb You can try to have your keyboard layout detected by not want to do this, you will be able to select your	poard pressing a series of keys. If you do keyboard layout from a list.
Go Back>	<yes> <mark><no></no></mark></yes>

	[!] Configure the keyboard
	The layout of keyboards varies per country, with some countries having multiple common layouts. Please select the country of origin for the keyboard of this computer.
	Country of origin for the keyboard:
	Irish Italian Japanese Japanese (PC-98xx Series) Kazakh Khmer (Cambodia) Korean Kyrgyz Lao Latvian Lithuanian Macedonian Macedonian Matese Maori Moldavian Mongolian Montenegrin Nepali Norwegian Persian Polish Portuguese (Brazil)
	<go back=""></go>
<tab< th=""><th>»> moves; <space> selects; <enter> activates buttons</enter></space></th></tab<>	»> moves; <space> selects; <enter> activates buttons</enter></space>

Figura 93 – Configuração de Idioma do Teclado

Uma das partes mais importantes da instalação é a criação do nome do servidor que deve ser escolhido com cuidado pois não poderá ser trocado quando o serviço de diretório estiver instalado e configurado.

Figura 94 – Nome do Servidor

Please enter th	ne hostname for thi	!] Configure the net s system.	work	
The hostname is know what your up your own hor	s a single word tha hostname should be me network, you can	t identifies your sy , consult your netwo make something up h	stem to the network. rk administrator. I ere.	. If you don't f you are setting
Hostname:				
ubuntuserver				
<go back=""></go>				<continue></continue>

Figura 95 – Usuário Administrador do Servidor

Full name for the new user: administrator <continue></continue>	non-administrative activities. Please enter the real name of this user. This information wil default origin for emails sent by this user as well as any pr the user's real name. Your full name is a reasonable choice	root account for l be used for instance as ogram which displays or uses
<go back=""> <continue></continue></go>	Full name for the new user: administrator	
	<go back=""></go>	<continue></continue>



le choice. The d by any combination
<continue></continue>

Figura 97 - Senha do Usuário Administrador do Servidor





he system will seamless utomatically unmount who	ly mount your encrypted home directory each time you login and
he system will seamless utomatically unmount who ncrypt your home directo	ly mount your encrypted home directory each time you login and
ncrypt your home direct	en you log out of all active sessions.
	pry?
<go back=""></go>	<mark><yes></yes></mark> <no></no>

Figura 99 – Configuração de Horário do Servidor

[!] Configure the clock Select a city in your time zone: Noronha Belem Fortaleza Recife Araguaina Maceio Bahia Sao Paulo Campo Grande Cuiaba Porto Velho Boa Vista Manaus Eirunepe Rio Branco Select from worldwide list <go back=""></go>	

Pela função do servidor ser inicialmente somente de controlador de domínio, o sistema será instalado em uma só partição com 16 Gb.

Figura 100 – Guia para Particionamento do Servidor

	[!!] Partition disks
The installer schemes) or, i still have a c	can guide you through partitioning a disk (using different standard if you prefer, you can do it manually. With guided partitioning you will chance later to review and customise the results.
If you choose should be used	guided partitioning for an entire disk, you will next be asked which disk d.
Partitioning m	method:
	Guided – use entire disk <mark>Guided – use entire disk and set up LVM</mark> Guided – use entire disk and set up encrypted LVM Manual
<go back=""></go>	

Figura 101 – Disco para Instalação

the disk you select will be erased, but not before you have ally want to make the changes.
ion:
3I3 (0,0,0) (sda) – 16.1 GB Msft Virtual Disk
S

Figura 102 – Salvar Configurações

		[!!] Partition o	disks	
Before the L to be writte	ogical Volume Mana n to disk. These cl	ger can be configure hanges cannot be unc	ed, the current par done.	titioning scheme has
After the Lo scheme of di decide if yo	gical Volume Manag sks containing phy u are satisfied wi	er is configured, no sical volumes are al th the current parti	o additional change Llowed during the i itioning scheme bef	s to the partitionin nstallation. Please ore continuing.
The partitic SCSI3 (0,	n tables of the fo 0,0) (sda)	llowing devices are	changed:	
Write the ch	anges to disks and	configure LVM?		
<yes></yes>				<no></no>

Figura 103 – Tamanho do Disco para Instalação

You may use the whole volume group for guided partitioning, or part of it. If you use only part of it, or if you add more disks later, then you will be able to grow logical volumes later using the LVM tools, so using a smaller part of the volume group at installation time may offer more flexibility. The minimum size of the selected partitioning recipe is 2.0 GB (or 12%); please note that the packages you choose to install may require more space than this. The maximum available size is 15.8 GB. Hint: "max" can be used as a shortcut to specify the maximum size, or enter a percentage (e.g. "20%") to use that percentage of the maximum size. Amount of volume group to use for guided partitioning:
<pre><go back=""> <continue></continue></go></pre>

Figura 104 – Salvar Alterações no Disco

If you contin	ue, the changes list	ed below will be	written to the di	sks. Otherwise, you
will be able	o make further chan	ges manually.		
The partition LVM VG ubu LVM VG ubu SCSI3 (0,0	tables o+ the follo ituserver–vg, LV roo ituserver–vg, LV swa .0) (sda)	wing devices are t p_1	changed:	
The following LVM VG ubu LVM VG ubu partition	partitions are goin htuserver–vg, LV roo htuserver–vg, LV swa 1 of SCSI3 (0,0,0)	g to be formatte t as ext4 p_1 as swap (sda) as ext2	d:	
Write the cha	nges to disks?			
<yes></yes>				<no></no>

Como não existe proxy configurado esse questionamento é deixado em branco.



	[!] Configure the package manager If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank. The proxy information should be given in the standard form of "http://[[user][:pass]@]host[:port]/". HTTP proxy information (blank for none):
l	
	<pre><go back=""> <continue></continue></go></pre>
	<pre></pre> <go back=""> Continue></go>
	<pre> <go back=""> <cont inue=""></cont></go></pre>

Figura 106 – Instalar Atualizações Automaticamente

[!] Configuring tasksel
Applying updates on a frequent basis is an important part of keeping your system secure.
By default, updates need to be applied manually using package management tools. Alternatively, you can choose to have this system automatically download and install security updates, or you can choose to manage this system over the web as part of a group of systems using Canonical's Landscape service.
How do you want to manage upgrades on this system?
No automatic updates <mark>Install security updates automatically</mark> Manage system with Landscape

Figura 107 – Instalação da Aplicação SSH

[!] Software selection At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.
Choose software to install: (*) OpenSSH server [] DNS server [] LAMP server [] Mail server [] PostgreSQL database [] Print server [] Samba file server [] Tomcat Java server [] Tomcat Java server [] Virtual Machine host [] Manual package selection
<cont inue=""></cont>

Figura 108 –	Instalar	o Carregador	de	Inicializac	ão
i iguiu i oo	motulai	o ounoguaor	au	nnoiunzuų	uu

ſ	[!] Install the GRUB boot loader on a hard disk			
	It seems that this new installation is the only operating system on this computer. If s it should be safe to install the GRUB boot loader to the master boot record of your fir hard drive.			
	Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.			
	Install the GRUB boot loader to the master boot record?			
	<go back=""> <</go>			

Figura 109 – Instalação Completa

_	
	[!!] PAM configuration Installation complete Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation. <go back=""> </go>
Após a instalação é preciso configurar o sistema.

5.2.3.2 Configuração do Controlador de Domínio

Inicialmente é preciso entrar com o usuário criado na instalação.

Figura 110 - Primeiro Acesso no Servidor



Em seguida configurar uma senha para usuário administrador.

Figura 111 – Configuração de Senha do Usuário



Figura 112 – Confirmação de Senha do Usuário



5.2.3.3 Configurar IP Estático

Para estabelecer um servidor que tem um serviço estático na rede é preciso atribuir um IP estático ao servidor. Para essa configuração foi usado o IP 192.168.1.100 classe C. Para fazer essa configuração é preciso modificar as configurações no diretório de redes do servidor usando o seguinte comando: *vi* /*etc/network/interfaces*. Com esse comando é possível editar as configurações da placa de rede.

Figura 113 – Verificação de IP



Figura 114 – Configuração da Interface



Figura 115 – Configuração da Interface com Valores Estáticos



5.2.3.4 Modificar o Nome do Computador

Para modificar o nome do computador é preciso editar o arquivo que contem o nome do computador com o comando: *vi /etc/hosts*. Assim completar o nome do host com nome dele no formato do futuro domínio que será MONOGRAFIA.LOCAL e o seu novo IP atribuído estaticamente.

Figura 116 – Acessando o Arquivo de Hosts







Figura 118 - Adicionando o Domino e o IP no Arquivo de Hosts





Figura 119 – Salvando a Configuração no Hosts

5.2.3.5 Atualizar o Sistema

Para fazer a instalação do SAMBA é preciso fazer a atualização completa do sistema, para isso é preciso rodar os comandos *apt-get update* e *apt-get upgrade*.

Figura 120 – Upgrade do Ubuntu Server



5.2.3.6 Pré-requisitos

Para que o SAMBA funcione como planejado é preciso instalar pacotes que são pré-requisitos para fazer o SAMBA se tornar um controlador de domínio, como o pacote *krb5-user* que fornece suporte a autenticação kerberus do Windows. Para isso é preciso instalar os pacotes com o seguinte comando: *apt-get install git build-essential libacl1-dev libattr1-dev libblkid-dev libgnutls-dev libreadline-dev python-dev python-dnspython gdb pkg-config libpopt-dev libldap2-dev dnsutils libbsddev attr krb5-user docbook-xsl libcups2-dev libpam0g-dev ntp –y*.

Uma vez instalado, o pacote krb5-user questiona qual será o nome do futuro domínio e o nome do servidor que terá o domínio, no caso o nome do domínio escolhido foi MONOGRAFIA.LOCAL e o nome do servidor *ubuntuserver*.

Figura 121 – Instalação do Kerberus



Figura 122 – Inclusão de Nome do Domínio





Figura 123 – Inclusão do Nome do Servidor Kerberus

Figura 124 - Inclusão do Nome do Servidor de Administração



5.2.3.7 Instalação do SAMBA

Para fazer a instalação do SAMBA é preciso fazer uma cópia do programa de uma página de downloads na internet e depois compilar o programa. De acordo com os tutoriais o SAMBA 4 precisa ser copilado pois ainda não existia no repositório do comando apt-get. O comando usado para baixar o SAMBA 4 é: *git clone -b v4-0-stable git://git.samba.org/samba.git samba4*. Uma vez baixado o programa é preciso ir até a pasta do programa e executar a seguinte sequencia de comandos para compila-lo:

- ./configure --enable-debug --enable-selftest
- make
- make install

Figura 125 – Comando Debug do Clone



Figura 126 – Comando Make

getcud takes a NULL argument	: nk
Checking for library gen	not found
Checking for getsmam	: nk
Checking for header sus/fs/ux mota h	10
Checking for header sus/mota.h	: Hes
Checking for header ufs/granta.h	: 00
Checking for header xfs/xmm.h	no
for XFS QUOTA in (sus/guota.h)	: not found
Checking for member dab fsoftlimit in struct dablk	: not found
Checking for member dab curbutes in struct dablk	: not found
Checking for header rocsvc/rguota.h	: ues
Checking for member getguota rslt u in struct getguota rslt	: ok
Checking for header ctdb.h	: not found
building without cluster support: ctdb.h is required for cluster support	
Checking whether we can compile with attribute ((destructor))	: ok
Checking whether seekdir returns void	
Checking for pthread attr init	
Checking for header gpfs gpl.h	
Checking for header linux/ioctl.h	: yes
Checking for header cephfs/libcephfs.h	: no
Checking for glusterfs-api >= 4	: not found
Checking for header api/glfs.h	
Checking for library gfapi	
Looking for neurses features	
Checking for program neurses5-config	: /usr/bin/ncurses5-config
Checking for /usr/bin/ncurses5-config	: yes
Checking for header neurses.h	
Checking for header menu.h	
Checking for header panel.h	
Checking for header form.h	
Checking for library neurses	: not found
Checking for initscr	: not found
Checking for library menu	: not found
Checking for set_menu_items	: not found
Checking for item_count	: not found
Checking for library panel	: not found
Checking for new_panel	: not found
Checking for show_panel	: not found
Checking for library form	i not found
Checking for hew_1 leld	not found
Checking for hew_form	: not rouna
neurses not dvallable, not bullaing regeatt	
Checking linker accepts -w1,-nu-underined	· yes
Checking linker accepts i -under meu, ugnamic_rookup i	
Checking fon - le vot needed	· ges
Checking configure summary	· ok
Checking complex for PIF support	• UK
Checking for lisustend-daemon	not found
Checking for header sustem/sd-daemon h	noo round
Checking for Jibrary system-daenon	no
Checking compiler accepts -g	: ues
configure' finished successfullu (3m22,907s)	
rootQubuntuserver:/home/administrator/samba4# make	

Figura 127 – Comando Make Install

[3796/3842]	Linking default/source3/modules/libufs-aio-fork.so
[3797/3842]	Linking default/source3/modules/libufs-default-quota.so
[3798/3842]	Linking default/source3/pysmbd.so
[3799/3842]	Linking default/source3/modules/libufs-fake-perms.so
[3800/3842]	Linking default/source3/modules/libufs-readonly.so
[3801/3842]	Linking default/source3/modules/libufs-smb-traffic-analyzer.so
[3802/3842]	Linking default/source3/modules/libufs-dirsort.so
[3803/3842]	Linking default/source3/modules/libuts-aio-posix.so
[3804/3842]	Linking default/source3/modules/libuts-nfs4acl-xattr.so
[3805/3842]	Linking default/source3/modules/libufs-acl-xattr.so
[3806/3842]	Linking default/source3/modules/libufs-xattr-tdb.so
[3807/3842]	Linking default/source3/modules/libuts-shadow-comu.so
[3808/3842]	Linking default/source3/modules/libuts-netatalk.so
[3809/3842]	Linking default/source3/modules/libuts-full-audit.so
[3810/3842]	Linking default/source3/modules/libuts-ratia so
[3811/3842]	Linking default/source3/andules/libus-recurde so
[3812/3842]	Linking default source3/modules/libus-cajo-thread so
[3813/3842]	Linking default/ sources/modules/libu(s-lake-acts so
[3814/3842]	Linking default/source3/modules/liby/s-streamystry so
[3815/3842]	Linking default/sources/modules/libus/sources/to-auto-so
13816/38421	Linking default/sources/modules/liby/s_con so
13010/30121	Linking default/source3/modules/libus-libus-vfc-grid on
[3010/3012]	Linking default/sources/condities/fibris/filmax/kis/sglu.so
[J010/J012]	Linking default/source/smuthant
13013/30423	Linking default/source2/visitest
13020730123	Linking default/sources/modules/fibris-streams-depluse
13021/30121	Linking default/sources/modules/libus/scaling.ob/
13022/30123	Linking default/source/modules/fibits-post-calb.so
13023/30421	Linking default/sources/modules/libuts-ot/ris.so
13024/30421	Linking default/sources/modules/liburs-addit.so
13023/30421	Linking default/sources/modules/linking/bisix_dcls.so
13020/30421	Linking default/source3/smbtatus
13027/30421	Linking default/sources/modules/libuts-sgncops.so
13020/30421	Linking def du L/sources/modules/libus-readanead.so
13829/38421	Linking default/source3/modules/libuts-time-audit.so
13830/38421	Linking default/sources/net
[3831/3842]	Linking default/source3/modules/libu/s-expand-msdfs.so
[3832/3842]	Linking default/sources/modules/libuts-shadow-copy2.so
13833/38421	Linking default/source3/modules/libuts-crossrename.so
13834/38421	Linking default/source3/modules/libvfs-acl-tdb.so
13835/38421	Linking default/source3/modules/libuts-preopen.so
13836/38421	Linking default/source3/modules/libufs-media-harmony.so
13837/38421	pidl.1p: pidl/pidl -> bin/default/pidl.1p
[3838/3842]	Parse::Pidl::Dump.3pm: pidl/lib/Parse/Pidl/Dump.pm -> bin/default/pidl/Parse::Pidl::Dump.3pm
[3839/3842]	Parse::Pidl::Wireshark::Conformance.3pm: pidl/lib/Parse/Pidl/Wireshark/Conformance.pm -> bin/default/pidl/Parse::Pidl::Wireshark::C
nformance.3	pn
[3840/3842]	Parse::Pidl::Util.3pm: pidl/lib/Parse/Pidl/Util.pm -> bin/default/pidl/Parse::Pidl::Util.3pm
[3841/3842]	Parse::Pidl::NDR.3pm: pidl/lib/Parse/Pidl/NDR.pm -> bin/default/pidl/Parse::Pidl::NDR.3pm
[3842/3842]	Farse::Pidl::Wireshark::NDR.3pm: pidl/lib/Parse/Pidl/Wireshark/NDR.pm -> bin/default/pidl/Parse::Pidl::Wireshark::NDR.3pm
Waf: Leavin	g directory =/home/administrator/samba4/bin'
'build' fin	ished successfully (40m35.860s)
root@ubuntu:	server:/home/administrator/samba4#
root@ubuntu:	server:/home/administrator/samba4#
root@ubuntu:	server:/home/administrator/samba4#
root@ubuntu:	server:/home/administrator/samba4# make install

Para fazer a instalação do domínio é preciso ir ao arquivo de configuração do SAMBA o samba-tool. Para isso foi usado o seguinte comando: /usr/local/samba/bin/samba-tool domain provision --realm=monografia.local – domain=MONOGRAFIA --adminpass="P@ssw0rd" --server-role=dc --dns-backend=SAMBA_INTERNAL.

Uma vez que o domínio está configurado é preciso iniciar o serviço do SAMBA usando o comando /usr/local/samba/sbin/samba.

Figura 128 – Criação do Domínio

* installing lib/testtools/testtools/testsuite.py as /usr/local/sanba/lib/python2.7/site-packages/sanba/external/testtools/testsuite.py
* installing lib/testtools/testtools/utils.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/testtools/utils.py
* installing lib/subunit/python/subunit/_initpy_as_/usr/local/samba/lib/python2.?/site-packages/samba/external/subunit/_initpy
* installing lib/subunit/puthon/subunit/chunked.pu as /usr/local/samba/lib/puthon2.7/site-packages/samba/external/subunit/chunked.pu
* installing lib/subunit/withon/subunit/details.nu as /usr/local/samba/lib/nuthon2.7/site-nackages/samba/external/subunit/details.nu
installing lib/subunit/cuthan/subunit/cilters nu as /usr/local/samba/lib/nuthan? 2/site-nackages/samba/external/subunit/cilters nu
installing lib/subunit/suthan/subunit/isoB601 nu as /usr/local/sabba/lib/suthan? 2/site-nackage/sabba/systemal/subunit/isoB601 nu
* installing lib/cubunit/puthon/cubunit/isoboting us/us/local/camb/lib/uthon? Zite-mackare/camba/cytemal/cubunit/morenees_model
 insuffing fib/suburity prenov suburity progress_mouting us y usiy rocary summarity prenome it ys the packagesy summarity progress_mouting, and any suburity progress_mouting, and
py w installing lik gubunit guthan gubunit gun mu an gung local gamba (lik guthan) 7 gaita-nagkagan gamba gaytannal gubunit gun mu
instairing in/subunit/python/subunit/run.py as /usr/iota/samba/in/pythona.r/site=package/s/samba/caternal/subunit/run.py
\sim installing TD subunity periods subunity tests (results, pg as year) local samuely TD period. (\sim 15 to packages samuely tests (results) and \sim tests, pg is installing TD subunity methods (reduced to be a front between the submethods) and the submethod of the submethod submethods (reduced to be submethods) and the submethod subm
* This affing The subunity pythony subunity tests restored, by a subry local samparity pythone. (Site packages samparesternal subunity tests restored, by a
μ y w installing lik (when it withou (when it starts) init we as show loss loss has the withou? Traits and some contains (when it starts) init
* Instanting The subunity periods subunity tests/_initpg/as/suse/incar/sanba/in/periods.r/site=packages/sanba/external/subunity tests/_init
μη ν installing lik gubusik guduan gubusik generale engine av en dessloeret engele dit guduar? Τα ide verkegene general gubusik generale enge
Installing lib/subunit/pytnon/subunit/tests/sample-script.py as /usr/local/samba/lib/pytnon2.//site-packages/samba/external/subunit/tests/sample-script.py as /usr/local/samba/lib/pytnon2.//site-packages/samba/external/subunit/tests/sample-script.pytnon2.//site-packages/samba/external/subunit/tests/sample-script.pytnon2.//site-packages/samba/external/subunit/tests/sample-script.pytnon2.//site-packages/samba/external/subunit/tests/sample-script.pytnon2.//site-packages/samba/external/subunit/tests/sample-script.pytnon2.//site-packages/samba/external/subunit/tests/sample-script.pytnon2.//site-packages/samba/external/subunit/tests/sample-script.pytnon2.//site-packages/samba/e
ie-script.pg
* Installing Indesubulit/python/subulit/tests/sample-two-script.py as /usr/local/samba/lib/python2.//site-patkages/samba/external/subulit/tests/
sample-two-script.py
* installing lib/subunit/python/subunit/tests/test_chunked.py as /usr/local/samba/lib/python2.//site-packages/samba/external/subunit/tests/test_
chunked.py
* installing lib/subunit/python/subunit/tests/test_details.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_
details.py
* installing lib/subunit/python/subunit/tests/test_progress_model.py_as_/usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/test
s/test_progress_model.py
* installing lib/subunit/python/subunit/tests/test_run.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/test_run.
* installing lib/subunit/python/subunit/tests/test_subunit_filter.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/test
s/test_subunit_filter.py
* installing lib/subunit/python/subunit/tests/test_subunit_stats.py as /usr/local/samba/lib/python2.?/site-packages/samba/external/subunit/tests
/test_subunit_stats.py
* installing lib/subunit/python/subunit/tests/test_subunit_tags.py as /usr/local/samba/lib/python2.?/site-packages/samba/external/subunit/tests/
test_subunit_tags.py
* installing lib/subunit/python/subunit/tests/test_tap2subunit.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/t
est_tap2subunit.py
installing lib/subunit/python/subunit/tests/test_test_protocol.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests
/test_test_protocol.py
installing lib/subunit/python/subunit/tests/test_test_results.py as /usr/local/samba/lib/python2.7/site-packages/samba/external/subunit/tests/
test_test_results.py
* installing bin/default/pidl/pidl.1p as /usr/local/samba/share/man/man1/pidl.1p
* installing bin/default/pidl/Parse::Pidl::Dump.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Dump.3pm
* installing bin/default/pidl/Parse::Pidl::Wireshark::Conformance.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Wireshark::Conformance.3pm
* installing bin/default/pidl/Parse::Pidl::Util.3pm as /usr/local/samba/share/man/man3/Parse::Pidl::Util.3pm
* installing_bin/default/pidl/Parse::Pidl::NDR.3pm_as_/usr/local/samba/share/man/man3/Parse::Pidl::NDR.3pm
* installing binzdefault/pidl/Parse::Pidl::Wireshark::NDR.3pm as zusrzlocalzsambazsharezmanzman3zParse::Pidl::Wireshark::NDR.3pm
Waf: Leaving directory '/home/administrator/samba4/bin'
'install' finished successfully (16m3.136s)
root@ubuntuserver:/home/administrator/samba4#
root@ubuntuserver:/home/administrator/samba4#
root@ubuntuserver:/home/administrator/samba4#
root@ubuntuserver:/home/administrator/samba4#
root@ubuntuserver:/home/administrator/samba4# /usr/local/samba/bin/samba-tool domain provisionrealm=monografia_localdomain=MONOGBOFIAad
ninpass="P@sw0rd"server-role=dcdns-backend=SAMBA_INTERNAL

Figura 129 – Iniciar Serviço do SMB



5.2.3.9 Configuração do DNS

Para configurar o DNS no domínio é preciso incluir o domínio no arquivo *resolv.conf* e editar o arquivo de configuração do SAMBA, o *smb.conf*. Para modificar o arquivo de configuração é preciso usar o comando: *vi* /usr/local/etc/smb.conf. Ao editar o arquivo é preciso substituir o forwarder para o IP do Google, 8.8.8.8, salvar e fechar o arquivo.

Figura 130 – Comando Configuração do DNS



Figura 131 – Arquivo de Configuração do DNS





Figura 132 – Arquivo de Configuração do DNS com IP do Google

Para configurar o *Kerberos* no Linux é preciso editar o arquivo de configuração *krb5.conf* entrando com o comando: *vi* /usr/local/samba/share/setup/krb5.conf. Ao entrar no arquivo de configuração é preciso substituir a expressão \$(REALM) por MONOGRAFIA.LOCAL e em seguida realizar um teste para verificar o funcionamento. Para realizar o teste é preciso usar a seguinte sequência de comandos: *kinit administrator*@MONOGRAFIA.LOCAL e *klist -e*.

^{5.2.3.10} Configurar o Kerberos





Figura 134 – Arquivo de Configuração do Kerberus





Figura 135 – Arquivo de Configuração do Kerberus com o Domínio

Figura 136 - Confirmação de Funcionamento do Kerberus



5.2.3.11 Pastas para Usuários

É muito importante criar a pasta *Users* no domínio para que o perfil dos novos usuários sejam criados organizadamente. Para isso deve-se executar a seguinte sequência de comandos:

mkdir -m 770 /Users chmod g+s /Users chown root:users /Users

Após criar as pastas para armazenamento é preciso configurar o arquivo do de configuração do samba para que o sistema entenda que os novos perfis devem ser criados no local determinado. O comando para editar o arquivo de configuração é: *vi /usr/local/samba/etc/smb.conf*. Ao entrar no arquivo de configuração é preciso acrescentar as seguintes linhas:

[Users] directory_mode: parameter = 0700 read only = no path = /Users csc policy = documents

Figura 137 – Comando para Edição de Smb.conf







Figura 139 – Arquivo de Configuração do SAMBA com Parâmetro de Usuários



5.2.3.12 Senha de Administrador

Após criada a senha do administrador do domínio é preciso fazer com que ela não expire usando o comando /usr/local/samba/bin/samba-tool user setexpiry administrator –noexpiry.

Figura 140 – Retirar Regra de Expiração de Senha



5.2.3.13 Configurar IP da Máquina Cliente

Para que computadores sejam adicionados no domínio, primeiro é preciso colocar o computador que entrará no domínio, cliente, na mesma rede em que o servidor está. Para este computador cliente foi criada uma maquina virtual com o Windows 8.1 da Microsoft. Para o caso deste trabalho é preciso colocar um IP estático devido a nenhum servidor DHCP ter sido configurado na rede. O IP escolhido foi o 192.168.1.110. Para configura-lo é preciso entrar no painel de controle da máquina e acessar a central de rede e compartilhamento. Em seguida acessar a placa de rede e configurar as propriedades da placa no que diz respeito ao IPv4.

Para confirmar se a configuração está correta é preciso acessar o prompt de comando do computador e usar o comando ICMP para checar a comunicação entre as maquinas: *ping 192.168.1.100*.



Figura 141 - Central de Rede e Compartilhamento do Windows

Figura 142 - Status de Conexão

1	¥	Network and Sharing Cen	ter	_ [x I
3	🕞 🏵 🔻 🕈 🔽 « Network ar	nd Internet 🔸 Network and Sharing Center	v C	Search Control Panel	Q
Recycle Bin	Control Panel Home	View your basic network informatic	on and set up co ×	opnections	
	Change adapter settings Change advanced sharing settings	General Connection — IPv4 Connectivity: No IPv6 Connectivity: No Media State: Duration:	Internet access Internet access Enabled 00:02:47	No Internet access	
		Speed: Details	10.0 Gbps	a router or access point.	
		Activity	Received 10.056.119	ting information.	
	See also HomeGroup		Close		
	Internet Options Windows Firewall				
					Windows 8.1 Enterpris Build 960
E	🚔 😝				18:15 28/09/2014



Figura 143 – Propriedades da Interface de Rede

Figura 144 – Inserção de IP Estático para a Estação de Trabalho





Figura 145 – Verificação de Comunicação de Rede com Servidor Linux

Figura 146 - Verificação de Comunicação de Rede com Estação de Trabalho



5.2.3.14 Adicionar Computador Cliente no Domínio

Da mesma forma que é feito no ambiente configurado com o controlador de domínio da Microsoft é preciso incluir o computador cliente manualmente no domínio. Para isso é preciso acessas as propriedades do computador e modificar as configurações. Ao acessar essas configurações é preciso colocar o nome do domínio completo no caso, monografia.local. Em seguida é preciso colocar as credenciais que foram configuradas no servidor para o administrador do domínio, no caso o *login* é administrator e a senha *P@ssw0rd*.

Figura 147 – Propriedades do Computador



	 (€) → ↑ (♥) > Control Panel > All Control Panel Items 	System – – ×
Recycle Bin	System Properties × Computer Name Hardware Advanced System Protection Remote	n about your computer
7	Windows uses the following information to identify your computer on the network.	ration. All Windows®
	For example: "Mitchen Computer" or "Mary's Domputer". Full computer name: clienteubuntu Workgroup: WORKGROUP To use a wizard to join a domain or workgroup, click Network ID Network ID. To rename this computer or change its domain or Change	Intel(R) Core(TM) iS CPU M 560 © 2.67GHz 2.66 GHz 1,54 GB 64-bit Operating System, x64-based processor No Pen or Touch Input is available for this Display nd workgroup settings clienteubuntu @Change settings clienteubuntu WORKGROUP
	OK Cancel Apply	Read the Microsoft Software License Terms -00000-AA825 Activate Windows
	Windows Update	
		Windows 8.1 Enterpris Build 960
	🗧 📴 💌 👘 👘	18:26 18:26 28/09/2014

Figura 148 – Renomear Computador e Adicionar um Domínio

Figura 149 – Incluindo Computador no Domínio

	1		System	×
Recycle Bin) 🔄 🧼 🔹 ↑ 🛃 ト Control Panel → All Cor	trol Panel Item	s 🕨 System 🗸 🗸 Search Control Panel	<u>م</u>
	System Properties	×	n about your computer	0
	Computer Name/Domain Changes	note		
	You can change the name and the membership of this computer. Changes might affect access to network resources.	omputer	ration. All Window	s 8
	Computer name:	ry's		
	clenteubuntu Full computer name: clienteubuntu More	c ID	Intel(R) Core(TM) i5 CPU M 560 @ 2.67GHz 2.66 GHz : 1.00 GB 64-bit Operating System, x64-based processor No Pen or Touch Input is available for this Display	
	Member of		nd workgroup settings	
	monografia.local	9e	clienteubuntu 😚 Cha	nge settings
	Workgroup: WORKGROUP		WORKGROUP	
	OK Cancel			
and the	OK Cancel	Apply	I. Read the Microsoft Software License Terms	
7		1460	-0000-AA825 Activ	ate Windows
	Windows Update			
				Windows 8.1 Enterprise Build 960
) 🚔 📴 🔍			18:39 28/09/2014

17		System – 🗆 🗙	
Recycle Bin	() → ↑ I → Control Panel → All Control Panel Iter	ms ► System v 🖒 Search Control Panel 🔎	
	System Properties	n about your computer	
	Windows Security ×		
Computer Enter the name domain.	Name/Domain Changes e and password of an account with permission to join the administrator Domain: monografia.local OK Cancel OK Cancel	Intel(R) Core(TM) i5 CPU M 560 @ 2.67GHz 2.66 GHz 1,00 GB 64-bit Operating System, x64-based processor No Pen or Touch Input is available for this Display vd workgroup settings clienteubuntu WORKGROUP I. Read the Microsoft Software License Terms	
	Windows Update		
		Windows 8	1 Enterpris Build 960
H (2)	🚔 😼 💌 👘 👘	P 🕅 🕼	18:41 28/09/2014

Figura 150 – Senha do Administrador do Domínio

Figura 151 – Boas Vindas ao Domínio



5.2.3.15 Instalar as Ferramentas de Gerencia do Domínio

Agora que o computador cliente está no domínio, é preciso fazer acessalo usando o único usuário criado no domínio que é o *administrator*.n Para isso é preciso entrar com o *login* monografia\administrator e senha.

Uma vez dentro da máquina é preciso instalar um pacote de línguas suportado pela ferramenta de administração, para isso é preciso fazer a atualização do sistema em seguida entrar nas configurações do computador e fazer o download do pacote de línguas escolhido.

Somente após a instalação do pacote de línguas, no caso o escolhido foi o pacote de português, é possível instalar uma atualização que adiciona ferramentas administrativas para gerencia de controlador de domínio remotamente. Para fazer o download da atualização é preciso acessar o sítio http://www.microsoft.com/en-ca/download/details.aspx?id=39296 fazer o download compatível com a versão do Windows e instala-la.



Figura 153 – Opções do Computador



Figura 152 – Acesso à Estação de Trabalho



Figura 154 - Configurações do Computador

Figura 155 – Adicionando a Língua Portuguesa

• Time and language	م	Country or region
Date and time		Windows and apps might use your country or region to give you local content Brazil
Date and time Region and language		Brazil ✓ Languages When you add a language, a keyboard is added so you can type in that language ↓ Add a language ↓ Portugués (Brasil) Set as primary Options Remove

Www.microsoft.com/en-ca/download/details.aspx?id=39296	
Microsoft Download Center Shop & Products & Categories & Support & Security &	٩
Remote Server Administration Tools for Windows 8.1	
Select Language: English • Download	Free PC updates
Remote Server Administration Tools for Windows 8.1 enables IT administrators to manage roles and features that are installed on computers that are running Windows Server 2012 or Windows Server 2012 R2 from a remote computer that is running Windows 8.1 Pro or Windows 8.1 Enterprise.	Security patches Software updates Service packs Hardware drivers Run Microsoft Update
Details	
↔ System Requirements	Microsoft suggests
(Install Instructions	Shop for a new Windows PC Browse our collection of

Figura 156 – Download das Ferramentas de Administração Remota do Servidor

Figura 157 - Painel de Controle



· · · · · · · · · · · · · · · · · · ·	Todos os Itens do Painel de	Controle		×
😧 🕲 I 💽 🔝 🖛 I	Ferramentas Admini	strativas		- 🗆 ×
Arquivo Início Com	artilhar Exibir			~ (
. (odos os Itens do Painel → Ferramentas Administr	ativas ⊧ v C	Pesquisar Ferrar	nentas Admin 🔎
🛠 Favoritos	Nome	Data de modificaç	Тіро	Tamanho
💻 Área de Trabalho	🐌 Serviços de Área de Trabalho Remota	25/09/2014 17:48	Pasta de arquivos	
🚺 Downloads	📝 ADSI Editar	22/08/2013 03:55	Atalho	2 KB
🔚 Locais recentes	쥕 Agendador de Tarefas	22/08/2013 03:55	Atalho	2 KB
	🛃 Atualização com Suporte a Cluster	22/08/2013 03:44	Atalho	2 KB
👰 Meu computador	E Central Administrativa do Active Directory	21/08/2013 20:50	Atalho	2 KB
	certification authority	22/08/2013 03:56	Atalho	2 KB
🗣 Rede	🛃 Configuração do Sistema	22/08/2013 03:53	Atalho	2 KB
	📸 Desfragmentar e Otimizar Unidades	22/08/2013 03:47	Atalho	2 KB
	🛃 DHCP	22/08/2013 03:45	Atalho	2 KB
	減 Diagnóstico de Memória do Windows	22/08/2013 03:52	Atalho	2 KB
	🛃 DNS	22/08/2013 03:55	Atalho	2 KB
	🚟 Domínios e Relações de Confiança do Ac	22/08/2013 03:55	Atalho	2 KB
	😹 Ferramentas de Ativação de Volume	21/08/2013 20:52	Atalho	2 KB
	🔗 Firewall do Windows com Segurança Ava	22/08/2013 03:45	Atalho	2 KB
	Fontes de Dados ODBC (32 bits)	21/08/2013 20:56	Atalho	2 KB
	📷 Fontes de Dados ODBC (64 bits)	22/08/2013 03:59	Atalho	2 KB
	👩 Gerenciador de Balanceamento de Carga	22/08/2013 03:46	Atalho	2 KB
	😹 Gerenciador de Cluster de Failover	22/08/2013 03:44	Atalho	2 KB
	Berenciador de Recursos de Servidor de	22/08/2013 03:52	Atalho	2 KB
	🛃 Gerenciador de Servidores	22/08/2013 03:55	Atalho	2 KB
	📷 Gerenciamento de Acesso Remoto	21/08/2013 20:43	Atalho	2 KB
44 itens	-			

Figura 158 – Ferramentas Administrativas do Computador

Figura 159 – Usuários e Computadores do AD

2					
	P	Todos os Iter	ns do Painel de Contro	ble	- 🗆 🗙
Lixeira	a 🍘 I 🗋 🖬 🖛 I	Ferrament	as de Atalho Fer	ramentas Administrativas	- 🗆 ×
		Usuários e Computadores	do Active Directory		× v 🕐
	Arquivo Ação Exibir Ajuda	9			Admin O
	← → 🔐 Q 🗔	8 2 1 7 2 2			/ Automic. /
	Usuários e Computadores do	Ac Nome Tipo	Descrição		manho ^
	Consultas salvas	Consultas sa	Pasta para armazenar su.		2 KB
	monografia.local	monografia Domínio			2 KB
		-			2 KB
					2 KB
					2 ND
					2 KB
					2 KB
					2 KB
					2 KB
					2 KB
					2 KB
					2 KB
					2 KB
					2 KB
					2 KB
					2 KB
					2 KB
					2 KB
	<	>			3 KB
					2 KB
	44 itens 1 item s	elecionado 1,13 KB	י 100 רר	2012-02-55 Atalba	
					Windows 8.1
- 6).			P 🕅 🕼 28



Figura 160 – Unidade Organizacional para Usuários do Domínio

5.2.3.16 Autenticação no Domínio

Para fazer a autenticação no domínio criado com o SAMBA no Linux, é preciso criar um usuário no sistema Linux em seguida no programa SAMBA. Usando o comando *adduser* cria-se o usuário no sistema Linux e o comando *smbpasswd –a* cria-se o usuário no SAMBA. Porém, como a administração do servidor Linux é feita remotamente usando um cliente Windows, podem-se usar as ferramentas de administração para criação de usuário. Uma vez criado o usuário é possível fazer acesso ao domínio com autenticação de senha.

O primeiro passo a ser dado é acessar o cliente Windows, abrir o painel de controle e acessar as ferramentas administrativas. Em seguida é preciso acessar o a ferramenta de administração "Usuários e Computadores do Active Directory", clicar com o botão direito no nome do domínio e criar uma nova unidade organizacional. Uma vez criado a unidade organizacional "usuários ubuntu" é preciso clicar no ícone de criar usuários e adicionar um novo usuário no domínio. Para este trabalho foram criados os usuário: usuario01, usuario02, usuario03, usuario04, usuario05 e usuario06. Os usuários 01 e 02 foram incluídos no grupo de Marketing, 03 e 04 no grupo de Recursos Humanos e 05 e 06 no grupo de Suporte Técnico.

9	Todos os Itens do Painel de Controle 🛛 – 🗗 🗙						×	
\odot	🔹 ↑ 📴 🕨 Painel de Controle 🕨	Todos	os Itens do Painel de Controle			~ ¢	Pesquisar Painel de Controle	Q,
Ajuste	e as configurações do comput	ador				Exib	ir por: 🛛 Ícones grandes 🔻	
	Barra de Tarefas e Navegação	þ	Central de Ações	٩	Central de Facilidade de Acesso	<u>.</u>	Central de Rede e Compartilhamento	^
\bigcirc	Central de Sincronização	-	Conexões de RemoteApp e Área de Trabalho		Configurações de Local	<u>.</u>	Contas de Usuário	
Ŕ	Criptografia de Unidade de Disco BitL	P	Data e Hora	20	Dispositivos e Impressoras	S.	Espaços de Armazenamento	
\$ =	Ferramentas Administrativas		Firewall do Windows	£	Flash Player (32 bits)	A	Fontes	
Q	Gerenciador de Credenciais	÷.	Gerenciador de Dispositivos	2	Gerenciamento de Cores	•	Grupo Doméstico	
	Histórico de Arquivos		Ícones da Área de Notificação	F	Idioma	Ĩ	Mouse	
P:	Opções da Internet	٢	Opções de Energia	R	Opções de Indexação	K	Opções de Pasta	
	Pastas de Trabalho	K	Personalização	ā	Programas e Recursos		Programas Padrão	
Ų	Reconhecimento de Fala	Ń	Recuperação	Ð	Região		Reprodução Automática	3
R	Sistema	A	Solução de problemas		Som	معند Ativar	Teclado o Windows	
(٢	Telefone e Modem	2	Vídeo	龃	Windows Defender	Ace te a computa	s Windows Fo Go o dor para ativar o Windows	s.
	Windows Update						17: 17: 	:07)/2014

Figura 161 – Painel de Controle

juste as conf 😤 🕞 🔝 =			itas de Atalho	Ferramentas Ad	Iministrativ	as 🗕 🗆 🗙	les 🔻	
	Arquivo Início Comp	artilhar Exibir Ge	renciar			~ (?		
Barra	💿 🍥 👻 🕇 🔞 « Todos os Itens do Painel 🕨 Ferramentas Administr			ativas → v Ċ	r Ferramentas Admin 🔎	e e		
Nave	ga 🗸 – .	Nome		Data de modificaç	Tipo	Tamanho	ento	
	Favoritos	👘 ocienciamento de impr	icssau	22/00/2013 03.44	Atamo	2 ND		
Centr	al Area de Trabalho	😹 Gerenciamento de Política de Grupo		22/08/2013 03:56	Atalho	2 KB	ário	
	Uownloads	🚰 Gerenciamento de Resp	Gerenciamento de Respondentes Online		Atalho	2 KB		
Cripto	Docais recentes	🚰 Gerenciamento DFS		22/08/2013 03:53	Atalho	2 KB		
Disco	В	🛃 Gerenciamento do com	putador	22/08/2013 03:54	Atalho	2 KB	to	
Ferra	Meu computador	😰 Informações do sistema 兪 Iniciador iSCSI		22/08/2013 03:53	Atalho	2 KB		
Admi	nis 👝 – .			22/08/2013 03:57	Atalho	2 KB		
6	🐂 Rede	📷 Limpeza de Disco		22/08/2013 03:57	Atalho	2 KB		
Gerer		📷 Módulo Active Director	y para Windows P	22/08/2013 03:55	Atalho	2 KB	ico	
Crede	en	🛞 Monitor de Desempenh	10	22/08/2013 03:52	Atalho	2 KB		
Histó	ric.	Monitor de Recursos		22/08/2013 03:52	Atalho	2 KB		
HISLO	nc -	🛃 Política de Segurança L	ocal	22/08/2013 03:54	Atalho	2 KB		
		😹 Roteamento e acesso re	emoto	22/08/2013 03:44	Atalho	2 KB		
Opçõ	es	🎓 Serviços de Component	tes	22/08/2013 03:57	Atalho	2 KB	ta	
		📷 Serviços e Sites do Activ	ve Directory	22/08/2013 03:55	Atalho	2 KB		
Pasta	sc	📸 Serviços		22/08/2013 03:54	Atalho	2 KB	Irão	
		🔝 Usuários e Computado	res do Active Dire	22/08/2013 03:55	Atalho	2 KB		
		🚼 Visualizador de Eventos		22/08/2013 03:55	Atalho	2 KB		
Recor	h	🔝 Windows PowerShell (x	86)	22/08/2013 12:34	Atalho	3 KB	utomática	
		😹 Windows PowerShell IS	E (x86)	22/08/2013 03:55	Atalho	2 KB		
Sister	na	😹 Windows PowerShell IS	E	22/08/2013 03:55	Atalho	2 KB		
		📷 Windows Server Update	Services	22/08/2013 04:00	Atalho	Ativar o Wiłłełows		
Tolofe	44 itens 1 item seleciona	44 itens 1 item selecionado 1,13 KB				Acesse as configuences	ls do	
reieto					consultador para ativar	Windows		

Figura 162 – Ferramentas Administrativas

Figura 163 – Criação de Unidade Organizacional

P			Todos os It	tens do Painel	de Controle				- 0	×
\odot	⇒ ↑ 兴 ► Painel de Controle → Todos os Itens do Painel de Controle v C Pesq							isar Painel	de Controle	,o
Ajuste	e as q	-	Unifican e Committee		Disectory		- D X	×	les 🔻	
	_	Usuarios e Computadores do Active Directory								
		Arquivo Ação Exibir Ajuda						• •		^
2	Barı		0 🖸 📑 🛛 🖬 👘 🕉 🍇	11 Y 2 3				<i>Р</i>	e e	
	Nav	Usuários e Computadores do Ac Consultas salvas	Nome	Tipo	Descrição			^	ento	
	Cen	✓ implementation and a monografia.local	👗 usuario01	Usuário				(B	ário	
igsim		Users						КB		
4	Crip	Computers						CВ		
N	Disc	Domain Controllers						(B	to	
	Ferr	ForeignSecurityPrincipal:						(B		
¶\$=	Adn	Computadores Ubuntu						(B		
ā	Ger	📓 Grupos Ubuntu						(B	ico	
2	Cre							(B		
	Hist							(B		
								(B		
P	Onc							(B	ta	
¥=	^{op}							(B	tu i	
	Past							(B	trão	
	1 45							(B	indo	
.	Rec							(B	itomática	
Ŷ	1.00	< >>						(B	Jeonnatica	
	Sist							(B		
Crow Col	5.50		windows Server Update Ser	rvices	22/08/2013 04:00	Atalho	Ativar o Wi ł	Mows		
(I)	Telef	00 44 itens 1 item selecionado	1,13 KB				Acesse as config	n der cels	÷	
		computador pa								
	Wind	lows Update								~
	1				and the second second			Da 05	17:0	8
				the second second	and the second second		the construction and the	0.00 000	02/10/2	2014
!				Todos os I	tens do Painel de Controle			- 0 ×		
------------------	--------	---------------------------------------	-------------------------	--	--	--	-------------------	-----------------		
0) - 1	Painel de Controle →	Todos os Itens do Paine	el de Control	e	v ♂ Pesq	uisar Painel	de Controle 🛛 🔎		
Ajuste	e as c	2	Usuários e	Computa	dores do Active Directory	- 🗆 ×	×	es 🔻		
		Arquivo Ação Exibir Aj	uda				~ ?	^		
\$ -	Barı	🗢 🄿 🖄 📰 📋 🗊	Q 🗟 🛛 🖬 🕺	2 🖬 🍸	<u>p</u> (2)		<i>р</i>	e e		
	Nav	Usuários e Computadores	do Ac Nome		Tipo Descrição Usuário		NU 10	ento		
\mathbf{igsim}	Cen	Users		Novo O	ibieto - Usuário X		(B	ano		
4	Crip	Computers Builtin		14070 0			КΒ			
N.	Disc	Domain Controller	Criar em:	monografia.	local/Usuarios Ubuntu		(B)	to		
(Chi	Ferr	ForeignSecurityPri Usuarios Ubuntu					(B			
	Aun	Computadores Ub	Nome:	usuario02	Iniciais:		KB			
0	Cree	Grupos Ubuntu	Sobrenome:				(B	ico		
			Nome completo:	usuario02			(B			
A	Hist		Home complete.				КВ			
	0		Nome de logon do usu	uário:	@managerfite.lagel		(B			
₹_	Opç		Ness de la se de un	de la la la de	emonograna.oca +		(B)	la		
	Past		MONOGRAFIA\	Jano (antenor a	usuario02		(B	Irão		
							КВ			
0	Rec						(B) (B)	utomática		
A.		<			< Voltar Avançar > Cancelar		(B			
	Sist_	····					KB			
			Windows Sen	ver Update Se	ervices 22/08/2013 04:00 At	alho Ativar o Wi	2Keows			
s.	Telef	On 44 itens 1 item seleci	onado 1,13 KB			Acesse as confi	ig uen els	o Windows.		
_						computation pr	are etter			
	Wind	dows Update	7.		the state of the s	and the second		17:09		
	C			and the set			13 17	02/10/2014		

Figura 164 - Criação de Usuário

Figura 165 - Criação de Senha





Figura 166 - Confirmação de Objeto Criado

Figura 167 – Usuário Dois Criado no Grupo



								•			
P					То	dos os Itens do Pai	nel de Controle				- 0 ×
\odot) - 1	🗅 📴 🕨 Pai	nel de Controle	▶ Todo	s os Itens do Painel de	e Controle			v Ċ Pe	squisar Painel	de Controle 🛛 🔎
Ajust	e as c	Ξ			Usuários e Co	omputadores do A	tive Directory		_ 🗆 ×	×	es 🔻
		Arquivo	Ação Exibir	Ajuda						✓ ?	^
X -	Bari	🗢 🔿 🔰	• 🗖 i i i	i a 🖬	è 🛛 🖬 🕄 📚	i 🝸 🍸 🗾 🗽				م	ee
X =	Nav	📃 Usuários	e Computador	es do Ac	Nome	Tipo	Descrição			^	ento
		Con:	sultas salvas		🚨 usuario01	Usuário	-				
\bigcirc	Cen	⊿ ∰ mon ⊳ 🛄 U	lografia.iocai Jsers		🔏 usuario02	Usuário				(B	ário
	Crip	> 📫 C	Computers		🐁 usuario03 🤱 usuario04	Usuário Usuário				KB	
1	Disc		Suiltin Domain Controll	ers	📕 usuario05	Usuário				КВ	to
<u> </u>	Ferr	> 🧰 F	oreignSecurityP	rincipal	🐇 usuario06	Usuário				КВ	
₩¥=	Adn		Jsuarios Ubuntu Computadores U	lbuntu						KB	
2	Ger	<u></u>	Grupos Ubuntu							KB	ico
2	Cre									КВ	100
	Hist									(B	
										(B	
e	Opc									CB	ta
v -	- 1									(B	
	Past									КВ	Irão
(jein)										(B	
0	Rec									(B	utomática
Y		<		>							
	Sist									KB	
- 34					Windows Server	Update Services	22/08/2013 04:00	Atalho	Ativar o V	ViłKelows	
4	Telef	on 44 ite	ns 1 item sel	ecionado	1,13 KB		-		Acesse as co	nfig 🚛 🔜 s	o Windows
				-30					computador	para ativar	o windows.
14	Wind	lows Upda	ate	_							v
	6			1						13 🕅	02/10/2014

Figura 168 – Usuários de Um a Seis Criados no Grupo

Figura 169 – Criando Grupo de Segurança

9			Todos os Itens do	Painel de Controle			- 0	×
(e) → ↑ [9] → Painel de Controle → Todos os Itens do Painel de Controle ∨ C							de Controle	Q
Ajuste	e as c		Usuários e Computadores c	o Active Directory	- 🗆 🗙	×	es 🔻	
S	Barı Nav	Arquivo Ação Exibir Ajuda (Arquivo Aj	 Q :> [] :::: 3. 2. 2:: [] ? Nome Tipo 	2 % Descrição		~ ? 	e e ento	^
۲	Cen	Consultas salvas monografia.local Ders Computers	Novo C	bjeto - Grupo 🛛 🗙		(B (B	ário	
Ŕ	Crip Disc	 ▷ □ Builtin ▷ □ Domain Controllers 	Criar em: monografia.	local/Grupos Ubuntu		(B (B	to	
÷	Ferr Adn	 ForeignSecurityPrincipal: Usuarios Ubuntu Computadores Ubuntu 	Nome do grupo:			(B (B		
	Ger Cre	📓 Grupos Ubuntu	Nome do grupo (anterior ao Window	s 2000):		(B (B	ico	
	Hist		Escopo do grupo O Domínio local	Tipo de grupo		(B (B		
	Орс		 Global Universal 	◯ Distribuição		(B (B	ta	
	Past			OK Capcelar		(B (B	Irão	
Ģ	Rec	< >>				(B (B	utomática	
	Sist.		Windows Server Update Services	22/08/2013 04:00 Atalho	Ativar o Wi	B B B B B B B B B B B B B B B B B B B		
(٢)	Telef	on 44 itens 1 item selecionado	9 1,13 KB	-	Acesse as confi computador pa	g ilia es s ira ativar	do Windows.	
1	Wind	lows Update						~
	e					R R	17:13 02/10/2	

5			1 1			
9			Todos os Itens do Painel de Controle		- 0	×
\odot	- 1	🖓 🕨 Painel	de Controle → Todos os Itens do Painel de Controle 🗸 🖒 Pe	squisar Painel	de Controle	Q,
Ajuste	e as c		Usuários e Computadores do Active Directory – 🗖 🗙	×	es 🔻	
		Arquivo Acã	o Fribir Aiuda	v 🕐		^
5	Barı	◆ ⇒ 2	Novo Objeto - Grupo	ч , р	e e	
	Nav	Usuários	Real Criar em: monografia.local/Grupos Ubuntu		ento	
۲	Cen	⊿ ∰ mon(⊳ 🗂 U		(B	ário	
	Crip	⊳ 🖆 C	Nome do grupo:	(B		
1	Disc	⊳ <mark>□</mark> B ⊳ □ D	Suporte recrico	КВ	to	
8	Ferr	> 🖺 F	Nome do grupo (anterior ao Windows 2000):	(B		
¶¥=	Adn		Suborte recirco	(B)		
8	Ger	🖬 G	Escopo do grupo	(B	ico	
2	Cre		Domínio local Segurança Otietrólavieño	KB		
	Hist			(B		
				(B)		
	Орс			(B	ta	
-			OK Cancelar	(B		
	Past			(B	Irão	
0				(B)		
Ų	Rec	<	>	(B	utomática	
				(B		
	Sist_		Windows Server Hadate Services 22/09/2012 04:00 Atalba Atalaa a	(3-KB		
	T-1-6	44 itens	1 item selecionado 1.13 KB	nfigues s	do	
	relet	on	computador	para ativar	o Windows.	
	Winc	lows Undate				~
	2				17:1	4
		10-0			02/10/2	2014

Figura 170 - Grupo do Suporte Técnico

Figura 171 – Grupos Criados





Figura 172 – Usuários Adicionados no Grupo Marketing







Figura 174 – Usuários Adicionados no Grupo Suporte técnico

Figura 175 - Acesso ao Domínio pelo Usuário 01





Figura 176 – Boas Vindas ao Domínio

CONCLUSÃO

O estudo permitiu compreender que as duas ferramentas analisadas no trabalho tem suas dificuldades. Durante os estudos alguns fatores puderam ser claramente observados causando grande discrepância entre as duas ferramentas. O fator de acesso a informação e estudos relacionados é muito diferente entre as duas ferramentas, para instalar e configurar o Active Directory encontram-se na internet muitos materiais dispostos, desde fóruns com discussões sobre o assunto até ao próprio site da Microsoft mostrando passo a passo para instalar e configurar a ferramenta. O OpenLDAP tem bastante informação na *web* mas na sua grande parte em fóruns. A maioria dos sites que chamam de *sites* oficiais acabam apresentando links para outros sites como se parte do sistema de serviço de diretório oferecido pela OpenLDAP pertencesse a outras marcar e programas. Existe uma grande dificuldade em conseguir materiais específicos com o passo a passo completo, pois as distribuições Linux dependem de uma série de programas que são pré-requisitos para que o sistema funcione, além de haverem divergências entre esses pré-requisitos e entre as distribuições.

Por um fator de complexidade na instalação e configuração, pode-se observar que as duas ferramentas também divergem muito. O Active Directory oferece uma interface gráfica interativa com o administrador do servidor. A cada clique dado existe uma sugestão do próximo clique. Cada função configurada no servidor é configurada através de WIZZARD que orienta o administrador e questiona quanto a serviços completares. O OpenLDAP não tem uma interface gráfica amigável, apesar de poder ser instalada, essa interface não oferece uma interação com usuário. Se o administrador do servidor não tiver o conhecimento necessário a nível de comando estruturado, tiver noção de redes básica, souber fazer configuração de partições de disco, virtualização de máquinas, entre outros conhecimentos básicos, o sistema não tem aplicabilidade.

Analisando o fator de eficácia, tanto o Active Directory como o OpenLDAP atendem ao que pode ser considerado básico em uma segurança de redes, a autenticação de usuários por meio de senha. Desta forma é observado que a ferramenta de administração de serviços de diretório da Microsoft é a melhor opção para administração de redes com segurança e suporte na visão do autor deste trabalho. Porém para pequenas redes, o OpenLDAP, por ser uma ferramenta grátis, pode ser uma opção, exigindo apenas que o administrador da rede tenha o conhecimento demandado.

REFERÊNCIAS

BUTCHER, M. Mastering OpenLDAP: Configuring, Securing and Integrating Directory Services. *Birmingham, UK*: Packet Publishing Ltd, 2007.

CARTER, G.; TS, J.; ECKSTEIN, R. Using Samba. Unites States os America: O'Reilly Media, Inc, 2007.

FOROUZAN, B. A.; FEGAN, S. C. **Protocolo TCP IP**. Porto Alegre: Mc Grall Hill, 2008.

IETF **RFC 2251**. Disponível em: <http://www.ietf.org/rfc/rfc2251.txt>. Acesso em 14/11/2013.

JACKIEWICZ, T. Deploying OpenLDAP. New York, USA: Apress, 2005.

MARINHO, R. **O que é o Active Directory**. Disponível em: http://www.linhadecodigo.com.br/artigo/2422/o-que-e-o-active-directory.aspx. Acesso em 02/09/2013.

MICROSOFT CORP. Configuring and Troubleshooting Windows Server 2008 Active Diretory Domain Services. Brazil: Cargraphics Gráfica e Editora Ltda, 2011

RIBEIRO, A. M.; COSTA, C. M.; MENEGUETTI, E.; GRANVILLE, L. Z. **ANAIS**. Porto Alegre: Evangraf Ltda, 2004, p. 91 – 94.

RICHARDS, J.; ALLEN, R.; LOWE-NORRIS, A. G. *Active Directory, Third Edition.* United States of America: O'Reilly Media, Inc, 2006.

SHERESH, B.; SHERESH, D. Understanding Directory Services. United States of America: SAMS, 2002, p. 299 – 302.