UNIVERSIDADE TUIUTI DO PARANÁ

MICHAEL ANDRÉ HEMPKEMEYER

INFRAESTRUTURA MÍNIMA DE SERVIDORES NECESSÁRIOS PARA UMA REDE BASEADOS EM SOFTWARE LIVRE

CURITIBA

2015

MICHAEL ANDRÉ HEMPKEMEYER

INFRAESTRUTURA MÍNIMA DE SERVIDORES NECESSÁRIOS PARA UMA REDE BASEADOS EM SOFTWARE LIVRE

Trabalho apresentado ao Curso de Especialização em Redes de Computadores e Segurança de Redes, da Universidade Tuiuti do Paraná, como requisito avaliativo da Monografia.

Professores: Roberto Néia Amaral

CURITIBA

2015

RESUMO

Trata do desenvolvimento de um conjunto de informações para que os administradores de redes possam compreender a função de alguns serviços essenciais para as redes atuais, baseando-se em software livre. O objetivo é reunir todas essas informações em um único documento, fornecendo conhecimentos básicos sobre os servidores e instruindo a implantação dos mesmos. Será abordado os serviços de resolução de nomes, ou DNS, obtenção de endereçamento de IPs automaticamente com o protocolo DHCP. Para servidores Web será abordado o software Apache e para servidores Proxy, o software Squid. Além disso, será passado um conhecimento teórico básico sobre os serviços de sincronismo de tempo com o protocolo NTP, servidor de arquivos com o protocolo Samba e sobre servidores de repositórios locais, com o software Apt-Cache. Todos esses serviços são baseados em software livre, ou seja, não é necessário pagar para poder utilizar. A distribuição Linux utilizada será o Debian na sua última versão disponível, sendo a 8.1. Por fim, os administradores de redes poderão utilizar este trabalho como manual ou fonte de pesquisa para eventuais dúvidas.

Palavras-chave: Servidores Linux. Software Livre. Redes de Computadores. Serviços de Redes.

LISTA DE FIGURAS

FIGURA 1 - RANKING DOS NAVEGADORES MAIS UTILIZADOS 14
FIGURA 2 - SERVIDORES WEB MAIS UTILIZADOS 14
FIGURA 3 - PERCENTUAL DE USO DO LINUX EM SERVIORES WEB.....20
FIGURA 4 – SOURCES.LIST PADRÃO.....22
FIGURA 5 – SOURCE.LIST PERSONALIZADA.....22
FIGURA 6 – COMANDO INSTALAÇÃO BIND 25
FIGURA 7 – COMANDO INSTALAÇÃO DHCP 28
FIGURA 8 – COMANDO INSTALAÇÃO APACHE.....30
FIGURA 9 – COMANDO INSTALAÇÃO PHP 30
FIGURA 10 – COMANDO INSTALAÇÃO EXTENÇÕES PHP 31
FIGURA 11 – COMANDO PESQUISAR OUTRAS EXTENÇÕES 31
FIGURA 12 – COMANDO INSTALAÇÃO SQUID 32
FIGURA 13 – ACL SQUID 1.....33
FIGURA 14 – ACL SQUID 2.....33
FIGURA 15 – REGRA SQUID 1.....33

SUMÁRIO

1 INTRODUÇÃO 5
2 CONCEITOS DE SISTEMAS OPERACIONAIS PARA SERVIDORES 6
3 CONHECENDO PRINCIPAIS SERVIÇOS DE REDE 11
4 SISTEMA OPERACIONAL DEBIAN 20
5 INSTALAÇÃO E CONFIGURAÇÃO DE DNS 25
6 INSTALAÇÃO E CONFIGURAÇÃO DE DHCP 28
7 INSTALAÇÃO E CONFIGURAÇÃO DE APACHE 30
8 INSTALAÇÃO E CONFIGURAÇÃO DE PROXY 32
9 CONCLUSÃO 35
REFERÊNCIAS 36
GLOSSÁRIO 38
APÊNDICE A – MANUAL DE INSTALAÇÃO DEBIAN 39
APÊNDICE B – ARQUIVO DE CONFIGURAÇÃO DNS 67
APÊNDICE C – ARQUIVO DE CONFIGURAÇÃO DHCP 70
APÊNDICE D – ARQUIVO DE CONFIGURAÇÃO DHCP FAILOVER 71
APÊNDICE E – ARQUIVO DE CONFIGURAÇÃO APACHE 74
APÊNDICE F – ARQUIVO DE CONFIGURAÇÃO SQUID 75

1 INTRODUÇÃO

Com o progresso da tecnologia, a cada dia os computadores estão mais presentes nas nossas vidas e no ambiente corporativo, principalmente. Para que os computadores possam ser utilizados, existe a necessidade de um sistema operacional instalado. Além disso, no caso dos servidores, há também os softwares que são empregados para fazer trabalhos que agilizam e facilitam as atividades dos usuários. Assim, se questiona: existe a possibilidade de obter o sistema operacional e os softwares sem custo de licenças e igual ou até superior dos mesmos itens pagos? Segundo a FREE SOFTWARE FOUNDATION, “Desenvolvedores de software livre garantem igualdade de direitos para os seus programas a todos. Qualquer usuário pode estudar o código fonte, modificá-lo e compartilhar o programa”.

Segundo ALVES (2010), “Software Livre é socialmente justo, economicamente viável e tecnologicamente sustentável e ainda produzido através do compartilhamento de conhecimento e saberes globais e compartilhado por redes e para todos”.

“Os gastos com licença costumam representar de 30% a 40% dos custos de um software”, afirma Rodolfo Gobbi, diretor da 4Linux, consultoria especializada em tecnologia. Essa afirmação foi dada em uma reportagem a uma matéria do programa “Pequenas Empresas & Grandes Negócios”, da Rede GLOBO, onde relata que as empresas estão cada vez mais aceitando os softwares livres nos seus equipamentos de informática.

Para completar, segundo a W3TECHS, site especializado em fornecer estatísticas sobre as tecnologias utilizadas na Internet, informa que “os sistemas operacionais e softwares mais utilizados na Web são Softwares Livres”.

Este trabalho tem como objetivo mostrar uma solução para os administradores de rede utilizando Software Livre sem complicação e com praticidade.

Enfim, apesar de não ser um assunto novo ou escasso na Internet, a finalidade de desenvolver este trabalho é agrupar os principais serviços nas redes locais em um só documento, descrevendo não apenas como configurar, mas também o porquê da configuração e para que serve.

2 CONCEITOS DE SISTEMAS OPERACIONAIS PARA SERVIDORES

Segundo a DELL, “um servidor é, basicamente, um computador mais potente que um computador comum. Ele foi desenvolvido para lidar com cargas de trabalho intensas e ininterruptas”. Porém para que o hardware do servidor seja bem utilizado é necessário que o sistema operacional seja compatível e que utilize o máximo possível da tecnologia sem prejudicar todo o conjunto eletrônico do servidor. Sistemas operacionais para servidores tem essa função.

Existem diversos sistemas operacionais, principalmente levando em consideração as distribuições baseadas no Kernel Linux. Apesar disso, o foco desta monografia será apenas sistemas Linux, pois estes, na sua maioria, são livres de encargos para utilização, ou seja, totalmente de graça, do contrário dos sistemas operacionais Windows, onde você deve pagar para poder utilizar.

A palavra Linux foi originado da mixagem de Linus e Unix, onde Linus é o primeiro nome do principal criador e Unix é um dos poucos sistemas operacional, em que foi baseado o Linux, mais robusto na década de 90.

O Linux foi desenvolvido para ser um sistema multitarefa e multiusuário, ou seja, é possível executar vários processos ao mesmo tempo e com diversos usuários simultaneamente.

Além disso, por ser um sistema operacional livre, é possível modificar os arquivos de configuração do sistema de acordo com as suas necessidades, conforme será mostrado no decorrer deste trabalho.

2.1 TIPOS DE SERVIDORES

Segundo MORIMOTO(2011, p. 16), “os sistemas Linux foram desenvolvidos para servidores”. Um servidor é uma máquina que fica o tempo todo ligada, sempre fazendo a mesma coisa e podem ser divididos em dois grandes grupos: servidores de rede local e servidores de Internet (MORIMOTO, 2011).

Servidores de rede local são normalmente os computadores que fornecem os serviços de DHCP, DNS, acesso a Internet, como o proxy. Outros exemplos de servidores de rede local são os usados para hospedar as páginas ds Intranet e sistemas de uso interno.

Já os servidores de Internet são os utilizados para hospedagem, principalmente, das páginas acessadas pela Internet.

2.1.1 Servidor rede local

Servidores de rede local são todos os servidores que tem relevância na rede(s) interna(s) apenas. Podemos exemplicar o DHCP, que oferece serviço de autoconfiguração de endereços lógicos para os dispositivos da rede.

Outros exemplos são os servidores de DNS internos, servidor Web que hospeda a página da Intranet da empresa, servidor Proxy, entre outros serviços que são acessados apenas se o computador estiver conectado na rede interna, sendo localmente através de um cabo conectando o computador com algum distribuidor de rede, como switches. Outra possibilidade de acesso aos servidores de rede local é a partir de conexões VPN, que permitem acessar uma rede interna por um link de Internet.

Esses servidores normalmente fornecem serviços que auxiliam os usuários acessarem a Internet, sistemas internos, impressoras compratilhadas e servidores de arquivos.

Geralmente, servidores de rede local não possuem dispositivos específicos para realizar a segurança de dados contra invasões ou usuários mal-intencionados. Isso ocorre porque esses dispositivos são acessados apenas por usuários da próprias empresa ou outros usuários de confiânça. Diferentemente dos servidores de Internet, que podem ser acessados por todo o mundo.

2.1.2 Servidor de Internet

Servidores de Internet são computadores que fornecem algum serviço disponível para todo o mundo. Exemplos mais comuns são servidores Web e de DNS. Sem esses dois tipos, nós não teríamos motivo e viabilidade de se conectar na Internet.

Primeiramente, sem servidores Web não haveria a Internet de hoje, já que todos os sites do mundo estão hospedados em algum servidor. Por último, sem

servidores DNS, seria muito trabalhoso gravar todos os endereços numéricos dos sites disponíveis. A função do DNS será mais bem abordada no sub capítulo 3.1.

Para este tipo de servidor é recomendado alguns dispositivos de segurança para realizar a proteção contra invasões de hacker ou usuários mal-intencionados. Segundo o site INTERNETLIVESTATS, em média 50 mil sites são invadidos todos os dias. Essas ações tem como finalidade o roubo de informações, danificação de servidores ou armazenagem de programas utilizados posteriormente em outras invasões.

Servidores Firewall dedicados e *IPS* (*Intrusion Prevention Systems*, ou Sistema de Prevenção de Intrusões em português) são dispositivos desenvolvidos para realizar a segurança de dados dos servidores de Internet. Evidentemente esses equipamentos não evitam 100% dos ataques. Uma política de segurança bem estruturada, softwares atualizados e uma equipe de profissionais qualificados são essenciais para diminuir a probabilidade de uma invasão.

2.2 DESEMPENHO DOS SERVIDORES

Por ser um software livre e código aberto, temos acesso os arquivos do sistema, possibilitando a realização de optimização do sistema operacional Linux, caso necessário.

O Linux possue o diretório “/proc”. Este diretório, segundo MORIMOTO (2009), “não armazena arquivos, mas sim informações sobre o hardware e sobre a configuração do sistema. Estas informações são usadas por utilitários de detecção e configuração do sistema, mas podem ser úteis também quando você quer checar alguma configuração manualmente”.

Neste diretório você também pode habilitar roteamento no sistema, bloqueios de mensagens ICMP e outras configurações de redes avançadas.

Há também o arquivo sysctl.conf, encontrado no diretório “/etc/”. Neste arquivo é possível configurar o kernel do sistema operacional para receber uma quantidade maior de conexões de rede simultâneas, além de habilitar uma resposta mais rápida na abertura e fechamento de conexões.

Enfim, mesmo sendo necessário um hardware robusto para redes de grande porte, o sistema operacional nas suas configurações padrão pode não suportar a

carga excessiva de trabalho diário. Para isso deve-se realizar configurações no kernel da distribuição, optimizando o sistema.

2.3 MELHORES PRÁTICAS

No site do CERT.BR, Centro de Estudos, Respostas e Tratamento de Incidentes de Seguraçan no Brasil, podemos encontrar diversar dicas de como melhorar a segurança das nossas infraestruturas de redes e algumas práticas que permitem diminuir a probabilidade de interrupção de serviços de rede fornecidas pelos servidores da rede local.

Dentre as recomendações, podemos destacar a necessidade de uma política de segunrança aprorpiada para a rede. Além disso devemos ter atenção em algumas atividades que normalmente parecem ser simples, tais como uma estratégia de particionamento na instalação do sistema operacional. Essa estratégia visa evitar problemas na utilização de uma única partição, pois caso uma partição seja corrompida por alguma razão, as outras partições podem não ser afetadas.

Segundo o CERT.BR (2003),” devemos evitar concentrar todos os serviços de rede em uma única máquina, dividindo-os entre vários sistemas. Isto é desejável pois aumenta a disponibilidade dos serviços na sua rede e reduz a extensão de um eventual comprometimento a partir de um deles”.

Devemos também sempre documentar as instalações dos sistemas e as configurações feitas nele. Essa documentação tem como objetivo auxiliar em casos que seja necessário reconstituir uma instalação.

Outra sugestão, que será melhor abordada no sub capítulo 4.3 do capítulo 4, é a instalação mínima dos pacotes no sistema. Segundo o CERT.BR (2003), “é comum que serviços não utilizados não sejam monitorados por falhas de segurança, o que aumenta a possibilidade de não ser aplicada uma correção necessária.” O CERT.BR (2003) completa, “A redução no número de pacotes instalados diminui a chance de que o sistema possua uma vulnerabilidade que possa vir a ser explorada por um atacante. Podemos incluir também a desativação dos serviços não utilizados pelo sistema”.

Uma advertência feita pelo CERT.BR é, sempre que possível, centralizar os *logs* dos sistemas. Normalmente os *logs* ficam armazenados localmente nos

servidores, porém essa prática pode colocar essas informações em riscos em casos de invasões, podendo ser destruídas pelo invasor.

Finalizando, práticas de melhorias de segurança devem ser planejadas e executadas constantemente, já que a cada dia essas práticas são repensadas e atualizadas.

3 CONHECENDO PRINCIPAIS SERVIÇOS DE REDE

Para que uma rede de computadores funcione com mais autonomia é necessário que haja alguns serviços disponíveis, facilitando o trabalho do profissional de TI responsável pela empresa e agilizando os trabalhos dos usuários.

Serviços como resolução de nomes dos sites acessados, obtenção de endereço lógico dos computadores automaticamente, sites internos, centralização e compartilhamento de arquivos em um só computador para todos são exemplos de serviços que são possíveis de configurar utilizando sistemas operacionais Linux.

Como já mencionado, é possível configurar os servidores Linux de acordo com a necessidade da empresa, ou seja, independente se sua empresa é de grande porte ou pequeno porte, é possível utilizar a mesma distribuição e o mesmo aplicativo, sendo o que vai diferenciar os dois serão, as opções ativas do arquivo de configuração.

3.1 CONCEITOS BÁSICOS DE DNS

Para que uma solicitação de acesso a um site seja realizada, é necessário que se tenha o endereço IP do servidor destino no qual o site está hospedado. Sendo assim, ou teriamos que gravar os endereços lógicos de todos os sites ou teriamos que ter um caderno com todos os números IPs e seu respectivo site, semelhante as antigas agendas telefônicas, para poder utilizar a Internet. Nos tempos de hoje isso se tornou quase impossível. O acesso via endereço IP não é impedido pelos DNS. O internauta continua podendo acessar os sites pelos endereços númericos. O serviço de tradução venho apenas para trazer mais comodidade e agilidade aos usuários Para isso, existem os servidores DNS.

DNS é a sigla em inglês para Domain Name System (Sistema de Nome de Domínio, em português), e segundo o site SIGNIFICADOS, “é o responsável por decodificar os nomes dos domínios dos sites que as pessoas digitam nos navegadores web em números IP”, ou seja, ao invés de digitarmos o endereço númerico do site, acessamos atravéz de um nome e os servidores DNS executam essa tradução do nome para o número.

Segundo o site REGISTRO DE DOMÍNIOS, “o Sistema de Nome de Domínio é uma arquitetura distribuída, onde cada entidade é responsável pela gestão do seu nome de domínio”. Ainda:

> Os servidores que correspondem aos domínios de mais alto nível (TLD) são chamados "servidores de nomes raiz". Existem treze servidores raiz no mundo, dos 13 root servers que existem no mundo, dez estão localizados nos Estados Unidos da América, um na Ásia e dois na Europa.

Esses servidores raiz delegam as zonas, ou seja, domínios, para outros servidores de nível mais baixo, como exemplo o domínio BR ou NET. Esses, por sua vez, podem também realizar outras delegações. O BR, por exemplo, possui a zona MIL, e o MIL possui a EB, que é o domínio militar e do Exército Brasileiro. Com essas delegações, existe um servidor DNS responsável pelas traduções ou até mesmo de outras delegações da zona “eb.mil.br”.

Toda essa estrutura é totalmente trasparente para o usuário final. A única configuração necessária é o endereço de um servidor DNS capaz de fazer as traduções nas configurações de rede do computador.

O servidor mais popular chama-se BIND (Berkeley Internet Name Domain). Segundo o site REGISTRO DE DOMÍNIOS, “trata-se de um software livre disponível nos sistemas UNIX, desenvolvido inicialmente pela universidade de Berkeley, na Califórnia, e mantido pelo ISC (Internet Systems Consortium)”.

3.2 CONCEITOS BÁSICOS DE DHCP

Com o objetivo de dois computadores se comunicarem, é necessário que ambos tenham um endereço IP. O serviço de DHCP venho para que essa configuração de IP seja feita automaticamente.

Se pensarmos em uma rede com dois ou três computadores, a obteção de endereço lógico automaticamente não é muito atrativa. Porém, se ao invés de uma rede, forem dezenas e cada rede possuir mais de cem computadores, ter um servidor DHCP é quase uma obrigatoriedade.

O DHCP ("Dynamic Host Configuration Protocol" ou "protocolo de configuração dinâmica de endereços de rede"), segundo MORIMOTO (2005),

“permite que todos os hosts da rede recebam suas configurações de rede automaticamente a partir de um servidor central, sem que você precise ficar configurando os endereços manualmente em cada um”.

Além do endereço de rede, é possível incluir o endereço do gateway, endereço dos servidores DNS, nome do domínio da rede, configurações de proxy para os navegadores, entre outros.

De um modo geral, o trabalho do DHCP é bastante simples. Um dispositivo, ou cliente, faz uma solicitação de endereçamento IP para todos os dispositivos da rede, por um pacote broadcast. O servidor DHCP irá responder essa solicitação, oferecendo um endereço. O cliente solicita o emprestimo desse endereço, enviando um outro pacote para o servidor DHCP. O servidor responde com a confirmação do emprestimo e realiza a reserva desse endereço para o cliente.

O servidor DHCP realiza uma verificação periodica dos IPs alocados na rede, sendo que, caso algum cliente que tenha um endereço empresta e não esteja mais ativo na rede, o empréstimo será desfeito e o endereço poderá ser alocado para outro cliente.

Segundo MORIMOTO (2011, p. 127), “o servidor DHCP mais usado no Linux é o ISC DHCP, desenvolvido pela ISC (Internet Systems Consortium), uma organização sem fins lucrativos dedicada a desenvolver serviços de infra-estrutura usados na Internet, incluindo o Bind”.

3.3 CONCEITOS BÁSICOS DE APACHE

As páginas Web funcionam na arquitetura cliente-servidor. Essa arquitetura funciona basicamente com o cliente realizando uma requisição e um servidor respondendo a essa requisição, ou seja, ou seja, um usuário utilizando um navegador e acessando um site.

Os navegadores, ou *browsers* em inglês, são softwares que realizam essa função de cliente Web. São basicamentes interpretadores de linguagens de programação Web, como PHP, HTML, CSS, entre outras. Eles que realizam o trabalho de solicitar os dados das páginas informado pelo usuário.

Essa solicitação de dados é, resumidamente, o download dos arquivos disponibilizados pelo servidor Web. Após baixar os dados, o navegador faz a interpretação do código e mostra a página para o usuário.

O navegador mais utilizado no mundo, segundo a W3SCHOOLS, é o Chrome, da Google.

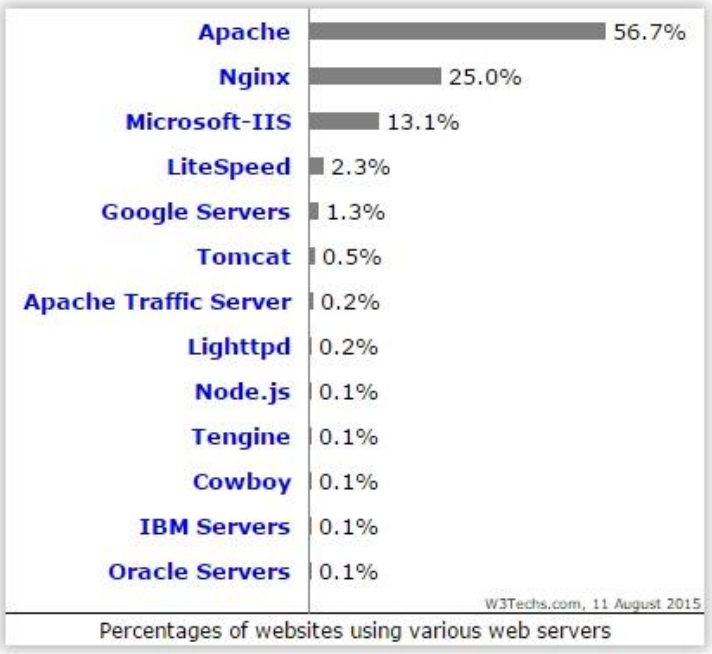
FIGURA 1 - RANKING DOS NAVEGADORES MAIS UTILIZADOS

2015	Chrome	IE	Firefox	Safari	Opera
June	64.8 %	7.1 %	21.3 %	3.8 %	1.8 %
May	64.9 %	7.1 %	21.5 %	3.8 %	1.6 %
April	63.9 %	8.0 %	21.6 %	3.8 %	1.5 %
March	63.7 %	7.7 %	22.1 %	3.9 %	1.5 %
February	62.5 %	8.0 %	22.9 %	3.9 %	1.5 %
January	61.9 %	7.8 %	23.4 %	3.8 %	1.6 %

Fonte: W3schools.com.

No outro lado da ponta, há o servidor Web. Esse servidor é reponsável em receber as requisições de acesso web e disponibilizar os dados da páginas solicitadas. O servidor Web mais utilizado no mundo, segundo a W3TECHS, é o Apache.

FIGURA 2 - SERVIDORES WEB MAIS UTILIZADOS



Fonte: W3Techs.

O Apache é tão popular devido a suas caracteristicas principais, que entre outras, podemos destacar os módulos de seguraça, que possibilitam criar uma camada de segurança extra e muito eficiência contra ataques de hackers, negociação de conteúdo, permitindo a exibição da página Web no idioma requisitado pelo navegador do usuário, suporte a criptografia SSL e certificados digitais.

Os servidores Apache também possibilitam a criação de um servidor que responde por multiplos sites, ou seja, ao invés de uma empresa, que fornece serviço de hospedagem de site, possuir um servidor exclusivo para cada cliente, com o Apache é possível hospedar diversos sites em um mesmo servidor. Essa função é chamada de “virtual hosting”.

Além de ser um software com licença livre, todas as opções, além das que foram mencionadas, podem ser ativadas ou desativas sem a necessidade da compilação do programa, bastanto, basicamente, modificar o arquivo de configuração principal do apache e reiniciar o serviço.

A inteção de ter um servidor Apache na rede local de uma empresa é a possiblidade de possuir uma página de Intranet, disponibilizando acesso centralizado de serviços e informações da empresa para os funcionários de uma maneira mais familiar nos tempos atuais, via navegadores Web.

3.4 CONCEITOS BÁSICOS DE PROXY

Segundo a MICROSOFT CORPORATION, “servidor proxy é um computador que funciona como intermediário entre um navegador da Web (como o Internet Explorer) e a Internet”. Ainda:

> Os servidores proxy ajudam a melhorar o desempenho na Web armazenando uma cópia das páginas da Web utilizadas com mais freqüência. Quando um navegador solicita uma página que está armazenada na coleção do servidor proxy (o cache), ela é disponibilizada pelo servidor proxy, o que é mais rápido do que acessar a Web. Os servidores proxy também ajudam a melhorar a segurança porque filtram alguns tipos de conteúdo da Web e softwares mal-intencionados.

Já segundo MORIMOTO (2011, p. 133), “usar um proxy é diferente de simplesmente compartilhar a conexão diretamente, via NAT. O proxy realiza o

trabalho de repassar as requisições, analisando todo o tráfego de dados, separa o que pode ou não pode passar e guarda informações para uso futuro.”

Para que um usuário utilize o proxy para navegar, é necessário que seja configurado no navegador.

Ao navegar com proxy, o usuário não faz mais solicitações diretamente com os sites da Internet, sendo o servidor proxy o responsável de fazer essas solicitações. Portanto para obrigar os usuários usarem as configurações de proxy no navegador, deve-se liberar no firewall da rede apenas solicitações de acesso a internet vindas do servidor proxy, caso contrário, bastaria que o usuário desativasse as configurações do navegador e o mesmo teria acesso a Internet sem nenhuma restrição ou controle.

O servidor proxy que será abordado neste trabalho será o Suid. Com o Squid podemos obter um controle de tráfego bastante flexivel e eficiênte. Ele é indicado desde pequenas empresas até grande empresas com mais de mil funcionários. O poder de processamento do servidor proxy deve ser escolhido de acordo com a quantidade de usuários que irão utilizar simultaneamente. Visto que ele será o responsável em receber todas as conexões de acesso a Internet e ao mesmo tempo realizar essas conexões. Portanto o sistema operacional e o hardware precisa suportar centenas de conexões simultâneas e ininterruptas.

O Squid permite fazer filtro de sites, domínios e endereços IPs. Permite também organizar sites e usuários por grupos de acesso. Podemos também configurá-lo para trabalhar em modo transparente, não sendo necessário configurações nos navegadores, ou em modo de autenticação, sendo necessário informar um usuário e senha, que podem ser de uma base de dados local, ou de outras fontas, como LDAP ou SAMBA.

Segundo o site INTERNETLIVESTATS.COM, existe quase um bilhão de sites no mundo e esse número não para de crescer. Imagina como seria atualizar as listas do que pode e não pode ser acessado no Squid. Seria uma tarefa quase impossível. Para isso existem programas que trazem listas prontas de sites de todo o mundo e os classifica do que é próprios e do que é impróprio, cabendo ao administrador de rede fazer alguns ajustes pequenos.

Um exemplo é o SquidGuard. Este software trabalha junto do Squid, através da classificação dos sites em uma base de dados própria. Segundo SHALLA SECURE SERVICES KG, atual mantenedor do software, “é um redirecionador de

URL usado para usar listas negras com o proxysoftware Squid. Há duas grandes vantagens para squidguard : é rápido e é gratuito.”

Com o SquidGuard podemos obter uma classificação mais otimizada dos sites, realizando atualizações diárias do banco de dados das listas de sites e minimizando os acessos indevidos dos usuários.

3.5 CONCEITOS BÁSICOS DE SAMBA

Segundo o site dos mantenedores do software SAMBA, “Samba é um aplicativo Unix que utiliza o protoloco SMB (Server Message Block)”. Ainda:

> Sistemas operacionais Windows utilizam este protocolo para compartilhar arquivos, pastas e impressoras. Com isso, para que os sistemas Linux pudessem acessar os compartilhamentos dos sistemas Windows, Andrew Tridgell realizou engenharia reversa no protocolo SMB e programou no Linux, possibilitando os dois sistemas compartilharem dados.

Samba é um software com licença livre e oferece, dentre outros, os seguintes serviços:

- Compartilhamento de um ou mais diretórios;
- Compartilhamento de impressoras;
- Quotas de uso no servidor de arquivos.

É possível integrar o Samba com outras bases de dados de usuários, como LDAP ou Active Directory, restringindo o acesso às pastas compartilhadas apenas a usuários autorizados. Além de permitir quais usuários podem ou não podem modificar os arquivos dos diretórios.

Podemos ainda configurar o Samba para mover os arquivos excluídos pelos usuários para uma pasta específica, evitando as exclusões de arquivos acidentalmente.

3.6 CONCEITOS BÁSICOS DE APT-CACHER

Servidores de Apt-Cacher são essencialmente servidor de proxy, porém fornecem um serviço diferente. Ao invés de fornecer acesso web aos usuários, esse servidor fornece os pacotes de uma instalação ou requisição de pacotes Linux.

Esse serviço é muito útil quando a maioria dos sistemas operacionais utilizados nas estações de trabalho de uma empresa são Linux, principalmente quando há distribuição padrão na rede.

Ao instalar ou atualizar um pacote no linux, o sistema operacional realiza o download diretamente da internet, consumindo banda, que podem ser limitados. Em um cenário de uma rede com mais de cem computadores e todos eles realizando atualizações periódicas, os usuários podem perceber uma latência continuar no acesso a Internet, devido essas atualizações.

Os servidores Apt-Cacher são utilizados para resolver esse problema. Há diversos tipos de servidores que fornecem esse serviço. Focaremos no Apt-Cacher NG.

O Apt-Cacher NG não exige um que o servidor tenha grande esaço em disco, pois o dowload dos pacotes são realizados sob demanda, ou seja, apenas quando é solicitado. Caso o servidor já tenha o pacotes localmente, o cliente realiza o download do próprios servidor, caso contrário, o servidor realiza o download do pacote, salva e copia para o cliente. Com isso, há uma economia considerável do uso da banda de Internet na realização das atualizações de sistemas ou instalação de pacotes.

Além disso, o Apt-Cacher NG é compatível com as principais distribuições Linux, como Debian, Ubuntu, OpenSuSE, Fedora, entre outras.

3.7 CONCEITOS BÁSICOS DE NTP

Segundo o NTP.BR, “o NTP (Network Time Protocol ou Protocolo de Tempo para Redes, em português) é o protocolo que permite a sincronização dos relógios dos dispositivos de uma rede como servidores, estações de trabalho, roteadores e outros equipamentos à partir de referências de tempo confiáveis”.

Apesar de não ser um serviço exigido para o funcionamento e acesso a rede de dados, ter os horários dos servidores e estações de trabalhos sincronizados é muito importante, principalemente no ramo de segurança de redes.

Os logs dos servidores, roteadores e firewalls são gerados juntos com o horário do dispositivo, portanto, caso não tenha um sincronismo, pode ser quase impossível de saber a sequência de um ataque de um hacker na rede.

4 SISTEMA OPERACIONAL DEBIAN

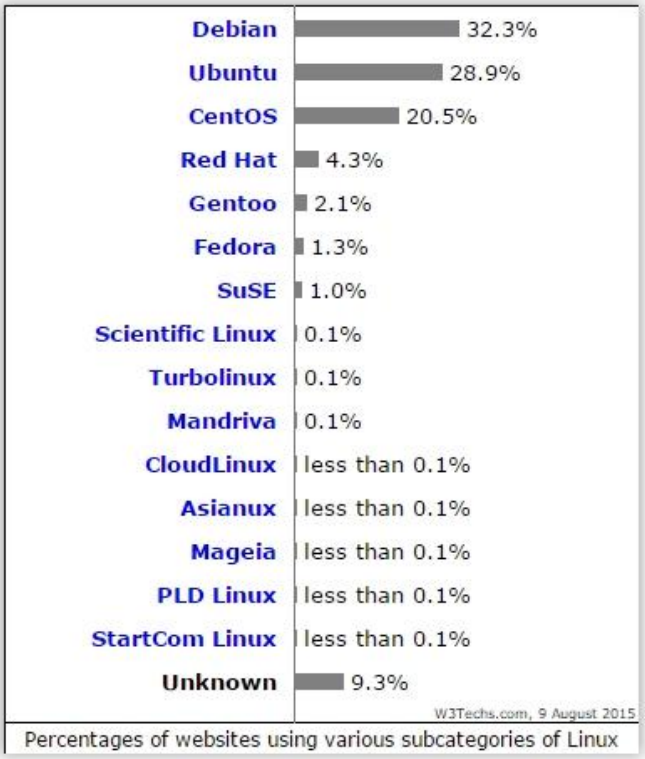
A Debian teve origem no Projeto Debian, fundado por Ian Murdock, em 1993. Segundo a SOFTWARE IN THE PUBLIC INTEREST, “esse projeto, composto por um grupo de voluntários do mundo todo, tinha como finalidade o desenvolvimento de um sistema operacional livre, composto inteiramente por software livre.”

A principal distribuição do projeto é o próprio Debian, que inclui o núcleo do Linux, desenvolvido por Linus Torvalds.

4.1 DEFINIÇÃO DO SISTEMA OPERACIONAL

A distribuição escolhido foi a Debian 8. Ela é voltada principalmente para servidores e totalmente de graça. O suporte é feito por uma comunidade de desenvolvedores e muito bem aceita pelas empresas, sendo a distribuição mais utilizada na internet, conforme a imagem do percentual de uso em servidores web a seguir, disponibilizada pelo site w3techs.com.

FIGURA 3 - PERCENTUAL DE USO DO LINUX EM SERVIORES WEB



Fonte: W3Techs.

Segundo a SOFTWARE IN THE PUBLIC INTEREST, “a Debian é a única distribuição que é aberta para que todo desenvolvedor e usuário possam contribuir com seu trabalho. É o único distribuidor significativo de Linux que não é uma entidade comercial”. Ainda:

> É o único grande projeto com uma constituição, um contrato social e documentos com políticas para organizar o projeto. A Debian também é a única distribuição que é micro-empacotada, usando informações detalhadas de dependência de pacotes para garantir a consistência do sistema em atualizações.

Os pacotes disponíveis no Debian são todos consideráveis estáveis, ou seja, passaram por testes e a maioria dos erros foram corrigidos, sendo assim o sistema se torna bem mais seguro quando utilizado em servidores. Evidentemente, erros novos aparecem continuamente, mas como a Comunidade Debian é bastante ativa, em pouco tempo aparecem as correções.

Por fim, a distribuição Debian é bastante recomendada para as empresas que querem economizar em licenças de softwares e obter suporte sem custo. Além disso, ele suporta diversas arquiteturas de CPU, como, conforme a própria Comunidade Debian, alpha, amd64, armel, hppa, i386, ia64, mips, mipsel, powerpc, s390, e sparc.

4.2 INSTALAÇÃO DO DEBIAN

Os procedimentos de instalação do sistema operacinal Debian 8 podem ser vistos na Apêndice A desta monografia. Apesar da instalação ser bastante interativa e simples, há algumas opções que, sem conhecimento prévio do que é perguntado, podem acarretar em configurações extras sem necessidade na pós-instalação.

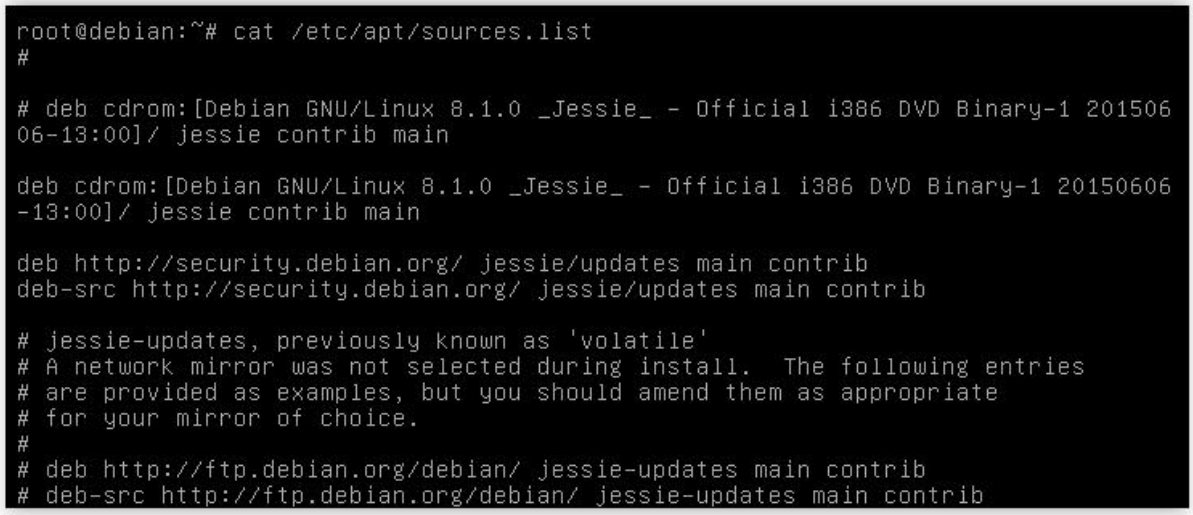
4.3 PÓS-INSTALAÇÃO

Após instalar o sistema operacional Debian no servidor, há algumas configurações que auxiliam o trabalho do administrador de rede e que para isso, é

necessário que sejam feitas antes de iniciar a instalação de pacotes do serviço almejado.

Inicialmente, é recomendado que seja feito a atualização dos pacotes. Com isso, o arquivo que contêm os repositórios oficiais dos pacotes Debian deve ser editado. Por padrão, as configurações que nele constam em um sistema recem instalado são apenas o próprios CD/DVD da instalação e dois repositorios para pacotes de segurança, conforme imagem a seguir.

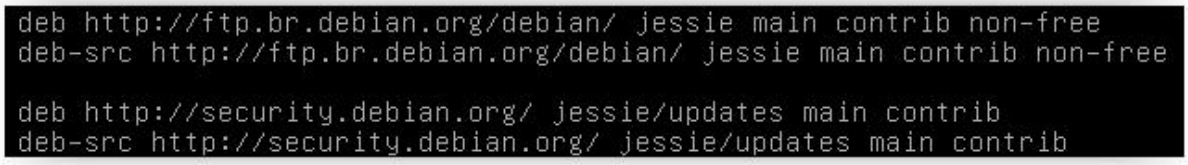
FIGURA 4 – SOURCES.LIST PADRÃO



Fonte: O próprio autor.

O arquivo “source.list” deve conter todos os endereços de repositórios de pacotes que o servidor venha a utilizar. O repositório oficial no Brasil pode ser observado na primeira linha da Figura 5, sendo o http://ftp.br.debian.org/debian/. Neste repositório podemos encontrar todos os pacotes que este trabalho irá mencionar.

FIGURA 5 – SOURCE.LIST PERSONALIZADA



Fonte: O próprio autor.

Um pacote muito útil em servidor Linux é o OpenSSH Server. Esse software permite que o administrador faça conexões via SSH no servidor, habilitando assim o

acesso remoto ao sistema. O SSH é um protocolo utilizado para realizar conexões remotas de forma segura. Conforme a própria equipe de desenvolvedores do programa, a OpenBSD, o OpenSSH encripta todo o tráfego, incluido as senhas, eliminando com eficiência o roubo de informações a partir de ataques de hackers. Inclui também segurança no estabelecimento da conexão, fornecendo um tunel exclusívo em todo o tráfego de dados, suportando ainda todas as versões do protocolo SSH.

Outro passo importante, e comumente não é utilizado, é aplicar regras no firewall interno do servidor. A Debian possue por padrão o firewall Iptables, sem nenhuma regra e com liberação total. Segundo o criador deste firewall, a NetFilter, “o Iptables é uma ferramenta para criar e administrar regras e assim filtrar pacotes de redes”.

Com o Iptables podemos filtrar as conexões entrantes no servidor, os pacotes que passam por ele, tradução de endereços com *NAT*, entre outras diversas opções. As regras que devem ser aplicadas no servidor dependem da política de segurança da empresa. Mesmo assim, uma opção é permitir apenas conexões para o servidor nas portas dos serviços instalados. Por exemplo, um servidor Apache, que utiliza a porta 80, não necessita da porta 53 liberada, visto que essa porta é utilizada pelo DNS.

Segundo a CERT.BR, “um sistema mais seguro começa pela instalação do mínimo possível de pacotes e componentes, especialmente os que implementam serviços de rede”. Este mínimo depende fundamentalmente do propósito do sistema em questão e do ambiente de rede no qual ele está inserido. Ainda:

> A justificativa para esta recomendação é bastante simples. É comum que serviços não utilizados não sejam monitorados por falhas de segurança, o que aumenta a possibilidade de não ser aplicada uma correção necessária. A redução no número de pacotes instalados diminui a chance de que o sistema possua uma vulnerabilidade que possa vir a ser explorada por um atacante.

Portanto, remover pacotes desnecessários no sistema podem aumentar a segurança do servidor contra ataques de hackers. Principalmente se os pacotes são utilizados no processo de invasão.

Exemplos de pacotes que podem facilicar o trabalho do hacker é o compilador de códigos na linguagem C, como o “gcc”. Caso não haja nenhum aplicativo que utilize o compilador, a recomendação é que seja removido do sistema.

Outro pacote que auxilia uma invação é o “NetCat” e o “Wget”. Este segundo é um software utilizado para fazer downloads de arquivos. Um hacker pode utiliza-lo para baixar algum script para seu servidor de forma válida, caso o pacote esteja instalado. Já o primeiro é uma ferramenta usada para ler e escrever dados em conexões de rede usando o protocolo TCP/IP. Dada sua grande flexibilidade, o Netcat é considerado pelos hackers o “canivete suíço” do TCP/IP, podendo ser usado para fazer desde leituras de portas abertas até ataques de força bruta.

Por fim, realizar atualizações periódicas no servidor, configurar um firewall, remover pacotes nocivos e configurar o servidor para acesso remoto são boas práticas a serem realizadas em servidores linux, facilitando o trabalho do administrador de redes e aumento a segurança contra invasões de hackers.

5 INSTALAÇÃO E CONFIGURAÇÃO DE DNS

Este capítulo tem como objetivo mostrar a simplicidade na instalação de um serviço em sistemas Linux e procura também explicar as opções de configurações nos arquivos de configuração do servidor DNS.

5.1 INSTALAÇÃO DE DNS

O servidor DNS escolhido foi o bind por ser um dos mais populares servidores DNS e também por ser software livre, ou seja, não há necessidade de pagar licenças de uso. Na figura a seguir, podemos observar o comando utilizado para a instalação do pacote “bind9”.

FIGURA 6 – COMANDO INSTALAÇÃO BIND

Fonte: O próprio autor.

5.2 CONFIGURAÇÃO DE DNS

Nessa seção iremos comentar sobre as opções dos arquivos de configuração que pode ser visto na Apêndice B deste trabalho. O arquivo deste trabalho deve ser utilizado apenas para servidores DNS internos, ou seja, não são servidores acessados pela Internet, apenas pela rede local.

Inicialmente faça um backup dos arquivos que iremos trabalhar com os comandos abaixo:

- ***cp named.conf named.conf-bkp***
- ***cp named.conf.options named.conf.options-bkp***
- ***cp named.conf.local named.conf.local-bkp***

Os arquivos podem ser encontrados no diretório “/etc/bind/”. Após isso é podemos limpar o arquivo de configuração e incluir as opções de acordo com a necessidade e conforme a rede local. Segue os itens e suas respectivas descrições do arquivo “named.conf”:

• include “/etc/bind/named.conf.options”: Realiza a inclusão do conteúdo do arquivo “named.conf.options” no arquivo “named.conf”.

• view “interna”: A clausula vier permite o bind prover diferentes funcionalidades para um grupo de clientes. Neste caso há apenas uma view englobando todos os clientes, mas podemos configurar funcionalidades diferentes para redes distintas..

• match-clients { any; }: Este parâmetro define quem pode utilizar este servidor como DNS. Neste caso foi definido qualquer um.

• include “/etc/bind/named.conf.default-zones”: Realiza a inclusão do conteúdo do arquivo “named.conf.default-zones” no arquivo “named.conf”.

• include “/etc/bind/named.conf.local”: Realiza a inclusão do conteúdo do arquivo “named.conf.local” no arquivo “named.conf”.

• logging: As configurações que estão inclusas no parâmetro “logging” são utilizadas para a realização de resolução de problemas. Utilizar apenas quando necessário devido a grande quantidade de logs que são gerados.

Segue os itens e suas respectivas descrições do arquivo “named.conf.options”:

• options: Inicio das opções do DNS.

• directory: Esse parâmetro indica o diretório que estarão os arquivos de zona.

• forwarders: Incluiremos neste item os IPs dos servidores DNS externos. Esses são servidores públicos que traduzem as páginas da Internet.

• auth-nxdomain no: define se o server será autoritativo.

• listen-on-v6: No arquivo desativamos as consultas de IPv6 com a opção “none”.

• listen-on: Define em qual porta e IP que o Bind vai receber as consultas.

• version: Essa opção é utilizada como forma de segurança, evitando que seja divulgada a versão do bind utilizado. Ao impedir a divulgação da versão do bind, evitasse a situação de um usuário mal-intencionado descobrir a versão utilizada e buscar vulnerabilidades da versão, evitando assim ataques hackers.

• allow-query: Nesta lista teremos as redes que podem requisitas consultas DNS.

• allow-recursive: Incluir as redes que podem fazer consultas no DNS para zonas que o servidor não conheça.

• blackhole: Incluir nesta lista os IPs que não poderão utilizar o servidor como DNS.

• allow-transfer: Incluir nesta lista os servidores DNS secundários que podem solicitar a transferência de zonas. Restringir as solicitações de transferência de zonas maximiza a segurança do servidor, impedindo que um hacker tenha acesso a todos os endereços dos servidores cadastrados nas zonas.

Segue os itens e suas respectivas descrições do arquivo “named.conf.local”:

• zone “filial01.com.br”: Inicio das configurações de uma zona. Indica o nome de domínio.

• type master: Informar que o servidor é do tipo primário para essa zona.

• file “filial01.com.br”: Informa o nome do arquivo da zona. Este arquivo deve estar na pasta “/var/cache/bind”, conforme a configuração do arquivo “named.conf.options” na opção “directory”.

O próximo arquivo encontrado na Apêndice B é um exemplo de uma zona. Existem ainda outras diversas opções no DNS. Os arquivos apresentados são apenas exemplos.

6 INSTALAÇÃO E CONFIGURAÇÃO DE DHCP

Este capítulo tem como objetivo mostrar a simplicidade na instalação de um serviço em sistemas Linux e procura também explicar as opções de configurações no arquivo de configuração do servidor DHCP.

6.1 INSTALAÇÃO DE DHCP

O servidor DHCP escolhido foi o ISC DHCP por ser um dos mais populares servidores DHCP e também por ser software livre, ou seja, não há necessidade de pagar licenças de uso. Na figura a seguir, podemos observar o comando utilizado para a instalação do pacote “isc-dhcp-server”.

FIGURA 7 – COMANDO INSTALAÇÃO DHCP

Fonte: O próprio autor.

6.2 CONFIGURAÇÃO DE DHCP

Nessa seção iremos comentar sobre as opções de um arquivo de configuração que pode ser visto na Apêndice C deste trabalho.

Inicialmente faça um backup do arquivo padrão do DHCP com o comando ***cp dhcpd.conf dhcpd.conf-bkp***,encontrado em “/etc/dhcp/”. Após isso, podemos limpar o arquivo de configuração e incluir as opções de acordo com a necessidade e conforme a rede local. Segue os itens e suas respectivas descrições:

• option domain-name-servers 8.8.8.8: Nesta opção informamos qual ou quais são os servidores de DNS que os dispositivos vão utilizar.

• option ntp-servers ntp.com.br: Nesta opção informamos qual servidor NTP .

• default-lease-time 604800: Tempo de empréstimo, em segundos, em que os clientes ficam com o endereço IP.

• max-lease-time 604800: Caso o cliente solicite um tempo maior, será informado esse novo tempo.

• authoritative: Essa opção.

• deny declines: Uma opção de segurança que evita um cliente enviar excessivas requisições DHCPDECLINE, ocasionando um *DoS* (*Deny of Service* ou, em português, Ataque de Negação de Serviço).

• deny unknown-clients: Outra opção de segurança, sendo que está nega a alocação de endereço IP para os clientes que não estejam previamente cadastrados no arquivo de configuração com o endereço físico correspondente. Essa opção é recomendada para evitar que dispositivos não autorizados tenham acesso à rede. Não utilize essa opção caso não seja necessário, já que ela acarreta em um trabalho extra para o administrador de rede ao cadastrar novos dispositivos de rede.

As opções que foram comentadas acima são interpretadas de maneira geral para todo o serviço de DHCP. As opções a seguir são configurações específicas para cada rede, visto que apenas um servidor DHCP pode alocar endereços para diversas redes, mas para isso o gateway da rede deve estar configurado para encaminhar as requisições DHCP de outras redes para o servidor em questão.

• subnet 10.0.0.0 netmask 255.255.255.0: Nesta opção estamos informando o endereço da rede e a máscara que será informada para os dispositivos.

• option domain-name seudominio.com.br: Informe o nome do domínio da sua rede, se houver.

• option routers 10.0.0.1: Informe o endereço do gateway da rede. Normalmente este é o endereço do roteador que faz a ligação para outras redes.

• range 10.0.0.11 10.0.0.254: Informe o intervalo de endereços IPs que serão alocados. Neste exemplo deixamos os dez primeiros endereços fora do intervalo para que estes sejam configurados estaticamente em servidor ou dispositivos de rede.

Não podemos esquecer que as opções de domínio, gateway e intervalo da rede devem ficar entre os símbolos colchetes, pois estes representam as opções da rede.

Na Apêndice D deste trabalho será mostrado um exemplo de arquivo de configuração de dois servidores DHCP, um primário e outro secundário. Não iremos abordar as configurações necessárias para que os dois servidores fiquem em sincronismo. Nele também haverá um exemplo de como devemos configurar o cliente quando utilizamos a opção “deny unknown-clients”. Existem ainda outras diversas opções no DHCP. Os arquivos apresentados são apenas exemplos.

7 INSTALAÇÃO E CONFIGURAÇÃO DE APACHE

Este capítulo tem como objetivo mostrar a simplicidade na instalação de um serviço em sistemas Linux e procura também explicar as opções de configurações nos arquivos de configuração do servidor Web.

7.1 INSTALAÇÃO DE APACHE

O servidor WEB escolhido foi o Apache por ser um dos mais populares servidores Web e também por ser software livre, ou seja, não há necessidade de pagar licenças de uso. Na figura a seguir, podemos observar o comando utilizado para a instalação do pacote “apache2”.

FIGURA 8 – COMANDO INSTALAÇÃO APACHE

Fonte: O próprio autor.

7.2 CONFIGURAÇÃO DE APACHE

O Apache não requer configuração adicional para funcionar como servidor Web, basta apenas incluir o site na pasta “/var/www/” e o site já estará funcionando. Evidentemente, caso o site tenha alguma linguagem específica, como PHP, Java ou tenha conexões LDAP, será necessário a instalação de um pacote um adicional no Linux.

Para instalar o PHP no servidor, basta utilizar o comando apresentado na Figura 9.

FIGURA 9 – COMANDO INSTALAÇÃO PHP

Fonte: O próprio autor.

Na Figura 10, podemos ver como instalar a exteção do PHP com o banco de dados MySQL e LDAP.

FIGURA 10 – COMANDO INSTALAÇÃO EXTENÇÕES PHP

Fonte: O próprio autor.

Para verificar outras exteções do pacote PHP, basta utilizar o comando apresentado na Figura 11. Neste comando será apresentado todas as exteções possíveis e suportadas pelo PHP da distribuição.

FIGURA 11 – COMANDO PESQUISAR OUTRAS EXTENÇÕES

Fonte: O próprio autor.

O Apache, por padrão, possuí algumas directivas não consideradas muito seguras. No arquivo “security.conf”, encontrado no diretório “/etc/apache2/conf.d/” no Debian 7 e no diretório /etc/apache2/conf-available/” no Debian 8, há duas opções que devem ser configuradas para deixar o servidor Web mais seguro. Segue abaixo as directivas e a descrição sobre ela. Elas podem ser encontradas na Apêndice E deste trabalho.

• ServerTokens Prod: Esse item informa quais informações o servidor Web vai divulgar sobre ele. A opção “Prod” informar apenas que é um servidor Apache. Há outras três opções que informa a versão do software, sistema operacional e os módulos instalados.

• ServerSignature Off: Essa opção omite o Apache de mostrar sua versão em casos de erros. Por padrão o item vem habilitada com “On”.

As opções acima deixam o servidor mais seguro, pois omite informações importantes utilizadas em uma invasão. Para aumentar a segurança do Apache para ataques de hacker devesse habilitar módulos de seguranças com o comando “a2enmod”. Outro pacote utilizado para aumentar a segurança do Apache é o “libapache2-mod-security2”. Apesar de não ser foco desta monografia, recomendamos a instalação do pacote e configuração do mesmo posteriormente.

Por fim, outra configuração que aumenta a segurança do servidor é a inclusão da directiva “Options – Indexes” no arquivo “apache2.conf”, encontrado em “/etc/apache2”. Essa opção não permite o servidor Web listar os diretórios do site.

8 INSTALAÇÃO E CONFIGURAÇÃO DE PROXY

Este capítulo tem como objetivo mostrar a simplicidade na instalação de um serviço em sistemas Linux e procura também explicar as opções de configurações no arquivo de configuração do servidor proxy.

8.1 INSTALAÇÃO DE PROXY

O servidor proxy escolhido foi o Squid por ser um dos mais populares servidores proxy e também por ser software livre, ou seja, não há necessidade de pagar licenças de uso. Na figura a seguir, podemos observar o comando utilizado para a instalação do pacote “squid3”.

FIGURA 12 – COMANDO INSTALAÇÃO SQUID

Fonte: O próprio autor.

8.2 CONFIGURAÇÃO DE PROXY

Ao invés de abordar todas as linhas de configuração do Squid, já que há comentários em cada uma das linhas no arquivo de configuração encontrado na Apêndice F, iremos tratar o funcionamento do serviço e como funciona a lógica das regras.

Inicialmente, o Squid realiza a leitura das linhas do arquivo de configuração em ordem sequencial, ou seja, da primeira até a última. Assim, a cada requisição, se o pacote enquadrar-se em alguma regra, é verificando a condição do mesmo, bloqueando ou permitindo. No final do arquivo há uma regra que enquadra todos os pacotes, assim, caso nenhuma regra condiz, é utilizado essa regra, novamente, permitindo ou bloqueando.

Para criação de regras, é utilizado as cláusulas “acl” e http_access”, onde a primeira cria a regra e a segunda é configurado como o Squid deve tratar essa regra.

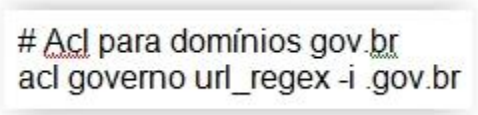
As ACLs podem ser organizadas das duas formas abaixo:

• acl NOME_DA_ACL TIPO_DE_ACL parâmetro

• acl NOME_DA_ACL TIPO_DE_ACL “/caminho/completo/arquivo”

Na primeira regra é definido todos os parâmetros em sequência, separando os por espaço e utilizado para regras com poucos parâmetros. Como o exemplo da imagem a seguir, que cria uma ACL para os domínios “gov.br”, ou seja, todos os sites que tem o domínio *.gov.br*:

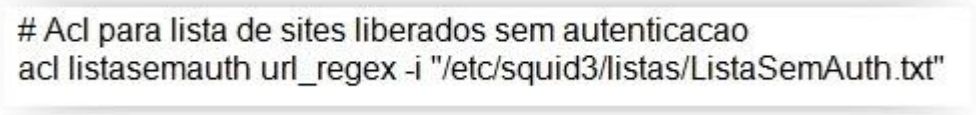
FIGURA 13 – ACL SQUID 1



Fonte: O próprio autor.

Na segunda regra é definido um arquivo para adição dos parâmetros linha a linha, ou seja, é informado todas as opções em um arquivo. As requisições são repassadas em todas as linhas para checagem. Abaixo há um exemplo dessa regra:

FIGURA 14 – ACL SQUID 2



Fonte: O próprio autor.

Todas as ACLs são tratadas com CASE-SENSITIVE, ou seja, letras maiúsculas e minúsculas são consideradas diferentes. Para desativar isso utilizamos a opção *-i* logo após o tipo de ACL.

Após criar uma ACL, é necessário, para que ela funcione, que seja criado uma regra “http_access”, informando a ação a se tomada. A organização básica da regra deve ser conforme abaixo e as opções de ação são de permitir (allow) ou negar (deny):

• HTTP_access ação NOME_DA_ACL

No exemplo da Figura 15 é informado dois nomes de ACLs. Neste caso a regra funciona permitindo o acesso da primeira ACL ao itens da segunda ACL.

FIGURA 15 – REGRA SQUID 1

Fonte: O próprio autor.

Há a possibilidade de usar o caracter ! (exlamação) na frente do nome da ACL. Essa opção nega a ACL, ou seja, caso a segunda ACL da regra a Figura 15 tivsse um ponto de exclamação, o Squid entenderia a regra como liberando a primeira ACL, exceto a segunda ACL.

Enfim, a lista de opções que o software Squid permite no arquivo de configuração é extença, podendo ser assunto de um trabalho futuro. O objetivo deste trabalho é mostrar o funcionando geral deste Proxy e exemplificando algumas regras.

9 CONCLUSÃO

Com a execução de um estudo com embasamento teórico, englobando manuais dos softwares, comunidades de programadores, empresas que tem como finalidade o desenvolvimento e divulgação de softwares livre, e aplicando esse conhecimento na prática, podemos obter sucesso na implantação de servidores em uma rede de computadores totalmente baseados em softwares livre, desde os aplicativos até o sistema operacional.

Aplicar uma arquitetura de software livre requer, inicialmente, um maior conhecimento e estudo do administrador da rede. Apesar de não ser um requisito, é importante que o responsável pelos servidores busque manuais e comunidades dos softwares, no objetivo de obter conhecimentos avançados. A importância disso é devido a não haver suporte de manutenção nos sistemas estudados neste trabalho. O que existe é uma comunidade de voluntários que respondem quando um administrador de redes expõe seu problema ou dúvida. Porém, totalmente de graça.

Com isso, pode-se constatar que aplicar tecnologias de softwares livre são ideais para empresas que querem economizar em licenças e suportes. Ideais também para os administradores de redes que sentem a necessidade de poder customizar seus serviços de redes conforme as características da empresa, já que todos os softwares apresentados são utilizados tanto para empresas de grande porte e empresa de pequeno porte.

Finalmente, apesar de inicialmente parecer mais um manual de aplicativos baseados em softwares livre, foi possível aprender que os conhecimentos de como esses serviços funcionam e sua utilidade em uma rede de computadores ou até a Internet são importantes no momento do planejamento de como se deve configurar e quais opções serão habilitadas, visto que todos os softwares apresentados possuem diversas diretrizes que não são apresentadas no arquivo de configuração padrão, cabendo ao responsável pela rede de dados o trabalho de estudo e pesquisa e escolha do que se deve aplicar.

REFERÊNCIAS

ALVES, Jesulino. 15 Motivos Para Utilizar Linux em casa, no Trabalho e na Escola. Disponível em: < http://softwarelivre.org/mslguarulhos/software-livre-quer-um-motivo-para-usar-linux-te-damos-15> Acesso: 14 ago. 2015.

BRASIL ESCOLA. História do Linux. Disponível em: <http://www.brasilescola.com/informatica/historia-do-linux.htm> Acesso: 09 ago. 2015.

CERT.BR. Práticas de Segurança para Administradores de Redes Internet. 2003. Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#subsec3.2> Acesso: 09 ago. 2015.

DELL COMPUTADORES DO BRASIL LTDA. O que é Servidor. Disponível em: <http://www.dell.com/learn/br/pt/brbsdt1/sb360/what-is-a-server> Acesso: 09 ago. 2015.

FREE SOFTWARE FOUDATION. Disponível em: < http://www.fsf.org/> Acesso: 14 ago. 2015.

INTERNET LIVE STATS. Total Numbers of Websites. Disponível em: <http://www.internetlivestats.com/> Acesso: 12 ago. 2015.

GLOBO. Dê adeus à licença. Disponível em: <http://revistapegn.globo.com/Revista/Common/0,,EMI81077-17156,00-DE+ADEUS+A+LICENCA.html/> Acesso: 14 ago. 2015.

MICROSOFT CORPORATION. O que é um servidor Proxy?. Disponível em: <http://windows.microsoft.com/pt-br/windows-vista/what-is-a-proxy-server> Acesso: 12 ago. 2015.

MORIMOTO, CARLOS E.DHCP. 2005. Disponível em: <http://www.hardware.com.br/termos/dhcp> Acesso: 12 ago. 2015.

MORIMOTO, CARLOS E. Linux Guia Prático - (Atualização Capitulo 8 Final). 2009. Disponível em: <http://www.hardware.com.br/livros/linux/entendendo-diretorios.html> Acesso: 13 ago. 2015.

MORIMOTO, CARLOS E.. Proxy (Servidor). 2005. Disponível em: <http://www.hardware.com.br/termos/proxy-servidor> Acesso: 12 ago. 2015.

MORIMOTO, CARLOS E. Servidores Linux – Guia Prático. Porto Alegre: Sul Editores, 2011.

NETFILTER. The netfilter.org "iptables" project. Disponível em: <http://www.netfilter.org/projects/iptables/Acesso: 12 ago. 2015.

NTPBR. O NTP. Disponível em: <http://www.ntp.br/ntp.php> Acesso: 11 ago. 2015.

OPENBSD. OpenSSH. Disponível em: < http://www.openssh.com/> Acesso: 12 ago. 2015.

UNIX-AG.Apt-Cacher NG. Disponível em: <https://www.unix-ag.uni-kl.de/~bloch/acng/ > Acesso: 11 ago. 2015.

SAMBA. Learning the Samba. Disponível em: <https://www.samba.org/samba/docs/using_samba/ch01.html> Acesso: 13 ago. 2015.

SIGNIFICADOS. O que é DNS. Disponível em: <http://www.significados.com.br/dns/> Acesso: 11 ago. 2015.

SHALLA SECURE SERVICES KG. Welcome to squidGuard. Disponível em: <http://www.squidguard.org/> Acesso: 12 ago. 2015.

SOFTWARE IN THE PUBLIC INTEREST. Uma Breve História do Debian. Disponível em: <https://www.debian.org/intro/why_debian.pt.html > Acesso: 09 ago. 2015.

SOFTWARE IN THE PUBLIC INTEREST. Razões para Escolher o Debian. Disponível em: <https://www.debian.org/doc/manuals/project-history/ch-intro.pt.html> Acesso: 12 ago. 2015.

SOFTWARE LIVRE BRASIL. Servidor Web Apache. Disponível em: <http://softwarelivre.org/php/servidor-web-apache/> Acesso: 14 ago. 2015.

REGISTRO DE DOMÍNIOS. Servidor de Nome de Domínio - DNS. Disponível em: <http://www.registrodedominios.net.br/dominios/servidor-de-nome-de-dominio-dns.html/> Acesso: 11 ago. 2015.

W3SCHOOLS. Browser Statistics. Disponível em: <http://www.w3schools.com/browsers/browsers_stats.asp> Acesso: 11 ago. 2015.

W3TECHS. Usage statistics and market share of Linux for websites. Disponível em: <http://w3techs.com/technologies/details/os-linux/all/all> Acesso: 09 ago. 2015.

W3TECHS. Usage of web servers for websites. Disponível em: <http://w3techs.com/technologies/overview/web_server/all> Acesso: 11 ago. 2015.

GLOSSÁRIO

Active Directory – O Active Directory é uma implementação de serviço de diretório no protocolo LDAP que armazena informações sobre objetos em rede de computadores e disponibiliza essas informações a usuários e administradores desta rede. É um software da Microsoft utilizado em ambientes Windows..

DHCP – O DHCP, Dynamic Host Configuration Protocol (Protocolo de configuração dinâmica de host), é um protocolo de serviço TCP/IP que oferece configuração automática de endereçamento para dispositivos em uma rede de dados.

Distribuição Linux – Uma Distribuição Linux (ou simplesmente distro) é um sistema operacional baseado no núcleo Linux.

Download – Transferir (baixar) um ou mais arquivos de um servidor remoto para um computador local.

Firewall – É um software ou um hardware que verifica informações provenientes da Internet ou de uma rede, e as bloqueia ou permite que elas cheguem ao seu computador, dependendo das configurações do firewall.

Hacker – é uma palavra em inglês do âmbito da informática que indica uma pessoa que possui interesse e um bom conhecimento nessa área, sendo capaz de fazer hack (uma modificação) em algum sistema informático..

LDAP – Lightweight Directory Access Protocol, ou LDAP, é um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede de Protocolo da Internet.

MySQL – É um sistema gerenciador de banco de dados de código aberto usado na maioria das aplicações gratuitas e utiliza a linguagem SQL.

Protocolo – É um conjunto de regras e procedimentos a respeitar para emitir e receber dados numa rede.

Repositório – Um repositório de software é um local de armazenamento de onde pacotes de software podem ser recuperados e instalados em um computador.

Roteador – Dispositivo que permite duas ou mais redes distintas se comunicarem.

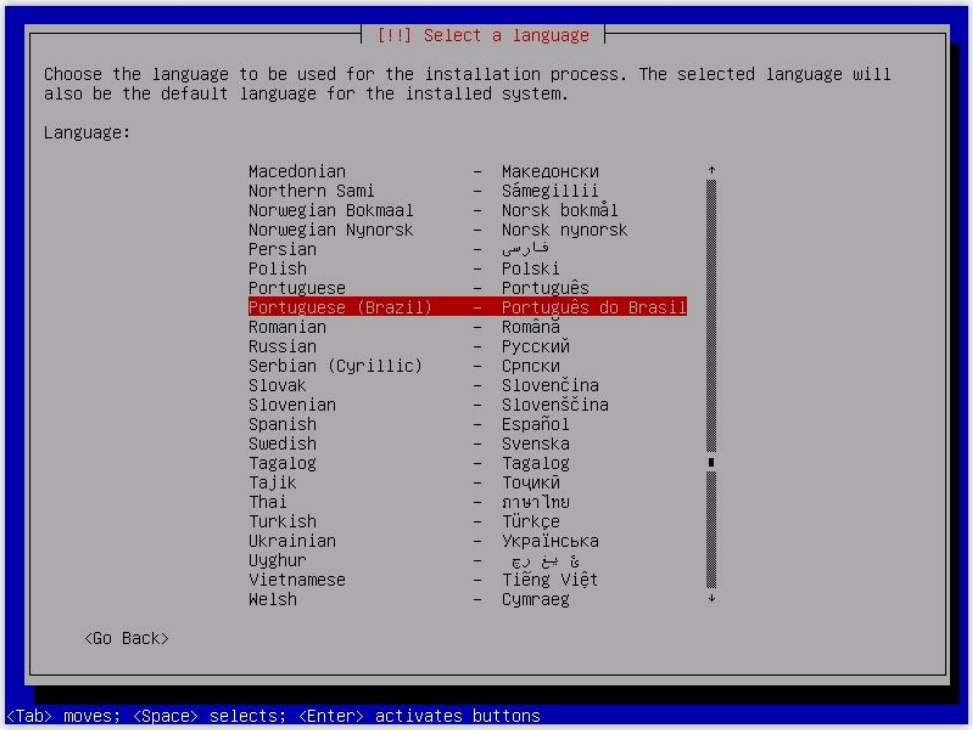
Swithces – É um equipamento que interliga os computadores em uma mesma rede.

APÊNDICE A – MANUAL DE INSTALAÇÃO DEBIAN

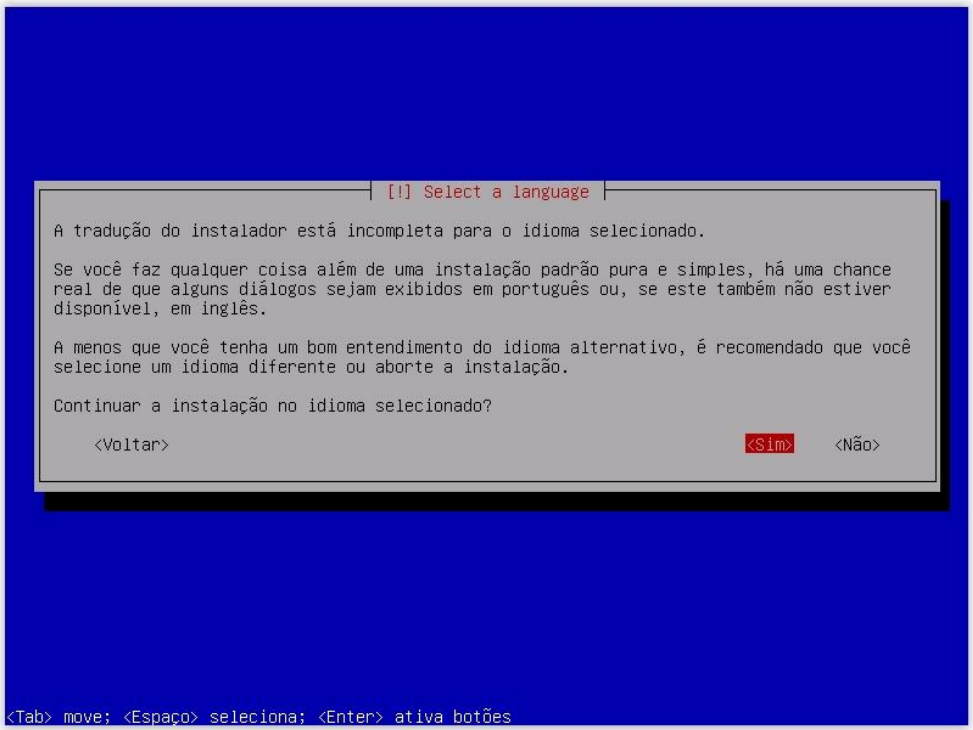
Inicialmente, configure seu computador para realizar o boot na mídia no qual estão os arquivos de instalação do Debian. Após isso, siga os passos para realizar a instalação do sistema operacional Debian 8:

1 – Há duas opções principais de instalação. Ambas são gráficas, porém a opção “Graphical install” possum um layout mais amigável. Este manual irá mostrar o modo gráfico mais simples, sendo a primeira opção, conforme a imagem:

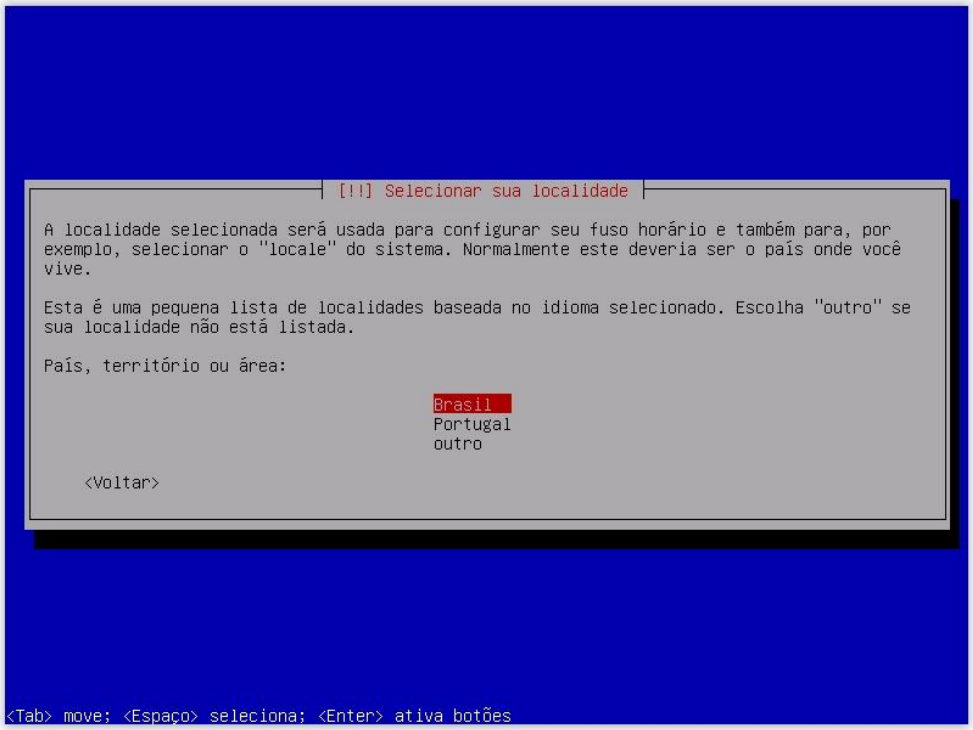
2 – Selecione o idioma Português do Brasil:



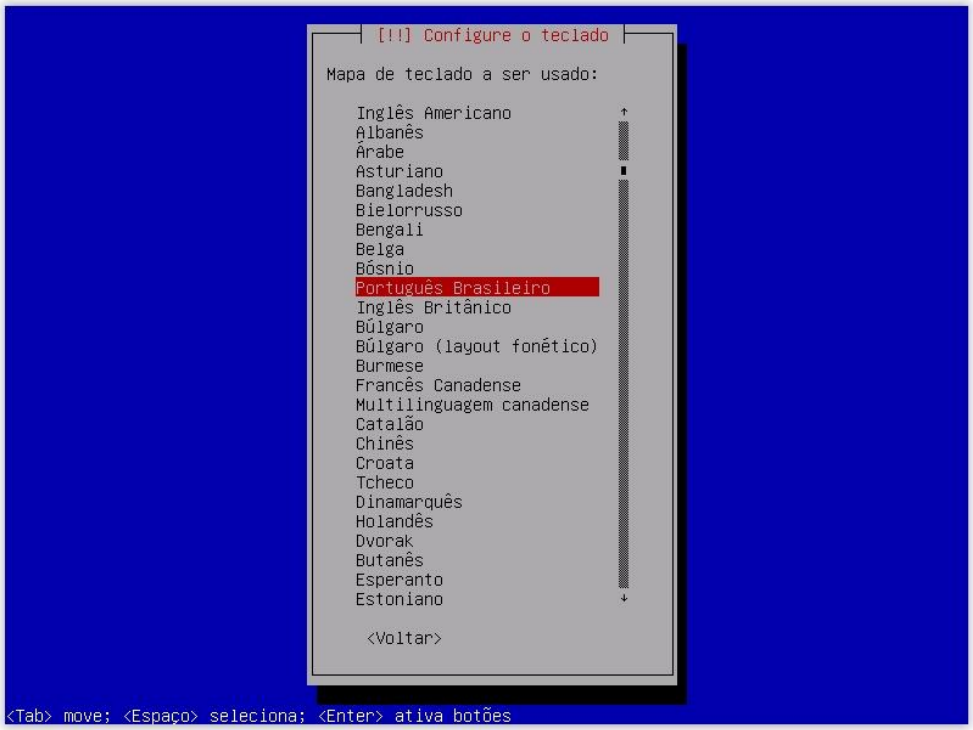
3 – A próxima tela informa que nem todo sistema ainda está traduzido para o Português do Brasil, sendo assim, quando não houver tradução, será mostrado os textos em inglês. A tradução do sistema é feita gradativamente, e com o tempo é disponibilizado pacotes de atualização com as traduções. Sendo assim, escolhemos a opção “Sim”, para continuar com o idioma selecionado posteriormente:



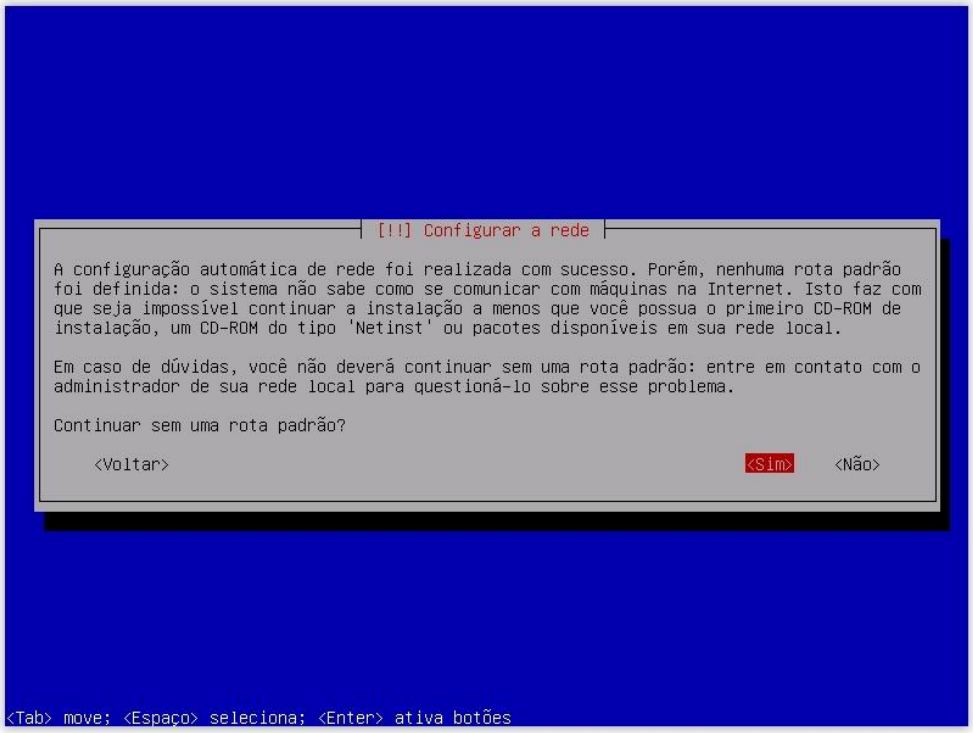
4 – Selecione o País da sua localidade:



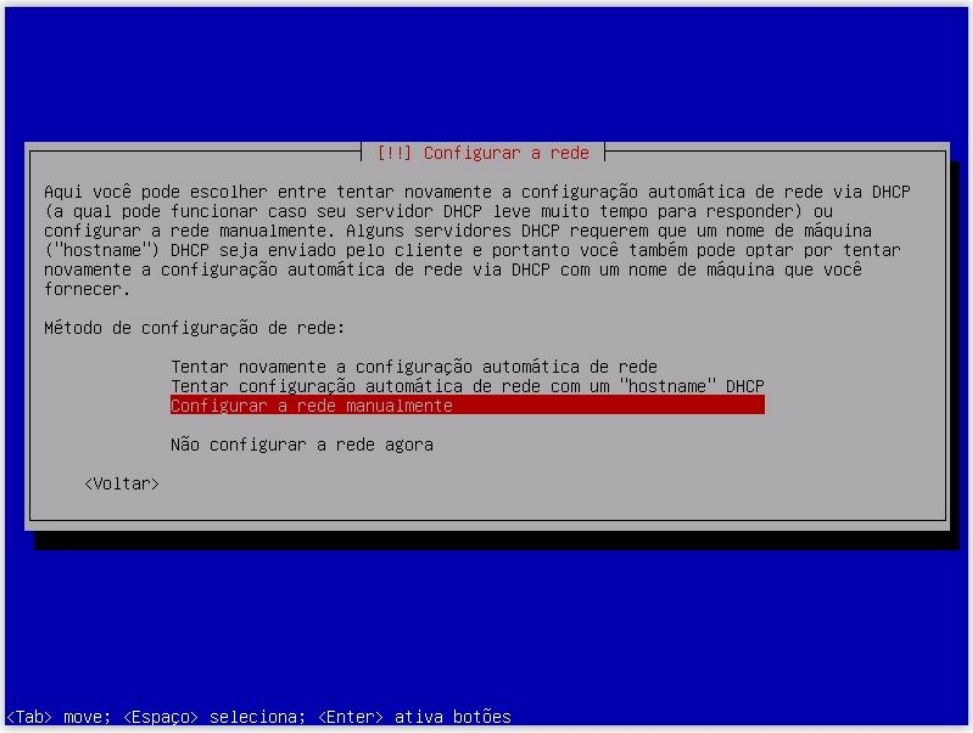
5 – Selecione o padrão do teclado utilizado:



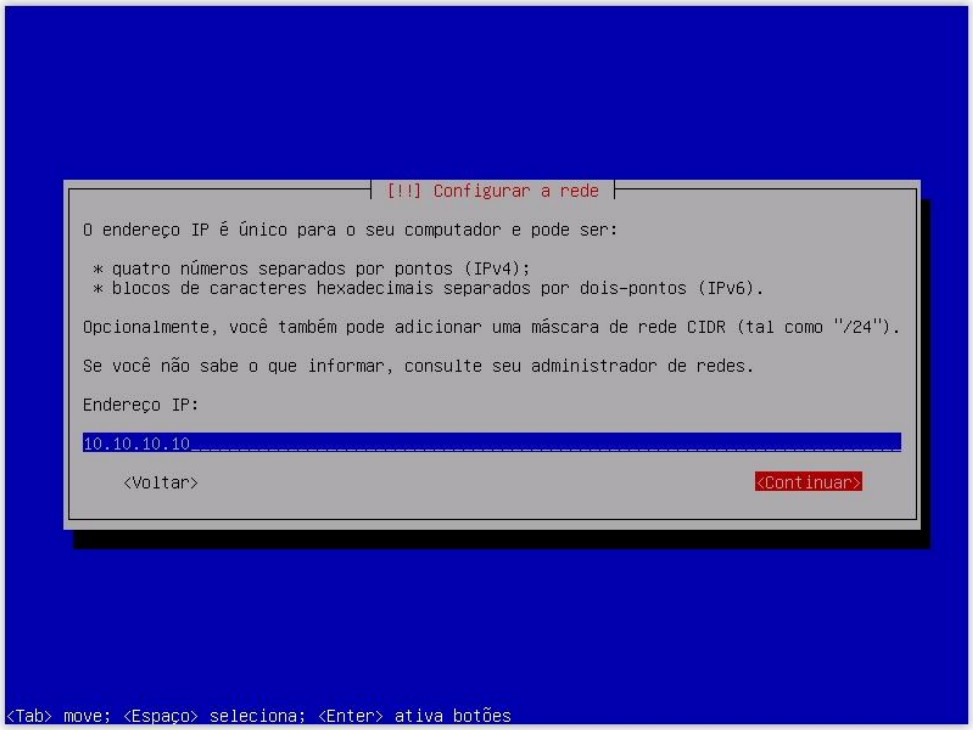
6 – Será feito a leitura da mídia e o carregamento de componente adicionais. Após isso, a instalação tentará alocar um IP automaticamente através de um servidor DHCP. Caso você já tenha um servidor DHCP configurado na sua rede, pule para o passo 12, caso contrário, siga os passos para configurar o endereçamento de rede manualmente. Selecione a opção “Sim”:



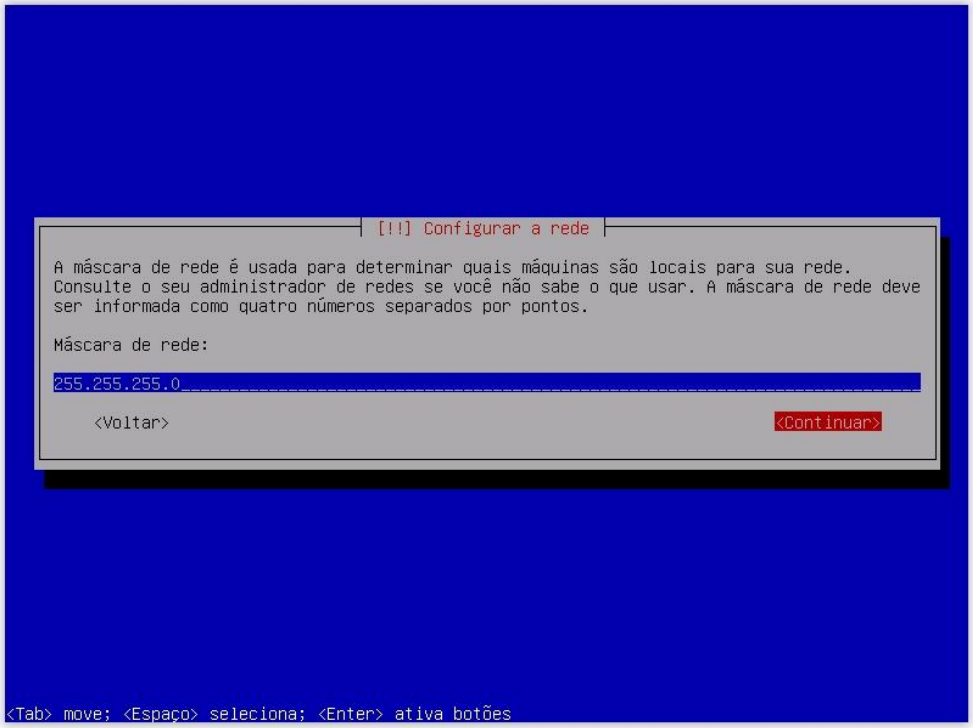
7 – Selecione a opção “Configurar a rede manualmente”:



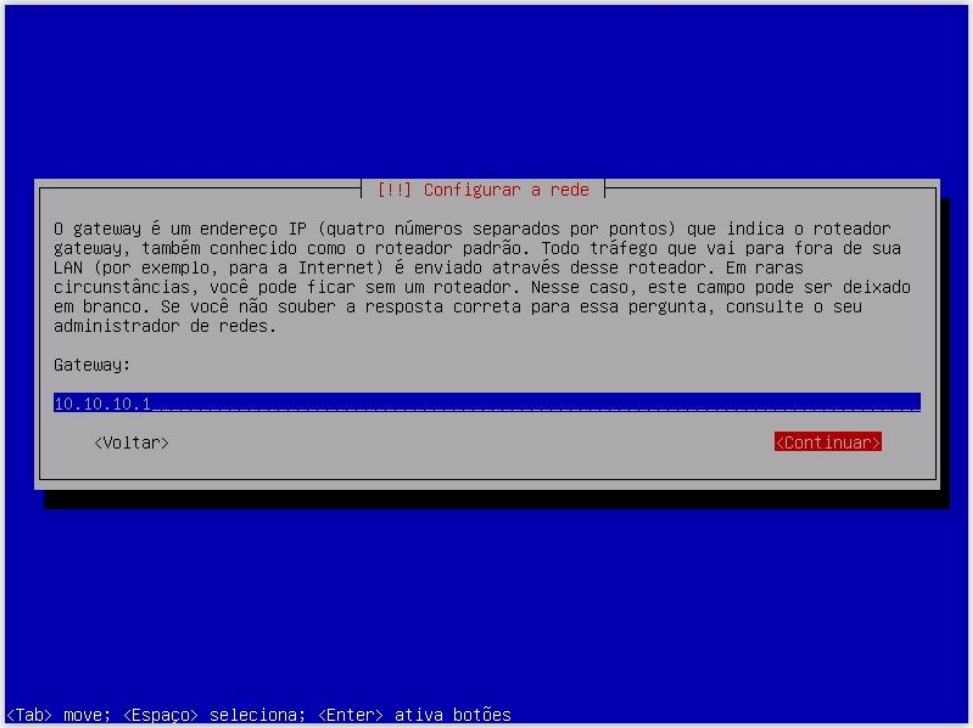
8 – Informe o endereço IP do sistema que está sendo instalado. Nessa opção você já pode informar a máscara de rede utilizando o prefixo da máscara, conforme informado na imagem:



9 – Informe a máscara de rede:

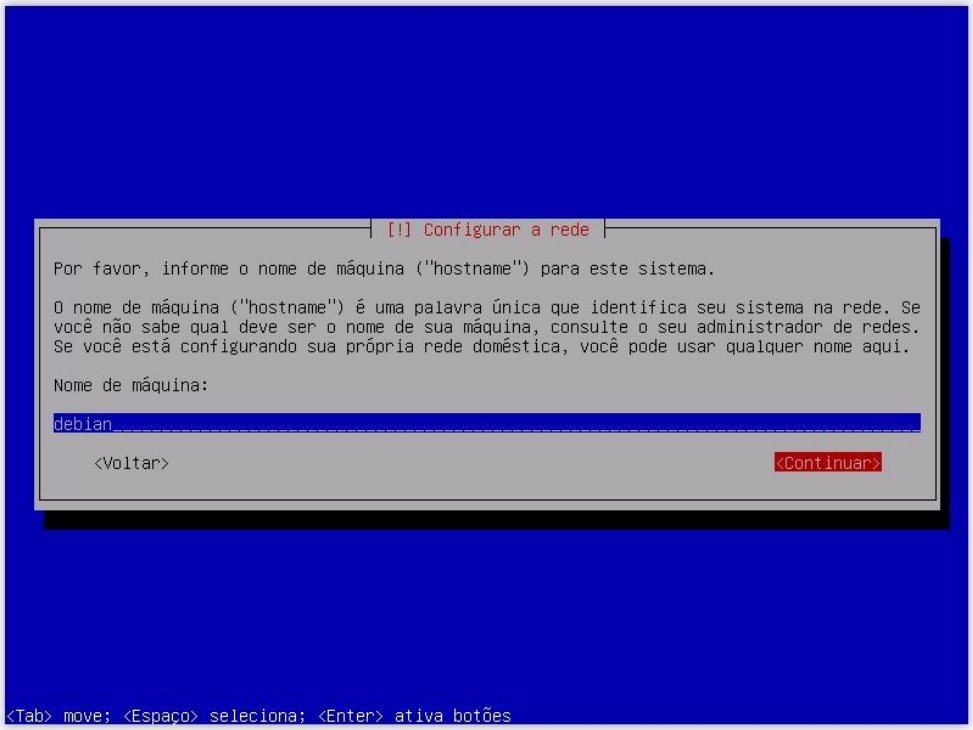


10 – Informe o endereço IP do Gateway padrão. Esse é normalmente o endereço do roteador da rede:

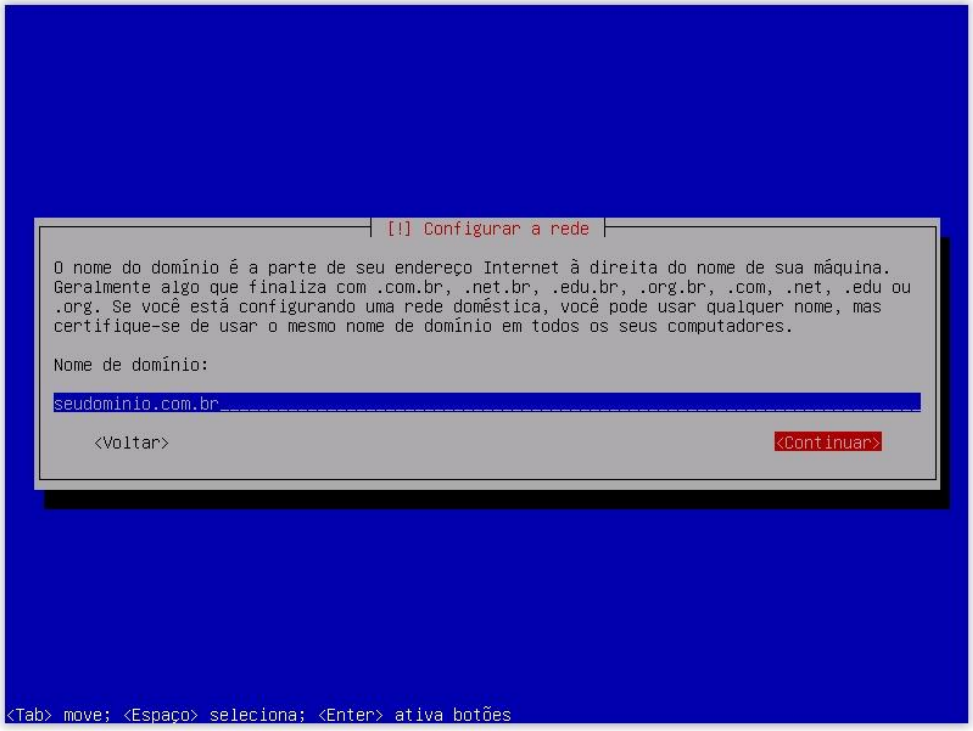


11 – Informe o endereço IP do DNS. Caso você não tenha um servidor DNS configurado na rede, informe um endereço de DNS de um servidor público, como exemplo o 8.8.8.8 da Google:

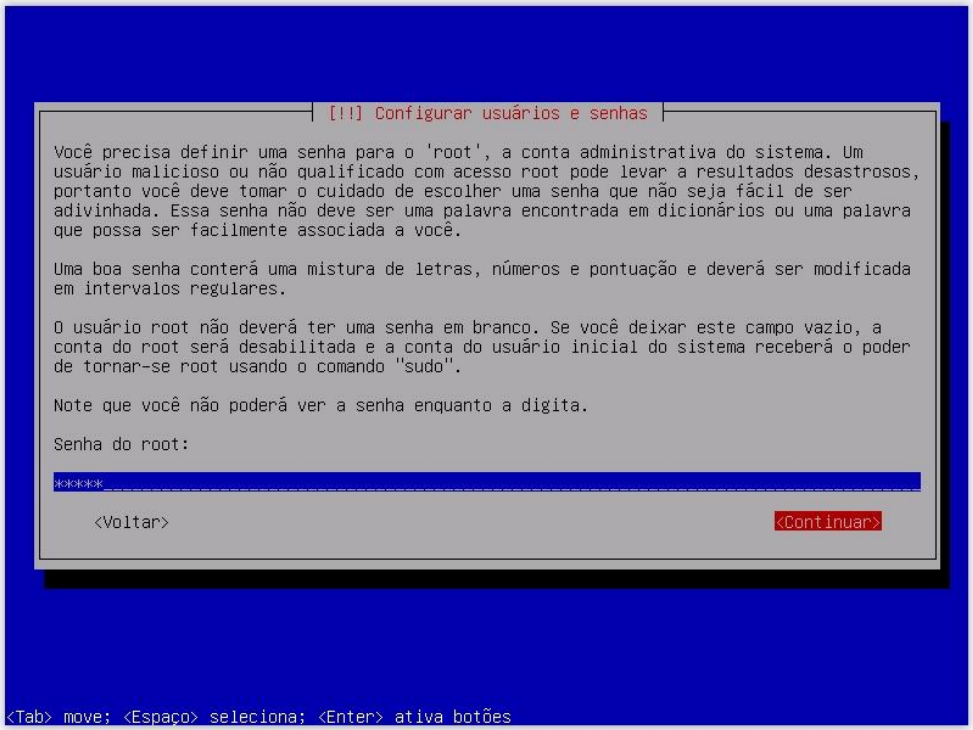
12 – Informe o nome da máquina. Caso seja um servidor, utilize algum nome que seja fácil de identificar a função dele na rede. Como exemplo: servidor-web, caso seja um servidor Apache:



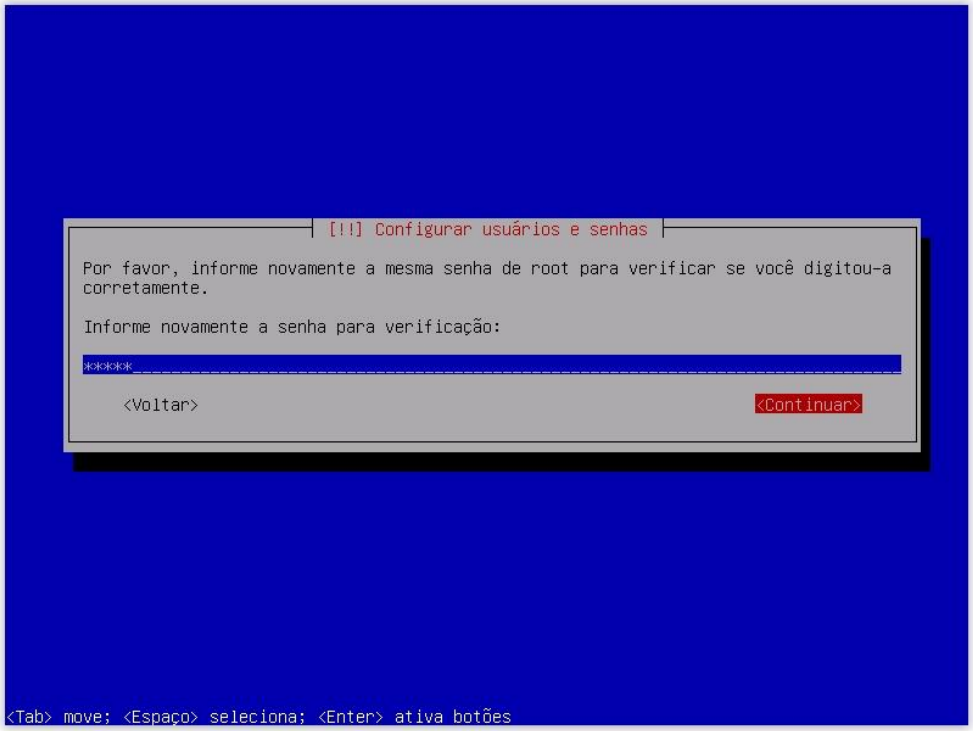
13 – Informe o nome do domínio da rede:



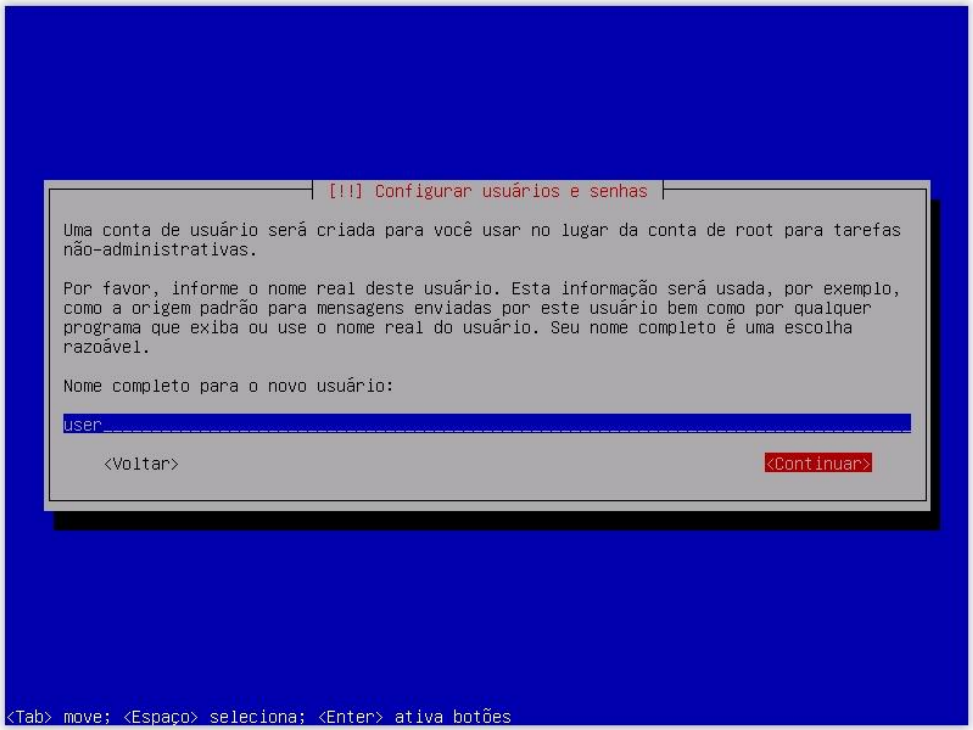
14 – O root é o usuário administrador do sistema Linux, portanto, escolha uma senha com letras maiúsculas e minúsculas, números e caracteres especiais, dificultando a descoberta da senha por ataques de hackers:



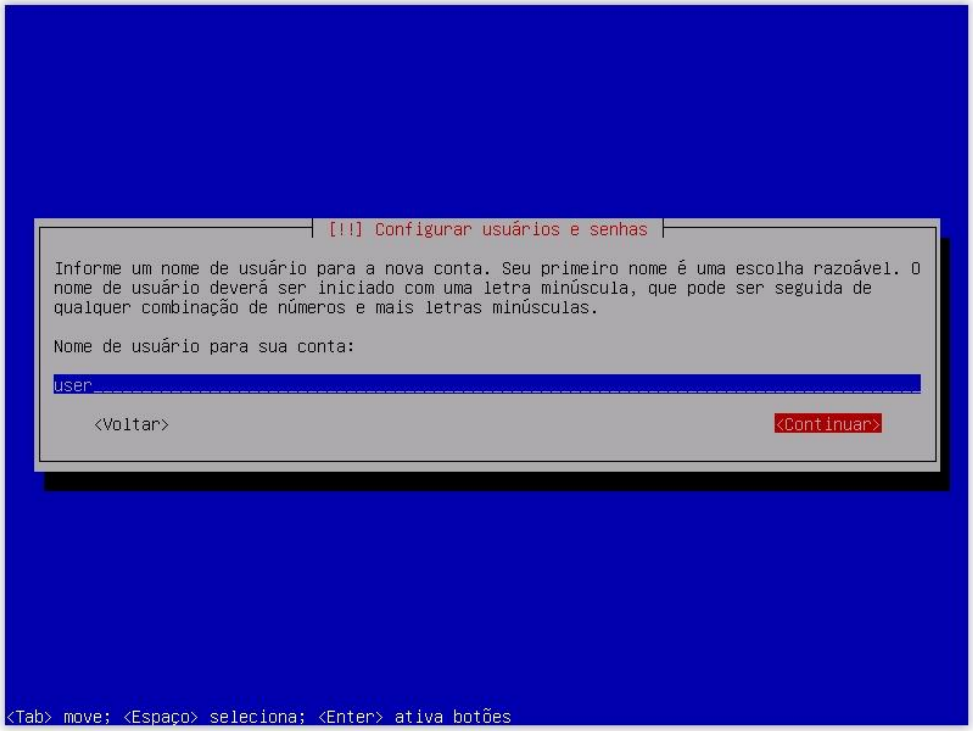
15 – Repita a senha informada anteriormente:



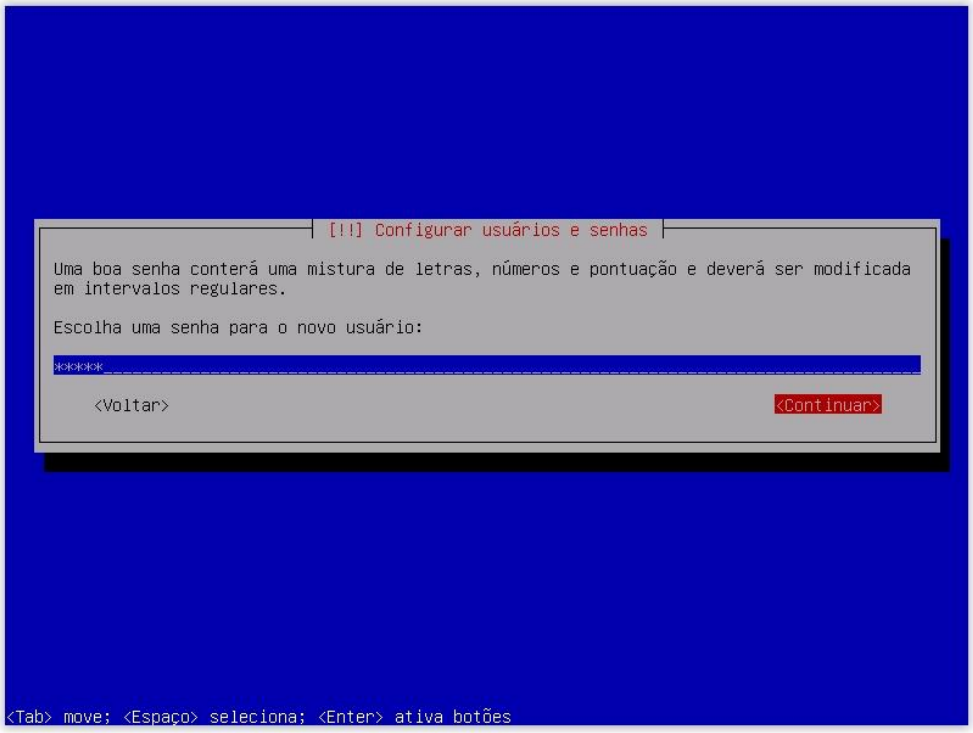
16 – Informe o nome completo do usuário. Esse nome não será utilizado para realizar acesso ao sistema. Esse nome é apenas informativo e utilizado na exibição de alguns programas:



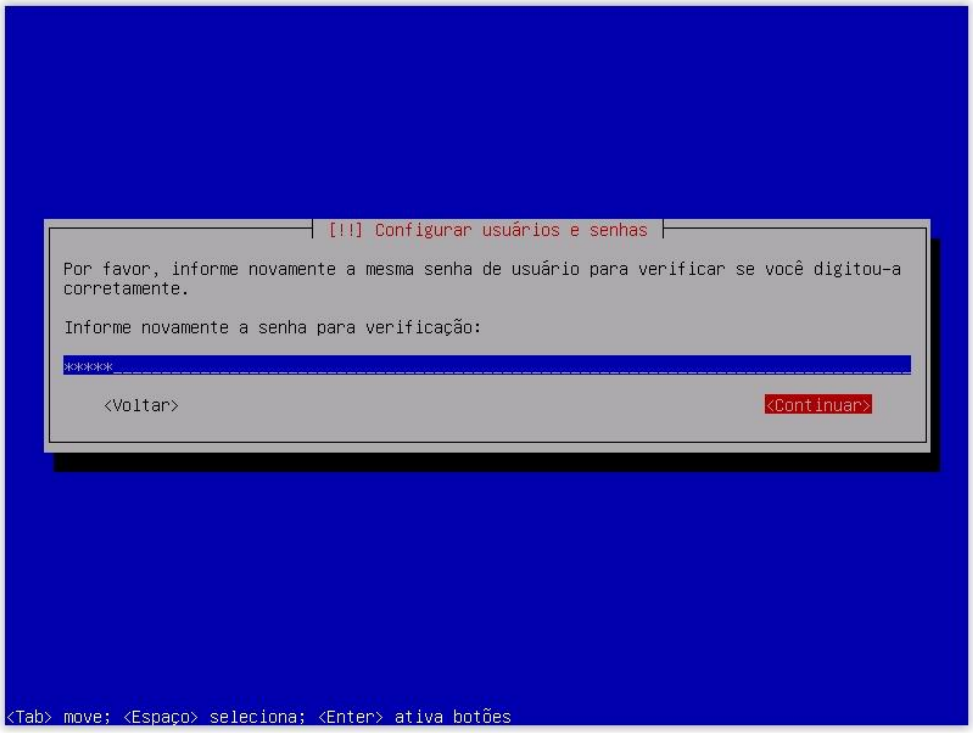
17 – Informe o nome do usuário. Esse usuário terá privilégios comuns. O nome informado será utilizado para realizar acesso ao sistema:



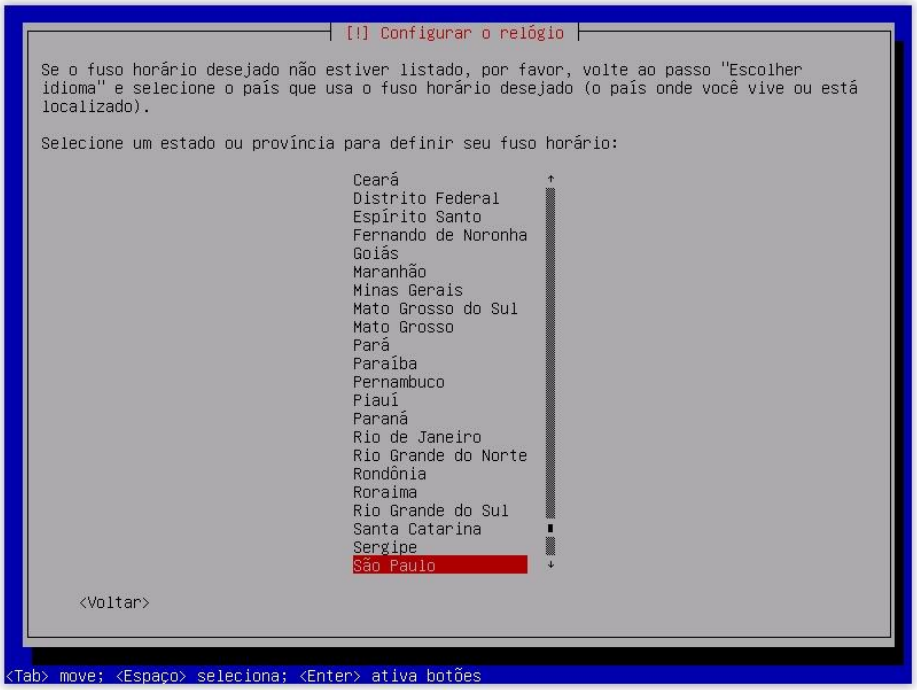
18 – Informe a senha para o usuário informado no passo anterior:



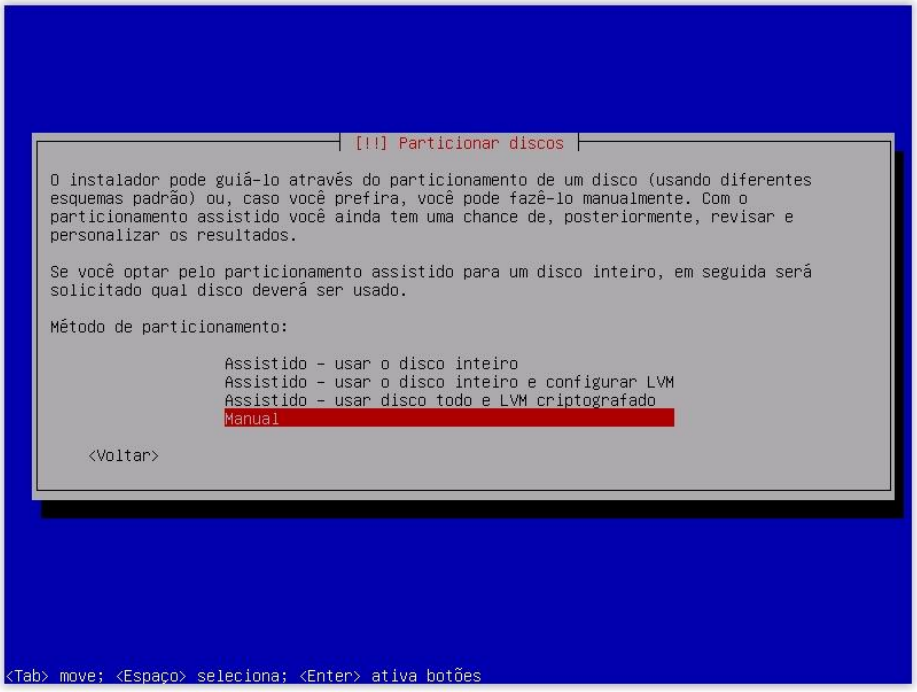
19 – Repita a senha informada:



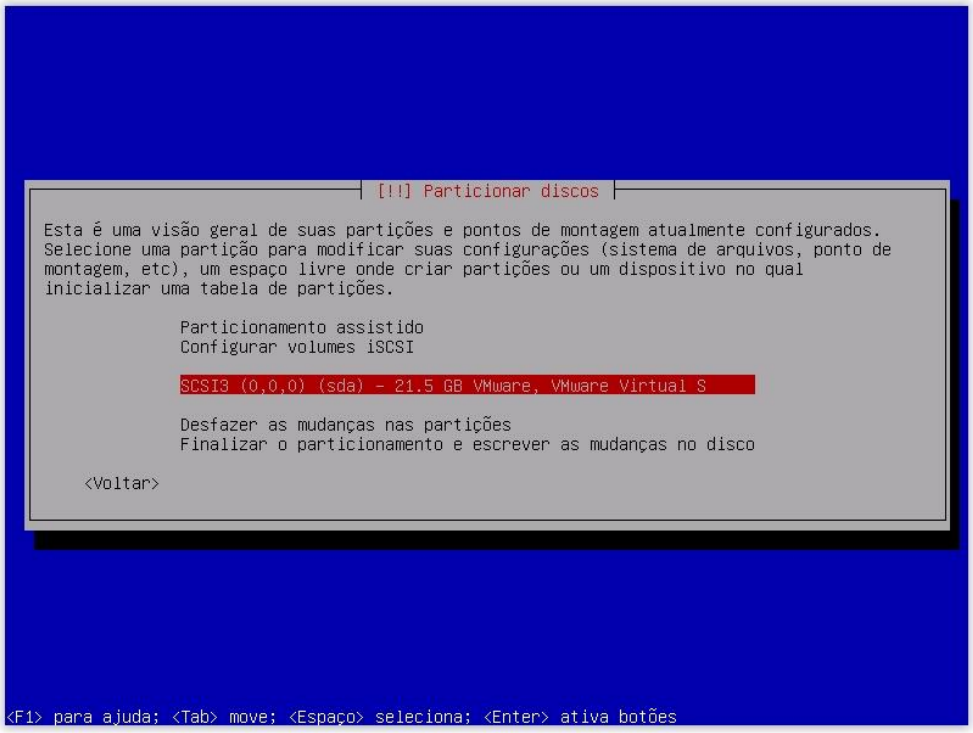
20 – O processo de instalação tentará sincronizar o horário e após isso solicitará que seja informado o estado no qual o servidor será empregado para configurar o fuso horário:



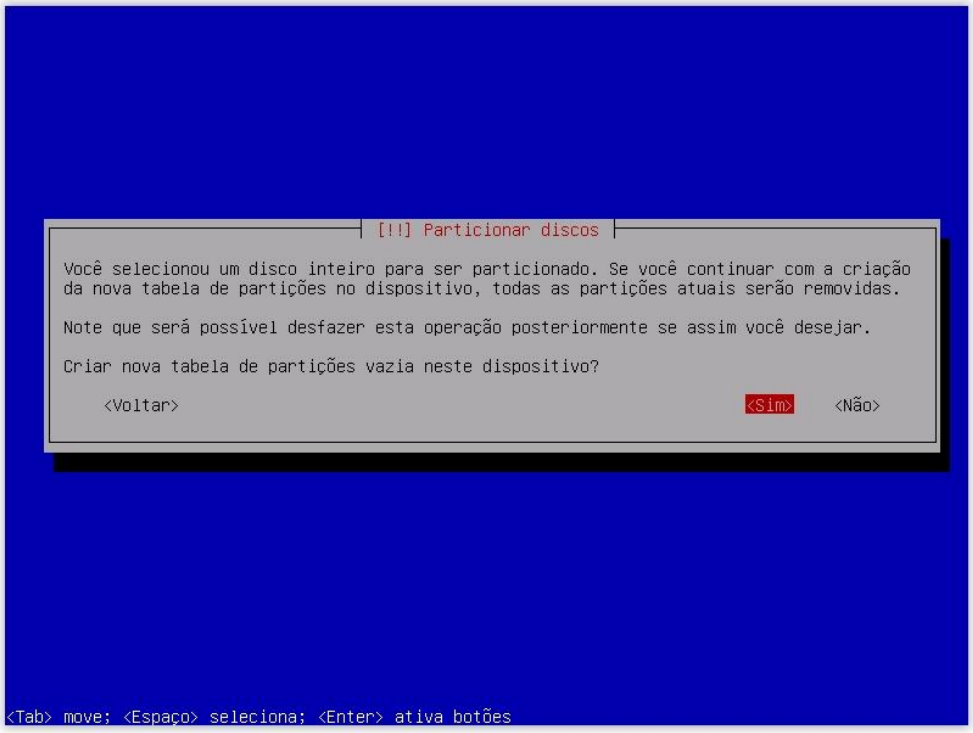
21 – Na próxima tela, será solicitado que seja informado o método de particionamento. A primeira opção, o sistema será instalado em apenas uma partição. As duas seguintes são opções para particionamento com LVM. O LVM possibilita o aumento da partição, mesmo depois do sistema instalado. A última opção será utilizada para realizar o particionamento manualmente:



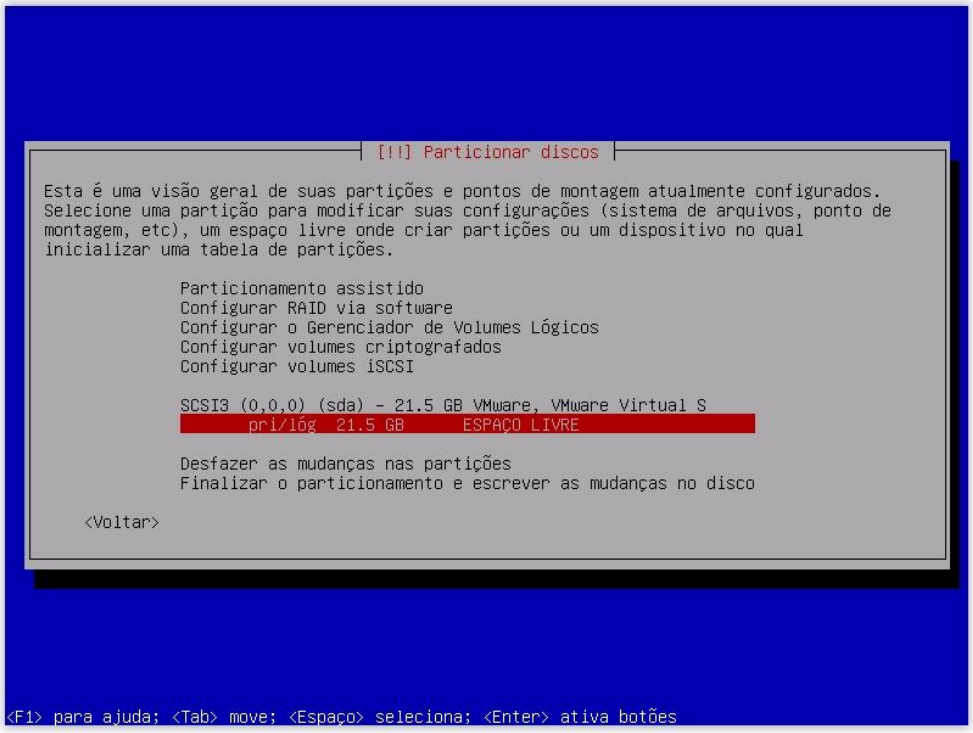
22 – Selecione o disco que será particionado:



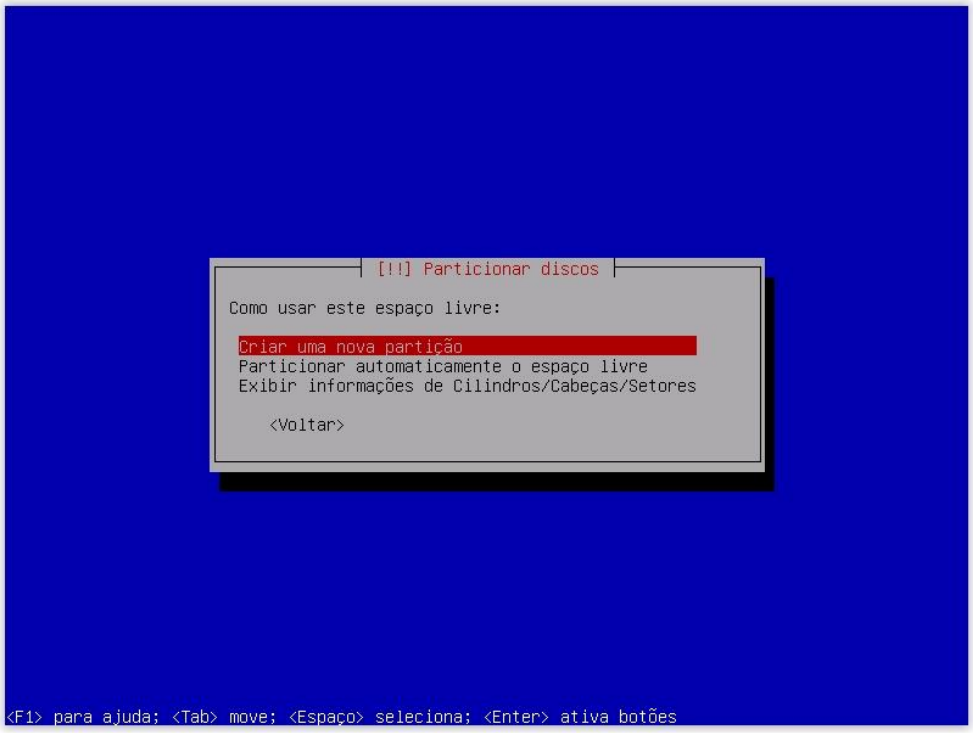
23 – Confirme a criação de uma nova tabela de partições:



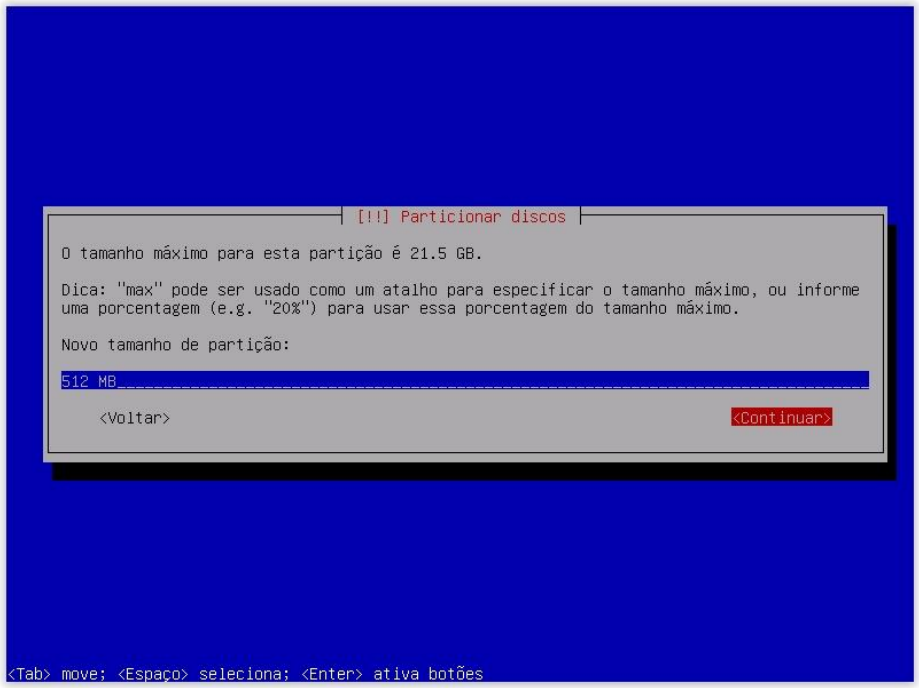
24 – Selecione o partição que está descrita como “ESPAÇO LIVRE”:



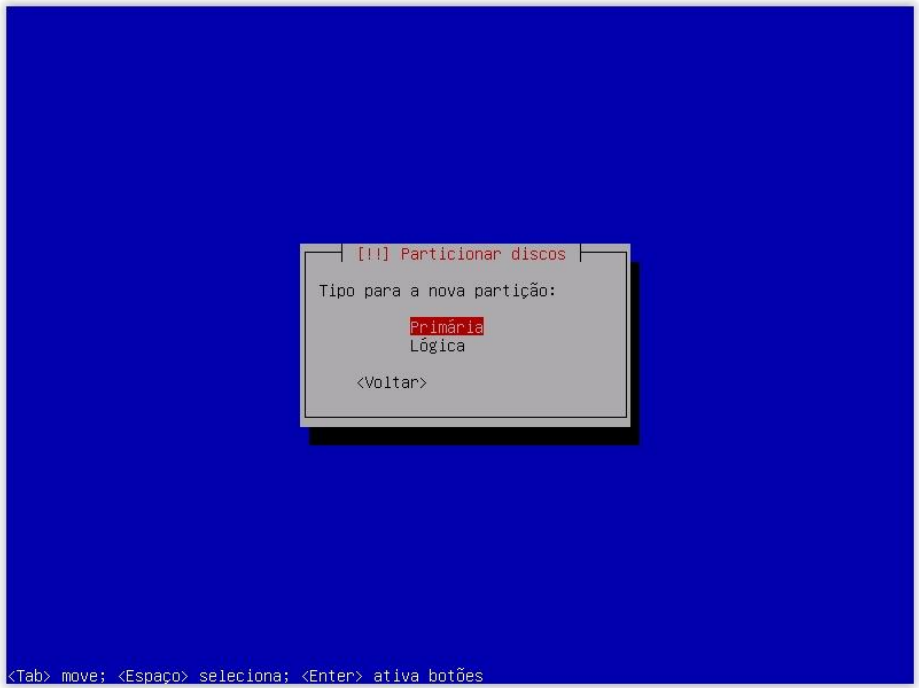
25 – Selecione a primeira opção, “Criar uma nova partição”:



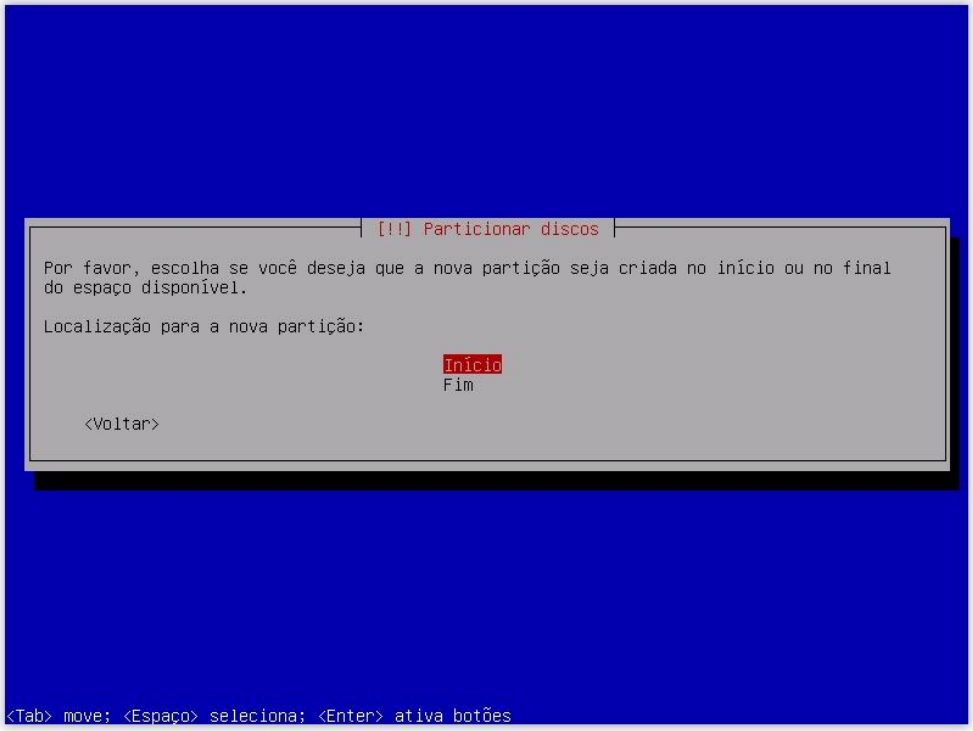
26 – Iremos criar a primeira partição como Swap. O Swap é uma área do disco reservada para paginação de dados voláteis, ou seja, caso todo o espaço da memória RAM seja ocupado, o sistema irá alocar e realizar paginação dos dados utilizados na área de Swap. Não há recomendação de quanto deve ser o tamanho do Swap, portanto informe de acordo com sua necessidade. Servidores com serviços mais críticos devem ter um espaço maior, visto que se o Swap encher por completo, o sistema irá reiniciar automaticamente:



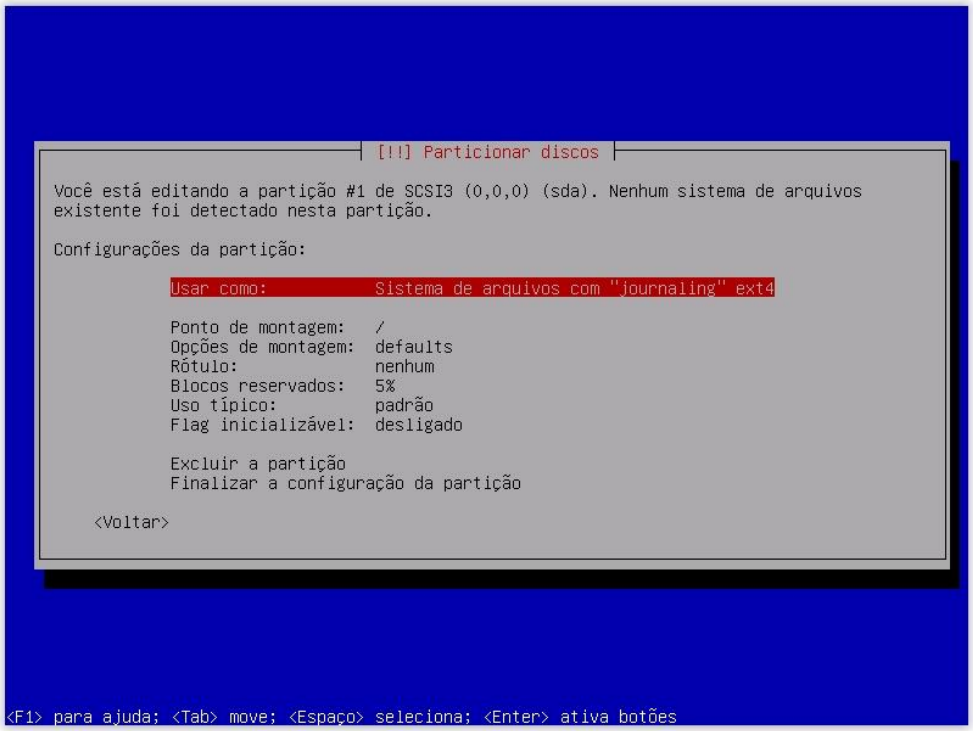
27 – Selecione a opção “Primária”:



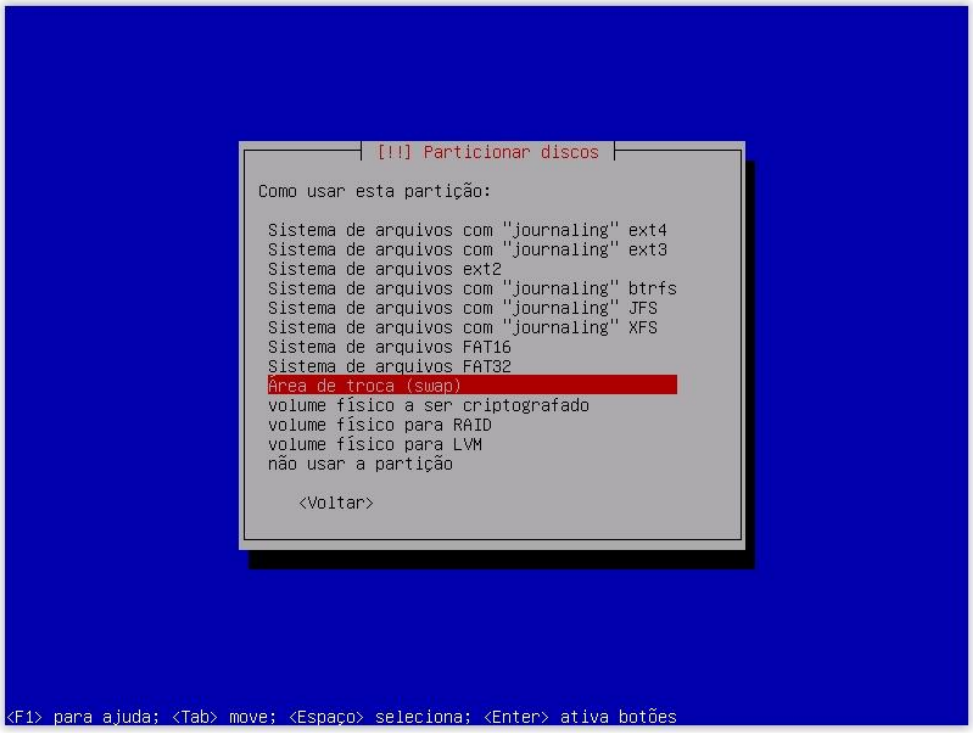
28 – Selecione a opção “Início”, para que a partição seja instalada no início do espaço disponível:



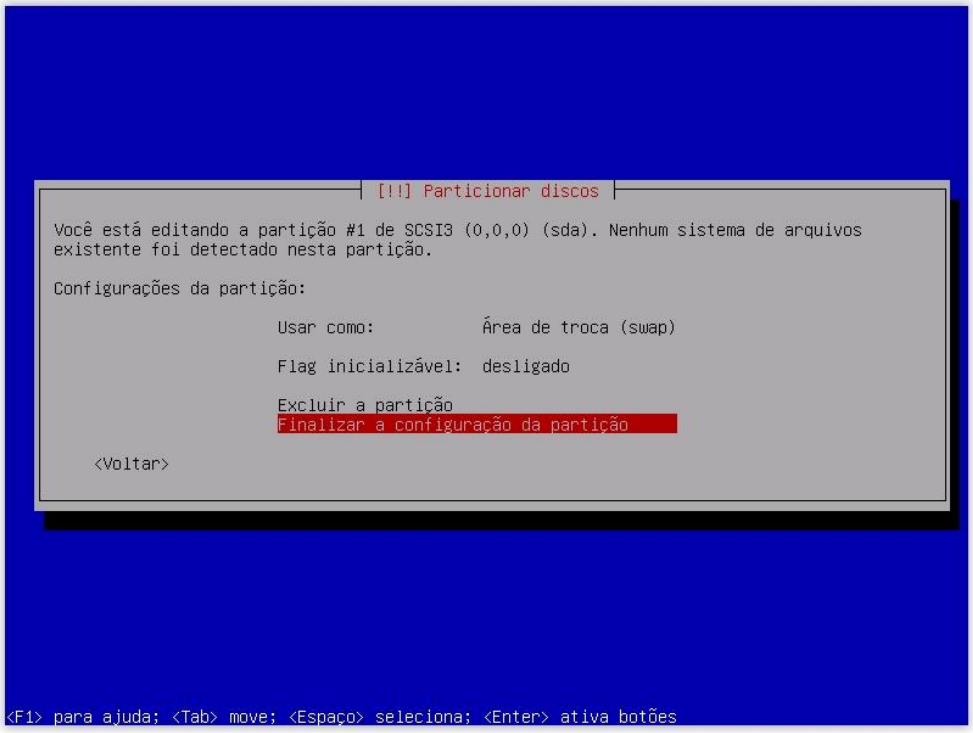
29 – A próxima tela representa as opções de configuração da partição. Pressione “Enter” na opção “Usar como” para alterar para Swap:



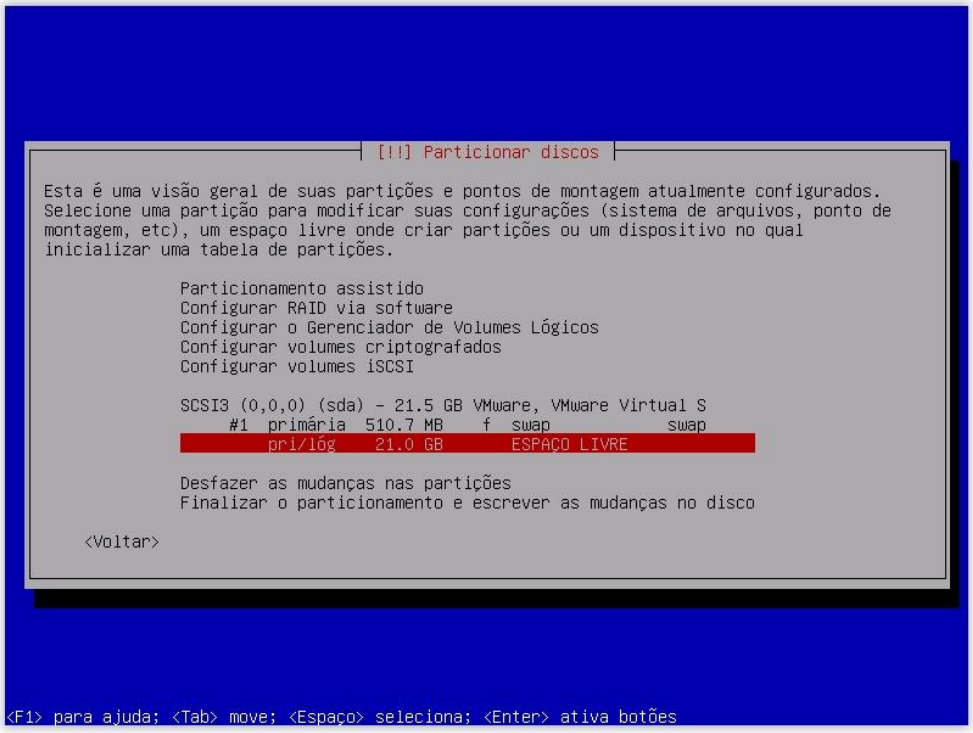
30 – Selecione a opção “Área de troca (swap)” e pressione “Enter”:



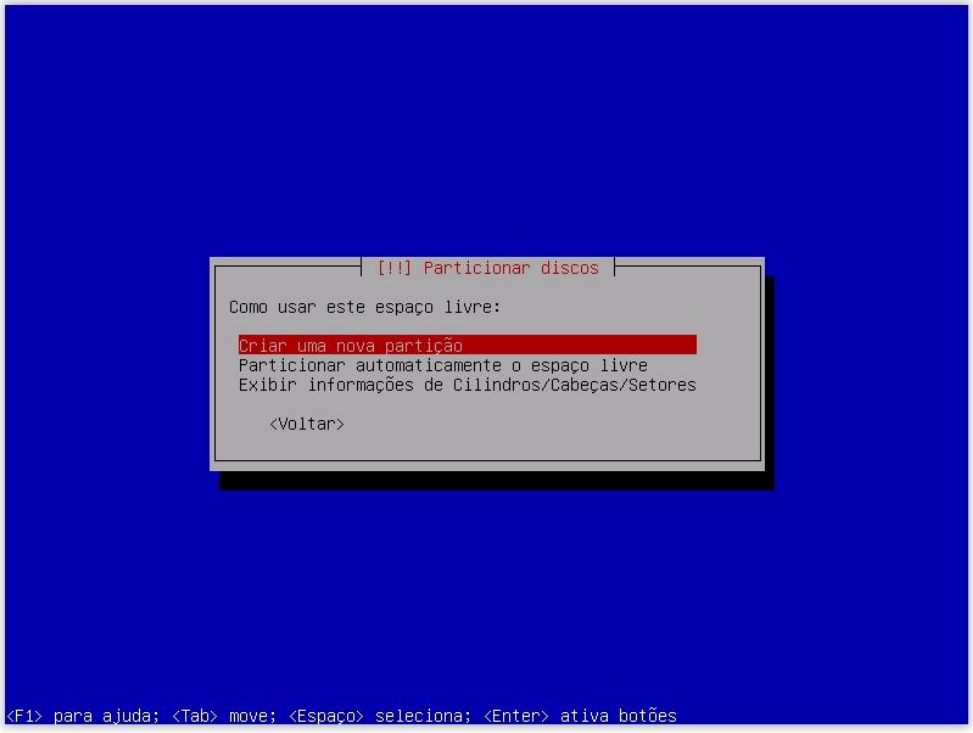
31 – Finalize a configuração da partição, conforme a imagem:



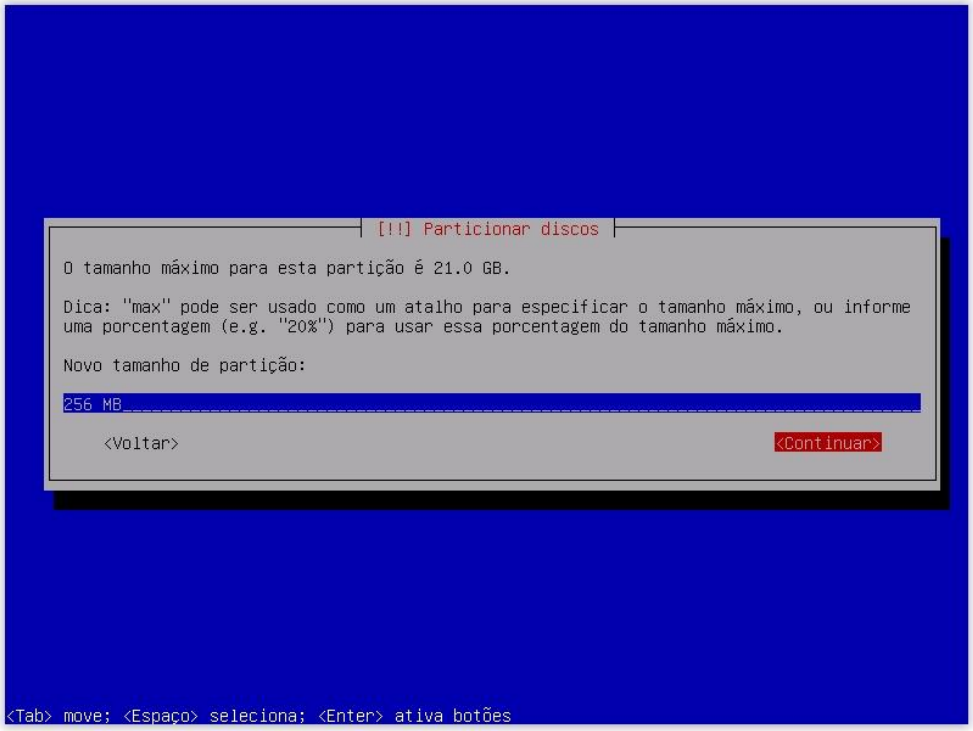
32 – Selecione novamente o “ESPAÇO LIVRE”:



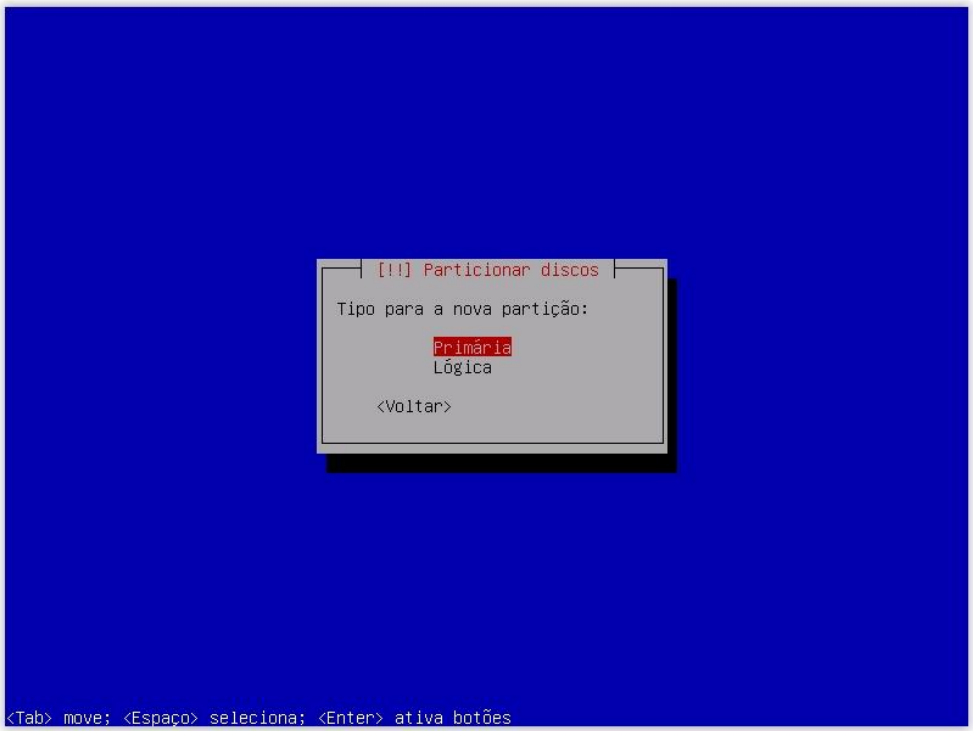
33 – Selecione a opção “Criar uma nova partição”. Agora vamos proceder na criação da partição /boot. Essa partição conterá os arquivos de boot do sistema:



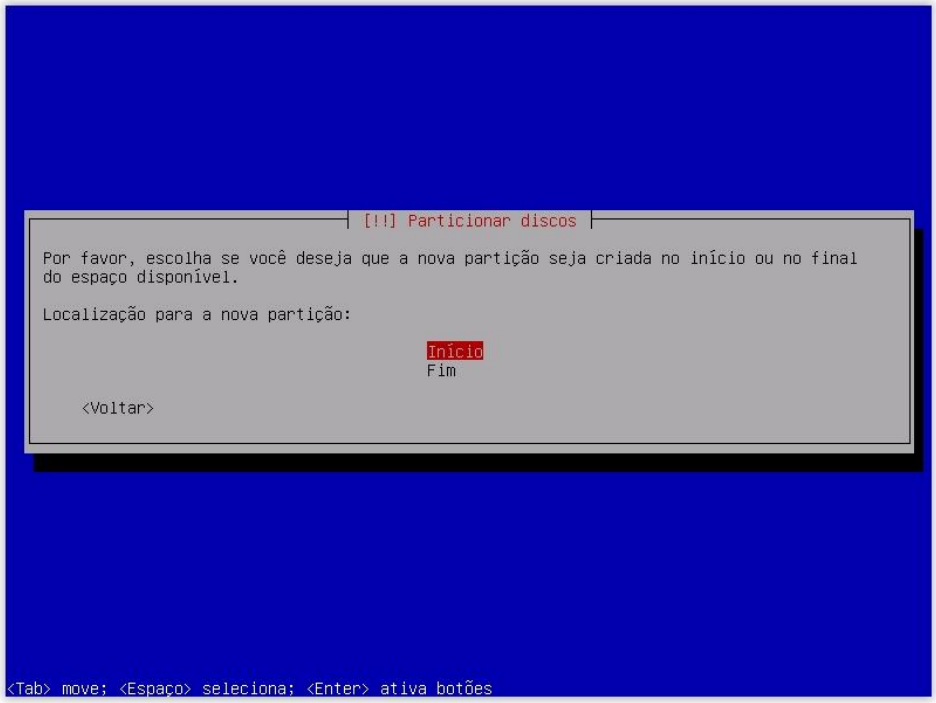
34 – Iremos utilizar essa partição com 256 MB. Apesar de parecer pequena a partição, o sistema utiliza poucos mais de 10% para realizar a instalação:



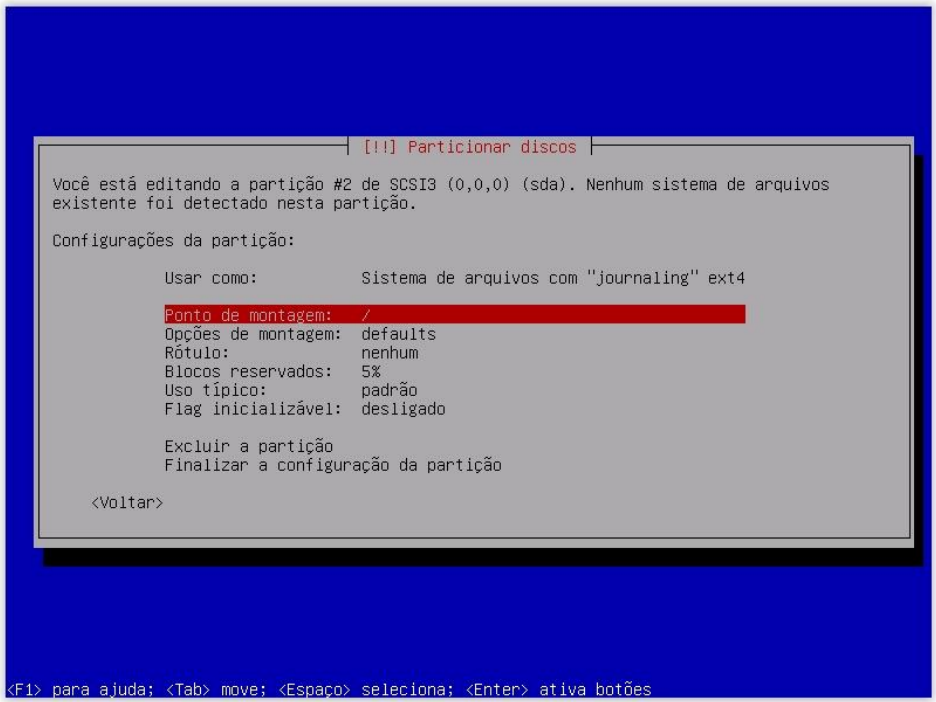
35 – Selecione novamente como sendo uma partição primária:



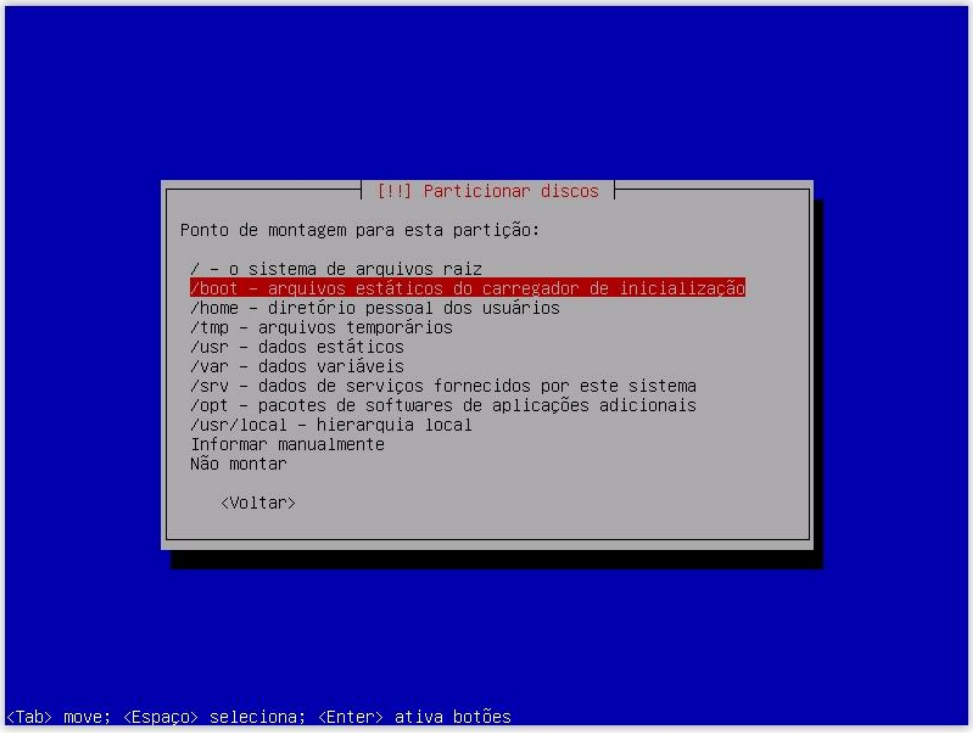
36 – Selecione a opção “Início”:



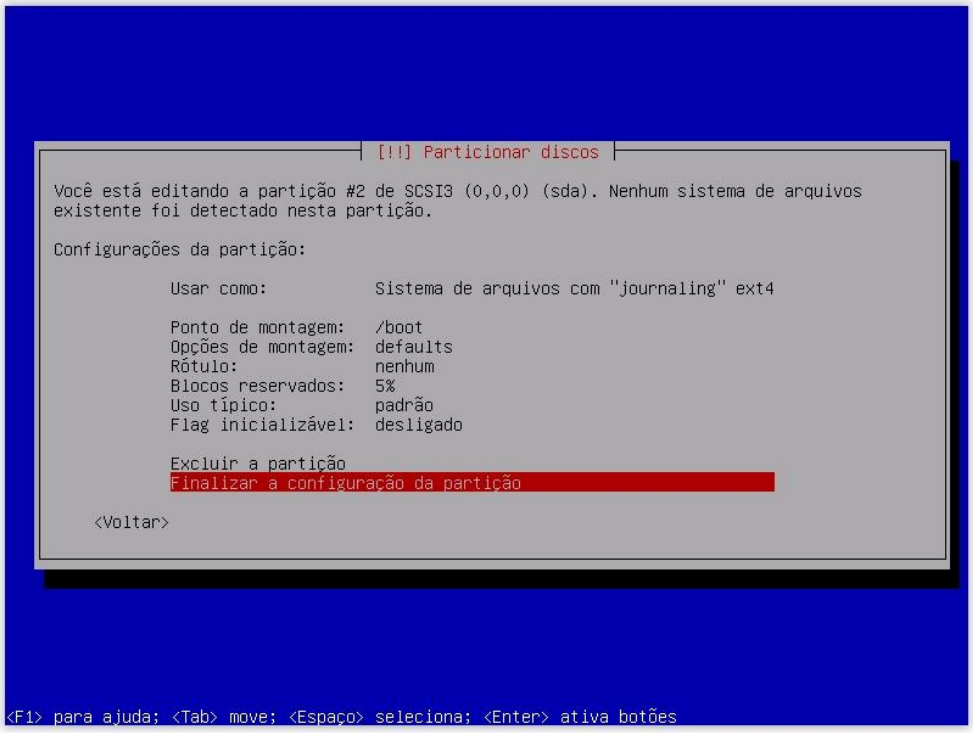
37 – Será utilizada a formatação ext4 com “journaling”. Um sistema de arquivos com journaling dá permissão ao sistema operacional de manter um log de todas as mudanças no sistema de arquivos antes de escrever os dados no disco. Essa opção oferece diminui a probabilidade do sistema sofrer corrupção de dados em caso de falha do sistema ou falta de energia, além de oferecer uma recuperação mais rápida:



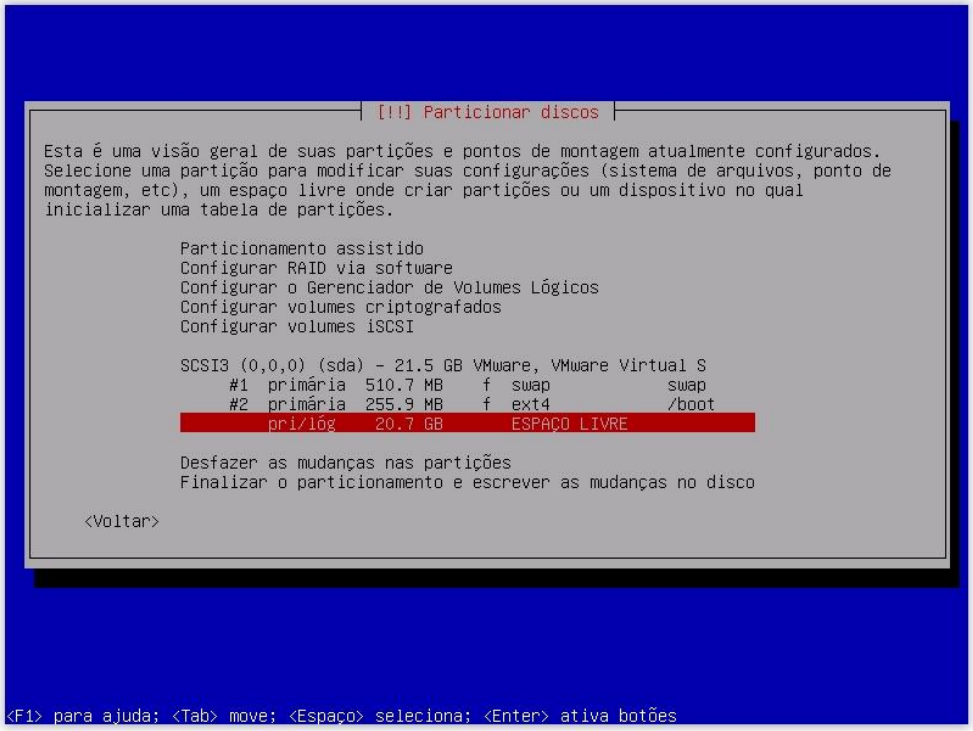
38 – Selecione o ponto de montagem da partição como “/boot”:



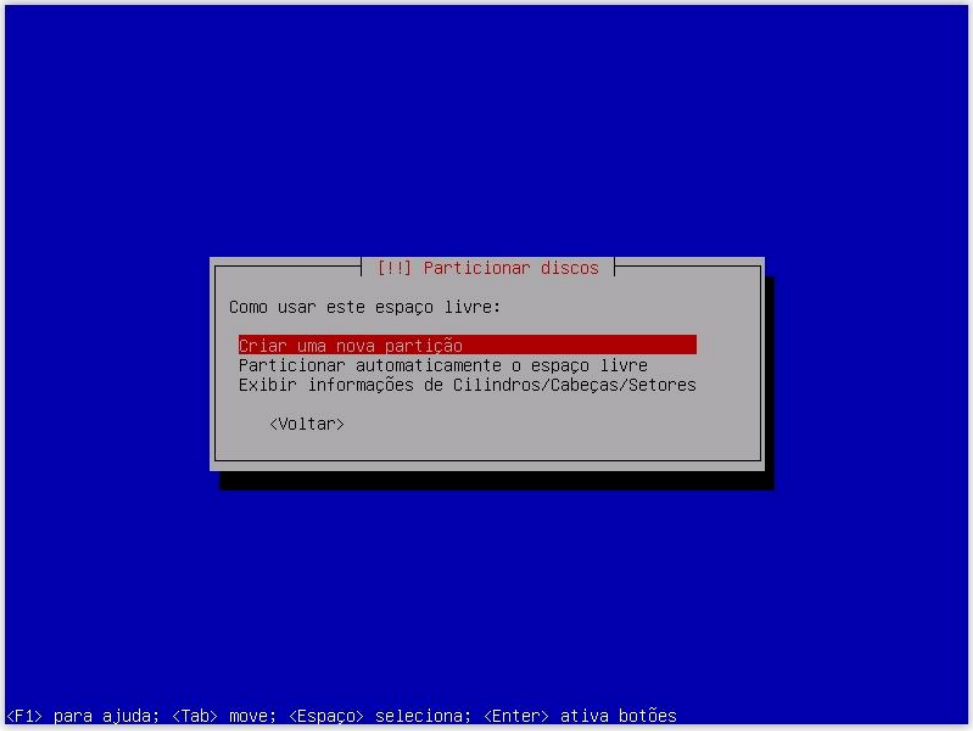
39 – Finalize a configuração da partição, conforme a imagem:



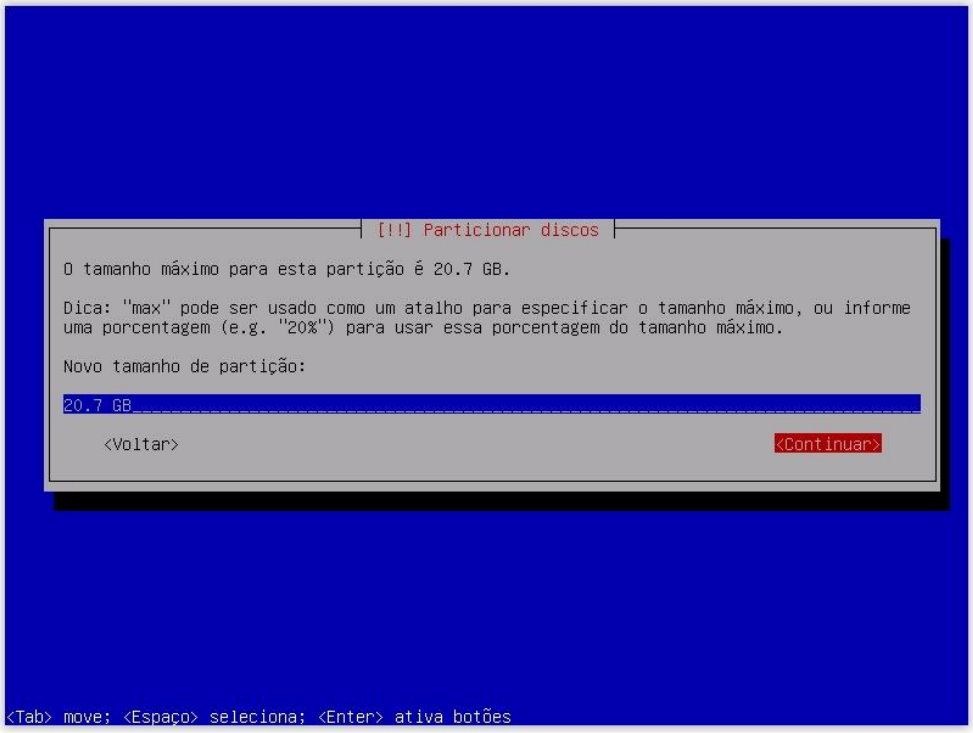
40 – Por fim, selecione o “ESPAÇO LIVRE” para criamos a última partição, sendo a partição principal do sistema:



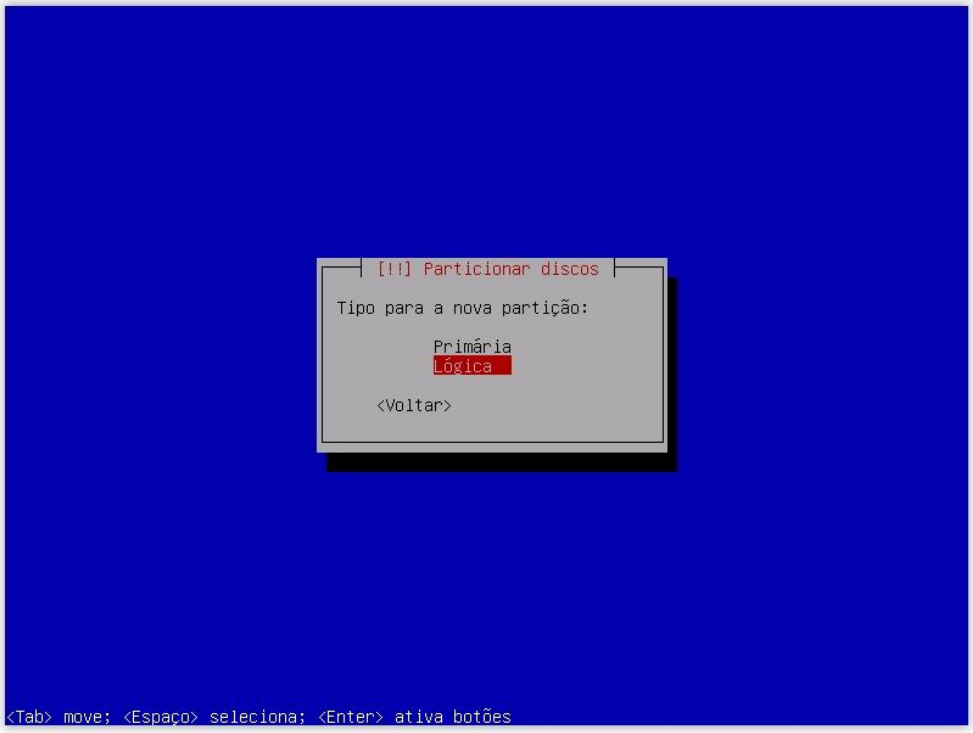
41 – Selecione a opção “Criar uma nova partição”:



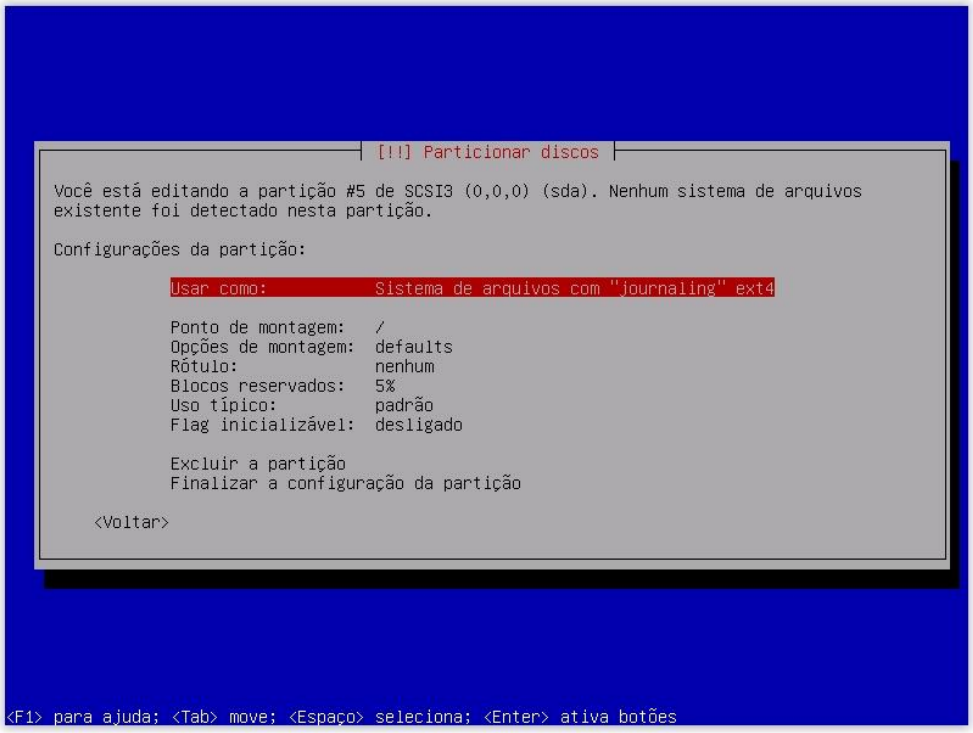
42 – Utilizaremos todo o espaço restante para a criação da última partição:



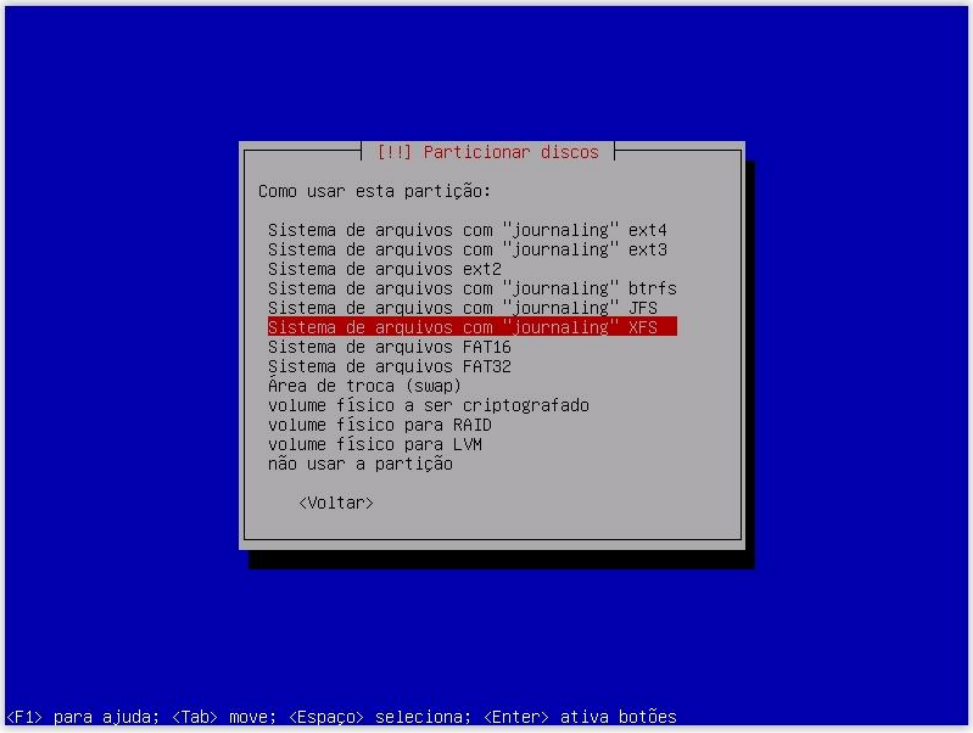
43 – Para essa partição podemos utilizar a opção “Lógica”:



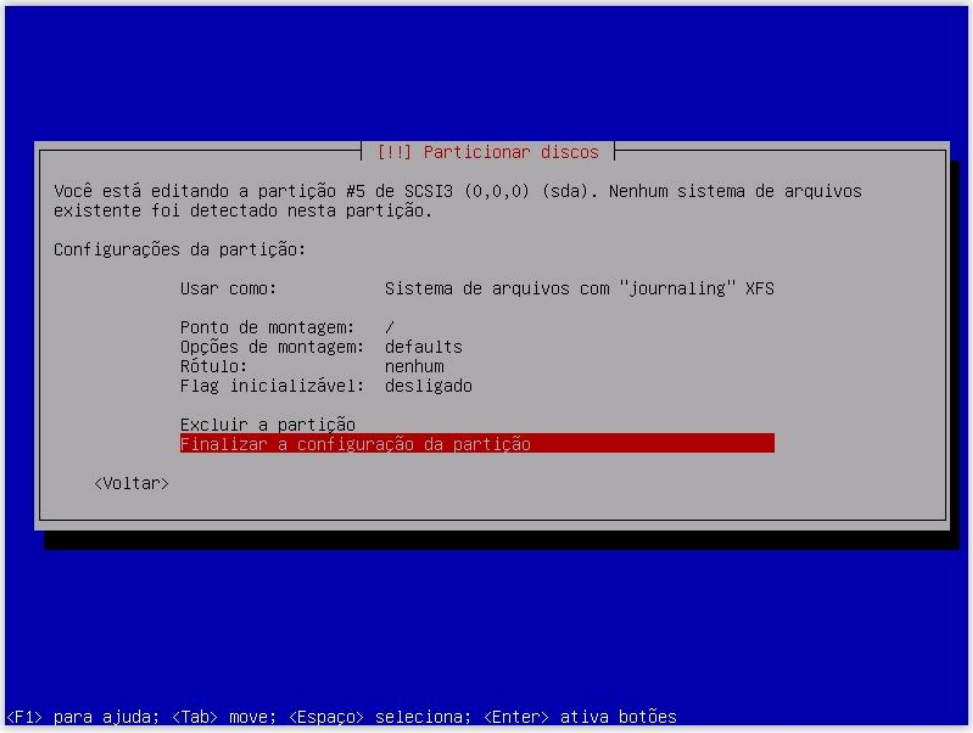
44 – Selecione o “Usar como” para mudarmos o tipo de sistema de arquivos:



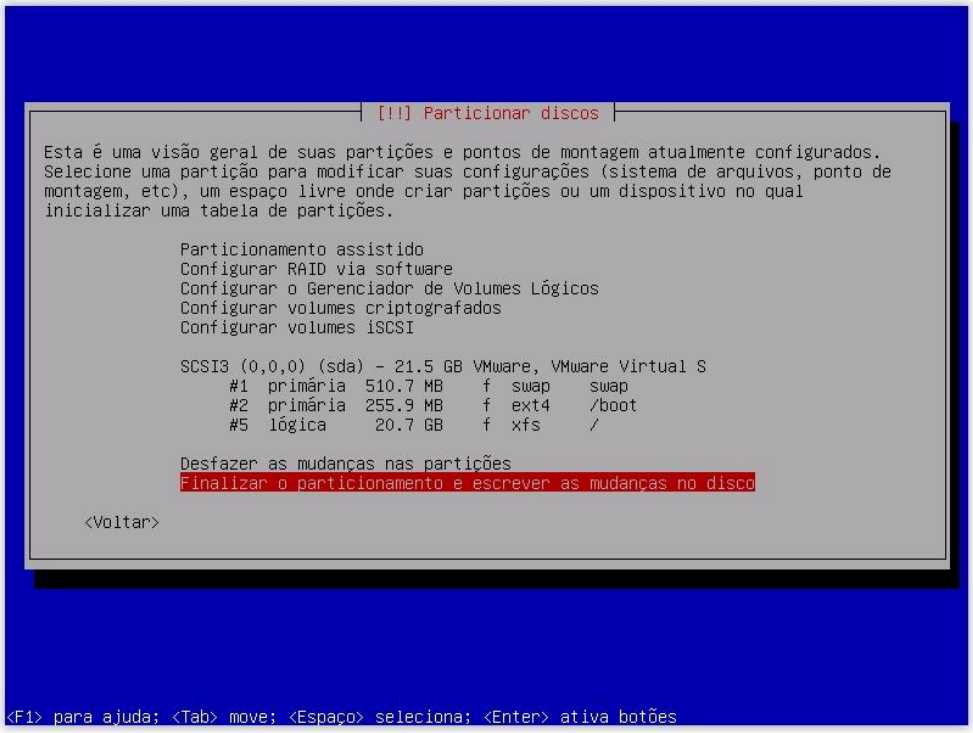
45 – Selecione a opção “Sistema de arquivos com “journaling” XFS”. Será escolhido esse sistema de arquivos devido a seu melhor desempenho, comparado ao ext4, e menor probabilidade de falha na partição:



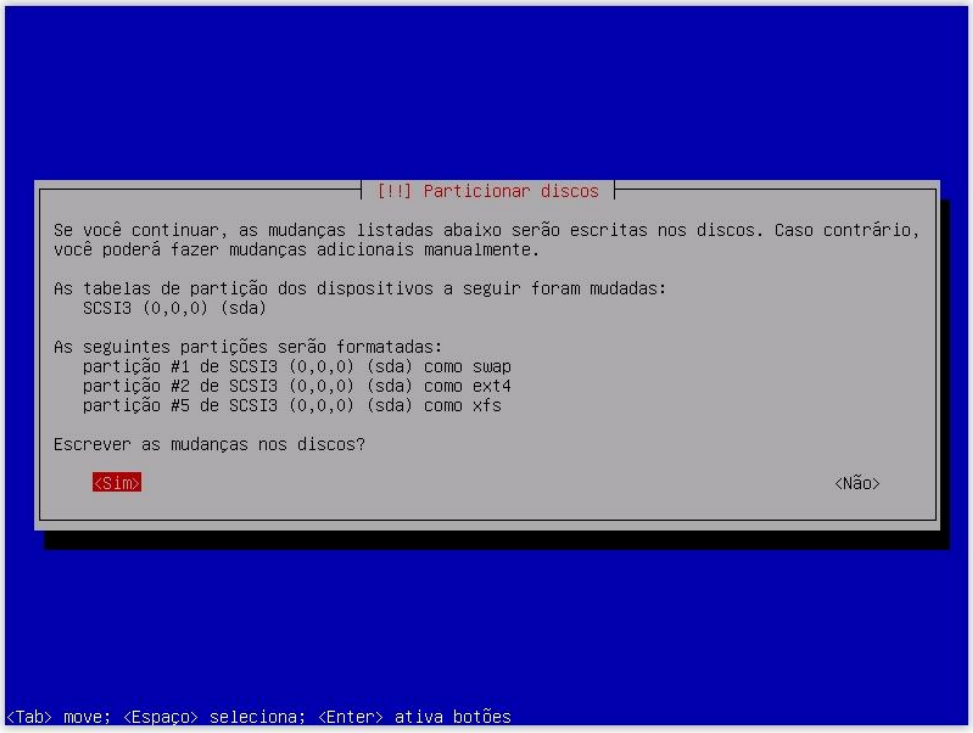
46 – Finalize as configurações da partição:



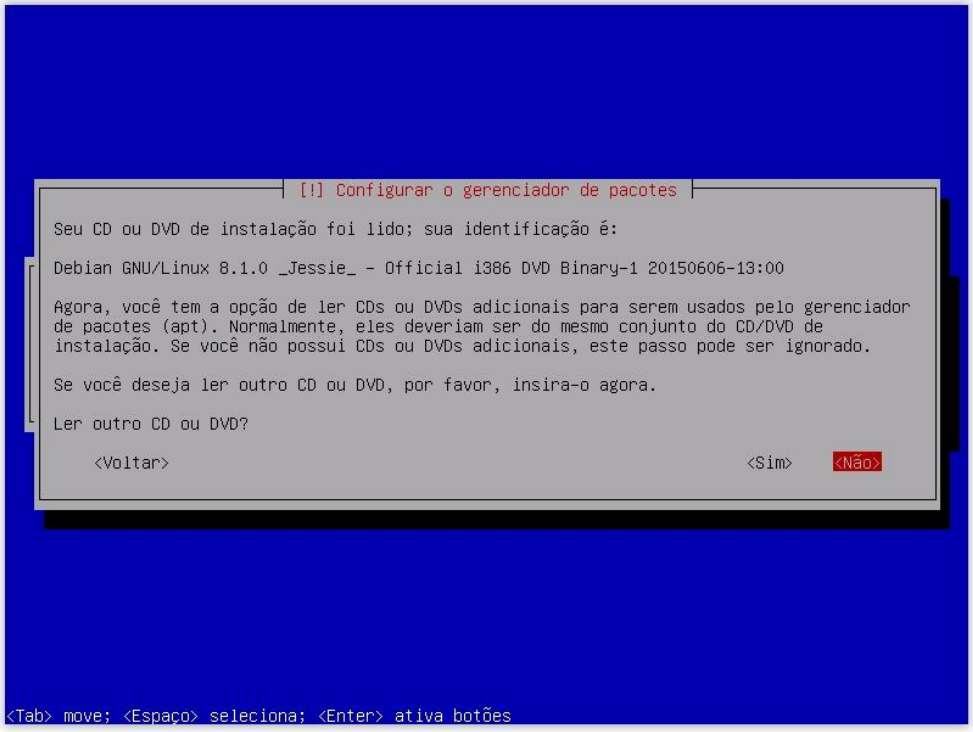
47 – Por fim, finalize o particionamento:



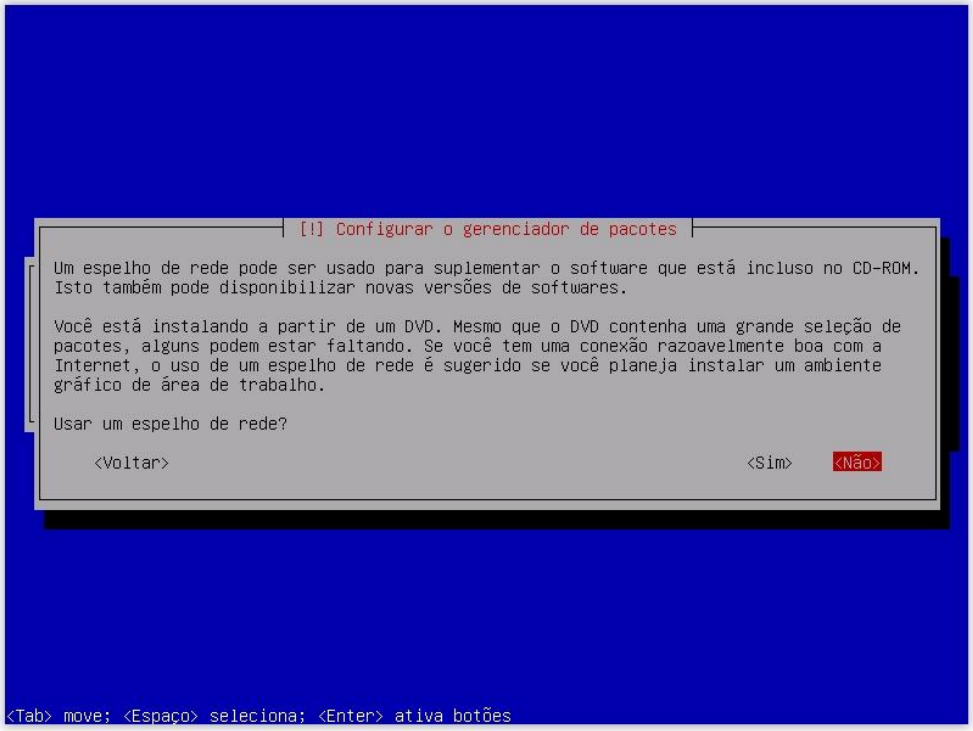
48 – Selecione a opção “Sim” para confirmar as partições e formatar o disco:



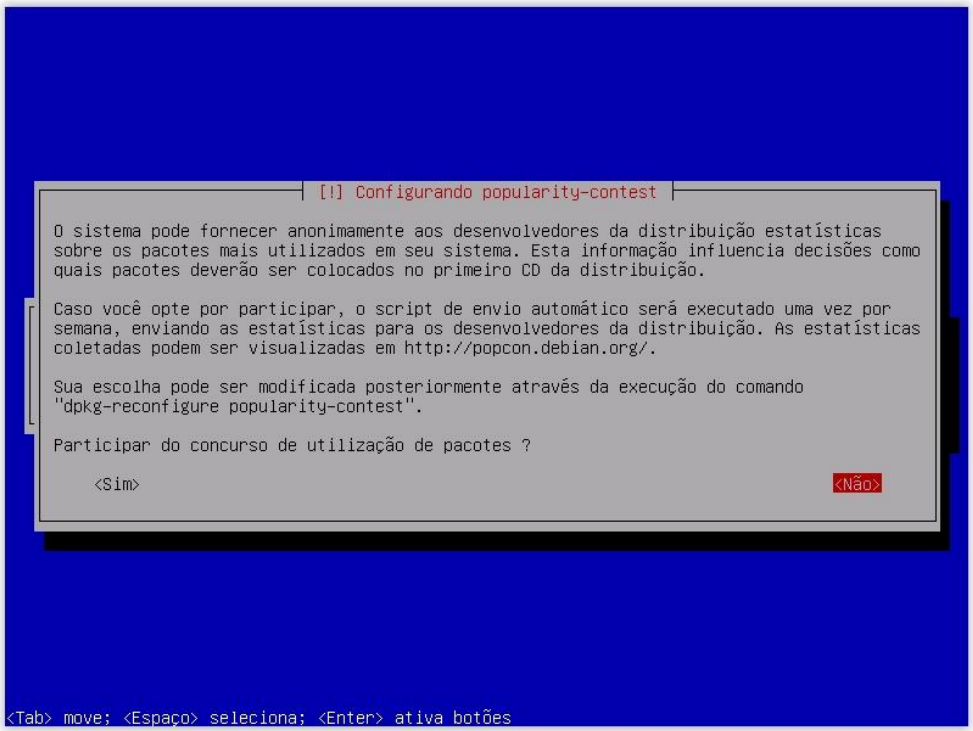
49 – Após a formatação, o Instalador irá perguntar se há outro CD/DVD de instalação. Caso negativo selecione a opção “Não” e continue o processo de instalação:



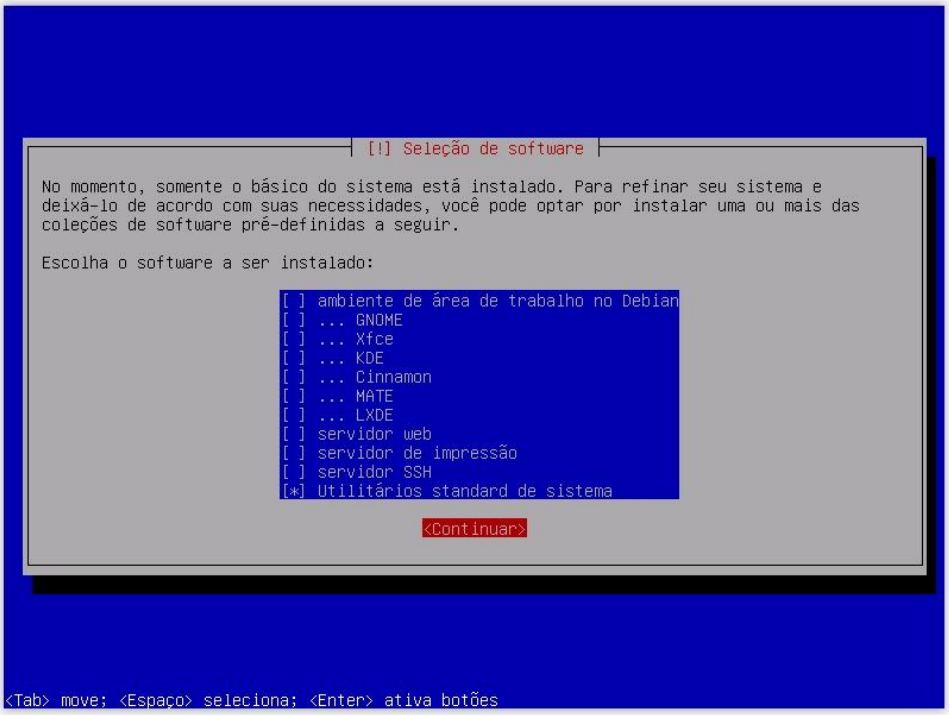
50 – Caso você tenho um servidor de repositório na rede, selecione a opção “Sim” e informe o endereço do servidor, caso negativo, selecione a opção “Não”:



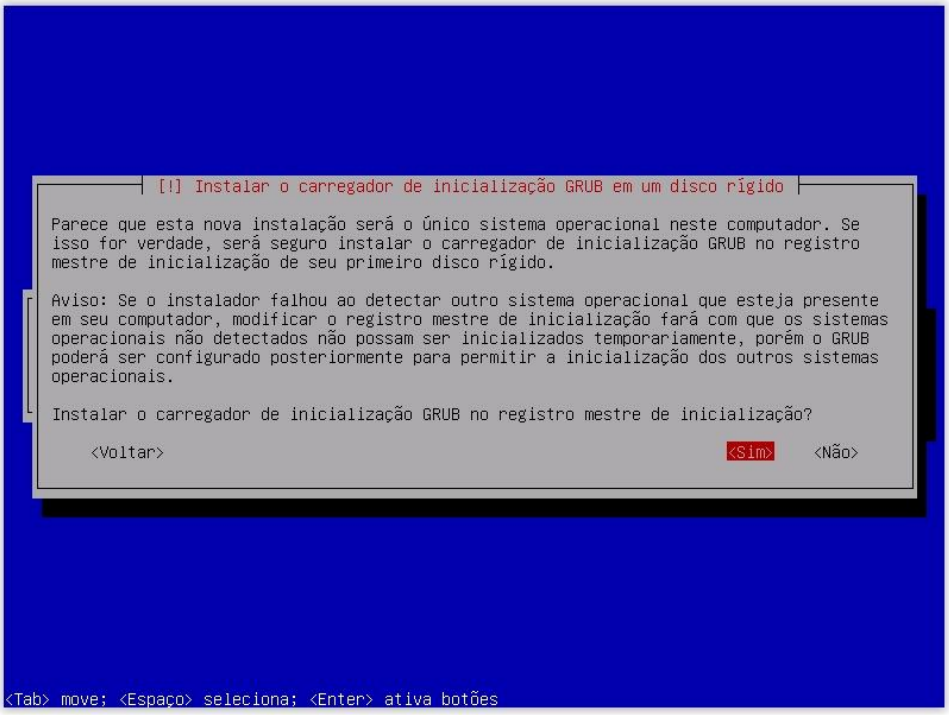
51 – Selecione a opção “Não” para não participar :



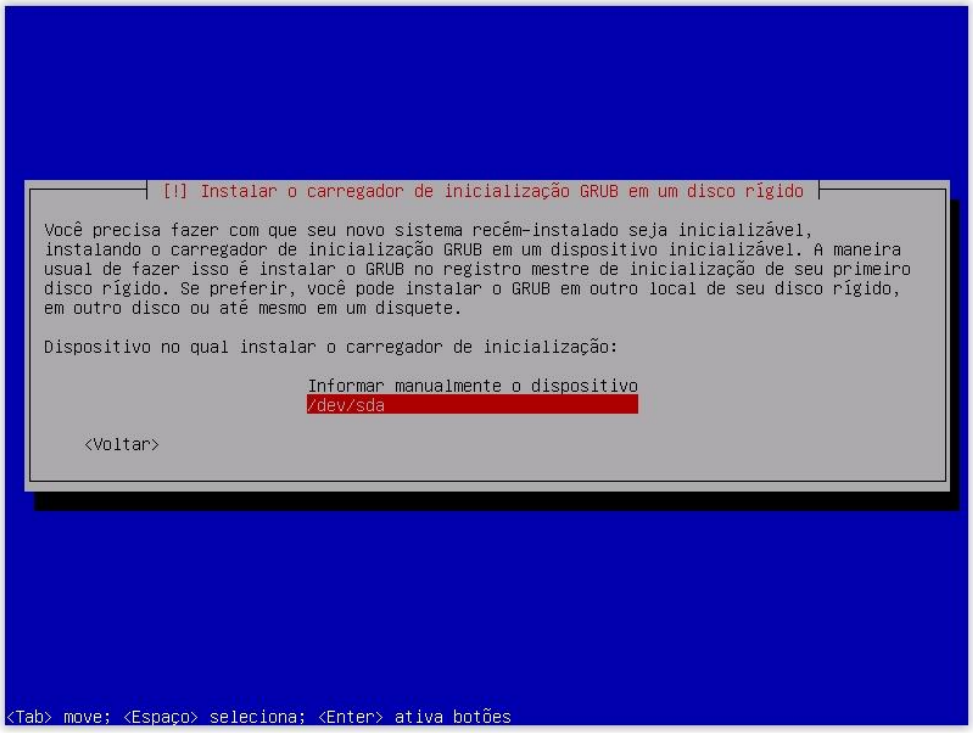
52 – Selecione apenas a opção “Utilitários standard de sistema”, caso seja um servidor. Essa opção não irá instalar o ambiente gráfico. Caso queira um ambiente gráfico, selecione uma das sete primeiras opções. Não há necessidade de selecionar as opções de servidor, mesmo que o sistema vá utilizar algum desses serviços, pois essas opções não permitem escolher quais pacotes serão instalados:



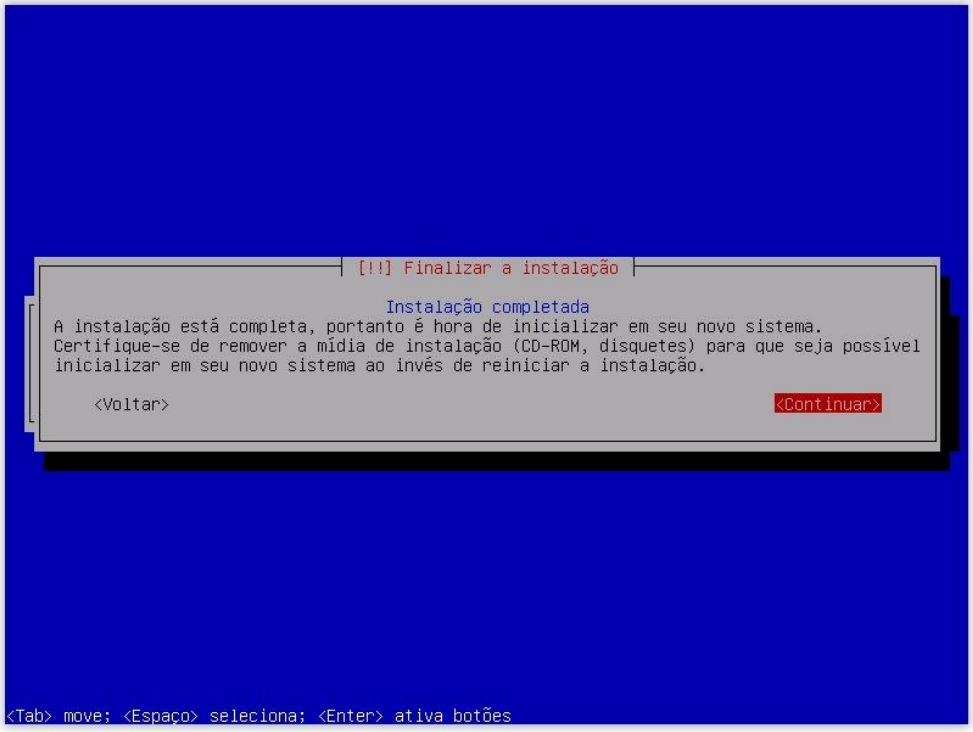
53 – Confirme a opção para instalar o GRUB no MBR do disco. Essa opção configura o disco para que o GRUB gerencie o boot dos sistemas instalados:



54 – Selecione o dispositivo no qual será configurado o GRUB:



55 – Pressione “Enter” para finalizar a instalação. O sistema será reiniciado após isso. Certifique que a mídia de instalação seja retirada e que o boot do computador será realizado na mídia no qual foi instalado o sistema.:



APÊNDICE B – ARQUIVO DE CONFIGURAÇÃO DNS

Segue os arquivos de configuração do DNS Bind. O arquivos abaixo foram testados nas distribuições Debian 7 e 8. Abaixo está o arquivo “named.conf”, encontrado no diretório “/etc/bind”:

```
////////////////////////////////////////////////////////////////////////////
///// Configuracao Servidor DNS – named.conf  ///
/////  Autor: Michael Andre Hempkemeyer          ///
////////////////////////////////////////////////////////////////////////////

include "/etc/bind/named.conf.options";

view "interna" {
        match-clients { any; };
        recursion yes;
        include "/etc/bind/named.conf.default-zones";
        include "/etc/bind/named.conf.local";
};

/*
// As configurações abaixo são utilizadas para auditorias e resolução de problemas
// Utilize apenas quando necessário. Geração excessiva de Logs.
logging {
  channel "security_debug" {
   file "/var/log/named.run.security";
    severity debug 2;
   };
  category "security" {
          "security_debug";
   };
};
*/
////////////////////////////////////////////////////////////////////////////
//// Fim das configuracoes                          ////
////////////////////////////////////////////////////////////////////////////
```

Abaixo está o arquivo “named.conf.options”, encontrado no diretório “/etc/bind”:

```
////////////////////////////////////////////////////////////////////////////////////////////
///// Configuracao Servidor DNS – named.conf.options  ///
/////  Autor: Michael Andre Hempkemeyer                        ///
////////////////////////////////////////////////////////////////////////////////////////////

options {
        directory "/var/cache/bind";

        forwarders {
                // SUL BBS (2ms)
                200.219.150.4;
                //dns1.optiglobe.net.br Optiglobe (7ms)
                200.185.6.131;
                //1ea.terra.com.br Terra (25ms)
                200.176.2.10;
        };
```

```
        auth-nxdomain no;
        listen-on-v6 { none; };
        listen-on { 127.0.0.1; 10.0.0.2; };

        version "SuaEmpresa";

        // ips que podem fazer consulta no servidor
        allow-query {
                        10.0.1.0/24;  //Filial 01
                        10.0.2.0/24;  //Filial 02
        };

        allow-recursion { 10.0.1.0/24; 10.0.2.0/24; };

        // lista de maquinas bloqueadas
        blackhole {
                //10.0.1.30;
        };

        // ips que podem solicitar transferencia de zona
        allow-transfer { 10.0.0.10; };
};
////////////////////////////////////////////////////////////////////////
//// Fim das configuracoes                          ////
////////////////////////////////////////////////////////////////////
```

Abaixo está o arquivo “named.conf.local”, encontrado no diretório “/etc/bind”:

```
//////////////////////////////////////////////////////////////////////////////////
///// Configuracao Servidor DNS – named.conf.local  ///
/////  Autor: Michael Andre Hempkemeyer                  ///
//////////////////////////////////////////////////////////////////////////////////
// zonas locais do servidor dns

zone "filial01.com.br" {
        type master;
        file " filial01.com.br ";
};

zone " filial02.com.br " {
        type master;
        file " filial02.com.br ";
};

////////////////////////////////////////////////////////////////////////
//// Fim das configuracoes                          ////
////////////////////////////////////////////////////////////////////
```

Abaixo está um exemplo de uma zona de DNS. Este arquivo é extraido a partir do arquivo “db.empty” e modificado de acordo com o perfil do domínio:

```
;
; zona do filial01
;
$TTL    86400
@       IN      SOA     ns. filial01.com.br. root.ns.filial01.com.br. (
                        2015120800      ; Serial
                        28800       ; refresh (8 hours)
                        7200        ; retry (2 hours)
                        604800      ; expire (1 week)
                        86400       ; minimum (1 day)
                        )

@                       IN      NS      ns.filial01.com.br.
@                       IN      NS      ns2.filial01.com.br.

www.filial01.com.br.    IN      A       10.0.1.5
ns.filial01.com.br.     IN      A       10.0.1.2
ns2.filial01.com.br.    IN      A       10.0.1.3

proxy.filial01.com.br.  IN      A       10.0.1.6
intranet.filial01.com.br.       IN      A       10.0.1.7

;CNAME
squid.filial01.com.br.  IN      CNAME       proxy.filial01.com.br.
```

APÊNDICE C – ARQUIVO DE CONFIGURAÇÃO DHCP

Segue o arquivo de configuração do DHCP. O arquivo abaixo foi testado nas distribuições Debian 7 e 8. O arquivo “dhcpd.conf” pode ser encontrado na pasta “/etc/dhcp/”.

```
# dhcpd.conf
#
# Arquivo de um servidor DHCP sem Alta Disponibilidade (Failover)
#
# Autor: Michael Andre Hempkemeyer
#

# Informe seu servidor de DNS
option domain-name-servers 8.8.8.8;
# Informe seu servidor NTP, ou outro servidor válido
option ntp-servers ntp.com.br;

# Tempo em que o endereço é alocado para o cliente
default-lease-time 604800;
# Tempo máximo de alocação caso o cliente solicite um tempo maior
max-lease-time 604800;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Evita DoS. Se um cliente enviar muitos DHCPDELINE pode consumir todos os recursos do servidor
deny declines;

#Rede Filial 01
subnet 10.0.0.0 netmask 255.255.255.0 {
  option domain-name "empresa01.com.br";
  option routers 10.0.0.1;
  range 10.0.0.11 10.0.0.254;
}

#Rede Filial 02
subnet 10.0.1.0 netmask 255.255.255.0 {
  option domain-name "empresa02.com.br";
  option routers 10.0.1.1;
  range 10.0.1.11 10.0.1.254;
}

#---------- Fim do arquivo de configuração -------------------------
# Autor: Michael Andre Hempkemeyer
```

APÊNDICE D – ARQUIVO DE CONFIGURAÇÃO DHCP FAILOVER

Os arquivos abaixo foram testado nas distribuições Debian 7 e 8. O arquivo “dhcpd.conf” pode ser encontrado na pasta “/etc/dhcp/”.

Segue o arquivo de configuração do do servidor DHCP com Failover Primário.

```
# dhcpd.conf
#
# Arquivo de um servidor DHCP com Alta Disponibilidade (Failover)
# Este arquivo deve estar no servidor PRIMÁRIO
#
# Autor: Michael Andre Hempkemeyer
#

# Informe seu servidor de DNS
option domain-name-servers 8.8.8.8;
# Informe seu servidor NTP, ou outro servidor válido
option ntp-servers ntp.com.br;

# Tempo em que o endereço é alocado para o cliente
default-lease-time 604800;
# Tempo máximo de alocação caso o cliente solicite um tempo maior
max-lease-time 604800;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Negar pcs que não estejam cadastrados
deny unknown-clients;

# Evita DoS. Se um cliente enviar muitos DHCPDELINE pode consumir todos os recursos do servidor
deny declines;

# configurações de DHCP Failover
failover peer "dhcp-failover" {
  primary; # declare this to be the primary server
  address 10.0.0.4; # endereço do servidor
  port 647; #porta que será feita a comunicacao
  peer address 10.0.0.12; # endereço do outro servidor
  peer port 647; #porta que será feita a comunicacao
  max-response-delay 30;
  max-unacked-updates 10;
  load balance max seconds 3;
  mclt 1800;
  split 128;
}

#Rede Servidores – Apenas para documentacao – Todos com IPs estáticos
subnet 10.0.0.0 netmask 255.255.255.0 { }

#Rede Filial 01
subnet 10.0.1.0 netmask 255.255.255.0 {
  option domain-name "empresa01.com.br";
  option routers 10.0.1.1;
```

```
  pool {
      failover peer "dhcp-failover";
      range 10.0.1.11 10.0.1.254;
  }
}

#Rede Filial 02
subnet 10.0.2.0 netmask 255.255.255.0 {
  option domain-name "empresa02.com.br";
  option routers 10.0.2.1;
  pool {
      failover peer "dhcp-failover";
      range 10.0.2.11 10.0.2.254;
  }
}

# Cadastro de dispositivos de rede
# Filial 01 – Informe o endereço MAC e o endereço IP que deseja para o dispositivo
host financeiro01 { hardware ethernet 00:00:00:00:00:01; fixed-address 10.0.1.11; }
# Filial 02 – Informe o endereço MAC e o endereço IP que deseja para o dispositivo
host recepcao01 { hardware ethernet 00:00:00:00:00:02; fixed-address 10.0.2.11; }


#---------- Fim do arquivo de configuração do Servidor Primário ---------------------------
# Autor: Michael Andre Hempkemeyer
```

Segue o arquivo de configuração do do servidor DHCP com Failover Secundário.

```
# dhcpd.conf
#
# Arquivo de um servidor DHCP com Alta Disponibilidade (Failover)
# Este arquivo deve estar no servidor SECUNDÁRIO
#
# Autor: Michael Andre Hempkemeyer
#

# Informe seu servidor de DNS
option domain-name-servers 8.8.8.8;
# Informe seu servidor NTP, ou outro servidor válido
option ntp-servers ntp.com.br;

# Tempo em que o endereço é alocado para o cliente
default-lease-time 604800;
# Tempo máximo de alocação caso o cliente solicite um tempo maior
max-lease-time 604800;

# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;

# Negar pcs que não estejam cadastrados
deny unknown-clients;

# Evita DoS. Se um cliente enviar muitos DHCPDELINE pode consumir todos os recursos do servidor
deny declines;
```

```
# configurações de DHCP Failover
failover peer "dhcp-failover" {
  secundary; # declare this to be the primary server
  address 10.0.0.12; # endereço do servidor primario
  port 647; #porta que será feita a comunicacao
  peer address 10.0.0.4; # endereço do servidor secundario
  peer port 647; #porta que será feita a comunicacao
  max-response-delay 30;
  max-unacked-updates 10;
  load balance max seconds 3;
}

#Rede Servidores – Apenas para documentacao – Todos com IPs estáticos
subnet 10.0.0.0 netmask 255.255.255.0 { }

#Rede Filial 01
subnet 10.0.1.0 netmask 255.255.255.0 {
  option domain-name "empresa01.com.br";
  option routers 10.0.1.1;
  pool {
      failover peer "dhcp-failover";
      range 10.0.1.11 10.0.1.254;
  }
}

#Rede Filial 02
subnet 10.0.2.0 netmask 255.255.255.0 {
  option domain-name "empresa02.com.br";
  option routers 10.0.2.1;
  pool {
      failover peer "dhcp-failover";
      range 10.0.2.11 10.0.2.254;
  }
}

# Cadastro de dispositivos de rede
# Filial 01 – Informe o endereço MAC e o endereço IP que deseja para o dispositivo
host financeiro01 { hardware ethernet 00:00:00:00:00:01; fixed-address 10.0.1.11; }
# Filial 02 – Informe o endereço MAC e o endereço IP que deseja para o dispositivo
host recepcao01 { hardware ethernet 00:00:00:00:00:02; fixed-address 10.0.2.11; }


#---------- Fim do arquivo de configuração do Servidor Secundário -------------------------
# Autor: Michael Andre Hempkemeyer
```

APÊNDICE E – ARQUIVO DE CONFIGURAÇÃO APACHE

Incluir no arquivo apache2.conf encontrado no diretório “/etc/apache2/”:

```
###################### Configurações extras Apache2.conf ########################

# Desativa a indexação dos diretórios da página
Options –Indexes
```

Arquivos security.conf, encontrado em “/etc/apache2/conf.d/” no Debian 7, e no diretório “/etc/apache2/conf-available/” no Debian 8. Neste segundo é necessário ativar através de um link simbólico na pasta /etc/apache/conf-enabled/” .

```
###################### Arquivo security.conf #########################

ServerTokens Prod
ServerSignature Off
```

APÊNDICE F – ARQUIVO DE CONFIGURAÇÃO SQUID

Segue um exemplo de arquivo de configuração do Squid. Existem outras opções de configuraççção além destas. O método de autentição utilizado será com o “basic_ncsa_auth”, sendo um método padrão do Squid. As outras opções deste arquivo foram descritas no sub capítulo 8.2 deste trabalho.

```
##### SERVIDOR PROXY DA SUA EMPRESA #####
# Autor: Michael Andre Hempkemeyer

# Nome que será apresentado na janela de autenticacao
visible_hostname Proxy_Empresa

# define que o Squid vai responder
http_port 3128

# dimensiona o espaço em disco para cache no diretorio /cache
cache_dir aufs /cache 60000 32 512

# arquivo e diretorio do Log do squid
access_log /var/log/squid3/access.log

# Diz qual regra bloqueou (cache.log)
### Utilizar para resolucao de problemas apenas. Geracao de Logs excessiva
#debug_options ALL,1 33,2 28,9
debug_options ALL,1

# Servidores DNS que o Squid irá utilizar
dns_nameservers 10.0.0.2
dns_nameservers 10.0.0.3

#### Configuracao de Autenticao #####
auth_param basic program /usr/lib/squid3/basic_ncsa_auth /etc/squid3/listas/usuarios.txt
auth_param basic children 5
auth_param basic realm Squid - Empresa
auth_param basic credentialsttl 2 hours

# ACL padrao do Squid
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32

#### Redes que podem solicitar requisicao ao SQUID ####
acl minhasredes src 10.0.1.0/24   # Filial01
acl minhasredes src 10.0.2.0/24   # Filial02

# Portas PERMITIDAS para conexão proxy-internet
acl SSL_ports   port 443  # https
acl SSL_ports   port 444  # https
acl SSL_ports   port 447  # https
acl SSL_ports   port 563  # https
acl SSL_ports   port 873  # https
acl SSL_ports   port 7443 # https
acl SSL_ports   port 1000 # https
acl Safe_ports  port 80   # http
```

```
acl Safe_ports  port 21   # ftp
acl Safe_ports  port 22   # ftp
acl Safe_ports  port 20   # ftp
acl Safe_ports  port 443 563 # https, snews
acl Safe_ports  port 70 # gopher
acl Safe_ports  port 210 # wais
acl Safe_ports  port 1025-65535 # unregistered ports
acl Safe_ports  port 280 # http-mgmt
acl Safe_ports  port 488 # gss-http
acl Safe_ports  port 591 # filemaker
acl Safe_ports  port 777 # multiling http
acl Safe_ports  port 631 # cups
acl Safe_ports  port 873 # rsync
acl Safe_ports  port 901 # SWAT
acl Safe_ports  port 1080
acl Safe_ports  port 1863
acl Safe_ports  port 8443 # https
acl Safe_ports  port 5222 # gTalk
acl Safe_ports  port 5223 # gTalk
acl Safe_ports  port 47057 # torrent

#
acl CONNECT method CONNECT

# Requer password para autenticacao
acl password proxy_auth REQUIRED

# Acl para domínios gov.br
acl governo url_regex -i .gov.br

# Acl para lista de computadores bloqueados por IP
acl IPsbloqueados src "/etc/squid3/listas/ListaMaquinasBloqueadas.txt"

# Acl para lista de sites liberados sem autenticacao
acl listasemauth url_regex -i "/etc/squid3/listas/ListaSemAuth.txt"

# Acl para lista branca, ou seja, todos podem acessar
acl listabranca url_regex -i "/etc/squid3/listas/ListaBranca.txt"

# Acl para lista de usuarios supervip
acl listasupervip proxy_auth "/etc/squid3/listas/ListaUsuarioSuperVIP.txt"

# Acl para lista de usuarios vip
acl listavip proxy_auth "/etc/squid3/listas/ListaUsuarioVIP.txt"

# Acl para libera site por meio de IP
acl ips_dst_liberados dstdom_regex "/etc/squid3/listas/ListaBranca_IPDestino.txt"

# bloqueia acesso de sites por meio de IP ex: http://200.193.140.98
acl todos_ips url_regex -i ^(http|https|ftp)+://[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+
acl todos_ips url_regex -i ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+

# Acl para bloqueia acesso de usuarios
acl listausuariobloqueado proxy_auth "/etc/squid3/listas/ListaUsuarioBloqueado.txt"

# Conf de cachemgr pela localhost - default
http_access allow manager localhost
http_access deny manager
```

```
# Negar requisições de portas inseguras
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports

# Negar requisições que não fazem parte da minhasredes
http_access deny !minhasredes

# Bloquear maquinas por IP
http_access deny IPsbloqueados

# libera sites sem autenticacao
http_access allow listasemauth

#libera ListaServers sem autenticacao
http_access allow listaserver

# Libera sites da lista branca independente do nivel do usuario
http_access allow password listabranca

# Bloqueia a lista de usuarios bloqueados
http_access deny password listausuariobloqueado

# libera sites gov.br
http_access allow password governo

# ips liberados para serem acessados diretamente
http_access allow password ips_dst_liberados

# bloqueia acessar site por meio de ip direto
http_access deny todos_ips

# squidGuard
redirector_access deny listaserver
redirect_program /usr/bin/squidGuard
redirect_children 8
redirector_bypass on

# Libera lista Super vip
http_access allow password listasupervip

# Libera lista vip
http_access allow password listavip

# Autoriza acesso de minhasredes e localhost
http_access allow password minhasredes
http_access allow localhost

# Regra final de negação de tudo
http_access deny all

# Leave coredumps in the first cache dir
coredump_dir /cache

#follow_x_forwarded_for para registrar ip origem
follow_x_forwarded_for allow minhasredes

# Precisa ser Transparente, pois o ON e OFF fazem alguns sites não funcionarem.
forwarded_for transparent

# Diretoria da pagina de erro
```

```
error_directory /usr/share/squid3/errors/Portuguese

#Tempo de atualizacao dos objetos relacionados aos prot ftp, gopher e http.
refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern (Release|Packages(.gz)*)$      0       20%     2880
refresh_pattern .               0       20%     4320
```