rede e-Tec Brasil

Sistemas Operacionais II

Marcelo Caramuru Pimentel Fraga

William Geraldo Sallum

Belo Horizonte-MG
2012

Presidência da República Federativa do Brasil

Ministério da Educação

Secretaria de Educação Profissional e Tecnológica

Este Caderno foi elaborado em parceria entre o Centro Federal de Educação Tecnológica de Minas Gerais e a Universidade Federal de Santa Catarina para a Rede e-Tec Brasil.

Equipe de Elaboração
Centro Federal de Educação Tecnológica de Minas Gerais – CEFET-MG

Coordenação do Curso
Adelson de Paula Silva/CEFET-MG

Professores-autores
Marcelo Caramuru Pimentel Fraga/CEFET-MG
William Geraldo Sallum/CEFET-MG

Comissão de Acompanhamento e Validação
Universidade Federal de Santa Catarina – UFSC

Coordenação Institucional
Araci Hack Catapan/UFSC

Coordenação do Projeto
Silvia Modesto Nassar/UFSC

Coordenação de Design Instrucional
Beatriz Helena Dal Molin/UNIOESTE e UFSC

Coordenação de Design Gráfico
Juliana Tonietto/UFSC

Design Instrucional
Gustavo Pereira Mateus/UFSC

Web Master
Rafaela Lunardi Comarella/UFSC

Web Design
Beatriz Wilges/UFSC
Mônica Nassar Machuca/UFSC

Diagramação
Bárbara Zardo/UFSC
Breno Takamine/UFSC
Liana Domeneghini Chiaradia/UFSC
Luiz Fernando Tomé/UFSC
Marília Ceriolli Hermoso/UFSC
Roberto Gava Colombo/UFSC

Revisão
Júlio César Ramos/UFSC

Projeto Gráfico
e-Tec/MEC

Catalogação na fonte pela Biblioteca Universitária da Universidade Federal de Santa Catarina

F811s Fraga, Marcelo Caramuru Pimentel
Sistemas operacionais II / Marcelo Caramuru Pimentel Fraga, William Geraldo Sallum. – Belo Horizonte : CEFET/MG, 2012.
92 p. : il.

Curso Técnico em Planejamento e Gestão em Tecnologia da Informação
Inclui bibliografia
ISBN: 978-85-99872-22-2

1. Sistemas operacionais (Computadores). I. Sallum, William Geraldo. II. Título.

CDU 681.31:519.687

Apresentação e-Tec Brasil

Prezado estudante,

Bem-vindo ao e-Tec Brasil!

Você faz parte de uma rede nacional pública de ensino, a Escola Técnica Aberta do Brasil, instituída pelo Decreto nº 6.301, de 12 de dezembro 2007, com o objetivo de democratizar o acesso ao ensino técnico público, na modalidade a distância. O programa é resultado de uma parceria entre o Ministério da Educação, por meio das Secretarias de Educação a Distancia (SEED) e de Educação Profissional e Tecnológica (SETEC), as universidades e escolas técnicas estaduais e federais.

A educação a distância no nosso país, de dimensões continentais e grande diversidade regional e cultural, longe de distanciar, aproxima as pessoas ao garantir acesso à educação de qualidade, e promover o fortalecimento da formação de jovens moradores de regiões distantes, geograficamente ou economicamente, dos grandes centros.

O e-Tec Brasil leva os cursos técnicos a locais distantes das instituições de ensino e para a periferia das grandes cidades, incentivando os jovens a concluir o ensino médio. Os cursos são ofertados pelas instituições públicas de ensino e o atendimento ao estudante é realizado em escolas-polo integrantes das redes públicas municipais e estaduais.

O Ministério da Educação, as instituições públicas de ensino técnico, seus servidores técnicos e professores acreditam que uma educação profissional qualificada – integradora do ensino médio e educação técnica, – é capaz de promover o cidadão com capacidades para produzir, mas também com autonomia diante das diferentes dimensões da realidade: cultural, social, familiar, esportiva, política e ética.

Nós acreditamos em você!

Desejamos sucesso na sua formação profissional!

Ministério da Educação
Setembro de 2012

Nosso contato
etecbrasil@mec.gov.br

Indicação de ícones

Os ícones são elementos gráficos utilizados para ampliar as formas de linguagem e facilitar a organização e a leitura hipertextual.

Atenção: indica pontos de maior relevância no texto.

Saiba mais: oferece novas informações que enriquecem o assunto ou "curiosidades" e notícias recentes relacionadas ao tema estudado.

Glossário: indica a definição de um termo, palavra ou expressão utilizada no texto.

Mídias integradas: sempre que se desejar que os estudantes desenvolvam atividades empregando diferentes mídias: vídeos, filmes, jornais, ambiente AVEA e outras.

Atividades de aprendizagem: apresenta atividades em diferentes níveis de aprendizagem para que o estudante possa realizá-las e conferir o seu domínio do tema estudado.

Sumário

Palavra dos professores-autores

Prezado estudante!

Nesta disciplina você aprenderá o funcionamento dos sistemas operacionais servidores. É importante que você domine os conceitos abordados na disciplina Sistemas Operacionais I, pois é a base desta disciplina.

Inicialmente, nosso curso será teórico para apresentação dos conceitos básicos. Porém, o foco da disciplina é a prática; por isso, serão disponibilizadas diversas videoaulas e tutorias para orientar o desenvolvimento das etapas práticas.

Este curso requer que as etapas sejam seguidas na ordem em que são apresentadas, pois além de evitar maiores problemas, o aprendizado será facilitado.

Espero que você aproveite o curso e descubra o mundo dos sistemas operacionais servidores!

Um grande abraço!
Prof. Marcelo Caramuru e Prof. William Sallum

Apresentação da disciplina

Sistemas Operacionais II é uma disciplina que apresenta um conteúdo bastante diversificado, contemplando a base prática da área de instalação, configuração, administração e segurança de sistemas operacionais (SO) servidores. Os seguintes tópicos serão abordados:

- evolução dos sistemas operacionais servidores;
- requisitos básicos para um projeto de uma arquitetura cliente/servidor;
- estrutura de domínios e contas;
- estrutura de diretórios e de arquivos a nível de compartilhamentos;
- tipos de servidores;
- instalação, configuração e administração de servidores;
- princípios básicos de segurança em sistemas operacionais servidores.

Projeto instrucional

Disciplina: Sistemas Operacionais II (carga horária: 60h).

Ementa: Conceitos, evolução, tipos, administração, configuração e segurança de sistemas operacionais servidores.

AULA	OBJETIVOS DE APRENDIZAGEM	MATERIAIS	CARGA HORÁRIA (horas)
1. Conceitos, evolução e requisitos em SOS	Conceituar e identificar os requisitos necessários para a elaboração de projetos de arquitetura de sistemas operacionais servidores.	Vídeos instrucionais; Indicações de leitura; Fórum de discussão; *Chats*, e glossário.	8
2. Tipos de servidores	Conhecer e identificar os principais tipos de servidores e serviços.	Vídeos instrucionais; Indicações de leitura; Fórum de discussão; *Chats*, e glossário.	7
3. Instalação de servidores	Entender os princípios de instalação de servidores.	* Vídeos: • Instalação do Oracle Virtual Box • Tutorial – Configuração da Máquina Virtual – Parte1 • Tutorial – Configuração da Máquina Virtual – Parte2 • Preparação da MV Windows 2003 Server • Instalação Windows 2003 Server.ppt • Instalando adicionais para convidado • Instalando configurações típicas de um servidor • Personalizando a aparência e configurações gerais do servidor. • Instalação do Windows XP • Configuração das placas de rede do servidor	8
4. Configuração de SOS	Entender os princípios de configuração de servidores.	* Vídeos: • Configuração do servidor DNS • Teste do servidor DNS • Configuração do servidor DHCP • Teste do servidor DHCP	8

Continua

AULA	OBJETIVOS DE APRENDIZAGEM	MATERIAIS	CARGA HORÁRIA (horas)
5. Domínios, acesso, contas e senhas	A partir de um ambiente virtual, conceituar e criar domínios de contas de clientes, métodos de acesso e políticas de contas e senhas.	Vídeos instrucionais; Indicações de leitura; Fórum de discussão; *Chats*, e glossário.	7
6. Diretórios, arquivos e compartilhamentos	Conhecer conceitos de estrutura de diretórios, arquivos e segurança bem como compartilhamento de recursos e arquivos.	* Vídeos: • Adicionando usuários e setando permissões • Criação de perfis móveis • Compartilhando pastas e configurando permissões de acesso	7
7. Administração de sistemas operacionais servidores	Conhecer os princípios de administração de redes; contratos e licenças; conexões simultâneas; técnicas de administração de sistemas operacionais de rede; e auditoria.	Vídeos instrucionais; Indicações de leitura; Fórum de discussão; *Chats*, e glossário.	8
8. Segurança em sistemas operacionais servidores	Ter conhecimentos sobre: segurança física; segurança lógica; *firewall*; *scanners* e antivírus; NAT; *proxy server*; criptografia; segurança de servidores; políticas de segurança.	Vídeos instrucionais; Indicações de leitura; Fórum de discussão; *Chats*, e glossário.	7
			Conclusão

* Todos os arquivos de apresentação e vídeos deverão ser baixados de: **http://www.4shared.com/dir/0J7R1VP8/sharing.html**

Aula 1 – Conceitos, evolução e requisitos em SOS

Objetivo

Conceituar e identificar os requisitos necessários para a elaboração de projetos de arquitetura de sistemas operacionais servidores

1.1 Conceito de sistema operacional servidor

Um sistema operacional servidor (SOS) tem a função de atender a requisições vindas de várias estações, sejam estas remotas ou locais, administrando várias tarefas de diferentes tipos ao mesmo tempo.

Um servidor presta serviços diversos à rede à qual está conectado, tais como: banco de dados, **proxy** de internet, armazenamento de arquivos, ***firewall*** e vários outros. Logo, para oferecer tais funções, um SOS necessita de mais recursos que um sistema operacional comum, tais como mais memória, maior velocidade de acesso ao disco e memória, mais espaço em disco, maior velocidade de processamento, etc. Contudo, ainda assim, os SOS possuem limites no oferecimento de serviços que devem ser administrados, pois se o número de requisições de serviço superar esse limite, comportamentos inesperados podem ocorrer. Um fato interessante sobre sistemas operacionais servidores é que a interação com o ser humano através de interface gráfica elaborada não é obrigatória, poupando recursos computacionais para uso na prestação de serviço.

A-Z

Proxy
Servidor que atende a requisições de um cliente e repassa os dados adiante, requisitando algum serviço, como um arquivo, conexão, página *web* ou outro recurso disponível no outro servidor.

Firewall
São dispositivos de *hardware* ou *software* que aplicam uma política de segurança a um determinado ponto da rede

Os desenvolvedores de sistemas operacionais servidores devem construir aplicativos que suportem um grande número de clientes conectados a eles. Esses servidores devem facilitar a construção de serviços independentes e confiáveis que ofereçam desempenho sem exigir que uma máquina inteira seja dedicada a cada serviço exclusivamente.

Por fim, um sistema operacional servidor consiste em um ambiente que, além das funções básicas de um SO comum, também deve responder a solicitações vindas de outras estações. Um SOS é multitarefa, permitindo que vários usuários e aplicações possam aproveitar os recursos do sistema simultaneamente, permitindo troca de informação entre computadores (modelo cliente-servidor).

1.2 Arquitetura cliente-servidor

A arquitetura cliente-servidor funciona da seguinte maneira: existe um processo cliente que envia requisições diversas a um processo servidor que, por sua vez, retorna ao cliente os resultados das solicitações feitas. Os processos são executados sobre o gerenciamento do sistema operacional, que também coordena os recursos do sistema computacional. Os processos clientes e servidores podem residir na mesma máquina ou não, sob o comando de um único SO ou de sistemas operacionais distintos. A metodologia cliente/servidor foi desenvolvida com o objetivo de possibilitar que vários tipos de aplicações se comuniquem entre si, sem que a execução de um processo interfira na de outro. Nessa arquitetura, o processamento da informação é dividido em processos distintos. Um processo é responsável pela manutenção da informação (servidor), enquanto que outro é responsável pela obtenção dos dados (cliente).

Ao concentrar os serviços em servidores especializados, tais como servidores de impressão, todas as requisições de impressão serão enviadas a esse servidor. Serviços diversos, tais como a troca de *e-mail*, o acesso à internet e banco de dados, são construídos com base no modelo cliente-servidor. Os clientes enviam requisições de dados a um ou mais servidores, que podem aceitar esses pedidos, processá-los e retornar as informações solicitadas para o cliente.

Essa arquitetura se tornou muito popular por várias razões: inicialmente, pela facilidade de implementação, devido à clara separação das funcionalidades de clientes e servidores. Além disso, delega tarefas mais simples às máquinas clientes, que são mais baratas e possuem *hardware* inferior, e as mais complexas ao servidor, que geralmente são mais caras e possuem *hardware* melhor. Outra razão é que o usuário pode executar uma interface gráfica mais adequada a seus conhecimentos, ao invés de usar a interface do servidor.

As funções básicas de um cliente são: iniciar pedidos; esperar respostas; receber respostas; conectar-se a um número limitado de servidores simultaneamente; interagir diretamente com os usuários finais e utilizar recursos da rede.

O servidor tem como características: esperar por pedidos de clientes; responder aos dados solicitados pelos clientes; comunicar-se com outros servidores e fornecer recursos à rede.

Por fim, as principais vantagens do modelo cliente-servidor são:

- centralização de recursos: o servidor deve gerir os recursos comuns a todos os utilizadores;
- melhor segurança: a concentração dos dados em um único ponto facilita o gerenciamento e compartilhamento adequado;
- administração: através do servidor é possível administrar toda a rede;
- escalabilidade e paralelismo: é possível acrescentar ou remover clientes de forma simples e sem interromper o funcionamento da rede.

Porém também existem algumas desvantagens no modelo, tais como:

- custo: os custos podem ser elevados, dependendo do serviço;
- confiabilidade: o servidor é o único responsável por manter a rede em funcionamento. Caso ocorram problemas no servidor, os serviços deixam de ser prestados;
- manutenção: as diversas partes envolvidas nem sempre funcionam bem juntas;
- gerenciamento: o gerenciamento do ambiente é complexo.

1.3 Evolução dos sistemas operacionais servidores

Nos primeiros computadores não existiam sistemas operacionais; os computadores eram programados através de chaves e relés mecânicos diretamente pelo homem. Na década de 1950, surgem os primeiros SOs, capazes apenas de gerenciar o *hardware* local, pois as redes ainda não existiam, e de executar apenas um aplicativo por vez. Nos anos 1960, surgem os SOs multitarefa e, em seguida, com o surgimento das redes de computadores e o serviço de computação comercial, percebe-se a necessidade de oferecer esses serviços a distância. Com o avanço dos serviços de computação comercial, surgem os sistemas operacionais servidores. A seguir serão mostrados os principais marcos dos SOS.

1.3.1 Windows

A Microsoft resolveu oferecer ao ambiente empresarial um SO de rede. A partir daí, várias versões de sistemas operacionais Windows servidores surgiram.

1.3.1.1 Windows NT

O Windows NT foi lançado em 1993 com o objetivo de fornecer segurança e comodidade aos que usavam o meio corporativo. O nome NT vem de *New Technology* ou Nova Tecnologia. É um SO de 32 *bits*, multitarefa e multiusuário, com multiprocessadores, multiplataforma (vários computadores/máquinas interligados) e com servidores simples, como por exemplo, banco de dados e arquivos.

1.3.1.2 Windows 2000 Server

Lançado em 2000 e originado a partir do núcleo do Windows NT, o Windows 2000 Server foi aclamado como o SO mais estável da Microsoft na época.

Foi implementado um novo serviço de diretório chamado de *Active Directory* (AD). O AD surgiu da necessidade de o usuário ter uma única senha para acessar todos os recursos disponíveis na rede, tais como conta de *e-mail*, conta de usuário local, etc. O diretório é como um banco de dados que armazena as informações dos usuários.

1.3.1.3 Windows Server 2003

Lançado em 2003, o Windows Server 2003 trouxe melhorias na *performance* e novidades na área administrativa do *Active Directory* que passou a ser voltada principalmente para servidores e empresas de grande porte. Não possuía virtualização nativa, ou seja, não executava servidores virtuais.

A-Z

Internet Information Services
Servidor *web* da Microsoft para seus sistemas operacionais para servidores.

Terminal Services
Implementação da Microsoft de cliente remoto para aplicações do Microsoft Windows

Assembly
Notação do código de máquina de uma arquitetura de computador específica, utilizada para programar dispositivos tais como microprocessadores e microcontroladores..

1.3.1.4 Windows Server 2008 (LongHorn)

O Windows Server 2008 (LongHorn) foi construído a partir do mesmo código do Windows Vista, compartilhando assim da mesma arquitetura e funcionalidade. Trouxe melhorias no IIS (***Internet Information Services***, Serviços de Informação da Internet), no ***Terminal Services*** (Serviços de Terminal) e o recurso de virtualização integrado ao sistema.

1.3.2 Unix

Implementado em 1969 pela AT&T nos EUA, o Unix inicialmente foi escrito em ***Assembly*** e reescrito em C em 1973. Foi adaptado e utilizado por instituições acadêmicas e empresas.

1.3.2.1 GNU

O GNU foi proposto por Richard Stallman em 1983 com o objetivo de desenvolver um SO similar ao SO Unix, porém gratuito e de código aberto. Em 1984, Stallman cria uma fundação chamada **Free Software Foundation**

(Fundação do *Software* Livre), cujo objetivo era apoiar o movimento do *software* livre. Diversos utilitários de um sistema operacional, tais como compiladores, editores de texto, ***debuggers***, etc. foram desenvolvidos, porém um módulo principal (***kernel***) capaz de executá-los ainda não estava pronto.

A-Z

Free Software Foundation
Organização que possui a filosofia de eliminar restrições sobre a cópia, redistribuição, estudo e modificação de programas de computadores.

Debuggers
Programa de computador usado para testar e depurar programas em desenvolvimento.

Kernels
Componente principal do sistema operacional, servindo de ponte entre as aplicações e as demais partes do SO e o *hardware*.

1.3.2.2 Minix

Escrito por Andrew S. Tanenbaum, o Minix é um sistema operacional baseado no Unix, voltado para a educação em ciência da computação. Era um SO livre, e foi adaptado para utilidades mais complexas.

1.3.2.3 Linux

Em 1991, Linus Torvalds terminou de desenvolver seu próprio SO, criando assim o *kernel* (núcleo) do Linux. O desenvolvimento deste foi iniciado no Minix e, mais tarde, o Linux ganhou forma e tornou-se possível o desenvolvimento nele próprio. Os desenvolvedores, então, começaram a trabalhar para integrar os componentes GNU com o Linux, e fazer um sistema operacional livre e funcional. Atualmente, as distribuições Linux são utilizadas amplamente, de computadores domésticos até sistemas embarcados, além de servidores diversos.

1.4 Características e requisitos básicos

O sistema operacional servidor gerencia os componentes de *hardware*, fornece recursos que possibilitam obter o controle de componentes diversos (para evitar, por exemplo, que um usuário não autorizado apague arquivos que não lhe pertencem), compartilhamento de recursos, administração e gerência, além de outras funções de rede necessárias. O SOS permite acesso de outras estações aos seus recursos por meio da rede. Está sempre em execução, aguardando ser chamado pelo cliente.

Um aspecto importante para a escolha desse tipo de sistema é a estabilidade. Ele deve ser compatível com o número de solicitações dos usuários. O *hardware* desse tipo de SO deve ser mais robusto, com grande capacidade de armazenamento e, principalmente, processamento, porque os dados de toda a rede serão armazenados e acessados através do servidor, ou seja, as informações serão centralizadas. O SO atende a pedidos de diversos clientes simultaneamente, presta serviços de forma distribuída e ainda responde a solicitações vindas de múltiplas estações. Para isso, os servidores estão equipados para lidar com mais capacidade de memória e operações do que um

computador *desktop* comum. Em um servidor, quando a qualidade da prestação dos serviços está ruim, pode ser um indicativo de que chegou a hora de adquirir mais recursos (processador/memória/disco).

Os recursos de interface gráfica nesse tipo de sistemas operacional são menores que em um SO comum, pois a interação direta com o usuário é feita, geralmente, apenas para configuração do sistema. É um sistema contínuo (esperando sempre a solicitação das estações/clientes) e reativo. Principais características:

A-Z

Backup
Cópia dos dados de um dispositivo de armazenamento para que possam ser restaurados em caso de perda dos dados originais.

- sistema de segurança rígido;
- recursos de proteção de memória,
- mecanismos de ***backup*** avançados para evitar perda de dados em caso de falhas, etc.

1.4.1 Como escolher um SO servidor

A escolha de um SO servidor é baseada em fatores diversos, tais como custo, requisitos do *hardware* do sistema, aplicativos que serão executados, eficiência do *hardware* e do sistema, escalabilidade, estabilidade, segurança – que serão vistos nas próximas aulas.

Conheça um pouco mais sobre o projeto GNU acessando http://www.gnu.org

Veja mais detalhes sobre o *Active Directory* em http://www.juliobattisti.com.br/fabiano/artigos/activedirectory.asp

Resumo

Nesta aula tratamos a respeito dos conceitos sobre o que é um sistema operacional servidor e como é a arquitetura do tipo cliente-servidor. Aprendemos um pouco sobre a evolução dos sistemas operacionais, focando nos sistemas Windows e variantes do Unix, tal como o Linux. Falamos sobre os requisitos básicos em sistemas operacionais servidores e, finalmente, abordamos a escolha de um sistema operacional servidor mediante suas características e necessidades.

Atividades de aprendizagem

1. Quais são os serviços mais comuns oferecidos por um servidor?

2. Caracterize a arquitetura cliente-servidor.

3. Cite vantagens e desvantagens da arquitetura cliente-servidor.

4. O que motivou o surgimento dos sistemas operacionais servidores?

5. Cite as principais características dos sistemas operacionais servidores.

6. Quais são as diferenças entre um SO comum e um SOS?

7. Pesquise as limitações de um SO não servidor, tais como: número máximo de conexões simultâneas, número máximo de arquivos abertos simultaneamente, etc.

8. Pesquise a arquitetura cliente-servidor em duas e três camadas. Qual a diferença entre elas?

9. Pesquisar os *softwares* de servidores mais comuns e explicar por que eles se destacaram dos demais. Ex.: Servidor web, *software* Apache.

10. Por que as interfaces gráficas dos SOS são menos elaboradas e podem até mesmo nem existir?

Poste suas respostas no ambiente virtual de ensino-aprendizagem (AVEA).

Aula 2 – Tipos de servidores

Objetivo

Conhecer e identificar os principais tipos de servidores e serviços.

2.1 Introdução

Um servidor é um sistema de computação que fornece serviços de natureza diversa a uma rede de computadores, tais como serviço de arquivos, serviço de correio eletrônico e serviço de impressão. Os computadores que solicitam os serviços de um servidor são chamados clientes. As redes que utilizam servidores são do tipo cliente-servidor, classificam-se como de médio e grande porte, e nelas a segurança é relevante. O termo servidor é largamente aplicado a computadores completos (*software* e *hardware*), embora um servidor possa equivaler a um aplicativo ou a partes de um sistema computacional, ou até mesmo a uma máquina que não seja necessariamente um computador.

A história dos servidores é relacionada com as redes de computadores. Com o crescimento das redes, surgiu a ideia de dedicar alguns computadores para prestar serviços aos demais computadores. O crescimento do uso da arquitetura cliente-servidor e da internet foi o grande impulso para o desenvolvimento e aperfeiçoamento de tecnologias para servidores. Existem diversos tipos de servidores; os mais conhecidos serão apresentados a seguir.

2.2 Servidor de arquivos

O servidor de arquivos disponibiliza área ou espaço para o armazenamento compartilhado de arquivos que podem ser acessados pelas máquinas clientes. Um servidor de arquivo geralmente não realiza quaisquer cálculos; ele é projetado principalmente para permitir o armazenamento de dados e a sua recuperação de forma rápida. Todo o processamento então é efetuado pelas estações de trabalho.

Esse tipo de servidor encontra-se conectado a uma rede cujo objetivo principal é proporcionar um local para o armazenamento compartilhado de arqui-

vos, tais como documentos, arquivos de som, fotografias, filmes, imagens, bases de dados, etc. onde podem ser acessados pelas estações clientes ligadas à rede de computadores.

2.2.1 Os modelos de servidores de arquivos

Servidores de arquivos podem ser de diferentes tipos: de *backup*, de compartilhamento de informações, de armazenamento remoto, etc. Cada servidor de arquivos possui modelos conceituais de funcionamento de acordo com a forma que recebe, armazena e disponibiliza as informações. Os três modelos mais utilizados são:

- o servidor possui a estrutura dos arquivos e pode realizar operações complexas sobre eles;
- o servidor não possui a estrutura interna dos arquivos; logo, não é capaz de resolver operações complexas, somente realiza a leitura e a escrita;
- o servidor possui hierarquia, tratando os arquivos em forma de árvore; este modelo é o mais comum e pode possuir a estrutura interna dos arquivos, permitindo operações complexas.

Saiba mais sobre servidores de arquivos Linux em http://www.hardware.com.br/artigos/186/

2.3 Servidor de aplicação

Disponibiliza um ambiente para a instalação e execução de certas aplicações. O servidor de aplicações atende a algumas questões comuns às aplicações, tais como segurança, garantia de disponibilidade, balanceamento de carga e tratamento de exceções. Estes servidores normalmente são munidos de bastante memória RAM e processamento para execução dos aplicativos que eles disponibilizam aos usuários clientes.

HTTP
É um protocolo de comunicação utilizado para sistemas de informação e está incluído no servidor de vários sistemas operacionais. É considerado o protocolo da internet.

HTML
É uma linguagem de marcação utilizada para produzir páginas na *web*. Documentos HTML podem ser interpretados por navegadores.

2.4 Servidor web

Trabalha com requisições de pedidos **HTTP** (*Hyper Text Transfer Protocol* ou Protocolo de Transferência de Hipertexto) de clientes, incluindo dados, tais como documentos **HTML** (*HyperText Markup Language* ou Linguagem de Marcação de Hipertexto) com objetos embutidos (imagens, som, etc.). Os servidores *web* têm a responsabilidade de armazenar e trocar informações com outras máquinas. Como são necessários dois participantes para o processo de troca de informações (o solicitante e o servidor), cada lado possui programas especializados na troca de dados. No cliente, pode ser um *browser* tal como o Internet Explorer e, no servidor, o Apache.

Os servidores, geralmente, necessitam de uma quantidade mais robusta de *softwares*, e todos têm uma tarefa semelhante: negociar transferências de dados entre eles e seus clientes via HTTP.

Os *softwares* a serem instalados em um servidor dependem de sua plataforma ou sistema operacional. Um exemplo é o IIS da Microsoft, muito popular para SO Windows; já para o Unix existe o Apache (que também pode ser executado em ambiente Windows).

A comunicação entre o cliente e o servidor *web* funciona da seguinte forma:

1. o *browser* do cliente decompõe o endereço da página (URL) em partes distintas, tais como o nome de domínio, nome da página e protocolo;
2. um servidor **DNS** traduz o nome de domínio informado em seu endereço IP;
3. o *browser* determina o protocolo que deve ser usado;
4. o servidor seleciona os arquivos solicitados e responde aos pedidos. Se não localizar o arquivo, o servidor envia a uma mensagem de erro para o cliente;
5. o *browser* recebe os dados do servidor, interpreta essas instruções e exibe os resultados para o usuário.

A-Z

DNS
O *Domain Name System*, ou Sistema de Nomes de Domínios, converte nomes de domínio em endereços IP. Nas próximas aulas daremos mais detalhes sobre o funcionamento dessa tecnologia.

Esse processo é repetido até que o cliente (*browser*) deixe o *site*, conforme a Figura 2.1 a seguir.

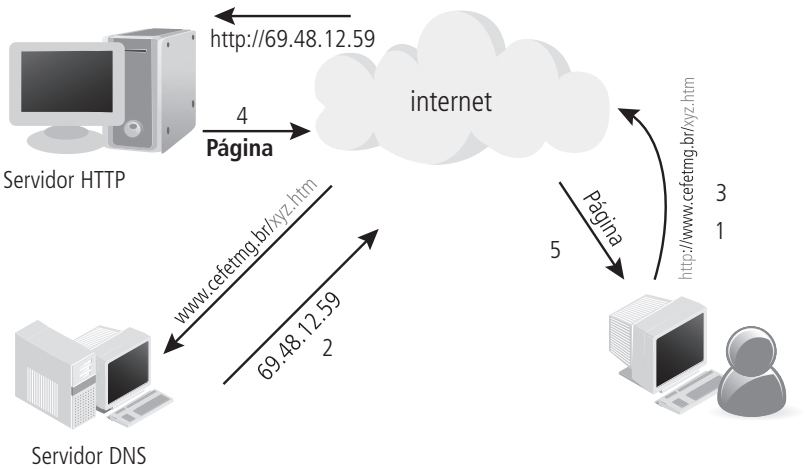


Figura 2.1: Relação entre cliente (solicita página) e servidor (fornece página)
Fonte: Elaborada pelos autores

As funções do servidor e do cliente são:

Servidor:

- armazenamento das páginas;
- manutenção das páginas;
- tradução das solicitações;
- controle de atendimento por portas;
- distinguir entre vários tipos de erros e dados.

Cliente:

- tradução da página;
- envio de solicitação de página e recebimento;
- distinguir entre vários elementos de uma página *web* (como figuras, sons, vídeos, etc.).

A-Z

Web
A *Web* ou *orld Wide Web* (Rede de alcance mundial) também é um sistema de documentos em hipermídia que são interligados e executados na internet. Muitas vezes também é utilizada como sinônimo para internet.

Dependendo da função do *site*, um servidor ***web*** pode também tratar de tarefas adicionais, como registro de estatísticas, segurança de manipulação e criptografia, servir imagens para outros *sites* (para imagens, mapas, etc.), gerenciador de conteúdo dinâmico, ou funções de comércio eletrônico.

2.5 Servidor *proxy*

Um servidor *proxy* é um computador configurado para ficar entre o computador do usuário e o computador destino de uma rede distinta, tal como a internet. Ele pode ser utilizado para registrar as requisições da internet e também para bloquear o acesso a algum *site* da *web*. O servidor *proxy* atende a requisições e repassa os dados à frente, conforme necessário. Um servidor *proxy* pode alterar uma requisição do cliente ou mesmo a resposta do servidor. Também pode disponibilizar esse recurso mesmo sem se conectar ao servidor especificado. Esse servidor tem uma série de usos:

- filtrar conteúdo;
- aumentar o desempenho;
- providenciar anonimato, entre outros.

O funcionamento do *proxy* HTTP pode ser visto quando o cliente requisita um documento na internet. O *proxy* procura o documento em sua memória interna, chamada **memória *cache***. Caso seja encontrado, o documento é retornado ao cliente. Caso contrário, o *proxy* requisita o documento a um servidor remoto (atuando como cliente), entrega-o ao cliente original e salva uma cópia em sua *cache*. Isso diminui a latência (tempo de resposta) para as próximas solicitações do mesmo documento, já que somente o servidor *proxy* e não o servidor remoto é requisitado, reduzindo o uso da banda.

A-Z

Memória *cache*
Na computação, *cache* é um dispositivo mais rápido que serve de intermediário entre o sistema e o dispositivo que se deseja acessar. A vantagem na utilização da *cache* consiste em evitar o acesso ao dispositivo – que pode ser demorado –, armazenando os dados e disponibilizando de forma mais rápida.

O servidor *proxy* pode funcionar como *firewall* e filtro de conteúdo. Esse tipo de servidor atua como um mecanismo de segurança. Essa forma é implantada por muitos provedores de internet e administradores de rede em intranets a fim de impedir o acesso ou filtrar os conteúdos considerados ofensivos ou prejudiciais para a rede e usuários. O *proxy* pode utilizar algoritmos para o controle de armazenamento de páginas no *cache*. Dois algoritmos simples são o *Least Recently Used* (LRU), ou Menos Usado Recentemente, que remove os documentos que passaram mais tempo sem serem usados, e o *Least Frequently Used* (LFU), ou Menos Frequentemente Usado, que remove documentos menos frequentemente usados.

2.6 Servidor de impressão

Um servidor de impressão é um conjunto de aplicativos voltados para controlar as tarefas de impressão enviadas por diferentes estações de trabalho que competem pela impressora conectada a um computador ou diretamente na rede. Pode ser um equipamento de *hardware* ou implementado em *software* que usa os recursos disponíveis no exercício dessa função. Sua principal importância é criar um local centralizado na rede para impressão, gerando controle de páginas e definindo ordem de prioridade das solicitações. Outra função é o armazenamento das impressões em fila de ordem de chegada, organizando as diversas solicitações originadas de diversos pontos da rede. Um servidor de impressão é um artifício voltado para redes com grandes volumes de impressão. Vide exemplo de uma rede e seu servidor de impressão na Figura 2.2 a seguir.

Conheça as novas tendências de tecnologia da Microsoft acessando http://technet.microsoft.com/pt-br/

Veja as novidades na área de *hardware* em http://www.hardware.com.br/

Mais detalhes sobre um servidor *Proxy* podem ser vistos em http://www.java.com/pt_BR/download/help/proxy_server.xml e

Uma visão geral de um servidor em http://pt.wikipedia.org/wiki/Servidor

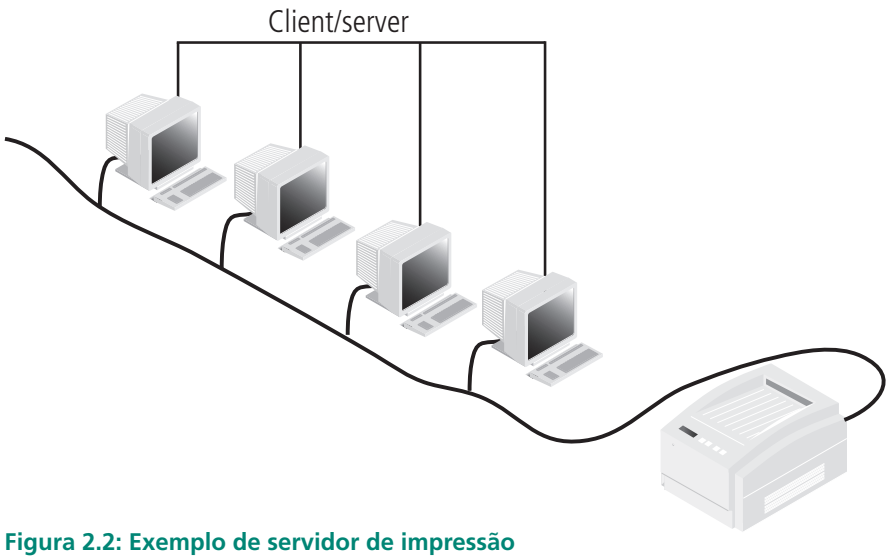


Figura 2.2: Exemplo de servidor de impressão
Fonte: http://f1tutorials.com/Tutorials/Network/chapter2.1.html

Resumo

Aprendemos nesta aula os tipos de servidores. Vimos como estão estruturados servidores de arquivos e alguns de seus modelos; servidores de aplicação; servidores de internet; servidores *proxy* e servidores de impressão.

Atividades de aprendizagem

1. Caracterize um computador servidor.

2. O que é um servidor de arquivos e quais suas funções?

3. O que é um servidor de aplicação e quais suas funções?

4. O que é um servidor *web* e quais suas funções?

5. O que é um servidor *proxy* e quais suas funções?

6. O que é um servidor de impressão e quais suas funções?

7. Dê um exemplo prático de um servidor de aplicação.

8. Baseado nos servidores que você estudou, descreva uma forma possível de funcionamento de um servidor de *e-mail*.

Poste suas respostas no ambiente virtual de ensino-aprendizagem (AVEA).

Aula 3 – Instalação de servidores

Objetivo

Entender os princípios de instalação de servidores.

3.1 Introdução

A instalação ou reinstalação de um sistema operacional ocorre por motivos diversos. Um deles seria pela necessidade de atualizar o sistema atual para um sistema operacional mais novo. Ou talvez o nosso computador esteja abarrotado de arquivos e aplicativos desnecessários, deixando o sistema lento. Talvez ainda por um acidente mais grave, tal como um vírus, uma falha de *hardware*, etc.

Outras referências: Aprenda um pouco mais sobre *device drivers* em http://pt.wikipedia.org/wiki/Driver_de_dispositivo

3.2 Instalação ou recuperação de um sistema operacional

A instalação de um sistema operacional em um computador novo ou a recuperação em um computador com problemas, às vezes, requer que comecemos a partir do zero; de um disco limpo, totalmente formatado. Um computador sem sistema operacional geralmente requer uma mídia de instalação deste, tal como um CD ou DVD. Quando não há sistema operacional instalado no computador, o **BIOS** vai permitir iniciar a sua máquina a partir de um dispositivo de memória secundária além do disco rígido. Devemos configurar, através dos menus do BIOS, que o computador inicie-se, por exemplo, a partir do leitor óptico se quisermos utilizar um CD/DVD. Em seguida, devemos inserir o CD do sistema operacional e iniciar o computador. O instalador do sistema operacional deve, então, guiar-nos através desse processo.

Depois de instalar o sistema operacional, precisaremos instalar os aplicativos necessários. Também será preciso identificar e instalar os *softwares* controladores (***drivers***) para os dispositivos de *hardware* que necessitem.

Localidades com muitos computadores (grandes empresas, universidades, etc.) podem utilizar meios alternativos para instalar sistemas operacionais, incluindo a implantação de "imagens" de computadores através da rede.

BIOS
O *Basic Input/Output System* ou Sistema Básico de Entrada/Saída é um programa de computador pré-gravado em memória permanente e executado por um computador quando ligado. Ele é responsável pelo suporte básico de acesso ao *hardware* bem como por iniciar a carga do sistema operacional.

Drivers
Um *driver*, também chamado de controlador de dispositivo, é um pequeno programa que faz a comunicação entre o sistema operacional e o *hardware*.

Alguns fabricantes fornecem "discos de recuperação" com seus computadores, em vez de mídia do sistema operacional original.

Os passos a seguir indicam etapas importantes para a instalação de sistemas operacionais.

3.2.1 *Backups*

Quando se planeja executar uma recuperação do sistema atual, o *backup* dos arquivos de usuários é de suma importância. Estar munido de CDs, DVDs e *pendrives* é a melhor maneira para fazer *backup* do disco rígido, especialmente se há uma grande quantidade de arquivos que ocupam muito espaço no disco. Podemos usar as unidades de *pendrive* para transferir arquivos para outro computador e depois gravá-los em mídias definitivas (CD/DVD/*Blu-ray*). Outra maneira é conectar o computador a outro utilizando um cabo de rede ou USB e, em seguida, transferir os arquivos. Além destas, um disco rígido externo também funciona muito bem como uma unidade de *backup*, assim como uma unidade de fita – que atualmente se encontra ultrapassada. Essas são algumas formas comuns e os passos básicos para realizar o *backup* de arquivos. É imprescindível guardar informações tais como arquivos pessoais, códigos de ativação do programa, dados da internet, dados do usuário e senhas, dados de perfis, ou qualquer outro tipo de informação importante.

3.2.2 Mídias de instalação de aplicativos e *drivers*

Um dos fatores que poupa muito tempo em uma instalação de SO é reunir todos os CDs de instalação dos *softwares* necessários e dos *drivers* de dispositivos do computador, tais como: impressora, *modem*, placa de vídeo, placa de som e outros dispositivos que têm o seu próprio *software* de instalação em separado.

Drivers de dispositivos ou controladores de dispositivos são programas que fazem a comunicação entre o sistema operacional e o *hardware*. O sistema operacional, através desses *drivers*, sabe como se comunicar com os dispositivos em questão. Sem os *drivers* adequados, os respectivos dispositivos poderão não funcionar ou funcionar parcialmente, pois o SO não conhecerá toda a funcionalidade do *hardware* que é informada pelos *drivers*.

3.2.3 BIOS

O primeiro *software* a atuar quando se liga o computador é o BIOS (*Basic Input/Output System*) ou Sistema Básico de Entrada/Saída. Durante a inicialização do computador (*boot*), o BIOS faz uma série de verificações do funcionamento do sistema. Um desses testes é chamado de POST.

O POST (*Power on Self Test*) ou Autoteste de Partida é uma sequência de testes no *hardware* realizada pela BIOS. Estes testes têm o intuito de verificar se o sistema possui algum problema. Caso algum problema seja detectado durante o POST, uma sequência de *bips* ou sons é emitida pelo BIOS para alertar o operador do computador sobre o problema. A sequência sonora é particular a cada fabricante de BIOS e a cada tipo de problema.

A maioria dos computadores acessa o BIOS ao pressionar uma tecla durante o *boot*, tais como as teclas: DEL, F1, F2, etc. Verifique se o computador está configurado para inicializar (dar "*boot*") a partir do dispositivo de memória secundária (HD, *pendrive*, CD, etc.).

3.2.4 Mídia do SO

Conecte/coloque a mídia contendo o sistema operacional no dispositivo adequado do computador. Ligue o computador e aguarde que o sistema acesse a mídia em busca da instalação do sistema operacional. Esta mídia pode ser um CD de um conjunto de CDs de recuperação, um *pendrive*, um HD externo, DVD, ou outro dispositivo.

3.2.5 Particionar e formatar

O instalador do SO então começa a ser carregado na memória do computador e, em determinado momento, solicita que o usuário informe em qual partição o SO deve ser instalado. Uma partição representa uma divisão de um disco rígido, sendo vista pelo usuário como se fossem discos individuais. Essas divisões são úteis para facilitar a manutenção e a segurança do sistema, permitindo isolar o acesso em cada disco virtual. Cada partição pode conter um sistema de arquivos diferente e, consequentemente, vários sistemas operacionais podem coexistir no mesmo disco. Preste muita atenção às instruções para particionar e formatar o disco rígido. Uma formatação apaga as informações de uma partição. O particionamento de um disco pode ser destrutivo ou não para as demais partições, mas é sempre uma operação de risco. Logo, sempre faça *backups* do conteúdo importante e que não pode ser perdido.

É interessante ter, no mínimo, duas partições em nosso disco. Dessa forma, podemos manter os arquivos pessoais em uma dessas divisões e o SO em outra. Assim, quando for necessário reinstalar o sistema, basta apenas copiar os arquivos da unidade do SO para a outra, facilitando o processo de instalação e *backup*.

3.2.6 Acompanhando a instalação

Siga as instruções que aparecem na tela e preste atenção no que está sendo feito. Essa etapa deve ocorrer sem maiores problemas. Contudo, caso algum problema apareça, anote as mensagens de erro e consulte os manuais do SO ou a internet para uma possível solução. Devemos verificar, em particular, as bases de conhecimento que existam *on-line* nos *sites* de fornecedores de SO ou do *hardware* com problema. Esses *sites* contêm informações valiosas que podem ajudar a superar até mesmo os problemas de instalação mais difíceis. A pesquisa deve ser diversificada. Podemos usar vários termos de pesquisa diferentes para procurar as soluções de que precisamos.

3.2.7 Atualização do SO

Após a instalação do SO, devemos atualizá-lo. Ao fazer as atualizações, o sistema ficará mais bem protegido contra falhas de segurança e vírus. É interessante configurar o SO para fazer as atualizações de forma automática; porém, isso pode se tornar um problema em alguns casos. Imagine um servidor com milhares de usuários, em que uma atualização acidentalmente impeça o acesso aos arquivos pessoais (ou até mesmo os apague!). Logo, em casos particulares, as atualizações devem ser instaladas em máquinas virtuais para verificar se não trarão outros problemas na instalação. Por fim, os demais aplicativos também requerem atualizações e estão sujeitos aos mesmos problemas.

3.2.8 Controladores de dispositivos

A instalação dos controladores de dispositivos (*drivers*) é uma etapa fundamental para o desempenho e funcionamento adequado do computador. Verifique o gerenciador de dispositivos para obter informações sobre dispositivo de *hardware* e instale o *driver* adequado.

3.2.9 Antivírus

Os antivírus são programas desenvolvidos para prevenir, detectar e eliminar vírus de computador. Os programas antivírus necessitam de atualização constante para que não fiquem obsoletos e continuem atuando de forma correta. Mas, mesmo em um sistema atualizado e bem planejado em termos de segurança, esse tipo de problema pode ocorrer. Novamente, a forma mais eficaz de evitar problemas é fazer *backups* periódicos para se proteger contra perda de dados importantes.

Mais adiante estudaremos os vírus detalhadamente.

3.3 Criando um ambiente virtual

Inicialmente, devemos preparar um ambiente que simule sistemas operacionais em nossa máquina. Isso é importante por dois motivos: primeiro, trabalhar num ambiente de simulação é mais seguro e didaticamente mais produtivo; segundo, o mesmo ambiente virtual pode ser utilizado para simular situações reais sem os custos e dificuldades inerentes a uma instalação real. Ou seja, podemos aprender a instalar e configurar um SO servidor sem termos um *hardware* específico para isso – apenas com o intuito de aprender!

O ambiente virtual que iremos utilizar se chama Oracle Virtual Box e esse tipo de *software* recebe a denominação de **máquina virtual** (MV).

Logo, vamos iniciar a parte prática do curso! No ambiente virtual de ensino-aprendizagem abra as apresentações intituladas:

SO2 – Instalação do Oracle Virtual Box
SO2 – Tutorial – Configuração da Máquina Virtual – Parte1
SO2 – Tutorial – Configuração da Máquina Virtual – Parte2

Na primeira delas, você acompanhará a instalação do *software* Oracle Virtual Box, que dará suporte às futuras máquinas virtuais em seu computador. Nas duas seguintes, aprenderá como instalar um SO qualquer em uma máquina virtual dentro do seu computador.

Compreender essas etapas é fundamental, pois será a partir delas que nossas aulas se desenvolverão

Antes de ir para a aula prática, leia um pouco sobre a técnica NAT *(Network Address Translation)* em http://pt.wikipedia.org/wiki/Network_address_translation

Conheça um pouco mais sobre a instalação de SO, acessando http://www.ligaturesoft.com/portuguese/cheap-computers/Instalacao-de-Sistema-Operacional.html

Máquinas virtuais
São aplicativos que permitem ao usuário simular outros sistemas operacionais dentro de uma janela, como se fosse um *software* comum. Dessa forma, é fácil para um programador testar se o *software* que ele desenvolve funciona adequadamente em SOs diversos. Além disso, as MVs permitem a conexão entre si, simulando o seu comportamento em redes.

3.4 Contratos e licenças

Uma licença ou contrato de *software* é uma definição de ações autorizadas (ou proibidas) pelo autor e concedidas (ou impostas) ao usuário desse aplicativo, em que o usuário pode ser uma pessoa ou empresa.

Uma licença comercial apresenta restrições sobre a autoria, o uso e a comercialização do *software*. Já uma licença de *software* livre estabelece diferentes restrições, reveladas a seguir.

Software livre é uma expressão cunhada por Richard Stallman, para os casos em que qualquer programa de computador cuja licença de direito de autor conceda ao usuário as quatro liberdades seguintes:

1. a liberdade de executar o programa, para qualquer propósito;

2. a liberdade de estudar como o programa funciona e adaptá-lo para as suas necessidades. O acesso ao código-fonte é um pré-requisito para esta liberdade;

3. a liberdade de redistribuir cópias;

4. a liberdade de aperfeiçoar o programa e liberar os seus aperfeiçoamentos para outras pessoas, beneficiando toda a comunidade. Acesso ao código-fonte é um pré-requisito para esta liberdade.

Conheça o Movimento de *Software* Livre, criado por Richard Stallman, em http://pt.wikipedia.org/wiki/Software_livre

Richard Stallman é um famoso hacker, ícone do projeto GNU e fundador da Free Software Foundation (FSF) (Fundação para o Software Livre). Veja mais em: http://pt.wikipedia.org/wiki/Richard_Matthew_Stallman

As licenças de *software* livre também se popularizaram, por darem a garantia jurídica aos utilizadores de que não estão cometendo atos de infração de direito de autor ao copiar ou modificar o *software*.

A remoção de qualquer uma dessas quatro liberdades descaracterizará sua condição de *software* livre.

3.5 Instalando sistemas operacionais

Instalar sistemas operacionais é uma tarefa relativamente simples, porém relativamente demorada, uma vez que o processo de instalação é praticamente automático. Em uma máquina real, basta inserir a mídia de instalação do sistema e configurar o computador (no BIOS) de modo que o *boot* (partida) seja efetuado pelo próprio dispositivo da mídia. Em uma máquina virtual, editaremos as configurações conforme os tutoriais passados e podemos utilizar arquivos ISO, que simulam uma mídia qualquer CD/DVD/*Blu-ray*.

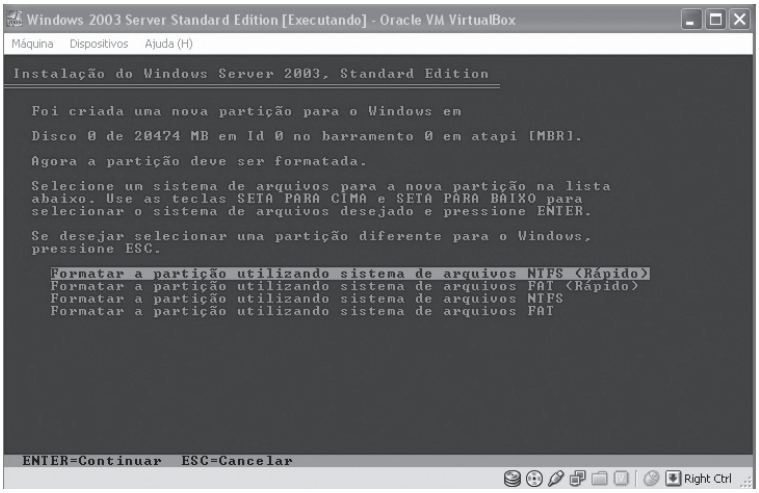


Figura 3.1: Janela de instalação do Windows Server 2003
Fonte: Windows 2003

Após o *boot* do SO, torna-se necessário definir um pedaço do disco, mais comumente chamada de partição, ou criá-lo, caso não exista, e a instalação será iniciada. Vide Figura 3.1. Em seguida, autorizamos a formatação ou não da partição de instalação e o SO começará a ser instalado. Na tela a seguir vemos o desencadear do processo de instalação.

Durante a instalação deveremos fornecer algumas informações básicas para que o SO seja instalado. Algumas delas estão listadas abaixo:

1. nome e organização;
2. chave do produto (caso necessária);
3. modo de licenciamento;
4. nome do computador;
5. senha do administrador;
6. data, hora e fuso horário;
7. configuração de rede;
8. nome do domínio ou grupo a qual o computador pertence.

3.5.1 Instalando o sistema operacional servidor

O detalhamento da preparação da máquina virtual e a instalação do Windows 2003 Server podem ser visto nas apresentações disponibilizadas no ambiente virtual de ensino-aprendizagem:

SO2 - Preparação da MV Windows 2003 Server
SO2 - Instalação Windows 2003 Server.ppt

Em um ambiente real, após a instalação do SO, é interessante atualizar o sistema imediatamente com o que existe de mais novo no *site* do fabricante. Dessa forma, o SO ficará melhor protegido contra falhas de segurança e vírus. Contudo, em nosso ambiente simulado, isso pode acarretar mudanças não previstas nas guias de aula. Logo, sempre que o SO sugerir atualizar o sistema, **não aceite a sugestão!**

O uso de máquinas virtuais requer controladores (*drivers*) virtuais que façam a ponte entre a máquina real (MR) e a virtual. Esses controladores permitem a troca de arquivos entre as máquinas, aumentam a *performance* geral da MV e permitem o acesso a dispositivos diversos da MR pela máquina virtual. Pode-se dizer que esses controladores ou pontes entre a MV e a MR são equivalentes aos controladores (*drivers*) da máquina real e os dispositivos de *hardware*, tais como placas de vídeo, som, rede, etc.

Na Oracle Virtual Box esses controladores são chamados de "Adicionais Para Convidado" e a forma de instalação pode ser vista na apresentação e vídeo disponibilizados no ambiente virtual de ensino-aprendizagem:

SO2 - Instalando adicionais para convidado

3.5.1.1 Instalando serviços no servidor

As etapas da instalação do *Active Directory* e dos serviços mais comuns em um servidor podem ser vistas na apresentação e vídeo disponibilizados no ambiente virtual de ensino-aprendizagem:

SO2 - Instalando configurações típicas de um servidor

O funcionamento e a configuração dos serviços instalados serão vistos na próxima aula. Em seguida, veja a apresentação e o vídeo citado abaixo para deixar a instalação com uma cara mais padronizada. Algumas opções servem apenas para fins estéticos; outras, para a melhora da *performance* e outras, para evitar problemas no futuro.

SO2 - Personalizando a aparência e configurações gerais do servidor.

3.5.2 Instalando o cliente

A instalação da máquina virtual do cliente pode ser vista na apresentação disponibilizada no ambiente virtual de ensino-aprendizagem:

SO2 - Instalação do Windows XP

Este arquivo oculta alguns detalhes da instalação já vistos antes na instalação do servidor. Caso tenha alguma dúvida, consulte as apresentações anteriores.

A máquina virtual do cliente servirá para testar o funcionamento dos serviços no servidor.

Caso tenha dúvidas na instalação dos sistemas operacionais nas aulas práticas, consulte os seguintes vídeos de outros autores:

Windows 2003/Server: http://www.videolog.tv/video.php?id=578316

Linux Ubuntu: http://www.youtube.com/watch?v=Wcp9VSfvXjQ

Instalando Windows e Linux num mesmo computador: http://www.youtube.com/watch?v=89ebO-69QXA&feature=related

3.6 Configurando a rede

Para nossas futuras aulas, será necessário configurar a rede entre as máquinas virtuais cliente e servidor. Veja também o vídeo citado abaixo e aprenda como fazer no servidor:

Configuração das placas de rede do servidor

Em seguida, repita os passos na máquina cliente (que só tem uma placa de rede) e configure a placa de rede desta forma:

- IP: 192.168.1.2
- Máscara: 255.255.255.0
- Gateway: 192.168.1.1
- DNS 1 e 2: 192.168.1.1

Resumo

Aprendemos, no decorrer desta aula, a instalação de sistemas operacionais. Vimos a importância de manter os *backups* dos dados atualizados em caso de falha do sistema. Soubemos quão importante é ter os *drivers* de instalação do sistema para o caso de necessitar efetuar a sua reinstalação. Aprendemos que existe um sistema anterior ao sistema operacional, conhecido como BIOS, responsável por preparar a máquina para o carregamento do SO. Entendemos a necessidade de preparo do disco de carga do sistema e seu respectivo particionamento. Acompanhamos a instalação de um ambiente virtual que simula um sistema operacional servidor. Entendemos os contratos de licença de uso de sistemas operacionais. Vimos a importância de se utilizar antivírus que possam dar segurança ao sistema contra ataques de vírus e de pessoas mal- intencionadas. Finalmente, aprendemos como configurar basicamente uma rede durante a instalação do sistema operacional servidor.

Atividades de aprendizagem

1. Cite alguns motivos pelos quais a reinstalação de um SO é necessária.

2. Por que não conseguimos tirar proveito de uma placa de vídeo 3D sem instalar os *drivers* dela?

3. O que são *backups*? Qual a sua importância?

4. O que são partições em um disco rígido?

5. O que são máquinas virtuais? Qual a sua importância/uso?

6. Pesquise e liste as principais formas de licenciamento de um servidor.

7. Um sistema que não usa *softwares* piratas necessita de antivírus? Justifique.

8. Como funciona um roteador em modo NAT?

9. Pesquise e liste outros *softwares* de máquina virtual como o *Oracle Virtual Box*.

10. Por que um administrador de redes não deve permitir atualizações de *software* indiscriminadamente?

Poste suas respostas no ambiente virtual de ensino-aprendizagem (AVEA)

Aula 4 – Configuração de SO

Objetivo

Entender os princípios de configuração de servidores.

4.1 Introdução

Nesta aula veremos o funcionamento e a configuração de alguns serviços de um servidor: o DNS e o DHCP (*Dynamic Host Configuration Protocol* – Protocolo de Configuração Dinâmica de *Host*). Faremos aqui o referencial teórico, e nas guias de aula o referencial prático, de forma que você entenda ambas as partes.

4.2 Endereços IP

O que são os famosos endereços IP? IP significa *Internet Protocol* ou Protocolo de Internet, e esses endereços, tradicionalmente, são constituídos de números de 32 *bits* normalmente apresentados como quatro "octetos" de *bits*. Um endereço IP comum tem a seguinte forma 200.131.3.193.

Os quatro números em um endereço IP são chamados de octetos, porque eles podem ter valores entre 0 e 255 (28 = 256 possibilidades por octeto). Ou seja, os valores binários podem variar de 00000000 até 11111111.

Em uma máquina Windows, você pode ver o seu endereço IP em um terminal de comandos através do comando "*winipcfg*" ou "*ipconfig*", dependendo da versão do Windows. No Linux/UNIX, o comando é o "ifconfig". Para saber o endereço IP de um computador qualquer, digite "*nslookup*" seguido pelo nome de máquina, tal como "nslookup www.cefetmg.br". O comando "*hostname*" exibe o nome da sua máquina.

Na internet, tudo que você precisa para ter acesso a um servidor é o endereço IP dele. Se digitar em seu navegador a URL http://200.131.3.193, você terá acesso ao servidor *web* do CEFET-MG. Nomes de domínio foram criados para facilitar nossa vida.

Inicialmente, a internet foi projetada como uma rede acadêmica e não previa o uso comercial. Contudo, com o início de sua utilização comercial, em 1993, aliado à política de alocação de endereços IP da época, percebeu-se que o espaço de endereçamento poderia se esgotar num prazo de dois ou três anos. O IP de 32 *bits* apresentado até agora é chamado de IPv4 ou IP versão 4. Embora o espaço de endereçamento do IP versão 4 tenha 32 *bits*, o que representa 232 = 4.294.967.296 endereços, a política inicial de distribuição dos endereços prejudicou a sua melhor utilização.

As previsões iniciais de esgotamento quase imediato dos endereços não se concretizaram devido ao desenvolvimento novas tecnologias. Uma das tecnologias cria endereços privados, não válidos na internet, para serem utilizados em redes internas, tais como as redes corporativas. Geralmente, esses endereços são utilizados em conjunto com a tecnologia NAT, permitindo que com um único endereço de internet, toda uma rede baseada em endereços privados tenha acesso à internet. O NAT, apesar de muito utilizado, também traz problemas, pois prejudica o modelo ponto a ponto (***peer to peer***) de algumas aplicações. Ou seja, apesar de o computador da rede interna ter acesso à internet, a comunicação precisa passar por diferentes níveis hierárquicos. Isso gera um alto custo de processamento e dificulta a comunicação direta entre os computadores.

A-Z

Peer to peer
É uma arquitetura caracterizada pela descentralização das funções na rede, na qual cada *host* (computador) realiza tanto funções de servidor quanto de cliente.

ADSL
É uma tecnologia que permite transferência digital de dados em alta velocidade por meio de linha telefônica comum.

Outra tecnologia criada foi o DHCP, que permite a alocação dinâmica de endereços IP aos computadores de uma rede. Dessa forma, os provedores de acesso podem reutilizar endereços IP de seus clientes em conexões não permanentes, como as realizadas através de linhas discadas ou **ADSL** (*Asymmetric Digital Subscriber Line*, ou Linha Digital Assimétrica para Assinantes).

Veja mais detalhes sobre ADSL em: http://www.abusar.org.br/adsl.html

O problema de esgotamento de endereços IPv4 pode ser visto em: http://www.ipv6.br/IPV6/ArtigoEsgotamentoIPv4

A demanda por novos números IP caiu drasticamente através dessas e outras tecnologias criadas e o esgotamento dos endereços IPv4 ainda não ocorreu. Como o esgotamento certamente irá ocorrer, uma nova forma de endereçamento, chamada de IP versão 6 começou a ser desenvolvida na década de 1990. O IPv6 tem como objetivo ser a solução definitiva para o endereçamento na internet. A principal diferença é o espaço de endereçamento, aumentado de 32 *bits* para 128 *bits*. Um endereço de 128 *bits* implica 2128 = 3,4 x 1038 endereços. Dessa forma, cada ser humano poderá ter 5,6 x 1028 endereços IP em média! Os endereços IPv6 são compostos de oito grupos de 4 dígitos hexadecimais, tal como 2001:0db8:85a3:08d3:1319:8a2e:0370:7344

Por fim, o IP versão 6 resolve a limitação atual de endereçamento na internet.

4.3 NAT

O NAT (*Network Address Translation*, ou Tradução de Endereços de Rede) é uma técnica que consiste em transcrever o endereço IP de um pacote de uma rede interna que passa por um roteador de maneira que esse pacote tenha acesso a uma outra rede exterior. O NAT somente reconhece pacotes TCP e UDP, não sendo possível fazer a ponte de outros pacotes.

O nosso servidor possui duas placas de rede instaladas. Uma dessas placas terá acesso à internet e a outra tem acesso à rede interna. Computadores na rede interna enviam pedidos HTTP (pacotes TCP e UDP) para o servidor NAT através da conexão da rede interna com o servidor. O servidor então retransmite o pedido para a internet (rede exterior) em nome do cliente. Quando o *site* responde à solicitação, a resposta é enviada para o servidor NAT, que, por sua vez, encaminha para o cliente que fez a solicitação original na rede interna.

4.4 DNS

O DNS (*Domain Name System*, ou Sistema de Nomes de Domínios) é um sistema hierárquico e distribuído de tradução de nomes. O DNS traduz nomes em endereços IP e vice-versa. Dessa forma, podemos acessar o *site* do CEFET-MG sem saber que o seu IP é 200.131.3.193. Ou seja, o serviço DNS facilita o acesso a recursos da rede, pois é mais fácil lembrar um nome do que sequências numéricas. O banco de dados dos servidores DNS com os nomes de *hosts* (computadores) e seus endereços IP é distribuído entre estes, balanceando a carga nos servidores que fornecem o serviço. Como o banco de dados é distribuído, seu tamanho é virtualmente ilimitado e o desempenho não degrada tanto quando se adiciona mais servidores nele. Um servidor DNS secundário é uma cópia de segurança do servidor DNS primário, projetada para o caso de uma eventual falha do servidor primário.

Atualmente, existem 13 grandes servidores DNS no mundo todo, dos quais toda a internet é dependente. Esses grandes servidores são chamados de servidores raiz de DNS. Destes, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa. Para aumentar a base instalada desses servidores, foram criadas réplicas localizadas por todo o mundo, inclusive no Brasil desde 2003.

A função de um servidor DNS envolve as seguintes características:

- existem bilhões de endereços IP em uso atualmente e a maioria das máquinas tem um nome legível também;
- diariamente são feitos bilhões de pedidos de DNS;
- nomes de domínios e endereços IP mudam constantemente;
- novos nomes de domínio são criados diariamente.

O DNS é um banco de dados que merece destaque, pois não existe outro banco de dados no mundo no qual milhões de pessoas fazem alterações com tanta frequência. Isso torna o DNS tão singular.

Se tivéssemos de lembrar os endereços IP dos *sites* que visitamos todos os dias, nós ficaríamos loucos. Os seres humanos simplesmente não gostam de lembrar sequências de números. Contudo, somos bons em guardar palavras e é aí que os nomes de domínio se destacam. Você provavelmente tem centenas de nomes de domínio armazenadas em sua cabeça. Por exemplo:

- **br-linux.org/**
- **www.google.com**
- **www.brasil.gov**

As porções ORG, COM e GOV desses nomes de domínio são chamados de domínio de nível superior ou de primeiro nível. Existem centenas de nomes de domínio de nível superior, incluindo COM, EDU, GOV, MIL, NET, ORG e INT, bem como únicas combinações de duas letras para cada país. Dentro de cada domínio de nível superior, há uma lista enorme de domínios de segundo nível. Por exemplo, no domínio de primeiro nível, você tem:

- **www.google.com.br**
- **www.brasil.gov.br**

Os nomes no domínio de nível superior devem ser únicos, mas pode haver duplicação entre domínios. Por exemplo, nome.com e nome.org são domínios completamente diferentes. Um domínio de terceiro nível seria bbc.co.uk. Em geral, até 127 níveis são possíveis, embora seja raro haver mais de quatro.

A palavra mais à esquerda, como www ou cefetmg, é o nome do *host* relacionado a uma máquina de endereço IP específico em um domínio. Um determinado domínio pode conter milhões de nomes de *hosts*, desde que todos eles sejam únicos dentro desse domínio. Como os nomes de um domínio precisam ser exclusivos, é necessário que uma entidade mantenha uma lista que garanta que nenhuma duplicação ocorra. Quando você registra um nome de domínio, ele passa por empresas especializadas que adicionam o nome à lista. Essas empresas, por sua vez, mantêm um banco de dados central conhecido como *whois*, que contém informações sobre o proprietário e servidores de nomes para cada domínio. No banco de dados *whois*, você pode encontrar informações sobre qualquer domínio.

Enquanto é importante ter uma autoridade central fazendo a atualização do banco de dados de nomes COM e outros domínios de nível superior, não é interessante centralizar a base de dados. Por exemplo, a Microsoft tem centenas de milhares de endereços IP e nomes de *host*. Ela mesma quer manter seu próprio servidor de nomes de domínio para o domínio microsoft.com. Da mesma forma, a França provavelmente quer administrar o domínio de nível superior .**fr**, o Brasil provavelmente quer administrar o domínio.**br** e assim por diante. Por essa razão, o sistema DNS é um banco de dados distribuídos. A Microsoft é completamente responsável por lidar com o servidor de nome para o domínio microsoft.com. Dessa forma, ela pode alterar o banco de dados para o seu domínio sempre que quiser, pois possui seus próprios servidores de nomes de domínio.

4.4.1 Funcionamento do DNS

Os serviços de DNS da internet encontram em servidores por todo o mundo que estão em bancos de dados que possuem a função de indicar qual IP está a cada nome de *host*. Ao pesquisar por um *host* em um domínio, tal como www.infowester.com, seu computador requer aos servidores de DNS de seu provedor de internet a localização do endereço IP associado ao *site*. Caso os servidores DNS de seu provedor não tenham a informação, ele se comunica com outros servidores DNS de nível hierárquico mais alto, até que o endereço seja encontrado. Os nomes de domínio são divididos de forma hierárquica, conforme exemplo a seguir.

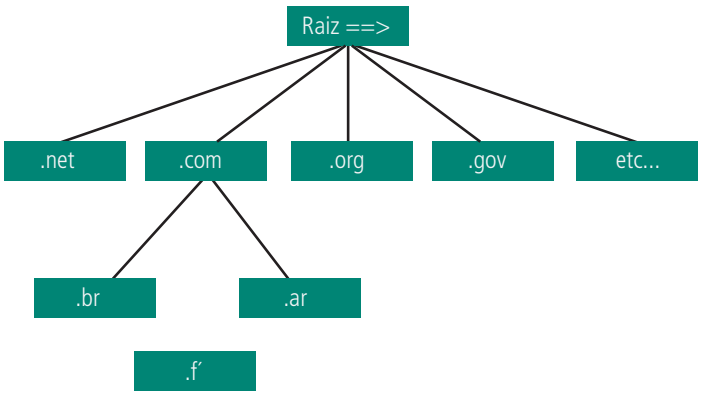


Figura 4.1: Exemplo hierárquico da estrutura da conexão de servidores DNS
Fonte: Elaborada pelos autores

Note, na Figura 4.1, que existem subdivisões dentro de cada domínio e essas subdivisões possuem entidades que as administram. Dessa forma, o domínio **.br** é gerenciado pelo Comitê Gestor da Internet no Brasil. Logo, para registrar um domínio, deve-se recorrer ao órgão competente relativo. O servidor raiz, principal servidor DNS, é representado por um ponto na figura e, seguindo a ordem de pesquisa, sua inserção é feita no final do nome. Assim, www.infowester.com deveria ficar como:

www.infowester.com.

Contudo, não é necessário incluir o ponto ao final do domínio, pois os aplicativos já adicionam automaticamente.

Por fim, ao visitar um *site* qualquer, tal como www.sitequalquer.com.br, inicialmente, o servidor raiz indica o servidor de terminação **.br**, que por sua vez, indica o servidor que cuida do domínio *site*qualquer.com.br que informa qual o seu IP, ou seja, em qual servidor está localizado o *site* em questão.

4.4.2 *Cache* de DNS

As informações de nomes e endereços IP são armazenadas em *cache* pelo servidor, acelerando o desempenho de resolução de DNS para consultas futuras e reduzindo o tráfego de consultas na rede. Um exemplo seria se você visitasse um *site* que nunca tenha sido resolvido pelo serviço de DNS de seu provedor, de forma que este tenha que fazer uma pesquisa em outros servidores de DNS. Para que essa pesquisa não tenha que ser refeita quando outro usuário quiser navegar no mesmo *site*, o serviço de DNS guarda a informação da primeira consulta. Logo, em uma futura solicitação, o servidor DNS do provedor já saberá o IP associado ao *site* em questão. Esse procedi-

mento é chamado de "*cache* de DNS". Quando a informação é armazenada em *cache*, um valor TTL (*Time to Live*) ou Tempo de Vida se aplica a todos os registros armazenados em *cache*. Enquanto o TTL de um registro em *cache* não expirar, o servidor DNS pode continuar a usar esse *cache*.

4.4.3 Hierarquia DNS

Devido ao tamanho da internet, armazenar todos os pares de domínio-endereço IP em um único servidor DNS é inviável por questões de escalabilidade que incluem:

- **confiabilidade:** se o único servidor de DNS falhasse, o serviço se tornaria indisponível;
- **volume de tráfego:** o servidor deveria tratar todos os pedidos DNS do mundo;
- **distância:** devido à centralização, a maioria dos usuários estaria distante do servidor e sofreria atrasos na resolução dos pedidos DNS;
- **manutenção do banco de dados:** o banco de dados seria enorme e atualizado com uma frequência muito alta.

A arquitetura DNS é um banco de dados hierárquico distribuído em um conjunto associado de protocolos que definem:

- Um mecanismo para consultar e atualizar o banco de dados.
- Um mecanismo para replicar as informações no banco de dados entre servidores.
- Um esquema do banco de dados.

4.4.4 Servidores autoritativos

O servidor autoritativo de um domínio possui os registros originais que associam aquele domínio a seu endereço de IP. Toda vez que um domínio adquire um novo endereço, essa informação deve ser adicionada a pelo menos dois servidores autoritativos (um principal, outro secundário). Isso é feito para minimizar o risco de perder todas as informações originais do endereço daquele domínio.

4.4.5 Servidor local

Esse tipo de servidor não pertence à hierarquia DNS, mas é fundamental para

o seu bom funcionamento. Em vez de fazer requerer a um servidor raiz, cada cliente requere a um servidor local, que, fisicamente, fica próximo ao cliente. Então, ele se encarrega de resolver a requisição. Com o uso de *cache*, esses servidores podem ter a resposta pronta, ou reconhecer algum servidor mais próximo ao autoritativo que o servidor raiz, reduzindo a carga nos servidores raiz.

4.4.6 DNS reverso

Geralmente, o DNS atua com a resolução do nome do domínio de um *host* qualquer para seu endereço IP correspondente. O DNS reverso resolve nome de domínio associado ao *host* através do endereço IP. Ou seja, quando temos disponível o endereço IP de um host e não sabemos o endereço do domínio (nome dado à máquina ou outro equipamento que acesse uma rede), tentamos resolver o endereço IP através do DNS reverso que procura qual nome de domínio está associado àquele endereço. Os servidores que utilizam o DNS reverso conseguem verificar a autenticidade de endereços, verificando se o endereço IP atual corresponde ao endereço IP informado pelo servidor DNS. Isso evita, por exemplo, que alguém faça uso de um domínio que não lhe pertence para enviar *spam*. Veja abaixo um exemplo de servidor de DNS reverso e uma pesquisa a ele. A Figura 4.2 mostra como se estabelece a resolução de DNS reverso.

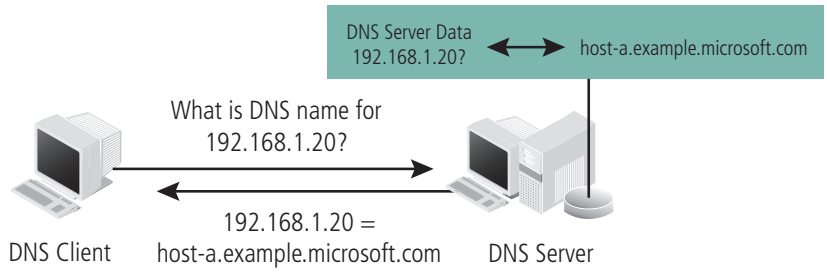


Figura 4.2: DNS reverso
Fonte: http://technet.microsoft.com/en-us/library/cc772774%28WS.10%29.aspx#w2k3tr_dns_how_ceap

4.4.7 Estrutura

Veja na Figura 4.3 a ilustração da estrutura hierárquica DNS. Observamos as interligações dos diversos domínios, a partir da raiz até uma empresa e seus respectivos subdomínios.

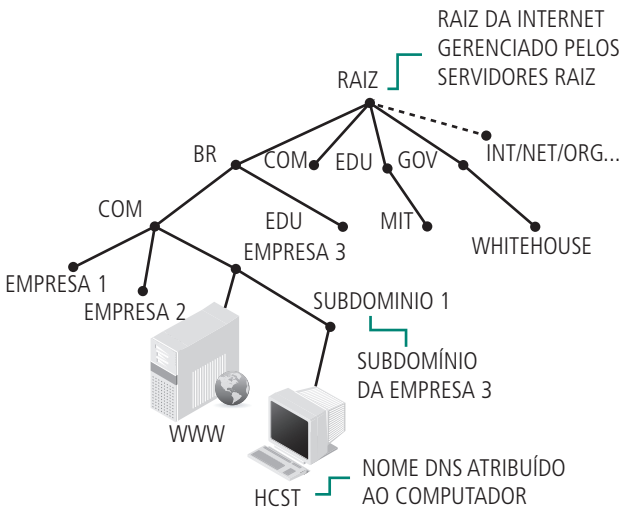


Figura 4.3: Exemplo de estrutura DNS
Fonte: http://www.abusar.org.br/dns_como.html

4.4.8 Obtenção de nomes de domínio e endereços IP

O espaço de nomes de domínio e endereços IP são recursos críticos para a internet, no sentido que requerem coordenação global. Cada endereço IP deve identificar um único equipamento, de forma que não é possível atribuir endereços IP de maneira descentralizada. Da mesma forma, um nome de domínio deve identificar o conjunto de computadores que o mantém. A organização responsável por atribuir nomes de domínio e endereços IP em nível global é a ICANN – Internet Corporation for Assigned Names and Numbers (órgão mundial responsável por estabelecer regras do uso da internet).

Aprofunde seu conhecimento em DNS consultando:

http://technet.microsoft.com/en-us/library/cc772774(WS.10).aspx#w2k3tr_dns_how_ceap

http://www.infowester.com/dns.php

http://pt.wikipedia.org/wiki/Domain_Name_System

4.5 DHCP

O **DHCP** (*Dynamic Host Configuration Protocol*, ou Protocolo de Configuração Automática de Computadores) é um protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de *host* e outros parâmetros de configuração para clientes de rede. Em suma, trata-se de um protocolo utilizado em redes de computadores que permite, de forma automática, a obtenção de um endereço IP. Esse protocolo é o sucessor do BOOTP, que se tornou limitado para as exigências atuais. O DHCP surgiu como padrão em 1993.

O DHCP consiste em dois componentes: um protocolo para a entrega de parâmetros específicos a partir de um servidor DHCP e um mecanismo que faça a atribuição de endereços de rede para *hosts*. Caso tenha que administrar uma rede pequena, não haverá muito trabalho para atribuir um número IP a

cada máquina. Mas se for uma rede grande, será preciso algum mecanismo que não entregue o mesmo número IP a duas máquinas diferentes, já que isso faria com que essas máquinas entrassem em conflito e não conseguissem utilizar a rede. Esse mecanismo é o protocolo DHCP.

Esse protocolo é uma solução eficiente para esse problema, já que um servidor distribui endereços IP na medida em que as máquinas solicitam conexão à rede. Quando um computador se desconecta, seu IP fica livre para uso de outra máquina. Para isso, o servidor geralmente é configurado para fazer uma avaliação dos endereços IPs em uso em intervalos predefinidos.

Esse processo assemelha-se ao sistema de telefonia empresarial conhecido como PABX. Nesse sistema, algumas linhas telefônicas são disponibilizadas para atender a um número maior de ramais. O que faz com que o sistema funcione é que nem todos os ramais ficam em funcionamento ao mesmo tempo. Existe um cálculo que verifica a média de utilização, o que permite a compra de apenas algumas linhas telefônicas. O PABX gerencia a demanda dos terminais e fornece um número de linha desocupada no momento em que estes necessitam conectar-se com outros números fora da empresa. O DHCP faz a mesma coisa. Nos dois sistemas, o ramal ou o *host* tem um número fixo só para ele (um número de telefone para o caso do exemplo do PABX e um número de IP para o caso do DHCP). No momento que é feito o pedido de conexão, é prestado ao solicitante um número para falar (PABX) ou transmitir dados (DHCP). Numa segunda solicitação, o solicitante pode não ter o mesmo número sua conexão prévia. Isso se deve pelo fato de que o número anteriormente utilizado pode estar sendo utilizado por outro *host*.

4.5.1 Funcionamento

Quando um computador configurado com DHCP se conecta a uma rede, ele não sabe o endereço do servidor DHCP e envia uma solicitação a todos os computadores da rede. O servidor DHCP então percebe que uma nova máquina cliente quer participar da rede e envia os parâmetros necessários. Caso o cliente aceite, esse número ficará indisponível a outros computadores que se conectarem a rede.

O administrador da rede pode configurar o protocolo DCHP para funcionar nas seguintes condições:

- **Automática**: uma determinada quantidade de endereços IP é definida para ser usada na rede. Assim, quando um computador fizer uma solicitação de conexão na rede, um dos endereços IPs em desuso é oferecido a ele.

- **Dinâmica**: é muito semelhante ao automático, exceto no fato de que a conexão à rede é feita por um tempo predeterminado.

- **Manual**: cada placa de rede possui um parâmetro de identificação exclusivo, conhecido por endereço MAC (*Medium Access Control*, ou Controle de Acesso ao Meio). Um endereço MAC é formado por 12 dígitos hexadecimais agrupados dois a dois, tal como: 00:00:5E:00:01:03. Como esse valor é único, o administrador pode reservar um endereço IP para o computador que possui um determinado valor de MAC. Assim, só esse computador utilizará o IP em questão. Esse recurso é interessante para quando for necessário que o computador tenha um endereço IP fixo.

O protocolo DHCP trabalha de uma forma bastante interessante. Inicialmente, a estação não possui um endereço IP e não sabe o endereço do servidor DHCP da rede. Então, ela envia um pacote de *broadcast* (para todos os computadores da rede) endereçado ao IP "255.255.255.255". O servidor DHCP recebe esse pacote e responde com um pacote endereçado ao endereço IP "0.0.0.0", que também é transmitido para todas as estações. Apesar disso, apenas a estação que enviou a solicitação lerá o pacote, já que ele é endereçado ao endereço MAC solicitante; e quando uma estação recebe um pacote destinado a um endereço MAC diferente do seu, ela ignora a transmissão. Dentro do pacote enviado pelo servidor DHCP estão especificados o endereço IP, máscara de rede, o ***gateway*** e os servidores DNS que serão usados pela estação.

A-Z

Gateway
É uma máquina destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos. Exemplos de *gateway* podem ser os roteadores e *firewalls*

Em resumo, endereçamento dinâmico simplifica a administração de rede, já que o *software* se mantém informado dos endereços IP em vez de exigir um administrador para administrar a tarefa. Isso significa que um computador novo pode ser adicionado a uma rede sem a necessidade de atribuir-lhe manualmente um endereço IP.

4.6 Instalando serviços no servidor

As etapas de configuração e teste dos serviços DNS e DHCP de nosso servidor podem ser vistas nas apresentações e vídeos disponibilizados no ambiente virtual de ensino-aprendizagem:

SO2 - Configuração do servidor DNS
SO2 - Teste do servidor DNS

SO2 - Configuração do servidor DHCP
SO2 - Teste do servidor DHCP

DHCP no Linux: http://fgrweb.com.br/wp/?p=93

DNS em Windows: http://fgrweb.com.br/wp/?p=88

DNS Reverso em Windows: http://fgrweb.com.br/wp/?p=91

Resumo

Aprendemos nesta aula como manipular algumas das configurações de sistemas operacionais servidores. Vimos endereços IPs, como se compõem, sua estrutura, finalidade e características de transporte de dados. Estudamos que NAT é uma técnica que permite economizar endereços IP ao transmitir dados entre uma rede interna e a internet. Entendemos como funciona a estrutura DNS e suas características e responsabilidade no que tange à tradução de nomes para endereços IPs e de endereços IPs para nomes. Entendemos o funcionamento do protocolo DHCP. Vimos que esse protocolo é responsável por gerenciar a distribuição de números IPs entre computadores de uma rede local.

Atividades de aprendizagem

1. É possível acessar um *site* da internet pelo seu endereço IP?

2. Por quantos *bits* é constituído um IPv4? E um IPv6?

3. Que fatores levaram ao surgimento do IPv6?

4. Descreva o funcionamento de um servidor DNS em uma linha.

5. O que é uma *cache* DNS?

6. Descreva o funcionamento de um servidor DNS reverso em uma linha.

7. Qual a importância do serviço DHCP?

8. Como o NAT contribuiu para o aumento do tempo de uso do IPv4?

Poste suas respostas no ambiente virtual de ensino-aprendizagem (AVEA).

Aula 5 – Domínios, acesso, contas e senhas

Objetivo

A partir de um ambiente virtual, conceituar e criar domínios de contas de clientes, métodos de acesso e políticas de contas e senhas.

5.1 Conceitos de domínio

Um domínio do Windows 2000 ou 2003 é uma estrutura lógica que compartilha serviços e diretórios através de uma política de controle. No Windows 2000/2003, a base de dados do diretório é conhecida como uma parte ativa do *Active Directory*.

O *Active Directory* (AD) é um serviço de diretório nas redes Windows Server. O serviço de diretório é um conjunto de atributos sobre recursos e serviços existentes na rede, ou seja, é uma maneira de organizar e simplificar o acesso aos recursos da rede, centralizando seu gerenciamento. Além disso, o uso do AD aumenta a segurança, protege o banco de dados dos recursos da rede contra intrusos e controla o acesso dos usuários internos da rede. O *Active Directory* mantém dados diversos, tais como contas de usuários, impressoras, grupos, computadores, servidores, recursos de rede, etc. O AD é totalmente escalonável, aumentando conforme a nossa necessidade. Todo recurso da rede é representado como um objeto no AD e esses objetos possuem propriedades que são denominados atributos. A base de dados do AD é um arquivo chamado NTDS.dit, onde todos os recursos são armazenados.

Conheça mais sobre o *Active Directory* em:
http://blogs.technet.com/b/brzad/archive/2008/12/11/conceitos-florestas-rvore-e-dom-nios.aspx

http://technet.microsoft.com/pt-br/library/cc759279(WS.10).aspx

http://technet.microsoft.com/pt-br/library/cc668412.aspx

Um domínio é constituído por computadores configurados nos controladores de domínio (*Domain Controllers* ou DC). Os usuários podem utilizar o domínio a partir de qualquer máquina que possua autorização e usufruir dos recursos da rede para os quais o administrador do domínio lhes der permissões.

5.1.1 O que são árvores de domínio

As árvores de domínio são estruturas de hierarquia de um ou mais domínios. Uma árvore é criada quando criamos o nosso domínio, sendo o nome da nossa árvore o mesmo nome que demos ao domínio. Podemos criar mais de um do-

mínio para departamentos diferentes na empresa. Por exemplo, para a nossa escola poderíamos ter o domínio CEFETDIV, Administrativo, Professores e Ensino. Se a mesma gerência for responsável por administrar todos os domínios, seria interessante organizar hierarquicamente os domínios. Um subdomínio é um domínio que está abaixo de outro na hierarquia da árvore. Todos os domínios da árvore compartilham informações e recursos cujas funções são únicas.

Os domínios em uma árvore são unidos por relações de confiança transitiva. Uma relação de confiança transitiva significa que se o domínio A confia em B, e o domínio B confia em C, então A confia no C. Ou seja, um domínio pertencente a uma árvore estabelece relações de confiança com cada domínio da árvore, acessando os objetos e atributos de todos os domínios da árvore.

5.1.2 *Global catalog*

O catálogo global ou *global catalog* (GC) é uma função desempenhada apenas por um servidor controlador de domínio. Ele desempenha um papel vital no processo de *logon* dos usuários de uma rede. Ao fazer o *logon* em uma rede, uma das informações necessárias é saber os grupos aos quais um usuário pertence. Baseado nos grupos aos quais o usuário pertence é que os acessos e direitos a objetos são concedidos ou negados. Porém, um controlador de domínio só consegue identificar os grupos a que um usuário pertence dentro do seu próprio domínio. Apenas o GC consegue identificar se o usuário pertence a um grupo de um outro domínio, por exemplo, os grupos do tipo "universal".

Portanto, no processo de *logon*, o controlador de domínio precisa contatar um GC para identificar quais grupos universais, de outros domínios, esse usuário pertence. Podemos considerar o GC como um "atalho" nesse processo, pois, caso contrário, cada controlador de domínio teria que, ele próprio, contatar cada controlador na floresta independentemente para descobrir tais informações. Outro papel do GC é que, em ambientes de múltiplos domínios, ele possibilita que um usuário faça *logon* em um controlador de domínio ao qual a sua conta não pertença. É o GC que possibilita que esse controlador "descubra" o domínio do usuário e permita o *logon*.

5.1.3 O que é uma floresta de domínio

Uma floresta é um grupo de uma ou mais árvores. A floresta fornece recursos de segurança, convenções, confianças e *global catalog*. Criar uma floresta é a maneira de organizar as árvores e manter os esquemas separados.

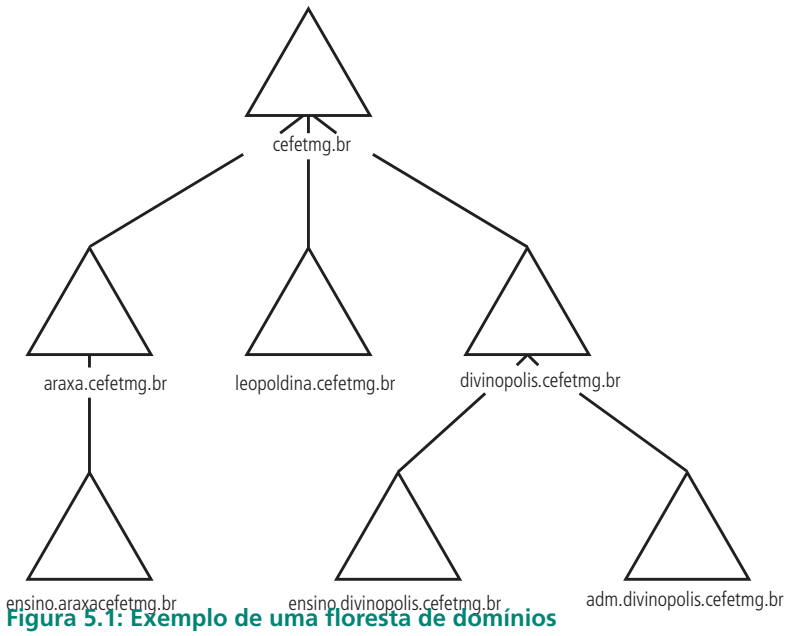


Figura 5.1: Exemplo de uma floresta de domínios
Fonte: Elaborada pelos autores

Como visto na Figura 5.1, uma floresta é uma ou mais hierarquias de árvore contíguas de domínio que formam uma determinada empresa. Algumas organizações podem ter vários domínios raiz, como por exemplo: araxa.cefetmg.br, leopoldina.cefetmg.br e divinopolis.cefetmg.br. Mas a organização propriamente é uma única entidade (como o caso do cefetmg.br). Em tais casos, essas várias árvores de domínio podem formar um espaço de nomes (*namespace*) não contíguo – que não é submetido às mesmas políticas de controle – e que pode ser chamado de floresta.

Logicamente, isso também significa que uma organização que tem somente um único domínio na sua árvore de domínio também é considerada uma floresta.

A Figura 5.1 mostra um exemplo (fictício) de uma árvore de domínios. Note que araxa.cefetmg.br e divinopolis.cefetmg.br são dois nós pais e também árvores da respectiva floresta cefetmg.br. Nesse contexto, ensino.divinopolis.cefetmg.br e adm.divinopolis.cefetmg.br são os domínios filhos da árvore divinopolis.cefetmg.br.

O proprietário do domínio gerencia os controladores de domínio e administra os serviços. Todos os proprietários de domínio, exceto o raiz, são irmãos, independentemente de sua posição no domínio; o proprietário de um domínio pai que não seja o raiz não possui controles administrativos padrões sobre o domínio filho.

5.1.4 Unidades organizacionais (OU)

As Unidades Organizacionais ou *Organizational Unit* (OU) são maneiras mais fáceis de delegar tarefas administrativas. Distribuindo os objetos para as OUs, podemos ter o controle de administração em vários níveis, permitindo que os objetos sejam reunidos e administrados centralmente na OU. Cada domínio pode implementar sua própria hierarquia de OU.

5.2 Contas de usuários

Usuários que desejam acesso aos recursos dos computadores em domínios (pastas compartilhadas, impressoras compartilhadas, etc.) devem estar inseridos no AD. O cadastro desses usuários é feito através da criação de uma conta de usuário e uma senha. Assim que se cadastra um usuário, várias informações como seção, nome completo, endereço, telefone, etc., podem ser cadastradas. As contas de usuários são representas como objetos do AD, o qual contém diversas informações sobre o usuário. É importante salientar que a conta precisa ser criada apenas uma vez, em um dos controladores de domínio. Tendo sido criada, a conta será replicada aos demais DCs do domínio.

A prática de criação de usuários e grupos locais, nos servidores e nas estações de trabalho, não é recomendada. Quando se trabalha em um domínio, o ideal é que contas de usuários e grupos sejam criadas somente no domínio, isto é, nos DCs.

Algumas recomendações e observações sobre contas de usuários:

- Dois ou mais usuários não devem acessar a mesma conta. Cada conta representa seu respectivo usuário. Todas as ações realizadas pelo usuário estão associadas à sua conta. O Windows 2003 Server tem um sistema de auditoria de segurança que registra, ao comando do Administrador, quais ações devem ser armazenadas no *log* de auditoria. Por exemplo, o administrador pode definir que as ações de tentativa de alteração de um determinado arquivo sejam registradas pela auditoria local. Se dois ou mais usuários estão compartilhando a mesma conta, fica difícil identificar qual usuário estava logado no momento.

- Com base nas contas de usuários e grupos, o administrador concede ou não permissões de acesso aos recursos da rede. Nesse sentido, o administrador pode restringir o acesso a pastas e arquivos compartilhados na rede, definindo quais usuários podem ter acesso e qual o nível de acesso de cada usuário – leitura, leitura e alteração, exclusão, e assim por diante. Mais um bom motivo para que cada usuário tenha a sua própria conta e senha.

A seguir são feitas algumas recomendações para a criação de nomes de *logon* para os usuários:

- Os nomes devem ter no máximo 20 caracteres.
- Os nomes de usuários devem ser únicos dentro do domínio.
- Os caracteres: " / \ : ; [ ] | = , + * ? < >, não podem ser utilizados.

Sempre que se cadastrar um usuário, deve-se também ser cadastrada uma senha para ele. O administrador pode especificar um número mínimo de caracteres aceito para a senha. O número máximo de caracteres da senha é 128.

No Windows 2003, existem três tipos de contas:

1. **de usuários**, que contém toda a informação referente a um usuário do domínio, tais como:

    - nome;
    - *password* (senha);
    - grupos a que pertence no domínio,
    - localização do perfil do usuário;
    - localização da pasta Meus Documentos.

2. **de computadores**, que guarda a informação necessária para identificar de forma única um computador do domínio;

3. **de grupos de usuários**, que é uma coleção de contas de usuários. Permissões e direitos de usuário devem ser prioritariamente associados a grupos de usuários, com todas as vantagens que daí advém. Isso permite facilitar a administração e a atribuição de permissões para acesso a recursos, tais como: pastas compartilhadas, impressoras remotas, serviços diversos, etc.

Devemos observar quanto a grupo de usuários, que:

- Grupos são uma coleção de contas de usuários.

- Os membros de um grupo herdam as permissões atribuídas ao grupo.

- Os usuários podem ser membros de vários grupos.

- Grupos podem ser membros de outros grupos.

- Contas de computadores podem ser membros de um grupo (novidade do Windows 2003 Server).

Existem dois tipos de grupos de usuários:

Grupos de distribuição

- não podem ser usados na atribuição de permissões de acessos e controle sobre recursos;

- têm funções não relacionadas com segurança (atribuição de permissões);

- são usados como listas de distribuição de *e-mail*.

Grupos de segurança

- são utilizados para atribuir permissões de acesso aos recursos da rede;

- em segunda instância, também podem ser usados como listas de distribuição de *e-mail*.

As contas são referências lógicas a objetos físicos, tais como usuários e computadores do AD. As contas de usuário também podem ser usadas como contas de serviço associado a alguns aplicativos. Essas contas, bem como seus respectivos usuários, são chamadas de objetos de segurança e estes objetos pertencem ao diretório em que os identificadores de segurança (SID) são atribuídos automaticamente e que podem ser usados para acessar recursos de domínio.

Nesse sentido, as contas de usuário e de computadores são usadas com as seguintes finalidades:

- autenticar a entrada de um usuário ou de computador no domínio (através do AD);

- autorizar ou negar acesso a recursos de domínio com base nas respectivas permissões previamente atribuídas a eles;

- auditar ações executadas usando a conta de usuário ou de computador com a finalidade de monitorar suas ações;

- administrar outros objetos de segurança.

O recipiente **Usuários**, localizado em **Usuários e Computadores** do AD, dispõem de três contas de usuário internas, criadas automaticamente quando da criação do domínio e são denominadas de: Administrador, Convidado e *HelpAssistant*.

Cada conta interna possui uma estrutura de direitos e permissões dentro do AD. A conta Administrador, por exemplo, possui direitos e permissões mais abrangentes que as outras contas.

- **Conta Administrador:** esta conta possui todo o controle do domínio. Ela detém a atribuição de conceder direitos e permissões de acesso a usuários. Pelo alto poder de controle sobre o sistema, esta conta necessita de elevado grau de segurança na sua senha, pois quem a tiver passa a ter o domínio sobre tudo e todos.

- **Conta Convidado:** esta conta tem sua utilização fundamentada na necessidade esporádica de que um usuário não cadastrado faça *logon* em um domínio. A conta Convidado é desabilitada por padrão e recomenda-se que permaneça assim.

- **Conta *HelpAssistant:*** Consiste em um tipo de conta limitada e específica para acesso como assistência remota ao computador e será excluída automaticamente se nenhuma solicitação da assistência remota estiver pendente.

5.2.1 Proteção das contas

Uma forma de proteger essas contas internas consiste em renomeá-las ou desabilitá-las. Por manter seus identificadores de segurança (SIDs), as contas de usuários renomeadas mantêm todas as outras propriedades e todas as permissões e direitos de usuário atribuídos a elas. Em outras palavras, a criação de uma conta de usuário individual para cada usuário que participa da rede usando Usuários e Computadores do *Active Directory* é uma boa prática de segurança.

Como visto anteriormente, cada conta de usuário pode ser inserida a um grupo para controle dos direitos e permissões relativos à conta. Além de melhor organizar, o uso de contas e grupos associados à rede garante que os

usuários que fizerem *logon* em uma rede possam ser identificados e acessem somente os recursos permitidos.

Senhas de difícil identificação são indispensáveis contra ataques ao domínio. Esse tipo de senha é de alto nível e, assim, reduz o risco de adivinhações inteligentes e ataques com dicionário de senhas.

Uma boa política de bloqueio de conta reduz qualquer possibilidade de ataques por meio de tentativas de bombardeio de *logons*.

5.2.2 Opções de conta

Várias opções relacionadas à segurança dos *logons* são disponibilizadas. A seguir podemos verificar algumas opções para configurar senhas e informações específicas de segurança para as contas de usuários:

- **O usuário deve alterar a senha no próximo *logon***
  Esta opção força o usuário a alterar a senha no próximo *logon*.

- **O usuário não pode alterar a senha**
  Esta opção impede que os usuários alterem suas senhas.

- **A senha nunca expira**
  Esta opção impede que uma senha do usuário expire, ou seja, tenha um tempo máximo de vida. Não é recomendado o uso arbitrário dessa opção.

- **Armazenar senhas usando criptografia reversível**
  Simplifica a forma de armazenamento de senhas para permitir alguns serviços, tais como o *logon* em uma rede Windows através de uma plataforma Apple. Não é recomendável ativar.

- **Conta desabilitada**
  Impede o *logon* do usuário na respectiva conta.

- **O cartão inteligente é necessário para o *logon* interativo**
  Requer que um usuário possua um cartão inteligente, através de um leitor específico, utilizando um número de identificação pessoal (PIN) válido para fazer *logon* na rede interativamente.

- **A conta é confiável para delegação**
  Permite que um serviço que está sendo executado na conta atual execute operações em nome de outras contas de usuário na rede.

- **A conta é sensível à segurança e não pode ser delegada**
  Permite o controle sobre uma conta de usuário, como uma conta de convidado ou temporária. Esta opção pode ser usada se esta conta não puder ser atribuída para delegação por outra conta.

- **Use os tipos de criptografia DES para esta conta**
  Determina suporte para o padrão de criptografia de dados do tipo DES que fornece suporte a vários níveis de criptografia, inclusive os tipos de MPPE e IPSecs.

- **Contas InetOrgPerson**
  As contas InetOrgPerson são usadas em vários serviços de diretório LDAP e X.500 não Microsoft, existem para representar pessoas em uma organização e têm o objetivo de tornar mais eficientes as migrações de outros diretórios LDAP para o *Active Directory*.

Saiba mais sobre criptografia de dados em:
http://technet.microsoft.com/pt-br/library/cc785633%28WS.10%29.aspx>

5.3 Contas de computador

Uma conta de computador é criada quando se insere um computador em um domínio. Estações de trabalho que rodam Windows 2000 ou Windows XP e que fazem parte do domínio devem ter uma conta de computador no AD. Essas contas podem ser alteradas, desabilitadas e excluídas pelo AD. As contas de computador são únicas, ou seja: não se pode ter uma mesma conta duplicada nos limites do AD. Sistemas do tipo Windows 9x não podem ter contas de computador atribuídas a eles, por não terem recursos de segurança avançados.

5.4 Métodos de acesso

O processo pelo qual usuários, grupos e computadores são verificados na rede é denominado de Controle de Acesso. Entende-se como Controle de Acesso: as permissões, os direitos do usuário e a auditoria de objetos.

- Permissões

  A um usuário ou grupo de usuários são dadas as permissões que definem o seu respectivo tipo de acesso e essas permissões são aplicadas a quaisquer objetos como arquivos, objetos do AD ou objetos do Registro.

  Pode-se conceder permissões a qualquer usuário, grupo ou computador. Atribuir permissões a grupos em vez de usuários é sempre uma boa ideia,

pois facilita o gerenciamento.

Configurar permissões é um processo pelo qual especificamos o nível de acesso para grupos e usuários. Isso pode ser feito para que impressoras possam, por exemplo, ter seu uso distinto às classes de usuários: alguns podem imprimir, outros podem deter controle total, etc.

- Propriedade de objetos

  Por padrão, objetos só existem mediante a sua ligação a um proprietário, que é o seu criador. O proprietário, por ser o criador, sempre poderá alterar as permissões de seus objetos criados.

- Herança de permissões

  O recurso de herança faz com que os objetos contidos em um recipiente herdem automaticamente as permissões desse recipiente, facilitando a disseminação para outros recipientes correlacionados.

- Direitos do usuário

  São os direitos do usuário, privilégios e direitos de *logon* específicos concedidos a usuários e grupos.

- Auditoria de objetos

  Auditar o acesso dos usuários a objetos é um procedimento de segurança que relata quando, como e por qual usuário o acesso ao objeto foi efetuado.

Resumo

Nesta aula aprendemos o que são domínios e como criá-los. Aprendemos também administração de acessos ao sistema e respectivas permissões. Entendemos como criar contas de usuários e como mantê-las seguras e dimensionadas, e conhecemos a segurança das senhas de acesso das contas.

Atividades de aprendizagem

1. O que é um domínio em um ambiente Microsoft?

2. Onde ficam armazenadas as informações do domínio?

3. É possível que um usuário cadastrado em um domínio faça *logon* em outro? Como?

4. É possível ter dois usuários com o mesmo nome de *login* em um domínio?

5. O que são métodos de acesso?

Poste suas respostas no ambiente virtual de ensino-aprendizagem (AVEA).

Aula 6 – Diretórios, arquivos e compartilhamentos

Objetivo

Conhecer conceitos de estrutura de diretórios, arquivos e segurança bem como compartilhamento de recursos e arquivos.

6.1 Conceitos

Os dados se tornaram um dos mais importantes elementos do "ativo circulante" das empresas, hoje em dia. Com as demandas de dados dos sistemas de comércio eletrônico, das aplicações com banco de dados e conteúdos multimídias em franco crescimento, tem havido uma explosão na quantidade de armazenamento nas empresas. Esse crescimento tem levado ao aumento da complexidade na gestão de recursos de armazenamento. Essa complexidade vem se tornando um desafio cada vez maior para as empresas de médio e pequeno porte que se submeteram a um crescimento. Agora, mais do que nunca, há uma exigência de maior sofisticação de recursos de armazenamento de provisionamento e gerenciamento das informações produzidas.

Os administradores empresariais, com vistas ao crescimento das empresas, vêm cobrando de seus gerentes de Tecnologia e Informação, soluções e planejamentos futuros que tenham maior eficiência e menores custos operacionais. Nesse sentido, o gerenciamento de armazenamento eficaz de informação tornou-se a chave para enfrentar esses desafios.

6.2 Grupos de trabalho

Nas aulas anteriores foi visto o compartilhamento de informações em uma rede cliente/servidor. Porém, existe também outra forma de compartilhamento de recursos chamada de Grupo de Trabalho ou *Workgroup*, que é utilizada quando optamos por administrar as máquinas individualmente (ponto a ponto). Dessa forma, para um usuário usufruir dos recursos (arquivos, impressoras, etc.), ele deverá possuir uma conta local em cada máquina associada ao recurso. Nesse caso, não há uma administração central dos acessos e da utilização dos recursos, gerando problemas na segurança e administração. Portanto, esse tipo de configuração é recomendado apenas para uma

rede com poucas máquinas, em que o fator da segurança e complexidade de gerenciamento não tem tanta importância. A utilização de grupos de trabalho não requer a instalação de sistemas operacionais servidores, pois é uma rede descentralizada.

6.3 Gestão de armazenamento

Um administrador de sistemas encarregado do gerenciamento de armazenamento enfrenta, hoje em dia, uma infinidade de desafios. Devido ao rápido crescimento do comércio eletrônico, os requisitos necessários ao seu funcionamento vêm crescendo a uma taxa entre 60-100% por ano.

O armazenamento de dados necessita de grande organização para ser cumprido. Os dados armazenados devem estar disponíveis de forma ininterrupta e as informações devem ser protegidas de uma variedade de riscos, tais como falhas de *hardware*, vulnerabilidades de segurança e desastres naturais.

Há cinco aspectos-chave nas soluções de armazenamento que devem ser tratadas em qualquer solução de gestão para atender às necessidades de empresários e administradores de sistemas:

- Escalabilidade;
- tolerância a falhas;
- proteção de dados;
- gerenciamento;
- rentabilidade.

Esta seção irá explorar cada uma dessas necessidades em detalhes.

6.3.1 Escalabilidade

Na gestão de armazenamento, a escalabilidade indica a aptidão do sistema em manipular uma porção crescente de trabalho, ou seja, se refere à habilidade em suportar um aumento da capacidade total de armazenamento quando novos recursos são requeridos.

Um sistema cujo desempenho aumenta proporcionalmente à capacidade acrescida, é chamado escalável. A escalabilidade existe de duas formas:

- Vertical (*scale up*) – adicionar recursos ao sistema (mais memória ou um disco rígido maior).

- Horizontal (*scale out*) – adicionar mais nós (computadores) ao sistema.

6.3.2 Tolerância a falhas

Em muitas empresas, o acesso ininterrupto de serviços a dados deve ser mantido 24 horas por dia e 365 dias por ano. Para algumas organizações com sistemas distribuídos, a replicação de dados para localizações ao redor do mundo é também uma obrigação que torna a manutenção do sistema prioritário. Esses requisitos criam uma necessidade de tolerância a falhas em componentes de *hardware* relacionados ao armazenamento, que pode ser resolvido por servidores redundantes, espelhando dispositivos de armazenamento e/ou subsistemas RAID.

Clustering ou "Clusterização" também pode fornecer um caminho para aplicações de missão crítica no sentido de manter os servidores sempre *on-line*. Os *clusters* são dois ou mais computadores que operam em conjunto um sistema e são gerenciados como sendo apenas um. Quando os componentes de *hardware* falham em uma solução de *cluster*, usuários podem ser redirecionados para outro computador com uma perda mínima ou nenhuma de serviços e dados.

6.3.3 Proteção de dados

Os administradores de sistema devem proteger os dados não apenas de falha de *hardware*, mas também da corrupção, de erros de usuários e de desastres diversos. A forma mais comum de proteção de dados é através de *backups* regulares. Em um ambiente distribuído, a responsabilidade de fazer *backup* dos dados é entregue aos administradores do sistema.

Embora o gerenciamento de *backups* possa ser simplificado, usando um servidor de *backup* centralizado, o tempo necessário para executar *backups* pode entrar em conflito com o objetivo de manter o sistema permanentemente ativo e os dados sendo atualizados a todo instante. Por exemplo, alguns softwares de *backup* ignoram os arquivos abertos em memória para evitar a corrupção de dados. Para evitar esse problema, os usuários devem fechar suas aplicações para que o *backup* completo seja concluído com êxito.

Portanto, *backups* devem ser agendados em curtos períodos durante a semana, de preferência nos momentos quando os usuários não estão tentando acessar seus arquivos através da rede. Normalmente esses procedimentos podem ser executados apenas à noite e nos finais de semana. Infelizmente, conforme as organizações produzem cada vez mais dados importantes, a frequência dos *backups* pode não ser suficiente para cumprir a meta de manter as informações críticas da empresa protegidas.

6.3.4 Gerenciamento

Os administradores de TI são os responsáveis pela gestão dos servidores, por manter a tolerância a falhas, por garantir o desempenho e alta disponibilidade dos serviços oferecidos. Administradores em organizações que tenham implementado redes de armazenamento podem também ser responsáveis pela gestão da disponibilidade dos dispositivos de armazenamento.

Além disso, os administradores são responsáveis pelo gerenciamento dos serviços tais como *backup*, mineração de dados e diversos testes diários. Como muitos aplicativos não estão preparados para as tarefa de armazenamentos, gerenciamento de dados, *backup* e transporte, o processo de administração pode ser complexo e ineficiente. Outro ponto de complexidade se encontra no crescente compartilhamento de dados entre os usuários.

6.4 GPO

Para atender a vários requisitos mencionados nos tópicos anteriores, a Microsoft criou o que se chama de GPO – *Group Policy Objects* ou Objetos para Gerenciamento de Grupo. E para isso disponibilizou um editor para gerenciamento dos grupos, como poder ser observado na Figura 6.1 a seguir.

Quem trabalha ou já trabalhou com a administração de redes tem ideia da complexidade de se gerenciar um parque de dezenas, centenas e até milhares de computadores em rede. Nesse contexto é possível mensurar algumas questões:

- Como é possível gerenciar tantas estações de trabalho?
- Como garantir que todas as estações de trabalho possuam as mesmas configurações?
- Como definir que somente usuários autorizados possam realizar tarefas administrativas nas estações de trabalho?

- Como aplicar configurações de segurança em todas as estações de trabalho?

- Como instalar e remover o mesmo *software* em tantas estações de trabalho?

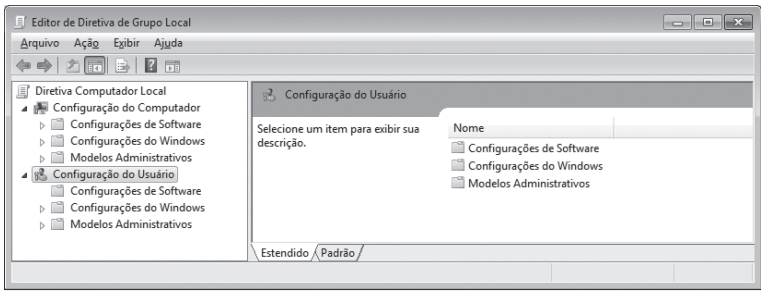


Figura 6.1: Editor de Diretivas de Grupo Local
Fonte: Windows 2003 Server

Em função de procurar atender a essas necessidades, a Microsoft efetuou a sua primeira tentativa nesse sentido lançando o GPO juntamente com o Windows NT. Esse recurso permitia que os administradores aplicassem uma série de configurações nas estações de trabalho, logo após os usuários efetuarem o *logon* no domínio. Essas configurações eram aplicadas no registro das estações de trabalho. Porém, era um recurso bem simples e possuía muitas limitações.

Com esse recurso, os administradores do sistema podem fazer uma série de tarefas interessantes, como por exemplo:

- Gerenciar centralizadamente configurações definidas no registro do Windows: as Diretivas de Grupo criam arquivos que possuem as configurações do Registro do Windows. Esses arquivos são carregados e aplicados nas estações de trabalho dos usuários, na parte da máquina local ou de usuário do banco de dados do Registro. As configurações de perfil de usuário específicas a um usuário que faz *logon* em uma determinada estação de trabalho ou servidor são gravadas no Registro em HKEY_CURRENT_USER (HKCU) e as configurações específicas do computador são gravadas em HKEY_LOCAL_MACHINE (HKLM).

- Atribuir *scripts*: através das GPOs, você pode também distribuir *scripts* para serem executados no *logon*, inicialização, *logoff* e desligamento dos computadores.

- Fazer o redirecionamento de pastas: é possível também configurar as GPOs de tal forma que algumas pastas, como por exemplo, Meus Documentos e Minhas Imagens, sejam redirecionadas automaticamente para

uma pasta compartilhada em um servidor. Com isso, os dados dos usuários estarão disponíveis no servidor e poderão ser acessados a partir de qualquer estação de trabalho da rede na qual o usuário faça o *logon*. Outra vantagem da utilização do redirecionamento de pastas é que você pode criar uma política de *backup* centralizada.

- Fazer o gerenciamento centralizado de aplicativos: outro recurso muito interessante das GPOs é a distribuição de *softwares*. Você pode fazer a distribuição dos *softwares* de forma automática nas estações de trabalho.

- Aplicar configurações de segurança: é possível também definir políticas de senha e políticas de bloqueio de conta. Por exemplo, você pode definir que a senha das contas de usuário devem ser trocadas a cada trinta dias e que o tamanho da senha deve ser de nove caracteres no mínimo. É possível ainda definir que se o usuário errar sua senha por três vezes em um período de trinta minutos, sua conta será bloqueada. Tudo isso de forma centralizada.

Por exemplo, se o administrador criou uma diretiva de grupo com configurações na sessão Configurações do Usuário (Figura 6.1), que se aplicam para a usuária Andréa, essas configurações serão aplicadas para a usuária Andréa todas as vezes que ela fizer o *logon* no domínio, independentemente da estação de trabalho que ela utilizar. Agora imagine que o administrador criou uma outra diretiva de grupo com configurações na seção Configurações do Computador, as quais são aplicadas para o grupo de computadores Contabilidade. Isso significa que essas configurações serão aplicadas em todos os computadores do grupo Contabilidade, independentemente do usuário que efetuar *logon*.

As diretivas também possuem uma série de opções interessantes que podem ser aplicadas nas estações de trabalho. As configurações definidas nessas diretivas são aplicadas apenas no computador onde elas forem configuradas. Algumas configurações não estão disponíveis nas diretivas locais, como por exemplo, redirecionamento de pastas e distribuição de *software*.

A-Z

Template
É um modelo de documento sem conteúdo, com apenas indicações e instruções sobre os tipos de conteúdo a serem preenchidos.

As GPOs são baseadas em **templates** que possuem uma lista de opções configuráveis de forma amigável.

A maioria dos itens de uma GPO tem três diferentes opções:

- *Enable*: especifica que aquele item será ativado.
- *Disable*: especifica que aquele item será desativado.
- *Not Configured*: deixa a opção neutra, nem ativa e nem desativa o item, ou seja, fica como está agora. Esta é a configuração padrão.

Vamos supor que se queira desabilitar o *prompt* de comandos (*command prompt*) dos *desktops* da rede. Para isso existe um item chamado *Disable the command prompt*; a configuração *default* para esse item é *Not Configured*.

Se configurarmos como *Enable*, o *command prompt* será desativado e se configurarmos como *Disable*, será ativado explicitamente.

Parece confuso o *Enable* desativar a opção, mas repare que a opção é "Desabilitar o *prompt* de comando", o *Enable* neste caso está ativando a opção de "Desabilitar o *prompt* de comando".

As configurações das GPOs podem ser aplicadas em dois tipos de objetos do *Active Directory*: Usuários e Computadores, desde que estejam em uma OU – *Organizational Units* ou Unidades Organizacionais. Se houver algum conflito entre as configurações dos computadores e dos usuários, as configurações dos usuários vão prevalecer.

No ambiente virtual de ensino-aprendizagem abras as apresentações e vídeos abaixo e aprenda a adicionar e configurar usuários no domínio, a configurar o compartilhamento de arquivos e pastas e a criar perfis móveis de usuário.

SO2 - Adicionando usuários e setando permissões

SO2 - Criação de perfis móveis

SO2 - Compartilhando pastas e configurando permissões de acesso

Links de referência:
http://technet.microsoft.com/pt-br/library/cc668545.aspx

http://www.fabianosantana.com.br/windows-server-2003/

Resumo

Nesta aula estudamos os diversos repositórios de dados no sistema operacional, tais como diretórios e arquivos. Observamos que o acesso a esses repositórios podem ser efetuados por grupos de usuários com finalidades comuns e que também são conhecidos como grupos de trabalho com suas respectivas permissões. Estudamos gestão de armazenamentos, que consiste em observar num sistema a sua escalabilidade, a sua capacidade em poder se ampliar; a sua tolerância a falhas, ou seja: capacidade de ter redundâncias em caso de possibilidade de paralisação do sistema; proteção de dados, ou seja: capacidade de manter os dados íntegros e longe de mãos indesejáveis.

Atividades de aprendizagem

1. Por que os dados são tão importantes para as empresas hoje em dia?

2. Diferencie um compartilhamento de uma rede cliente/servidor de um compartilhamento baseado em grupos de trabalho. Cite vantagens e desvantagens.

3. Quais são os fatores-chave da Gestão de Armazenamento?

4. Qual a vantagem de um sistema possuir tolerância a falhas?

5. O que são GPOs e qual a sua aplicação?

Poste suas respostas no ambiente virtual de ensino-aprendizagem (AVEA).

Aula 7 – Administração de SO

Objetivo

Conhecer os princípios de administração de redes.

7.1 Introdução

A administração de uma rede exige o controle de atividades como a monitoração dos recursos materiais e lógicos fisicamente distribuídos pela rede. Dessa forma, procura-se assegurar a confiabilidade dos dados, tempos de resposta aceitáveis e a segurança das informações.

O modelo clássico de gerenciamento pode ser descrito em três etapas:

- Coleta de dados: consiste na monitoração sobre os recursos gerenciados.
- Diagnóstico: consiste no tratamento e na análise dos dados coletados. Tem o intuito de determinar a causa do problema no recurso gerenciado.
- Ação ou controle: consiste na resolução do problema diagnosticado.

É objetivo da administração de redes viabilizar o funcionamento delas, realizando a instalação, configuração e manutenção dos dispositivos (*hardware*) e serviços (*software*) que a compõem. A operação de uma rede envolve uma série de habilidades básicas que poderão ser vistas a seguir.

7.2 Manutenção de computadores

Situação proposta: precisa-se passar aquele documento urgente, daqui a cinco minutos, mas agora o *mouse* não funciona. Na empresa todos os *mouses* estão ocupados, o que fazer? E se o processador queimou? E se for necessário instalar mais memória? E se for uma rede de 50 computadores? Então os conhecimentos básicos de manutenção de computadores são extremamente necessários!

7.2.1 Conhecer o sistema operacional

Alguns conhecimentos sobre o sistema operacional são imprescindíveis: particionamento do disco, formatação, instalação do sistema operacional, instalação de programas aplicativos, instalação de novos periféricos e dispositivos, configurações em geral.

7.2.2 Conhecer os protocolos

É necessário saber para que servem os protocolos TCP, IP, FTP, HTTP, etc., como utilizá-los e como configurá-los.

7.2.3 Conhecer o funcionamento básico de um servidor

Para que se possa fazer a manutenção de computadores é necessário saber como configurar contas de usuários, impressoras, como otimizar o trabalho e o que fazer em diversas situações do cotidiano.

7.2.4 Conhecer política de segurança e missão crítica

Um sistema bancário é um típico ambiente crítico. Nesse caso, para a manutenção dos seus computadores é necessário saber como verificar vulnerabilidades, senhas, vírus, *hacker*, criptografia, registro e política de segurança.

7.2.5 Preparar-se e especializar-se na resolução de problemas

Para que o profissional se prepare e se especialize na resolução de problemas, é necessário que ele tenha conhecimento do projeto lógico e físico da rede a ser criada ou dar manutenção; ele deve também ter ciência sobre a configuração do servidor e de cada máquina da rede.

Para isso, o profissional deve ter alguns requisitos básicos: ser organizado; conhecer o espaço físico dos HDs de cada máquina, conhecer a quantidade de memória RAM, conhecer o *setup*, saber sobre as placas de vídeo, de som, de rede. Procurar padronizar o ambiente de rede estabelecendo um mesmo esquema de nomeação das máquinas. Procurar estar informado sobre o fluxo de informações transitadas na rede; onde estão sendo armazenadas; de onde vêm e para onde vão, etc.

7.2.6 Atualizar os conhecimentos

Em informática, as atualizações e criações de novas tecnologias são muito frequentes. Portanto, faz-se necessária uma maior dedicação aos estudos de maneira a se manter atualizado com novas versões, novos programas e soluções.

7.2.7 Aprimorar a comunicação no ambiente de trabalho considerando a ética profissional

Este item é muito importante. Ignorá-lo pode comprometer todo o trabalho anteriormente relacionado já que é a base de inter-relação entre os membros. Se os membros da equipe não respeitam as normas, os próprios colegas e a hierarquia, nem os fornecedores, todo o trabalho poderá ruir.

7.3 Requisitos e características de uma rede

A criação de uma rede exige ampla pesquisa para coleta de informações relevantes. O custo de uma rede é a soma dos custos das estações (terminais, *laptops*, *tablets*, etc.), acrescentada aos custos de cabeamento e conexão, mais o custo do meio de comunicação e da mão de obra técnica.

1. As redes devem ser montadas de modo a ser padronizadas e modularizadas, facilitando assim a implantação de novos terminais quando de sua manutenção.

2. As redes precisam ser tolerantes a falhas de manutenção.

3. As redes devem permitir fácil modificação e expansão.

4. As redes devem atualizar todo o registro do projeto físico e lógico.

5. As redes devem proporcionar a realização de *backups* automáticos.

6. A segurança física e lógica das redes devem ser mantidas e revisadas periodicamente.

As ameaças à segurança física estão relacionadas a aterramentos, desabamentos, enchentes, descargas atmosféricas, invasões, entre outros.

As ameaças à segurança lógica estão relacionadas ao acesso de usuários, senhas, criptografias, *softwares anti-spywares*, antivírus, *worms*, etc.

Trataremos com mais detalhes esses dois itens de segurança na próxima aula. Apenas nos interessa saber que essas questões de segurança perpassam pela administração de redes de computadores e devemos ter em mente que elas são imprescindíveis.

7.3.1 Equipamentos para redes

A administração de uma rede de computadores envolve administrar, além da própria rede em si, computadores e demais elementos de *hardware* e *software*. Uma rede de computadores exige, além do cabeamento propriamente dito, dispositivos de *hardware* e *software* cuja função é controlar a comunicação entre os diversos componentes da rede.

Uma rede utiliza vários dispositivos (Figura 7.1) e cada um deles possui funções específicas. Como exemplo podemos citar: as placas de rede, *hubs*, *switches*, *bridges*, roteadores, etc., que têm por finalidade, interpretar os sinais oriundos da rede e encaminhá-los ao seu destino, obedecendo a um determinado padrão e protocolo.

Essa interação entre dispositivos permite o compartilhamento das informações entre todos os usuários da rede.

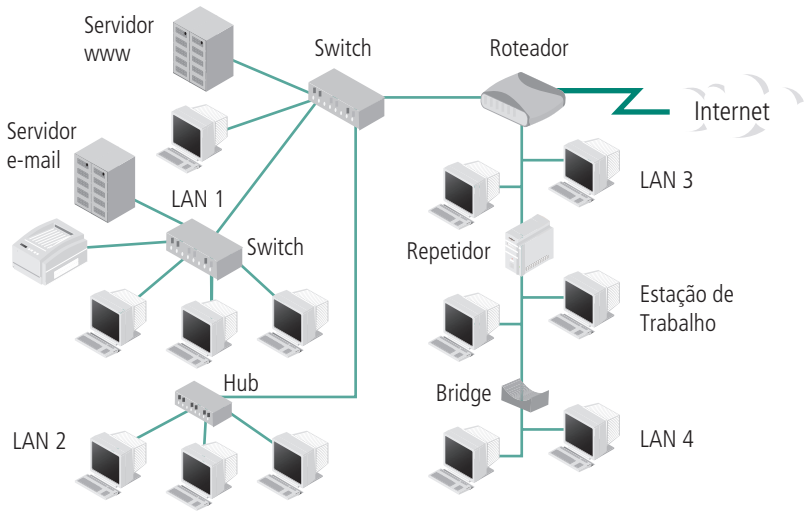


Figura 7.1: Exemplo de equipamentos em uma rede de computadores
Fonte: http://www.projetoderedes.com.br/tutoriais/tutorial_equipamentos_de_redes_01.php

7.3.2 Aplicativos para gestão de rede

As redes variam quanto ao aspecto de tamanho, topologia e tipo. Redes pequenas podem ser facilmente administradas e de forma até personalizada. Porém, quando nos deparamos com redes que possuem cinquenta,

quinhentos ou mesmo cinco mil computadores, a coisa muda de figura. Para nos ajudar a administrar redes de médio e grande porte, necessitamos de *softwares* para essa finalidade. Existem vários aplicativos no mercado que podem nos fornecer a visualização de funcionamento e operação de toda uma rede, tais como os pacotes trafegados, os *sites* visitados, os gargalos encontrados, acesso remoto de computadores, etc. Alguns *softwares* mais sofisticados chegam até a propor soluções para alguns dos problemas encontrados, como poder visto no Quadro 7.1 a seguir.

Monitoramento de rede: http://www.youtube.com/watch?v=lInGlwRH-4s&feature=related

Quadro 7.1: *Softwares* para gerenciamento de rede

Software	Descrição
 Ultr@ VNC	Programa que permite acessar outros computadores remotamente com diversos recursos.
 ShowMyPC	Programa que acessa computadores remotamente pela sua rede e controla *desktops* sem que se precise estar diante deles.
 TZ Connection Booster Wizard	Programa que permite configurar qualquer *modem* de ADSL, Cable, DSL e LAN para máxima *performance*.
 Advanced IP Scanner	Programa verificador de rede, é um *scanner* avançado de IP, ótimo para LANs.
GFiLANguard	Programa que realiza auditoria da segurança da sua rede
 NetSpeedMonitor	Programa de monitoramento em tempo real que permite acompanhar a velocidade de conexão.
WIRESHARK Wireshark	Programa analisador de protocolos de rede com recursos de captura de dados e informações detalhadas. Antigo Ethereal.

Fonte: Elaborado pelos autores

7.3.3 O Administrador de redes

Em informática, o administrador de redes é o responsável por projetar e/ou manter uma rede de computadores em funcionamento (mais comumente redes locais). Tem como atribuição principal o gerenciamento da rede local bem como dos recursos computacionais relacionados direta ou indiretamente a ela.

Esse profissional deve ter formação adequada, ser capacitado em Redes de Computadores e/ou ser uma pessoa com grande experiência na área de informática. É importante que esteja familiarizado com os equipamentos e *softwares* com os quais trabalha ou trabalhará, tendo como forma de comprovação de sua experiência e habilidades as certificações emitidas por empresas (normalmente grandes empresas) através de provas. São exemplos de certificados: MCP, MCSA e MCSE – certificações profissionais da Microsoft; Certificações Linux: LPIC-1, LPIC-2 e LPIC-3; Cisco-CCNA que é tida para muitos profissionais em início de carreira como requisito obrigatório no sentido de garantir uma vaga no mercado das grandes empresas.

7.4 Auditoria

De acordo com a Wikipedia, uma auditoria "é um exame cuidadoso e sistemático das atividades desenvolvidas em determinada empresa ou setor, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos" (AUDITORIA, 2012).

Na informática, compreende-se por auditoria de sistemas e redes o processo em que é averiguado o nível de segurança de uma infraestrutura ou sistema. O processo é baseado em metodologias de avaliação rigorosas em todos os níveis da infraestrutura. A diferença entre uma auditoria e um teste de intrusão é que na auditoria toda a infraestrutura é detalhadamente testada, enquanto no teste de intrusão apenas são testados os possíveis vetores de ataque. Além disso, a auditoria prevê um acesso às especificações da infraestrutura por parte dos auditores.

7.4.1 O porquê de uma auditoria

As razões para a realização de uma auditoria de sistemas e redes são muito variadas e variam de caso a caso. Vão desde o foro técnico e administrativo até ao foro comercial. Contudo, todas elas encontram-se no mesmo objetivo: garantir a segurança da sua informação e das suas infraestruturas. Mesmo no caso da existência de uma equipe responsável pela TI, a realização de

serviços desse tipo torna-se um complemento obrigatório, visto tratar-se de um serviço altamente especializado.

Algumas das razões mais comuns para a realização de uma auditoria de sistemas e redes são:

- identificar as ameaças à sua informação, de maneira a ser possível quantificar o seu nível de risco;
- estruturar as respectivas medidas necessárias para aniquilar essas ameaças.

Quando executada periodicamente, garante o mais alto nível de segurança possível. Garante a proteção da informação que sustenta os objetivos do negócio. Previne gastos resultantes de catástrofes informáticas relacionadas com segurança, valorizando assim o investimento feito na segurança informática.

7.4.2 Tipos de auditoria

A auditoria pode ser executada em âmbitos diferentes; nomeadamente, pode englobar testes de segurança física ou teste a redes telefónicas para além da convencional carga de testes à rede de computadores. Por isso o **CSIRT** disponibiliza vários tipos de Auditoria:

- Auditoria à rede informática e sistemas adjacentes.
- Auditoria à rede telefônica e sistemas adjacentes (fora do escopo desta aula).
- Auditoria à segurança física relacionada com a infraestrutura.
- Auditoria a políticas de segurança.

A-Z

CSIRT
Computer Security Incident Response Team
Também chamado de Grupo de Resposta a Incidentes de Segurança, é uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores.

Saiba mais um pouco sobre auditoria em http://www.cert.ipn.pt/pt/dw/panfletos/AuditoriaPT.pdf

7.5 Conexões simultâneas

O Windows 2000 Professional ou o Windows XP podem ser usados como servidores de redes, porém apenas dez PCs podem acessar os servidores simultaneamente. Acima disso, esses sistemas operacionais passam a recusar novas conexões, pois não foram desenvolvidos para funcionarem como servidor. O limite é de dez conexões simultâneas, não de dez clientes no total. Pode-se ter quantos clientes quiser, desde que no máximo dez usem o servidor de

Como instalar ferramentas administrativas em estações XP em http://www.youtube.com/watch?v=uuWSp1oOfwE

A limitação de conexões em SO Windows não servidores em http://www.hardware.com.br/faq/comunicacao/so-10-conexoes-simultaneas.html

http://social.technet.microsoft.com/Forums/pt-BR/winxppt/thread/a5c97f34-83ff-4d40-9f37-2847d954db2c

cada vez. Uma solução seria migrar para um sistema operacional servidor ou qualquer outro que não tenha essas limitações. No Windows XP Home o caso é ainda mais grave, pois são permitidas apenas cinco conexões simultâneas.

Uma opção de servidor de arquivos é a dupla Linux e Samba, pela sua simplicidade de configuração, pois oferecem os mesmos recursos de segurança dos Windows servidores.

Resumo

Estudamos nesta aula a administração de sistemas operacionais servidores. Verificamos todas as características e requisitos necessários para o funcionamento de uma rede bem como os respectivos equipamentos e *softwares* aplicados ao seu funcionamento e, principalmente, sua gestão. Estudamos auditoria de sistema e como utilizá-la para extrair informações que permitam verificar se as configurações e utilizações do sistema estão de acordo com as disposições planejadas e/ou estabelecidas previamente. Estudamos também os tipos de auditorias necessários e disponibilizados.

Atividades de aprendizagem

1. Qual a função de um administrador de redes?

2. Quais habilidades um bom administrador de redes deve possuir?

3. Cite três *softwares* utilizados para controle remoto de computadores.

4. Cite dois *softwares* para monitoramento de pacotes em uma rede.

5. Para que servem as auditorias em um SO?

6. Por que um SO comum, mesmo munido de *softwares* especiais, tem maiores limitações quando comparado a um SO servidor?

Poste suas respostas no ambiente virtual de ensino-aprendizagem (AVEA).

Aula 8 – Segurança em SO

Objetivo

Conhecer sobre segurança de sistemas operacionais servidores.

8.1 Introdução

Nos dias de hoje, com a expansão da internet e do comércio eletrônico, a segurança da informação se tornou um componente integrante e necessário aos negócios. A segurança é certamente um dos mais importantes itens para a sobrevivência de uma empresa, se não o mais importante. De acordo com (SYMANTEC, 2012), nos últimos anos vem ocorrendo um crescimento significativo no comportamento criminoso direcionado às corporações.

Por isso, é necessário que as empresas garantam a integridade de suas informações para que seus clientes e parceiros tenham acesso a seus produtos e serviços através de redes abertas como a internet. Esse processo oferece riscos de comprometimento de sua reputação e a qualidade de sua marca, caso essas informações sejam sabotadas. Nesse sentido, a necessidade de proteção da estrutura e da imagem da empresa demanda um gerenciamento efetivo da segurança de informações e de equipamentos.

Empresas são movidas pelo desejo de proteger suas informações lógicas e a estrutura física responsável por mantê-las. Há uma crescente aceitação da mobilidade e do trabalho remoto de funcionários. Porém, as LANs e WANs corporativas tradicionais não são suficientes para suportar o crescimento do número de funcionários **off-site**, dos acessos de colaboradores, fornecedores e clientes às empresas. Dessa forma, à medida que o acesso às redes corporativas aumenta, aumenta também a necessidade de proteção na transmissão de informações para os pontos locais e remotos.

A-Z

Off-site
Indica uma representação da empresa fora de sua área física, tal como um funcionário que trabalha em casa, ou dentro de outras empresas.

Indica uma representação da empresa fora de sua área física, tal como um funcionário que trabalha em casa, ou dentro de outras empresas.

Finalmente, devemos pensar em equalizar as necessidades de compartilhamento e segurança da informação com o investimento em equipamentos, *softwares* e infraestrutura.

8.2 Segurança física

Entende-se como estrutura física todo o arsenal de equipamentos com objetivos computacionais para prover acessos e produção de TI existentes em uma empresa.

A segurança física abrange os procedimentos adotados quanto aos aspectos relacionados a eventos que exijam contato físico com os equipamentos. Além disso, uma série de eventos pode colaborar para falhas no sistema físico computacional.

8.2.1 Falhas na alimentação elétrica

As falhas na alimentação elétrica ou a má qualidade das linhas de transmissão são um importante fator para a instabilidade dos sistemas. Essas falhas normalmente levam à indisponibilidade do sistema, podendo provocar ainda perdas de dados, inutilização de aplicações e avarias de *hardware*.

Vários tipos de dispositivos de prevenção podem ser instalados. Esses dispositivos englobam um parque de opções de *no-breaks* (Figura 8.1) e, dependendo do tamanho do sistema, até geradores movidos a combustíveis líquidos.

Os *no-breaks* são uma fonte de alimentação ininterrupta, também conhecida como UPS, do inglês *Uninterruptible Power Supply*; são munidos de baterias capazes de produzir energia elétrica durante algum tempo.

Figura 8.1: *No-break* – UPS
Fonte: http://www.guanabara.info/2009/02/estabilizador-nao-no-break-sim

Para manutenção do equipamento operacional durante falhas de alimentação prolongadas, é necessário prever ainda a instalação de geradores elétricos. Vide exemplo de gerador elétrico na Figura 8.2 a seguir.

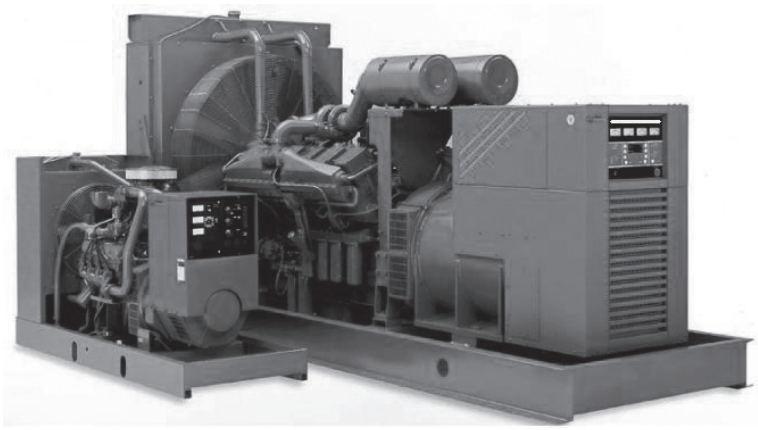


Figura 8.2: Gerador elétrico
Fonte: http://www.dee.feb.unesp.br/~ead/gerador.htm

É importante observar que falhas podem ter o caráter de falta ou de oscilações tensionais. Em ambos os casos existem equipamentos adequados ao provimento e normalização da alimentação elétrica.

8.2.2 Catástrofes naturais de diversos tipos

Falhas decorrentes de catástrofes do tipo: incêndios, inundações, tempestades, sismos, descargas atmosféricas (Figura 8.3), etc., são consideradas de alta periculosidade para todos os sistemas eletroeletrônicos.

Figura 8.3: Raios: descargas atmosféricas
Fonte: http://pion.sbfisica.org.br/pdc/index.php/por/Multimidia/Imagens/Eletromagnetismo/Raios!

Podemos evitar alguns desses eventos adotando medidas preventivas, tais como: estudos topológicos, geológicos e pluviométricos que indiquem melhor local físico para instalação dos prédios onde estarão os equipamentos

computacionais. Outros estudos devem girar em torno de instalações de para-raios nos prédios que acondicionam os equipamentos mais críticos, incluindo os servidores.

Além dessas medidas preventivas de caráter físico, podemos ainda minimizar as possíveis consequências destes tipos de eventos mantendo cópias de segurança (*backups*), atualizadas e armazenadas em local fisicamente distante do original. Essa distanciação entre os dados originais e os *backups* é necessária para os casos extremos de falhas, ataques, ou qualquer outro tipo de desastre que possa comprometer o espaço físico em que se encontram esses dados.

Outro ponto a considerar, seria a utilização de sistemas redundantes de segurança no sentido de implementar tolerância a falhas, mantendo assim, a disponibilidade permanente do sistema em situações extremas.

8.2.3 Eventos premeditados

Estes tipos de eventos são considerados ilícitos (Figura 8.4) e podem ser evitados de acordo com investimentos na segurança de acesso físico aos sistemas e à sua infraestrutura.

Figura 8.4: Invasão e/ou roubo de informação
Fonte: http://www.informaticaeducacional.com/downloads/index2.php

Além dos aspectos relacionados à destruição física dos equipamentos, sua desativação ou furto, é interessante abordar outras possibilidades de violação de segurança que o contato físico pode proporcionar. Um exemplo seria alterar a senha do administrador, apagar arquivos ou alterar a configuração do sistema ou dificultar acesso a informações confidenciais.

8.3 Segurança lógica

Segurança lógica abrange o aspecto de configuração dos servidores no que tange aos acessos e permissões de usuários e computadores no âmbito dos domínios da rede.

Os servidores, normalmente, vêm munidos de aplicativos de configuração que permitem aos administradores gerenciar a segurança de seu sistema. Essas configurações são classificadas como diretivas de segurança local, de senha, de conta, entre outras.

Gerenciando a Segurança Corporativa em www.nerdbb.com/download/file.php?id=3033

8.3.1 Diretivas de segurança local

As diretivas de segurança são componentes importantes do Windows que permitem definir o que os usuários podem ou não fazer no computador e na rede. São utilizadas para proteger os computadores em um ambiente corporativo ou doméstico. Antes de configurar as diretivas de segurança, faz-se necessário planejar as restrições, permissões e respectivos direitos sobre o sistema computacional.

Assim como as contas e grupos de usuários, as diretivas de segurança também podem ser criadas e aplicadas localmente (um único computador) ou no domínio (toda a rede).

Nesta aula, iremos focar apenas as políticas de senha e contas. Essas diretivas de conta afetam diretamente os parâmetros de segurança relacionados com as contas de usuários.

8.3.2 Diretivas de senha

As diretivas de senha, relacionadas no exemplo da Figura 8.5, podem ser utilizadas tanto para contas locais quanto para contas de domínio. Nas configurações locais de segurança, temos as seguintes opções para diretivas de senha:

- **A senha deve satisfazer a requisitos de complexidade;**
- **Aplicar histórico de senhas;**
- **Armazenar senhas usando criptografia reversível;**
- **Comprimento mínimo da senha;**
- **Tempo de vida máximo da senha;**
- **Tempo de vida mínimo da senha.**

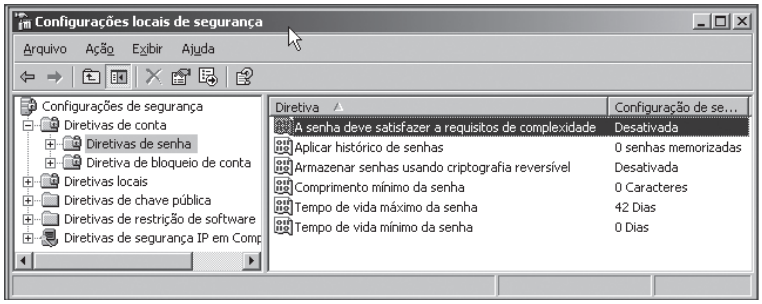


Figura 8.5: Janela das configurações locais de segurança em "Diretiva de senha"
Fonte: Windows 2003 Server

8.3.3 Diretivas de bloqueio de conta

Estas diretivas definem qual será o comportamento do Windows caso o usuário digite sua senha incorretamente por várias vezes.

O erro na digitação de senhas pode ou não ser causado por algum tipo de invasão da conta. O usuário pode se confundir, esquecer a senha, estar com o teclado desconfigurado, a tecla CAPS-LOCK estar ativa, etc.

Os seguintes parâmetros, conforme relacionados na Figura 8.6 estão disponíveis:

- Duração do bloqueio de conta;
- Limite do bloqueio de conta;
- Zerar contador de bloqueio de conta após tempo predeterminado.

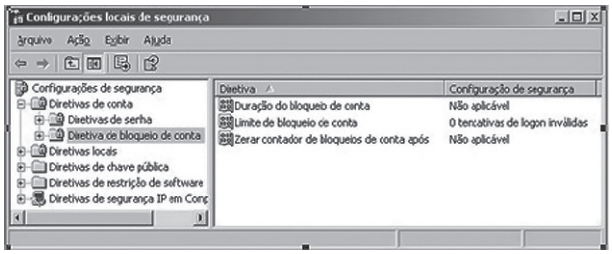


Figura 8.6: Janela das configurações locais de segurança em "Diretiva de bloqueio de conta"
Fonte: Windows 2003 Server

8.4 *Firewall*, serviços e antivírus

O termo *firewall* é uma analogia a uma porta corta-fogo existente nos prédios residenciais e comerciais. Essas portas têm o objetivo de evitar que o fogo transpasse a outro ambiente e, ao mesmo tempo, em caso de normalidade, permitir que pessoas passem por elas. No meio computacional esse termo pode representar dispositivos de *hardware* ou *software* e tem por objetivo impedir o acesso indevido ou não autorizado a um sistema por *softwares* maliciosos e não autorizados. Vide exemplo de *firewall* da Figura 8.7 a seguir.

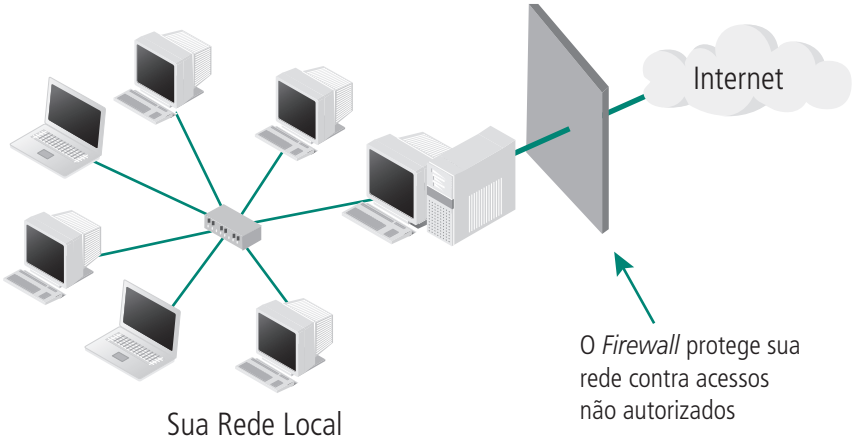


Figura 8.7: Esquema de um *firewall*
Fonte: http://www.gta.ufrj.br/grad/08_1/firewall/definition.html

Existem diversas formas de se controlar o que entra e sai de um sistema, desde a execução de aplicativos até mesmo a limitação dos aplicativos de usuários.

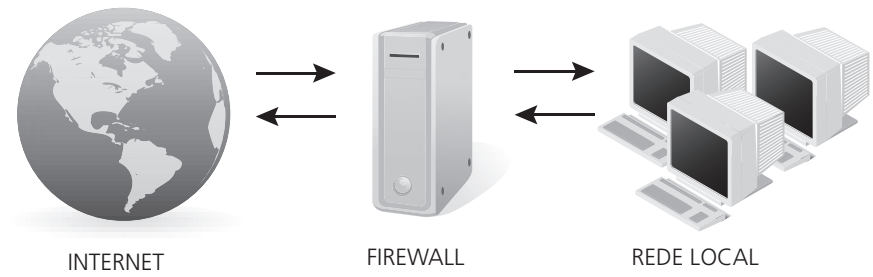


Figura 8.8: *Firewall* implementado por *software*
Fonte: http://www.dinx.com.br/2009/07/firewall-uma-abordagem-simples-e-direta/

Os *firewalls* por *software* (Figura 8.8) são implementados a partir de um computador de relativo baixo poder de processamento, munido de placas de rede e *softwares* tais como *Proxy* e antivírus, instalados entre o meio externo (internet) e o meio interno (LAN).

Os *Firewall* por *hardware* (Figura 8.9) são normalmente implementados em redes de grande porte e necessitam de rapidez e maior exatidão nos filtros.

Figura 8.9: *Firewall* por *hardware*
Fonte: http://tuffclassified.com/ads/cyberoam-utm-hardware-firewall-mumbai/

Tanto os *firewalls* montados por *software* quanto por *hardware* utilizam de aplicativos para sua gerência e estabelecimento do funcionamento adequado. Tais *softwares* se encarregam de barrar acessos indevidos, tanto de fora do sistema, quanto de dentro. Esses programas podem impedir que o sistema seja acessado de uma máquina externa ou bloquear o funcionamento de serviços internos diversos, como o TCP/IP – responsável pelo acesso à internet. Um *firewall* pode ainda barrar o tráfego de saída do computador/rede impedindo a divulgação de informações confidenciais.

8.5 Vírus e "Cavalos de Troia" (*Trojans*)

Um vírus de computador é um programa que pode alterar (ou infectar) outro programa de computador, de forma a incluir uma cópia de si mesmo.

Stephen Hawking é um dos maiores cientistas ligados ao campo da Física de todos os tempos. Veja mais em: http://pt.wikipedia.org/wiki/Stephen_Hawking

Segundo estatísticas recentes, os vírus e *malwares* (*softwares* criados com o intuito de cometerem alguma "maldade") são responsáveis pela maior parte dos problemas ocasionados por erros em programas, perdas de informações e paralisações de sistemas operacionais.

Parodiando os vírus biológicos, Stephen Hawking se referiu ao vírus de computador como a primeira forma de vida construída pelo homem. Realmente, a denominação de programa-vírus vem de uma analogia com o vírus biológico, que transforma a célula em uma fábrica de cópias. No caso do vírus

digital, a sua duplicação se dá dentro dos arquivos infectados. Os vírus são capazes de se reproduzir sem a ajuda do homem e assim determinam as suas respectivas sobrevivências.

Os vírus, ao longo de sua vida, receberam várias denominações de acordo com suas funções e objetivos. Os vírus do tipo cavalo de Troia são aqueles aparentemente inofensivos, mas que capturam senhas ou outras informações sem o conhecimento do usuário e as enviam para o seu criador. Muitos desses programas são utilizados para descobrir senhas de acesso à internet *banking*, por exemplo.

8.6 *Hackers*

Fórum de discussão sobre produtos Microsoft - http://forums.microsoft.com/technet-br

Os *hackers* são indivíduos com conhecimentos profundos em segurança de sistemas, que penetram furtivamente nos sistemas alheios, com objetivos escusos. Os *hackers*, em sua grande maioria, utilizam-se da falta de experiência dos administradores de sistemas ou usuário para conseguirem concluir suas intenções "criminosas".

Existem os *hackers* mais sofisticados que disponibilizam *software* na internet para que os usuários utilizem-se dele sem saber que seu real objetivo é o de abrir o seu sistema para uma invasão.

8.7 Criptografia

A criptografia já estava presente no sistema de escrita hieroglífica desde os egípcios. Foi utilizado por César, na antiga Roma, para transitar informações entre as tropas sem que o inimigo soubesse.

Desde então vem sendo muito utilizada, principalmente para fins militares, diplomáticos e, principalmente, comerciais. É de grande importância no âmbito da computação, uma vez que propõe garantir a segurança em todo o ambiente computacional que necessite de sigilo em relação às informações manipuladas.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S

Q	R	S	T	U	V	W	X	Y	Z
T	U	V	W	X	Y	Z	A	B	C

Figura 8.11: Imperador César junto a duas tabelas alfabéticas
Fonte: http://www.portalsaofrancisco.com.br/alfa/imperio-romano/caio-julio-cesar-2.php

Na Figura 8.11 é apresentada uma tabela semelhante a que fora utilizada por César para criptografar informações. Por exemplo: para criptografar a palavra CORDILHEIRA, fazendo-se o paralelo de cada letra da linha de cima com a linha de baixo na tabela, tem-se: FRUGLOKHLUD.

A criptografia pode ser usada para codificar dados e mensagens antes que estes sejam enviados. Quando enviados, mesmo que sejam interceptados no caminho, dificilmente poderão ser decodificados, garantindo a privacidade da informação.

A criptografia computacional é usada para garantir autenticação de usuários, sigilo e integridade de informações. Assim, na computação, uma informação pode ser codificada através de algum algoritmo de criptografia, de modo que, tendo conhecimento do algoritmo utilizado e da chave utilizada na criptografia, é possível recuperar a informação original fazendo o percurso contrário da encriptação, que é a decriptação.

Um vídeo interessante sobre criptografia pode ser visto em http://www.youtube.com/watch?v=ajniLnQTabw

Em suma, os algoritmos criptográficos são funções matemáticas usadas para codificar os dados, garantindo segredo e autenticação. Um sistema de criptografia deve ser seguro mesmo quando os algoritmos de cifrar e decifrar sejam conhecidos. As informações só são conhecidas para quem detém a chave de criptografia.

Finalmente, um sistema seguro é assim denominado somente se for teoricamente inquebrável.

Resumo

Nesta aula conhecemos segurança de sistemas operacionais servidores. Entendemos a diferença entre segurança física e lógica. Vimos como podem ocorrer as falhas de ordem elétrica, de causas naturais e mesmo de eventos criminosos ou premeditados e como preveni-las. Quanto à segurança lógica, aprendemos como podemos prevenir ataques efetuando configurações nas diretivas do sistema operacional. Aprendemos *firewalls*, que são os responsáveis pela segurança, entrada e saída de informações e acessos ao sistema. Compreendemos como os vírus atacam e como podemos preveni-los, além de aprendermos a bloquear a ação dos *hackers* e como montar e trafegar informações escondidas pelos métodos de criptografias.

Atividades de aprendizagem

1. Por que atualmente a segurança da informação é uma grande preocupação das empresas?

2. Explique o dilema da segurança e compartilhamento da informação.

3. Suponha um sistema de segurança 100% virtualmente seguro (que não possua falhas no compartilhamento de informação *on-line*). Como alguém poderia ter acesso às informações contidas nesse sistema?

4. Cite duas diretivas de senha e seu funcionamento.

5. Cite duas diretivas de conta e seu funcionamento.

6. O que é um *firewall*?

7. Faça um algoritmo que implemente a criptografia criada por César.

8. Faça um algoritmo que, baseado na criptografia de César, leia um valor de deslocamento no alfabeto e uma frase de entrada qualquer, gerando a saída criptografada. Exemplo:

   Deslocamento: 2 (A → C, B → D, C → E, etc.)
   Entrada: CEFET-MG
   Saída: EGHGV-OI

Poste suas respostas no ambiente virtual de ensino-aprendizagem (AVEA).

Referências

AUDITORIA. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2012. Disponível em: <http://pt.wikipedia.org/w/index.php?title=Auditoria&oldid=31210350>. Acesso em: 20 jul. 2012

BATISTI, Júlio, **Guia de estudos para o MCSE 70-290**. e-book , 2003 Disponível em: <http://www.slideshare.net/vagnerks/guia-de-estudos-para-o-mcse-70-290-julio-battisti>. Acesso em: 25 jul. 2012.

BATISTI, Júlio, **Windows Server 2003:** curso completo. Rio de Janeiro: Axcel Books, 2003.

BADDINI, F., **Windows Server 2003 em português:** implementação e administração. 4a ed. São Paulo: Érica, 2003.

Gerenciando a Segurança Corporativa. SYMANTEC. Disponível em: <www.nerdbb.com/download/file.php?id=3033>. Acesso em: 25 jul. 2012.

MACHADO, Francis Berenger; MAIA, Luiz Paulo. **Arquitetura de sistemas operacionais.** São Paulo: 3a ed. LTC, 2002.

TANENBAUM, Andrew S. **Sistemas operacionais modernos.** 2a ed. São Paulo: Prentice Hall, 2007.

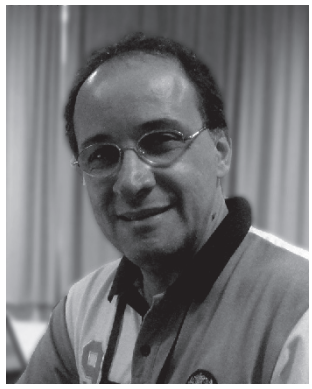
SILBERSCHATZ, Abraham. **Sistemas operacionais.** Rio de Janeiro: Editora Campus, 2001.

KAASHOEK, M. Frans; Dawson, R. Engler; Gregory, R. Ganger; Wallach, Deborah A., **Server Operating Systems,** M.I.T. Laboratory for Computer Science, 1996.

MEYERS, Mike. **Dominando os sistemas operacionais**: teoria & prática. Rio de Janeiro: 5a ed. Alta Books, 2006.

Currículo dos professores-autores

Marcelo Caramuru Pimentel Fraga é professor efetivo do Centro Federal de Educação Tecnológica de Minas Gerais (CEFET-MG) das disciplinas Sistema Operacionais I e II. Possui mestrado em Modelagem Matemática Computacional e graduação em Engenharia Mecânica, ambos pelo CEFET-MG. É aluno de doutorado na Universidade Federal de Minas Gerais (UFMG). Possui experiência na área de Pesquisa Operacional, com ênfase em Programação Linear e Não Linear, atuando principalmente em Roteamento de Veículos e Metaheurísticas Computacionais.



William Geraldo Sallum é professor da disciplina de Aplicativos para Web I e professor efetivo do CEFET-MG, no curso de Informática. Está cursando Doutorado em Ensino de Ciências e Matemática pela UNICSUL. Concluiu o mestrado em Tecnologia da Informação pelo CEFET-MG (2002), *Lato Sensu* em Análise de Sistemas pelo Cenex (1990) e graduação em Matemática pela Faculdade de Filosofia Ciências e Letras de Belo Horizonte (UNIBH), possuindo também habilitação para o ensino de Física e Desenho. É membro titular da Comissão Permanente de Pessoal Docente (CPPD) do CEFET-MG e atua como subcoordenador de Curso da Pós-graduação em Gerenciamento de Infraestrutura de TI do CEFET-MG.