Projeto de Redes Seguras com SUSE Linux 10 SP3

LEONARDO DA SILVA PIMENTA

Trabalho de Conclusão de Curso, monográfico, apresentado como exigência da disciplina de Projeto Final, requisito obrigatório para conclusão do curso de pós-graduação MBA em Tecnologias de Redes de Computadores das Faculdades Integradas Simonsen.

LEONARDO CIOTI DE QUEIROZ FERREIRA
Orientador

Faculdades Integradas Simonsen
Curso de pós-graduação – MBA em Tec. Em Redes de Computadores
Rio de Janeiro
Julho / 2009

Sumário

1. INTRODUÇÃO

O Linux foi criado em 1991 por Linus Torvalds, então estudante finlandês, e hoje é mantido por uma comunidade mundial de desenvolvedores (que inclui programadores individuais e empresas como a IBM e a HP), coordenada pelo próprio Linus, agora um desenvolvedor reconhecido mundialmente e o mais representativo integrante da Linux Foundation.

Em palavras simplificadas, Linux é apenas o kernel do sistema operacional, ele depende de uma série de ferramentas para funcionar, a começar pelo programa usado para compilar seu código-fonte.

O Linux adota a GPL, uma licença de software livre que fornece uma série de possibilidades como base para serviços, podendo ser um servidor de arquivos (Samba), de páginas web (Apache), de banco de dados (MySQL ou Oracle Database) ou ainda de correio eletrônico (Lotus Notes).

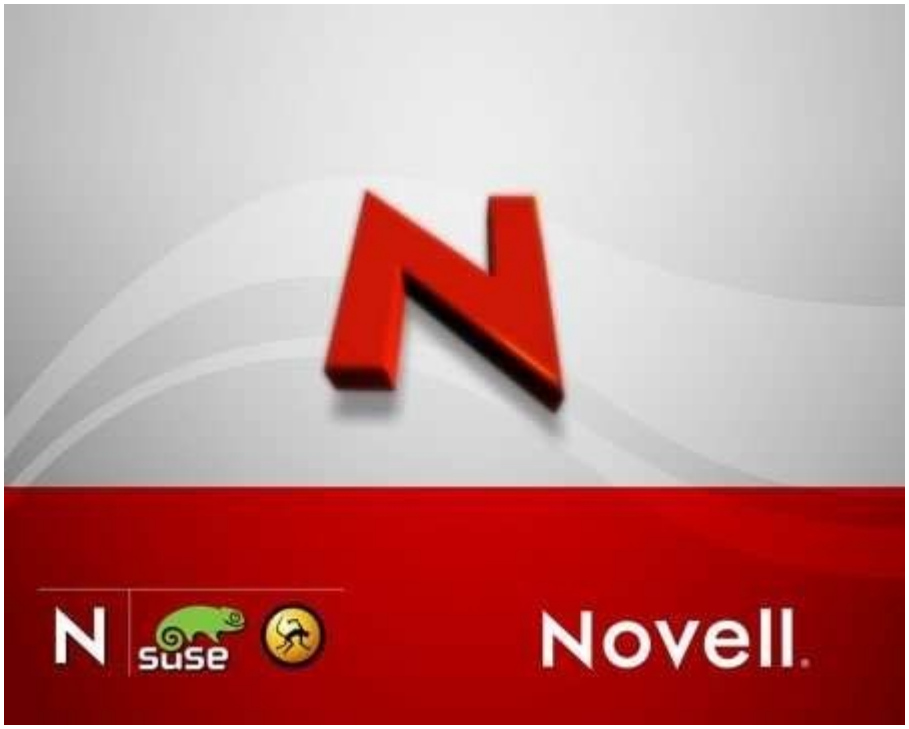
O Linux possui várias distribuições. Atualmente a distribuição Linux que vamos utilizar é a Suse Linux Enterprise 10 SP3, mantida pela Novell.

Este projeto apresenta a instalação básica que servirá para implementar qualquer dos serviços citados acima, substituindo servidores utilizando sistema operacional de rede Microsoft Windows Server 2003 e Novell Netware 6.5. Para servidores de correio eletrônico utilizados pela Marinha do Brasil, foi desenvolvido um projeto específico que não será abordado aqui, seria uma instalação para servidores Domino.

Para a compreensão do conteúdo apresentado, é necessário que o leitor seja capaz de reconhecer os componentes básicos de um servidor, como disco rígido, unidade de CD- ROM, além de ser capaz de configurar a BIOS. Deverá também estar familiarizado com o protocolo TCP/IP, serviço de nomes (DNS) e alguns outros protocolos e **serviços como o SSH** e o LDAP.

2. PREPARANDO A INSTALAÇÃO

Antes de iniciar a instalação é necessário ter em mãos o jogo de CDs ou DVDs de instalação do Suse Linux Enterprise Server 10 SP3.



OBSERVAÇÕES:

Recomendamos realizar um planejamento para definir a configuração deste servidor antes da instalação. Para isso, verifique os tópicos abaixo:

1) Propósito para o qual o servidor será destinado;

2) Quantidade de discos e espaço disponível em cada um deles;

3) Tamanho de memória física (RAM);

4) Nome a ser atribuído ao servidor;

5) Domínio de nomes (DNS) que será atribuído ao servidor (Ex.: marinha.mil.br);

6) Endereço IP a ser atribuído ao servidor;

7) Máscara de sub-rede a ser atribuída ao servidor;

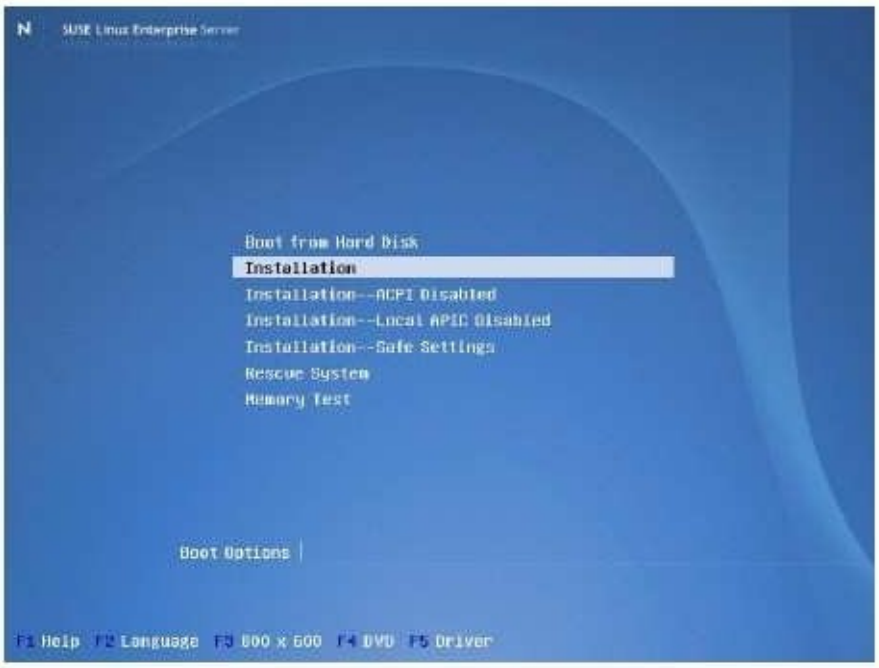
8) Endereço de gateway que será utilizado pelo servidor;

9) Endereço DNS a ser utilizado pelo servidor: 199.214.224.4 (primário) e 199.214.224.6 (secundário).

3. INÍCIO DA INSTALAÇÃO

a) Configure a BIOS para inicializar a partir do CD-ROM;

b) Insira o (CD-ROM / DVD) na unidade leitora e inicialize o servidor até aparecer a tela abaixo;



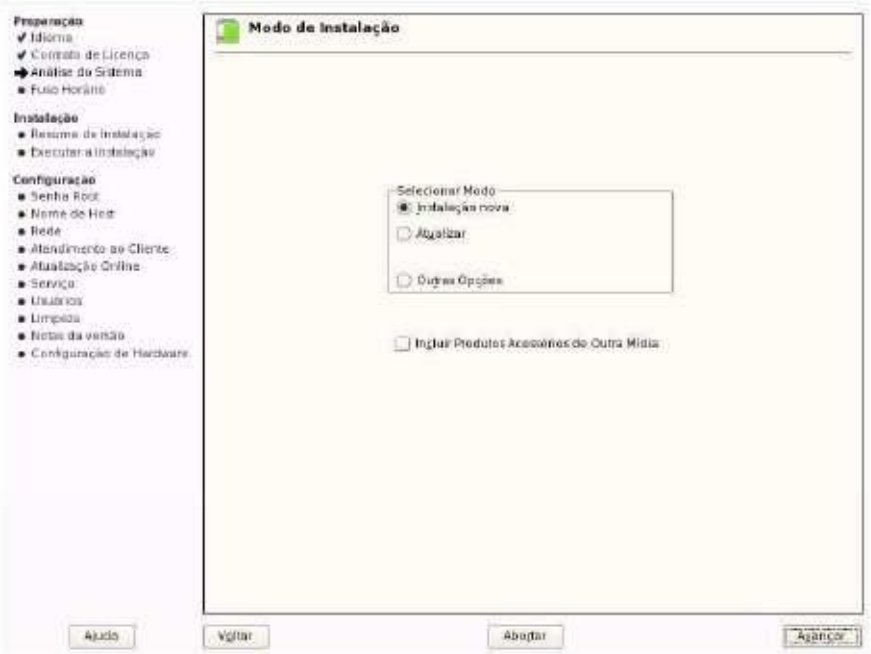
c) Na primeira tela pressione F2 para selecionar o idioma;

d) Selecione a opção Instalação e pressione <ENTER>;

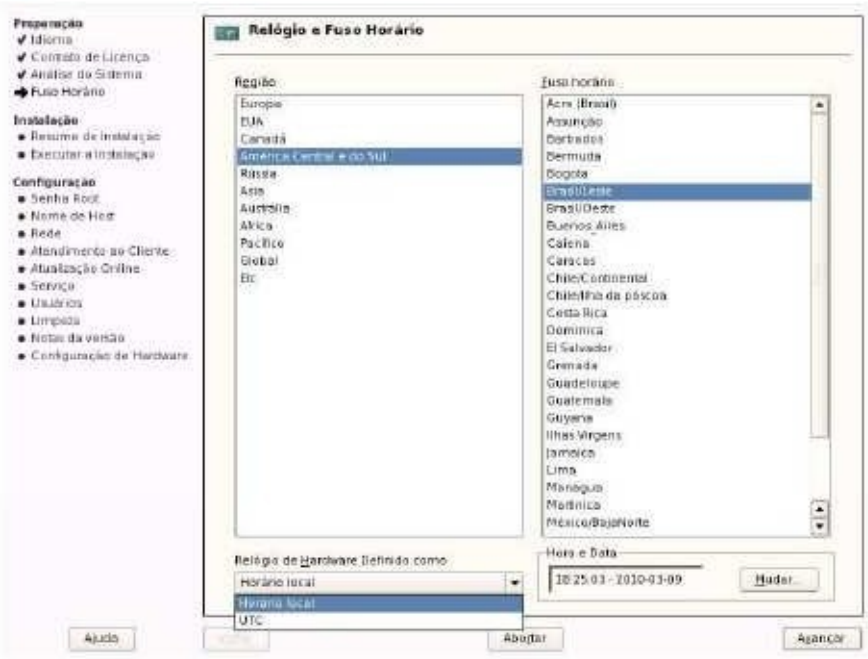
e) Na tela seguinte será apresentado o contrato de licença.

Clique em “Sim, Eu Aceito este Contrato de Licença” e depois em Avançar;

f) Selecione “Instalação nova” e clique em Avançar;



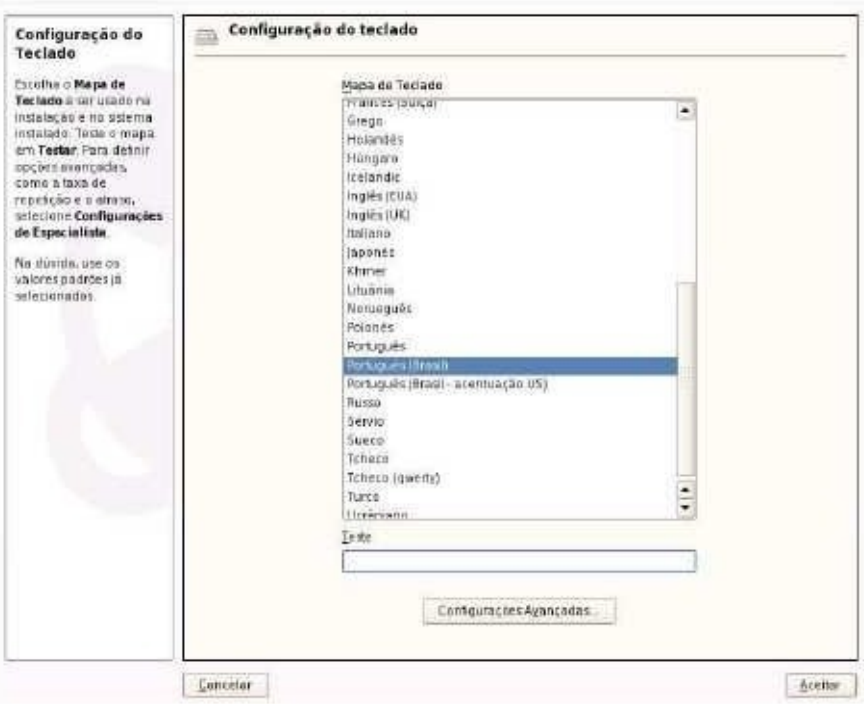
g) Agora selecione o fuso horário onde o servidor está localizado e, na caixa “Relógio de Hardware Definido Como” selecione a opção “Horário Local”;



h) A tela seguinte apresenta o resumo da configuração a ser efetuada.

- Aqui é possível alterar cada um dos itens exibidos.

i) O instalador detecta automaticamente o tipo do teclado, caso o teclado seja diferente do tipo indicado na tela, clique no link “Mapa do Teclado” e selecione o layout adequado conforme a tela abaixo:



Faça o teste do teclado. Caso tudo funcione corretamente, clique em “Aceitar”.

j) O instalador retornará ao ponto do “Resumo da Instalação”.

4. PARTICIONAMENTO DO DISCO

Particionamento ou formatação do disco significa dividir o disco em setores endereçáveis, permitindo que os dados possam ser gravados e posteriormente lidos de maneira organizada. Primeiramente devesse compreender que existem três tipos de partições: partição primária, partição estendida e partição lógicas.

4.1 PARTIÇÃO PRIMÁRIA

A divisão do disco em trilhas, setores e cilindros é chamada de formatação de baixo nível, agregando à tal a definição de um sistema de arquivos, que é um conjunto de estruturas lógicas e de rotinas, que permitem ao sistema operacional controlar o acesso ao disco rígido. Possui o limite de quatro partições primaria por HD.

4.2 PARTIÇÃO ESTENDIDA

O limite de quatro partições é insuficiente?

Para ultrapassar o limite de quatro partições primárias, utiliza-se a partição estendida, que é uma partição primária que serve de repositório para outras partições (lógicas).

OBSERVAÇÃO: As partições estendidas não podem conter os arquivos de inicialização de um sistema operacional.

4.3 PARTIÇÃO LÓGICA

É uma partição que contém um sistema de arquivos, contida em uma partição estendida. Para que partições estendidas possam ser utilizadas, é necessário que sejam divididas em partições lógicas.

Assim, a partição estendida deve ser encarada como um container de partições

lógicas e as partições lógicas como aquelas que serão utilizadas de fato para alocação de dados.

LIMITAÇÕES:

- ✔ Um disco rígido pode conter quatro partições primárias e, no máximo, uma partição estendida;
- ✔ Em uma partição estendida pode ser criada até 60 partições lógicas para discos IDE e 12 para discos SCSI;
- ✔ No total, dependendo do esquema de particionamento, um disco IDE terá no máximo 63 partições (três primárias e 60 lógicas) e até 15 partições em discos SCSI (três primárias e 12 lógicas).

4.4 PLANEJANDO O PARTICIONAMENTO DO DISCO

De posse das informações anteriores e lembrando que a forma na qual o disco foi particionado influência na performasse do sistema. Abaixo será explanado um padrão de acordo com os serviços oferecidos pelo servidor:

- ✔ Swap – Deverá ter no mínimo o tamanho da memória física e no máximo o dobro. Em servidores de Banco de dados e Notes Domino a swap sempre terá o dobro do tamanho da RAM. Em servidores de arquivos ou web a swap poderá ter o mesmo tamanho da RAM desde que o servidor disponha de pelo menos 512mb de RAM;
- ✔ / (Chamada de “barra” ou “raiz”) - Deverá ter no mínimo 4GB;
- ✔ /boot – Armazenará os arquivos de inicialização e deverá ter entre 100MB e 512MB;

✔ /tmp – Deverá variar entre 512MB e 2GB, dependendo do tamanho do disco disponível;

✔ /var – Armazenará, principalmente, arquivos de log e deve possuir espaço suficiente para guardar registros de um tempo razoável. Para alguns servidores de banco de dados e proxies é também onde ficam armazenados os arquivos para serviços, sendo necessária essa consideração no cálculo de seu tamanho. Recomenda-se ter pelo menos 5GB.

Ao realizar o planejamento, o Admin deverá se atentar à finalidade do servidor. Por isso,esclarecemos abaixo a necessidade de um particionamento adequado para que não ocorram problemas futuros. Dependendo do serviço que este fará, disponibilize mais espaço numa partição específica. Exemplos:

Particionamento para Servidores de Arquivos (SAMBA)

✔ /home – (Utilizada para armazenar os arquivos dos usuários).

Particionamento para Servidores de Correio Eletrônico (Notes Domino)

✔ /local – (Utilizada para armazenar as bases de dados Notes).

✔ /opt – (Utilizada para armazenar os arquivos executáveis).

Particionamento para Servidores de Banco de Dados

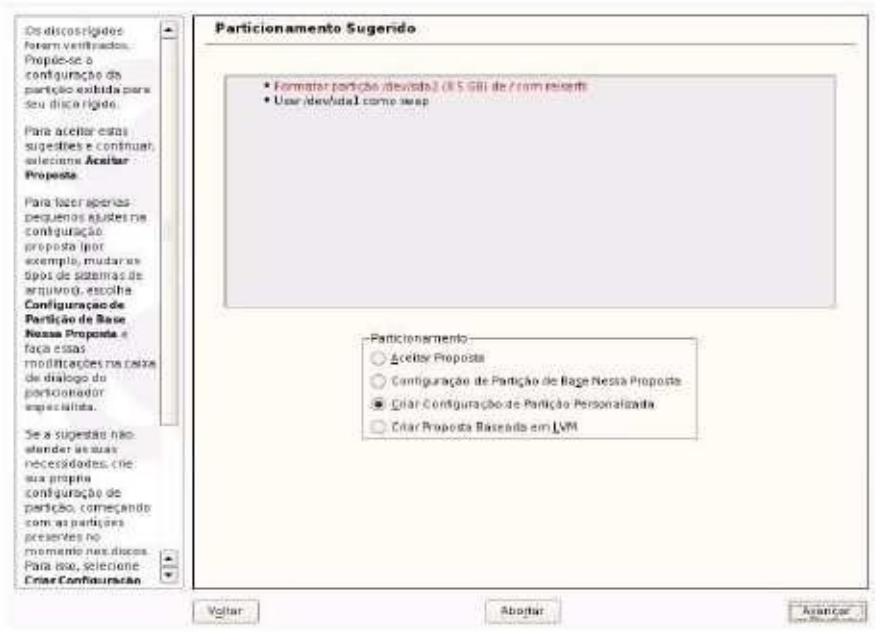
✔ /opt – (Utilizada para armazenar os arquivos executáveis).

Particionamento para Servidores Web

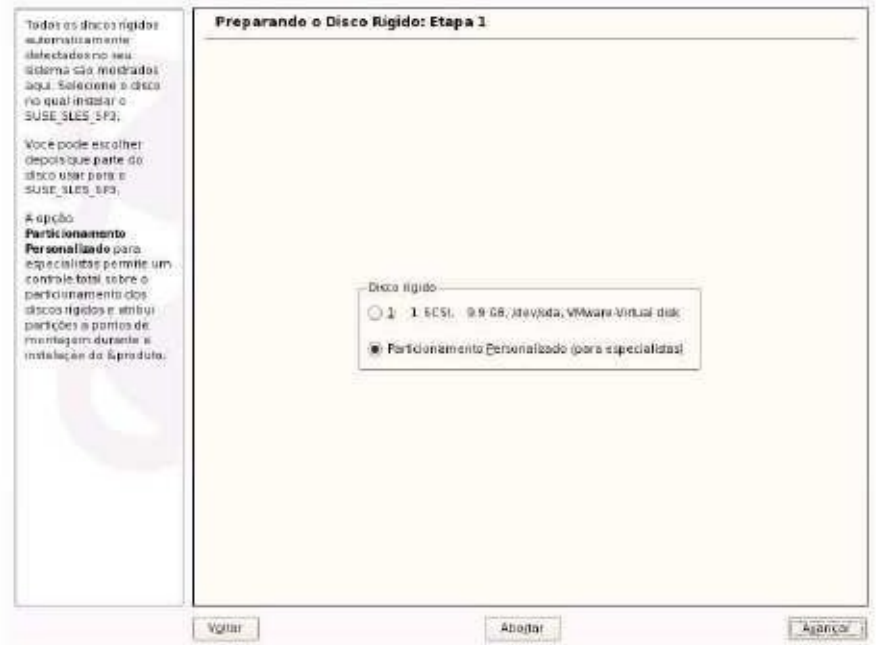
✔ /srv – (Utilizada para armazenar as páginas publicadas pelo servidor).

4.5 PARTICIONANDO O DISCO

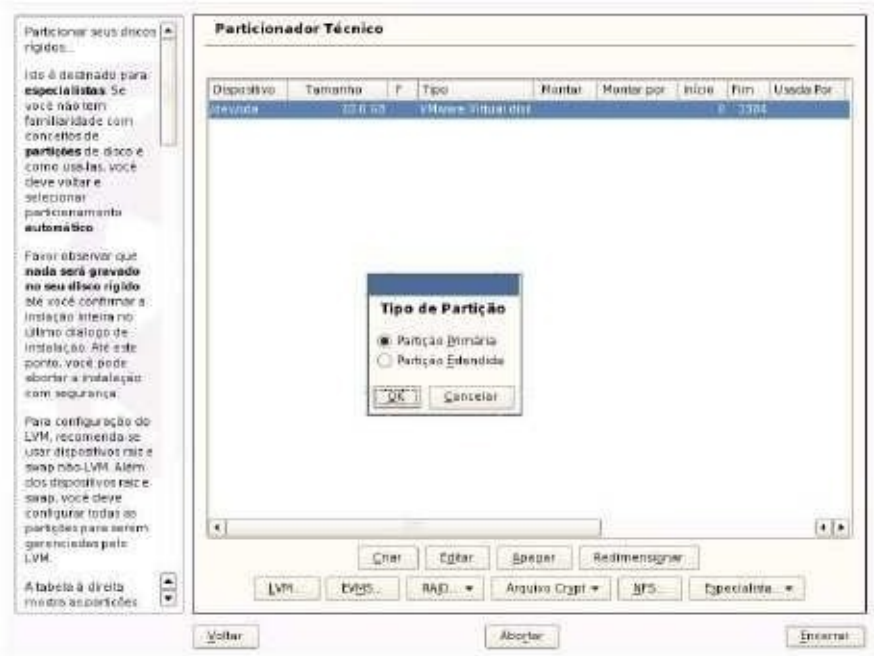
No resumo da instalação, clique em “Particionamento” e, na tela seguinte, em “Criar Configurações de Partição Personalizada”.



Na tela seguinte clique em “Particionamento Personalizado (para especialistas)”.

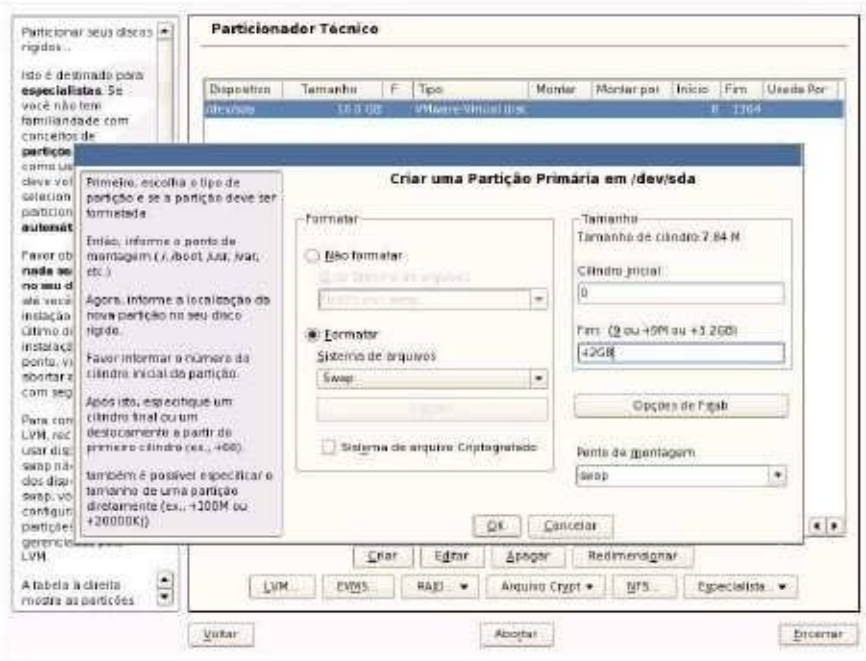


OBSERVAÇÃO: É extremamente importante que, neste ponto, o planejamento das partições já tenha sido realizado. Como por exemplo, que tenha sido definido corretamente quais serão as partições e o espaço reservado para cada uma.
Na tela do particionador, selecione e apague qualquer partição existente usando o botão “Apagar”. Logo depois, clique em “Criar” para criar uma nova partição. Caso o computador possua mais de um HD, aparecerá uma tela perguntando qual HD a partição será criada. Então, selecione “Partição Primária” e depois em “OK”.



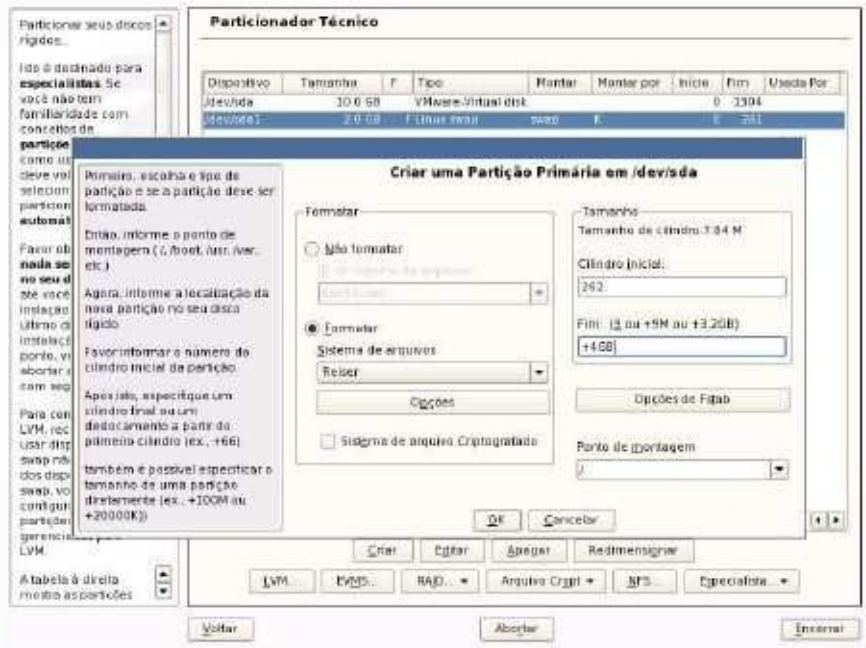
Selecione o sistema de arquivos para “Swap” e defina o ponto de montagem para “swap”. O tamanho da partição swap deverá ser definido conforme já explicado no Item 4.4.

Clique em “OK” e depois clique em “Criar” para criar uma nova partição.



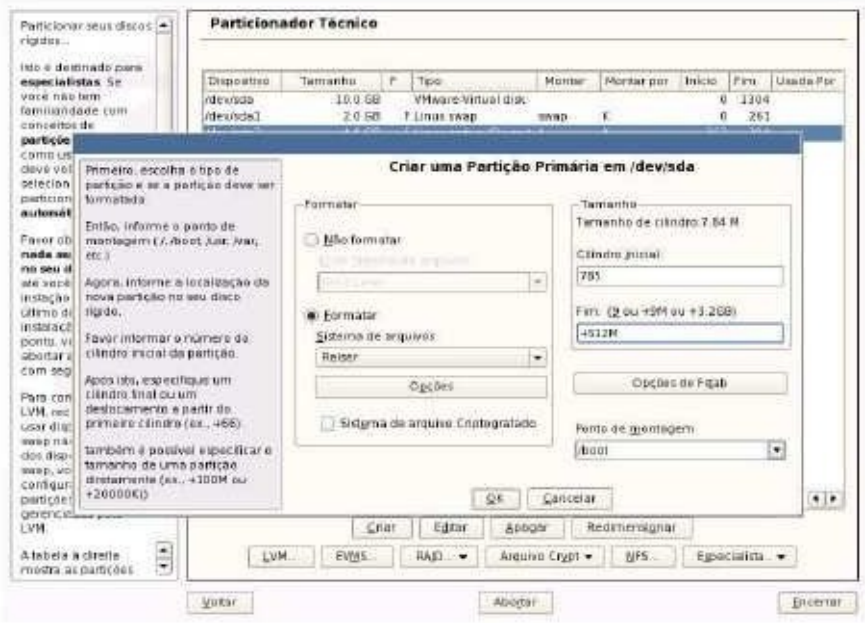
Selecione o sistema de arquivos para “Reiser” e defina o ponto de montagem para “/” para a instalação do sistema operacional. O tamanho da partição deverá ser definido conforme já explicado no Item 4.4.

Clique em “OK” e depois em “Criar” para criar mais uma partição.

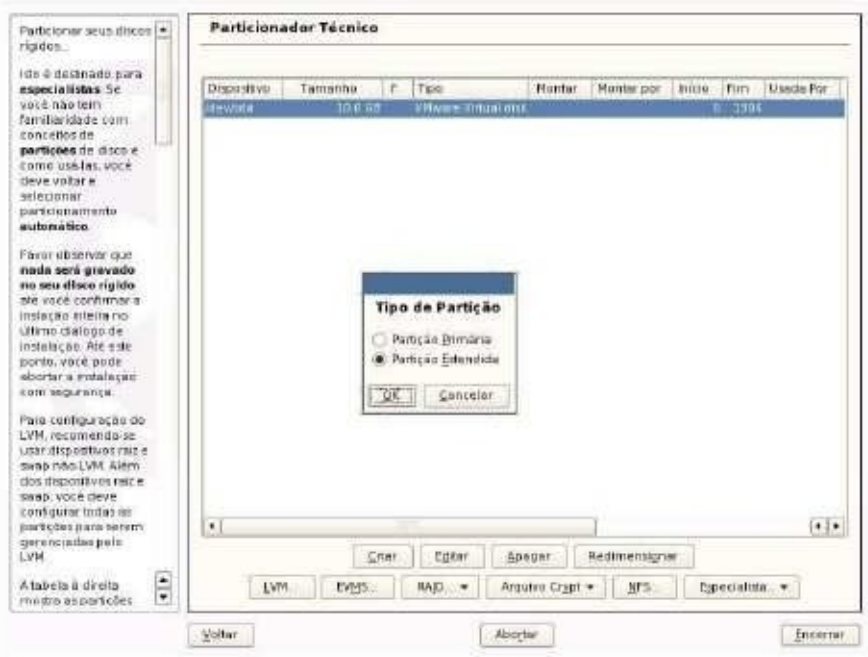


Selecione novamente o sistema de arquivos para “Reiser” e o ponto de montagem para

"/boot". Clique em "OK" e depois em "Criar" para criar mais uma partição.



Agora é preciso criar uma partição estendida ocupando o restante do espaço em disco. Nessa partição as demais partições serão criadas como partições lógicas. Selecione a opção “Partição Estendida” e na tela seguinte apenas clique no botão “OK”.



Continue a criar todas as partições necessárias, seguindo as orientações contidas no Item 4.4.

5. ESCOLHENDO OS SOFTWARES

Nesta etapa da instalação, as partições do disco estão configuradas. Prosseguindo com a instalação, selecione os softwares que serão configurados inicialmente com seu servidor. Esta é uma etapa delicada, pois o script de configuração do instalador realiza uma série de procedimentos e configurações que são difíceis de serem realizados manualmente numa instalação posterior. Caso especialmente notado com o servidor LDAP.

Além de evitar futuros problemas recomendamos que a analise do propósito do servidor e configure seu sistema para ser instalado com os software afins.

Note que com isso não estamos dizendo para marcar todos os softwares que serão disponibilizados na instalação, o que poderia criar uma problema de segurança e de desempenho.

Ao clicar no link “Software”, será exibida a tela a seguir, que permitirá escolher grupos de software pré-selecionados de pacotes para serem instalados.

Na classe “Funções Principais”, estão dispostos os pacotes de software conforme os serviços pretendidos.

A figura a seguir exibe tela de instalação dos pacotes. Selecione os seguintes itens:

- Sistema de base de Servidor;
- Ambiente Desktop;
- Ambiente Desktop GNOME para Servidores;
- Sistema X Window;
- Servidor de Arquivos;
- Servidor Web e LAMP;
- Servidor de Diretório (LDAP);
- C/C++ Compilador e Ferramentas;

Os itens em azul são específicos aos serviços de Arquivos e Web, enquanto que o item verde não é necessário aos serviços de Correio Eletrônico.

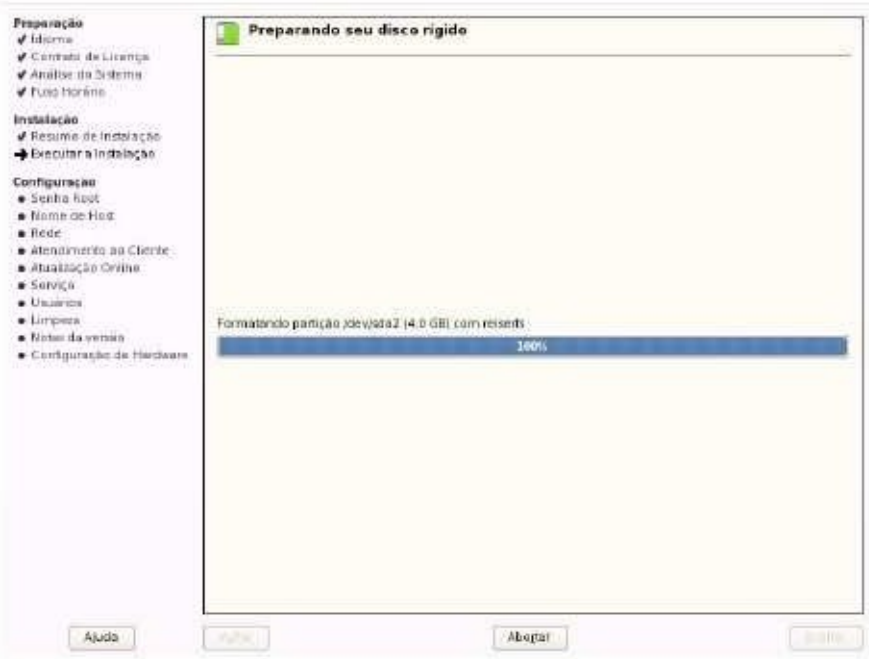
Não marque itens além desses. Clique em “Aceitar”.

6. FINALIZANDO A INSTALAÇÃO

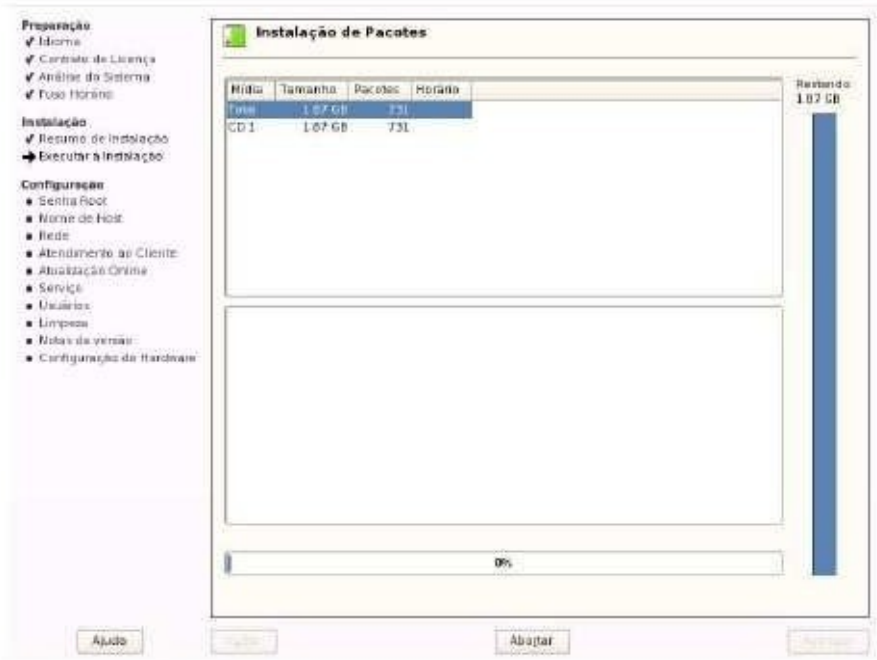
Nesta etapa, a configuração da instalação estará concluída. Será exibida uma tela semelhante à tela a seguir, com o resumo da instalação:

Clique em “Aceitar” e confirme a Instalação clicando em “Instalar”:

Após será exibida a tela abaixo:



O sistema realizará a cópia dos arquivos e pedirá o segundo DVD / CD de instalação.

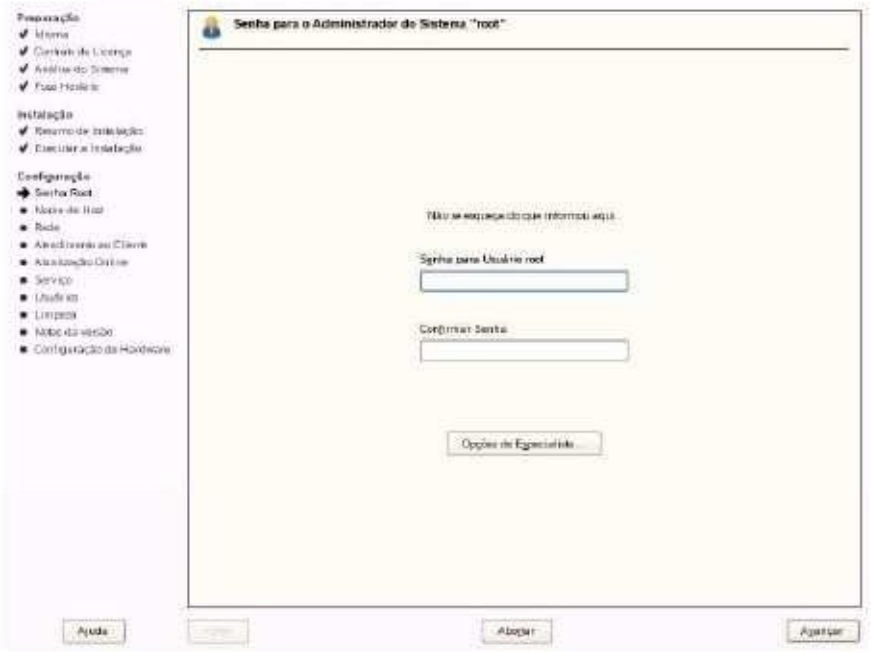


Quando terminar o servidor será reinicializado automaticamente.

7. SERVIDOR LDAP

A partir deste ponto, será realizada a configuração inicial do servidor, onde serão definidos a senha do administrador, o nome do servidor, o endereço IP e o tipo de autenticação que será aceita entre outros parâmetros.

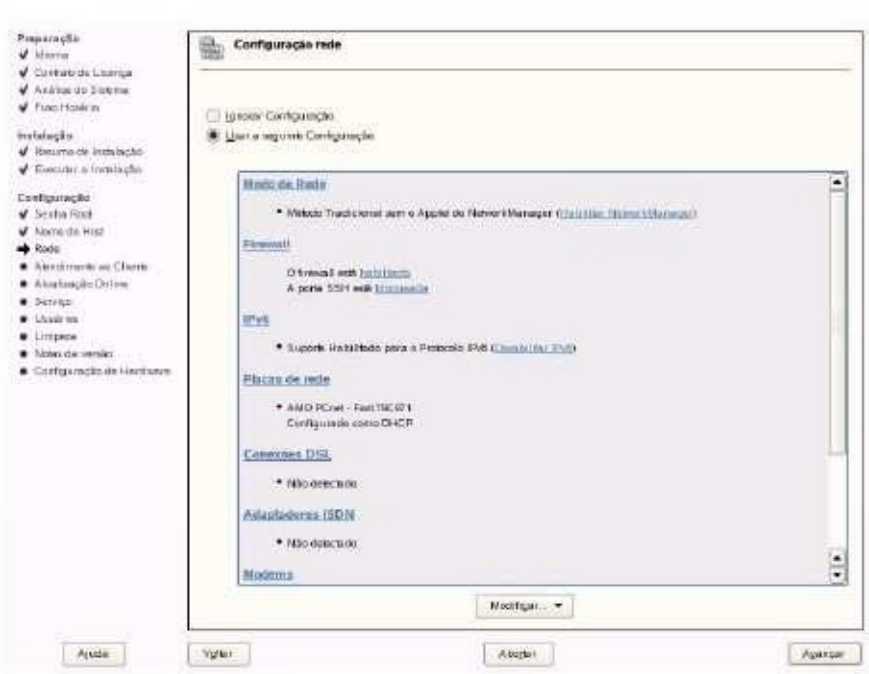
A primeira informação solicitada será a senha do root:



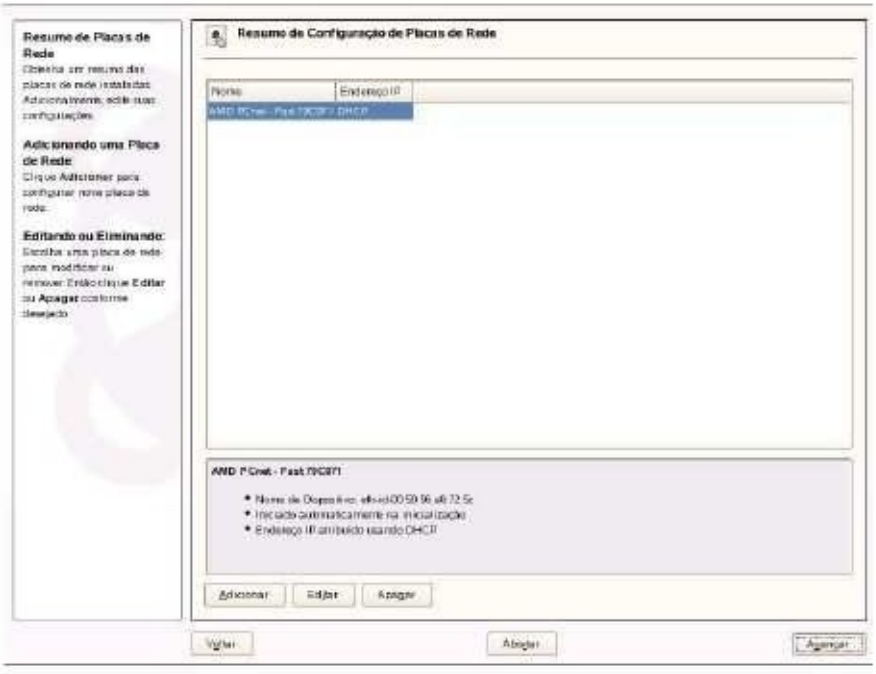
Esta senha deverá ser mantida em sigilo, pois possibilita controle completo sobre o servidor. Na tela seguinte informe o nome que será dados ao servidor, o domínio (Ex.: ctim.mb) e desmarque a opção “Trocar Nome de Host via DHCP”.

A tela seguinte apresenta o resumo da configuração de rede. Desbloqueie o acesso via SSH para poder gerenciar o servidor remotamente, para isso clique em “A porta SSH está bloqueada”, que deverá mudar para “A porta SSH está aberta”.

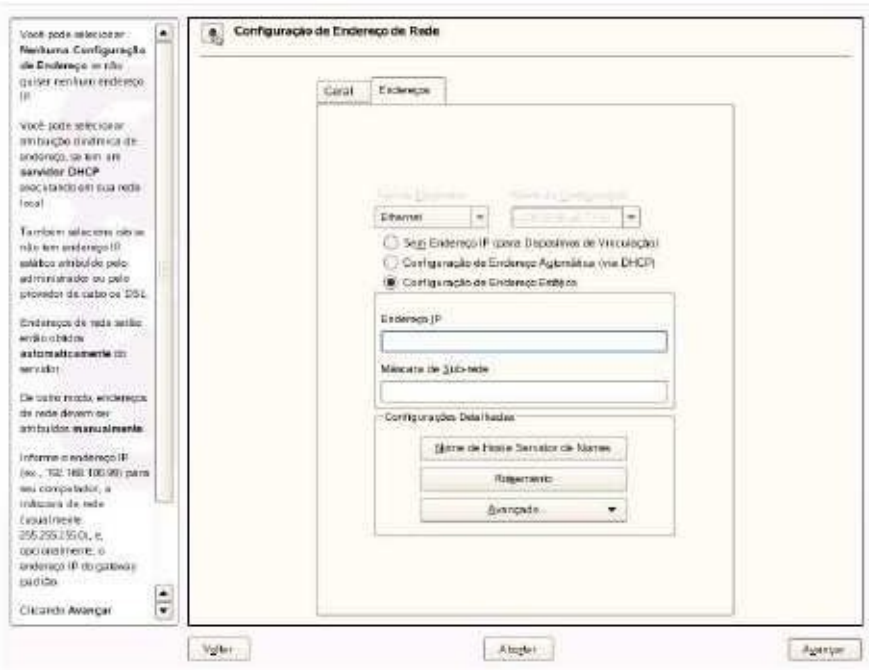
Clique em “Placas de Rede” para iniciar a configuração das interfaces.

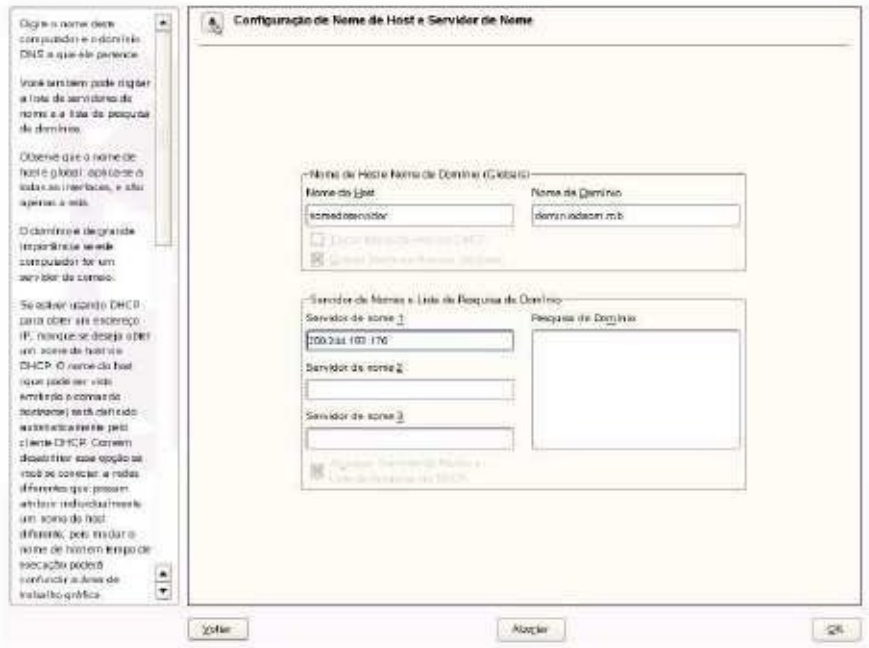


Selecione a placa a ser configurada e clique no botão “Editar”.



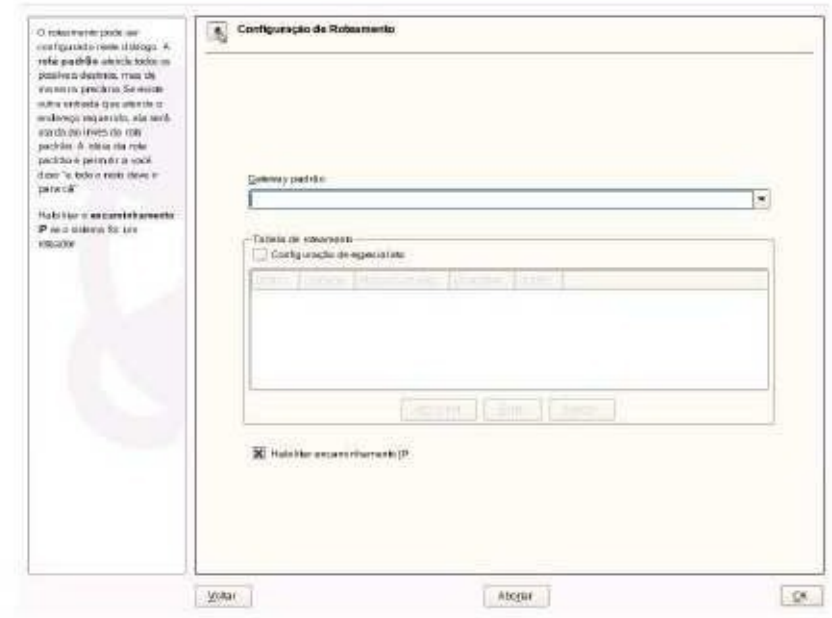
Nesta tela, clique em “Configuração de Endereço Estático”, configure o IP e a Mascara de Sub-rede a ser usado pelo servidor, após clique em “Nome do Host e Servidor de Nomes”.



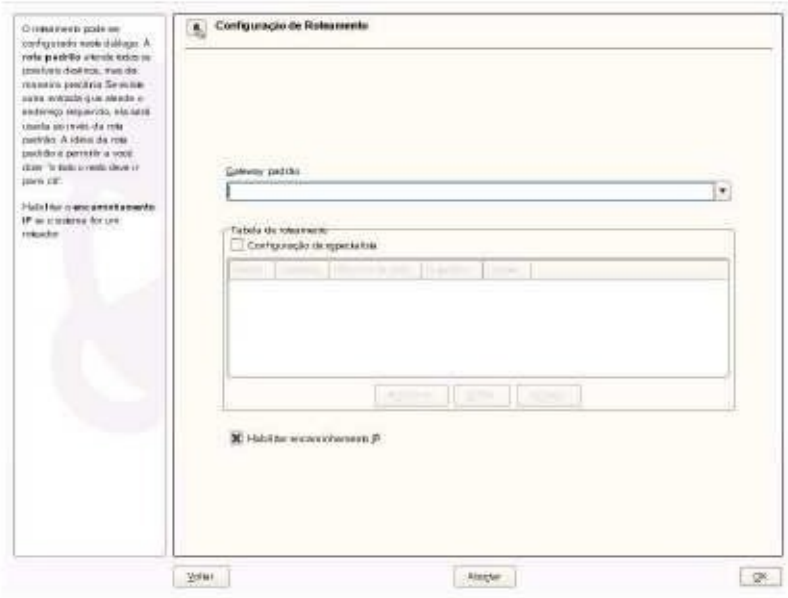


Defina o Nome do Host e Nome de Domínio. No campo “Servidor de nome 1” e “Servidor de nome 2” digite o DNS da sua área.

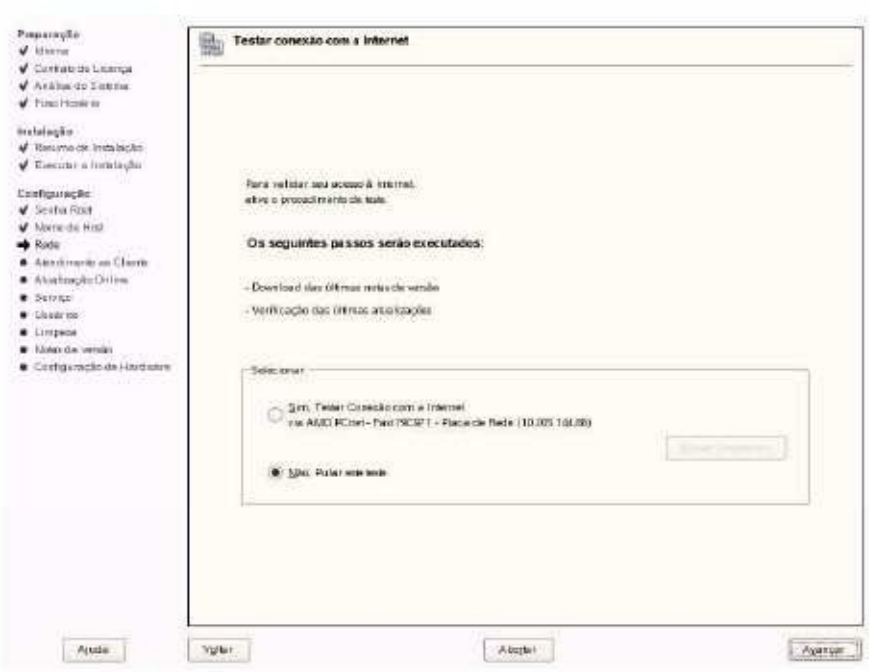
Informações de DNS estão disponíveis no site do CTIM > Gerência da RECIM > DNS.



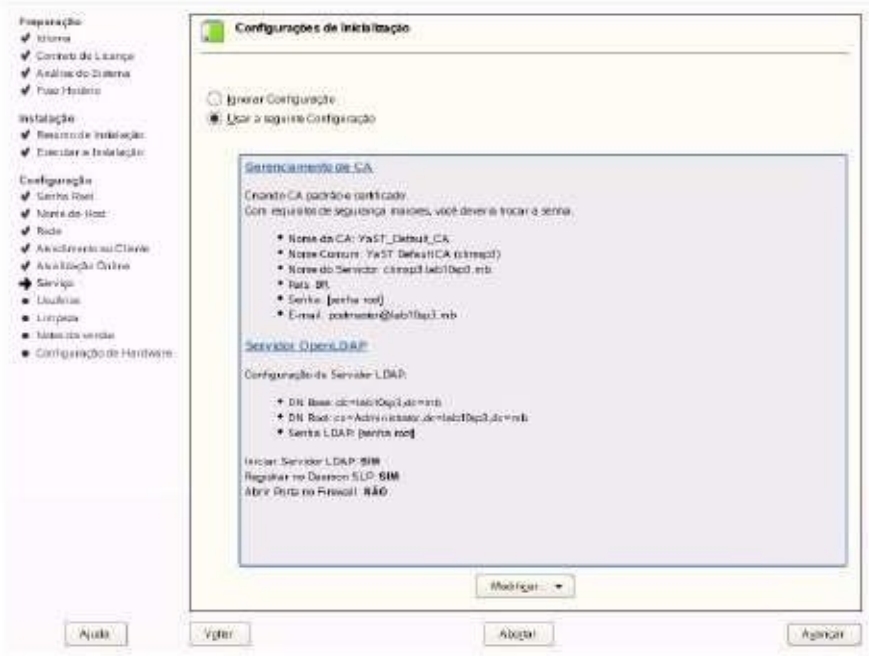
Digite o endereço do Gateway no campo “Gateway Padrão”.



Na tela seguinte será solicitado um teste de conexão com a internet. Clique em "Não, pular este teste".



Na tela de configuração seguinte clique no link "Gerenciamento de CA".



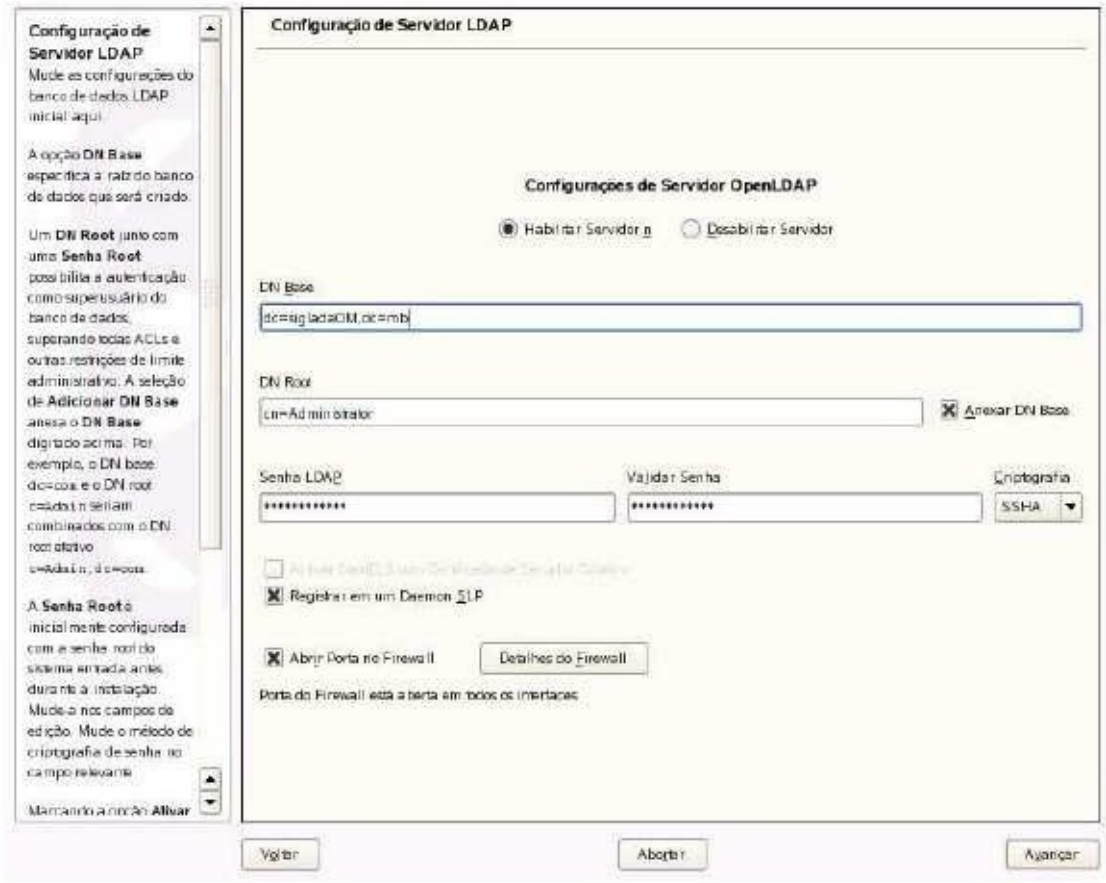
Selecione a opção "Não Criar CA e Certificado":

7.1 CONFIGURAÇÃO DO SERVIDOR LDAP

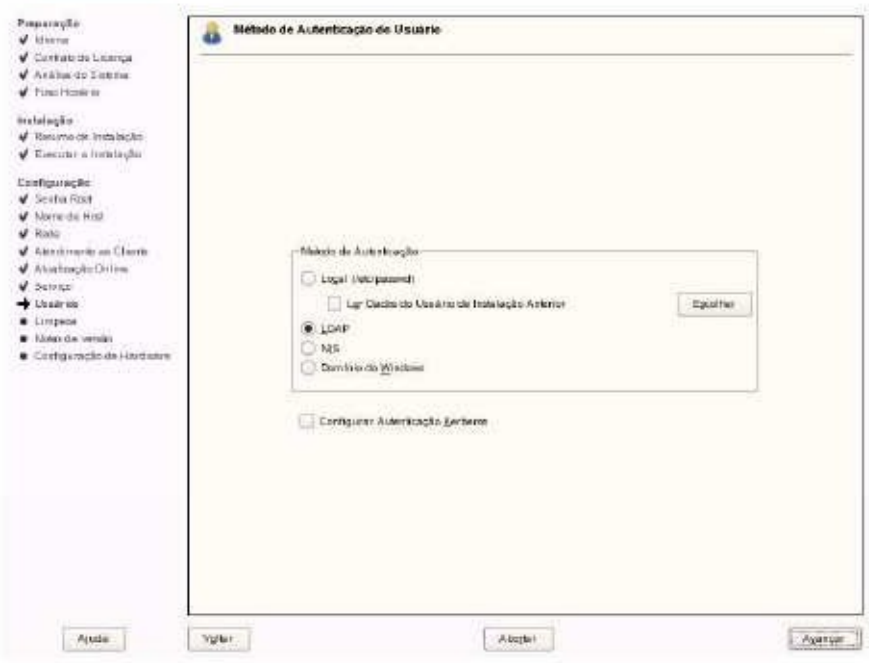
Observação: Os próximos passos de Configuração LDAP não são necessários para os servidores Domino (Notes) e Epo.

Clique em “Servidor LDAP” e clique em “OK” na caixa de confirmação que aparecerá em seguida. Clique em “Habilitar Serviço n” e “Abrir Porta no Firewall”.

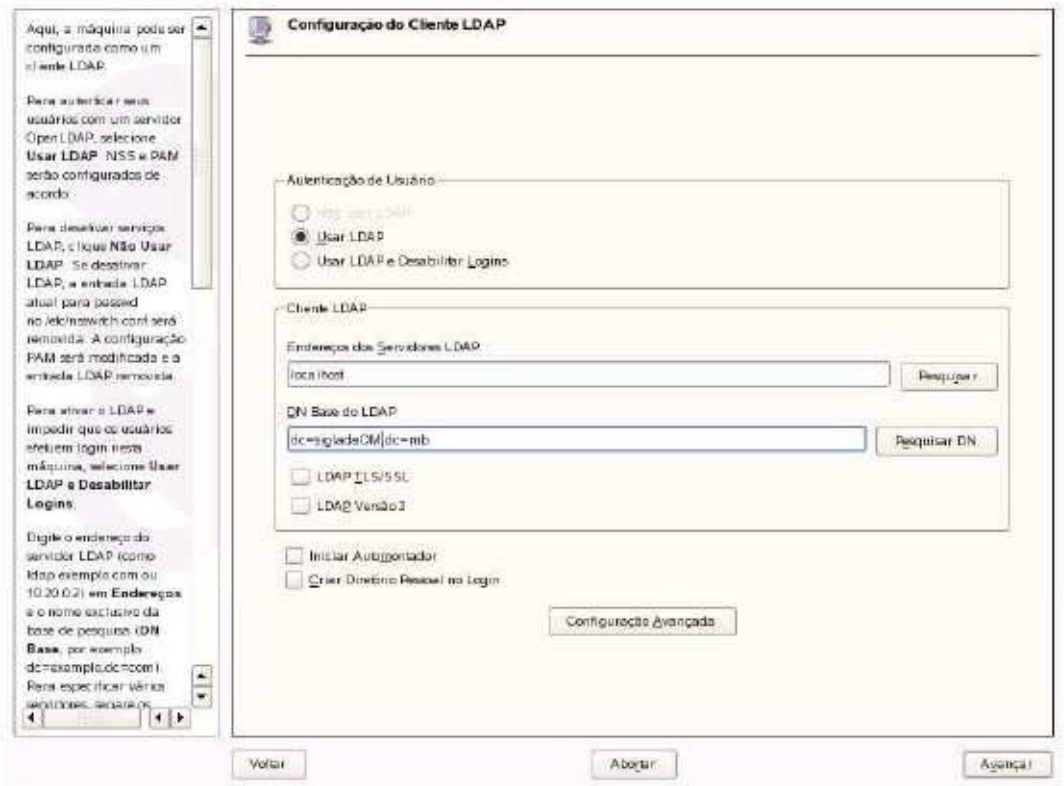
Defina o DN Base, que deve obedecer o padrão “cn=sigla_da_OM,dc=mb” e defina a senha do LDAP.



Na tela seguinte, certifique-se de que o método de autenticação selecionado é “LDAP” (exceto para servidor Notes Domino, que utilizará a opção “Local”).

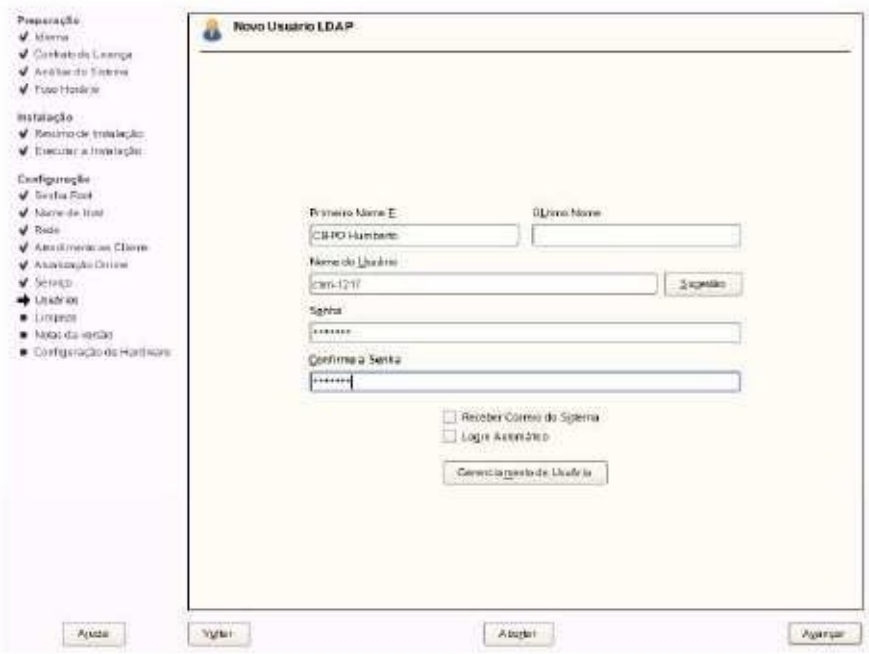


No passo seguinte, apenas clique em “Avançar”.

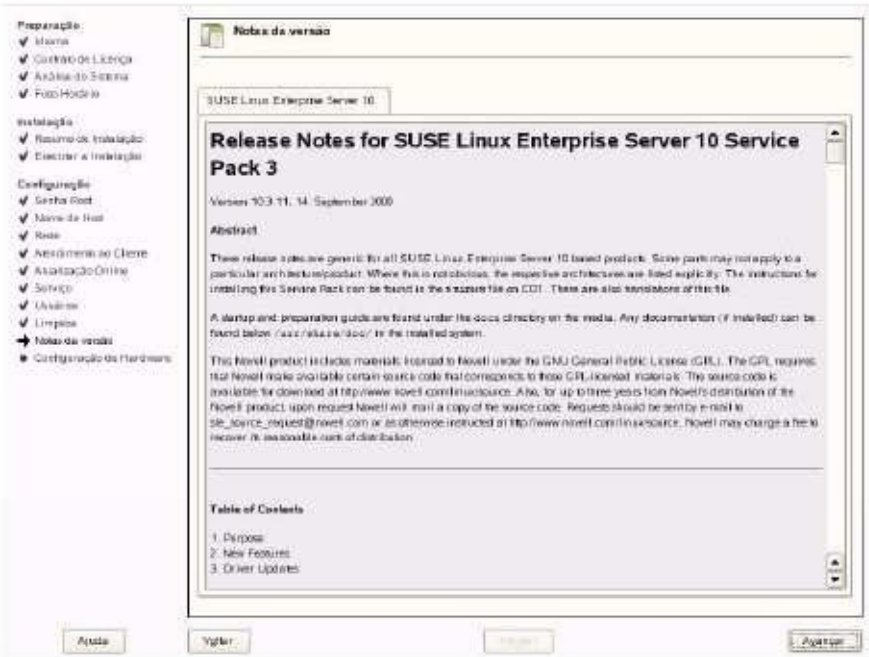


Caso seja solicitado, insira o CD ou DVD de instalação e clique em “Avançar”.

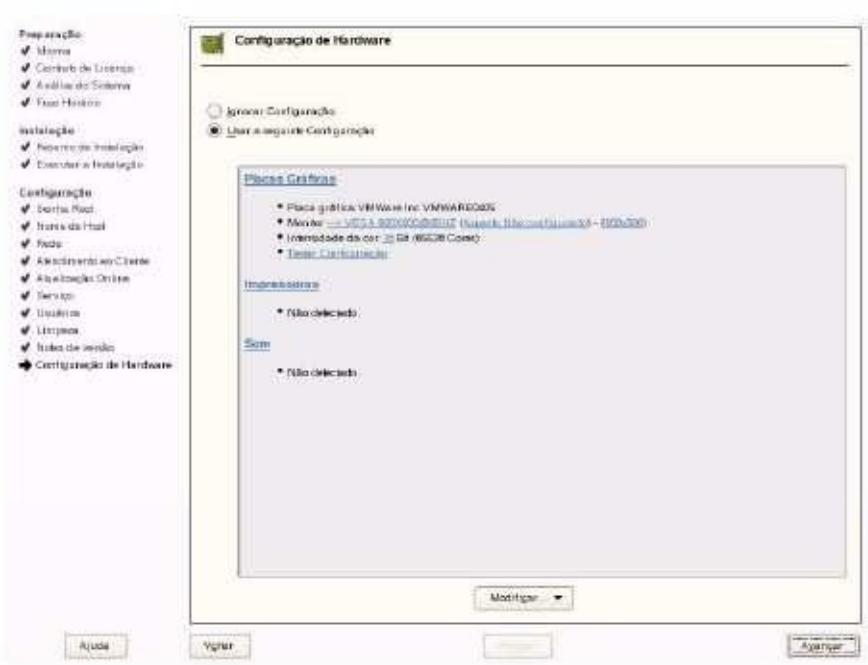
A tela seguinte permite a criação de um usuário que deve ser utilizado inicialmente para acessar o servidor.



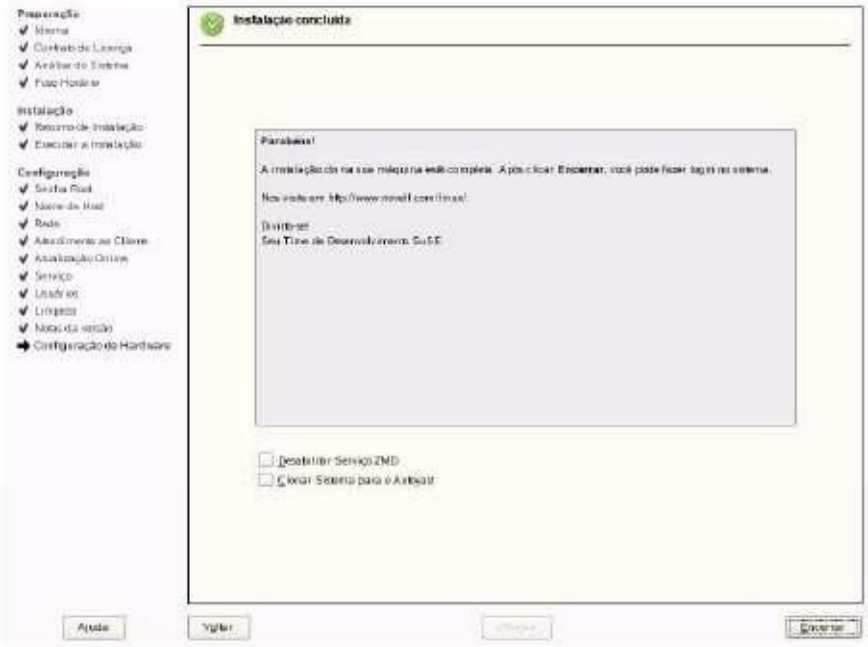
A tela seguinte apresenta as últimas modificações e novidades da versão.



Na sequência, será exibida uma tela com o resumo da configuração do hardware reconhecido.



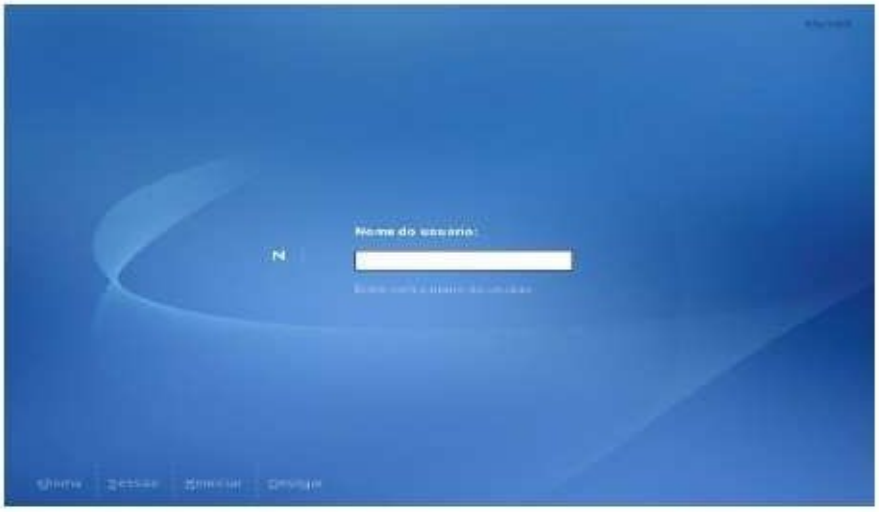
Ao clicar em “Avançar”, será exibida a tela de conclusão de instalação.



Parabéns ! A instalação do SUSE LINUX SP3 foi concluída com sucesso.

Agora abordaremos a configuração de pós-instalação que consiste de uma etapa importante e de conformidade para o correto funcionamento do servidor.

8. CONFIGURAÇÃO PÓS-INSTALAÇÃO



Na tela de Login, digite o nome e a senha do usuário criado anteriormente.

Quando o ambiente gráfico estiver carregado, clique no menu “Computador”, localizado a esquerda da barra de tarefas. Clique em “YaST”.

O YaST é o equivalente ao Painel de Controle do Windows e oferece uma série de possibilidades de configurações de hardware e serviços.

A partir do YaST, é possível realizar praticamente qualquer configuração do servidor, sempre que é acionado, a senha do usuário root (administrador do servidor) é solicitada.

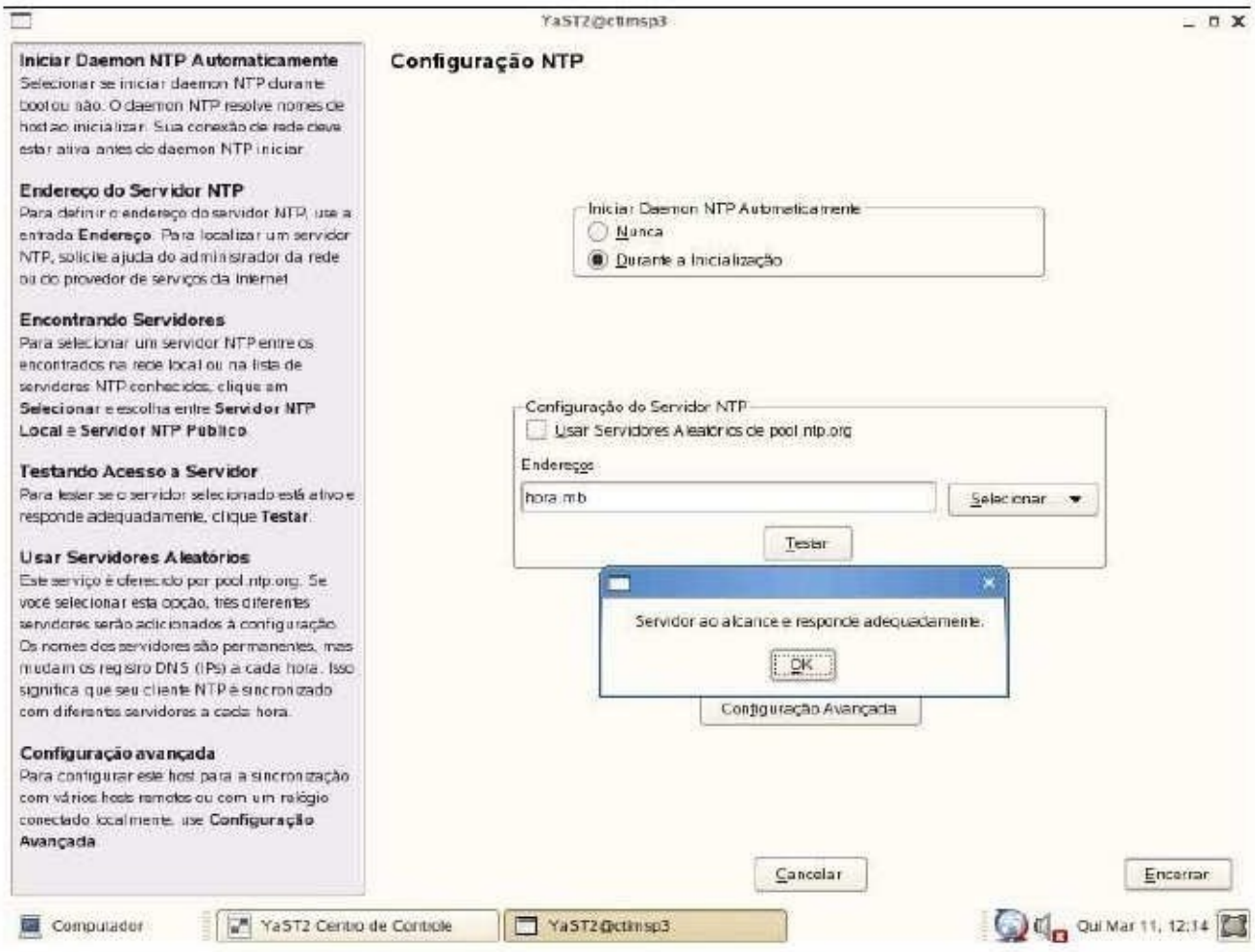
Após a instalação do servidor, a primeira configuração necessária é a de Sincronismo de Hora.

Para iniciar essa configuração, clique em “Serviços de Rede” no painel esquerdo do YaST e em “Configuração NTP”.

Na caixa “Iniciar Daemon NTP Automaticamente” selecione “Durante a Inicialização”.

No Campo “Endereços A” digite “hora.mb” (sem as aspas) e clique no botão “Testar”.

Se a rede estiver configurada corretamente, será exibida uma caixa avisando que o servidor está ao alcance e responde adequadamente. Clique no botão “Encerrar”.

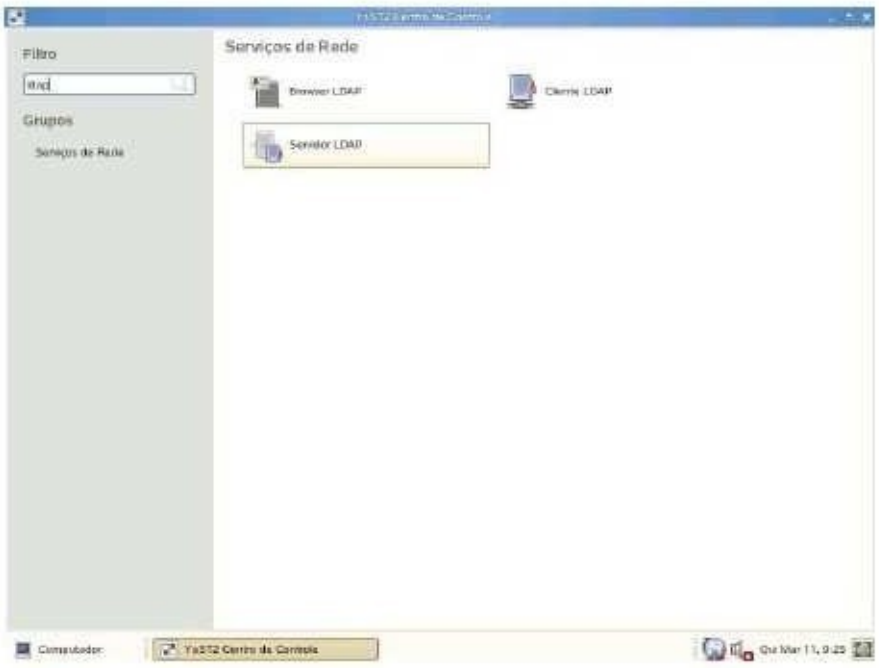


Observação: Configure o Serviço de Hora de acordo com a sua região.

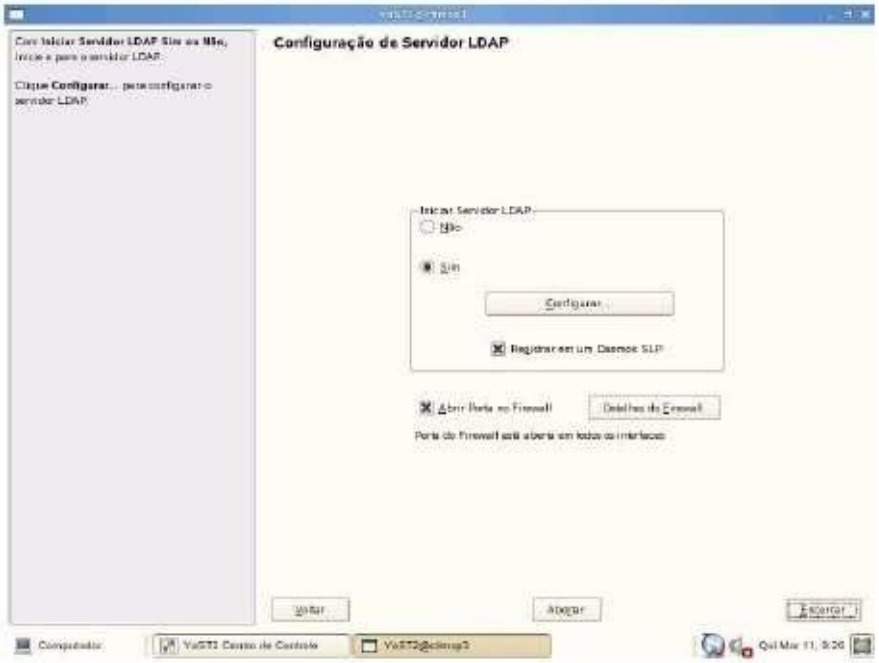
Exemplo: Servidores da Área da sede de Manaus = hora-manaus.mb.

8.1. PÓS-INSTALAÇÃO DO SERVIDOR LDAP

Clique agora em Servidor LDAP. Note que você pode usar a guia “Filtro” para realizar pesquisar rápidas.

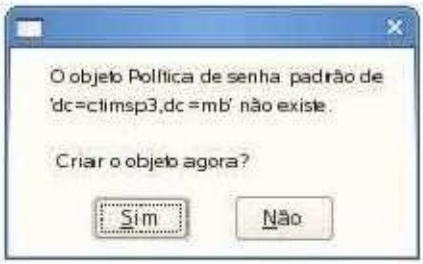


Certifique-se de que as opções “Sim” e “Abrir porta no firewall” estão selecionadas. Clique no botão “Configurar”.



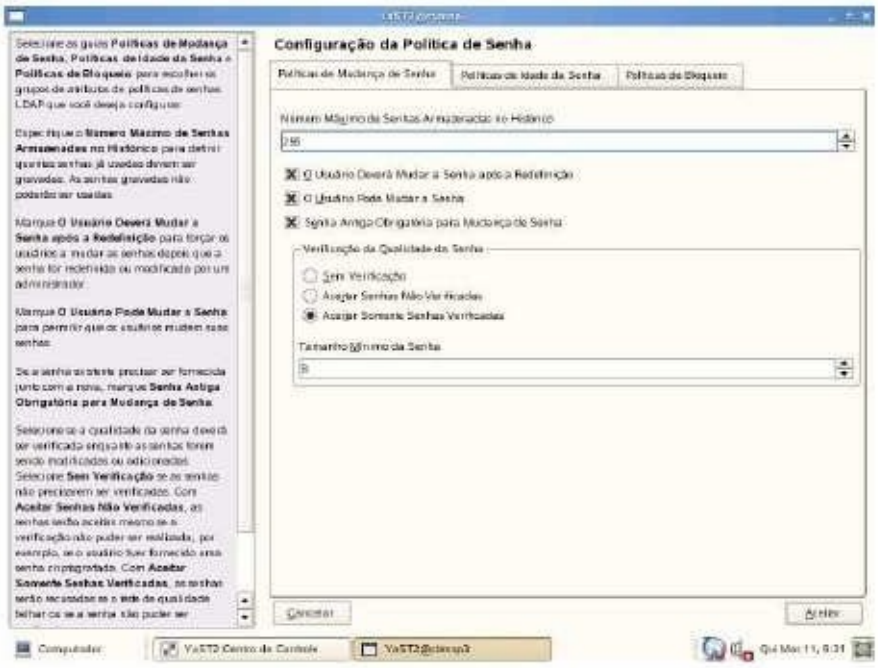
Na tela seguinte clique no sinal “+” ao lado de “Banco de dados” para expandir a seleção. Selecione o domínio do servidor. Digite a senha do LDAP e clique na caixa “Habilitar Políticas de Senha” e em seguida no botão “Encerrar”.

Confirme a criação do objeto Política de Senha.



Digite a senha do Administrador.

8.2 DEFININDO AS POLÍTICAS DE SENHA

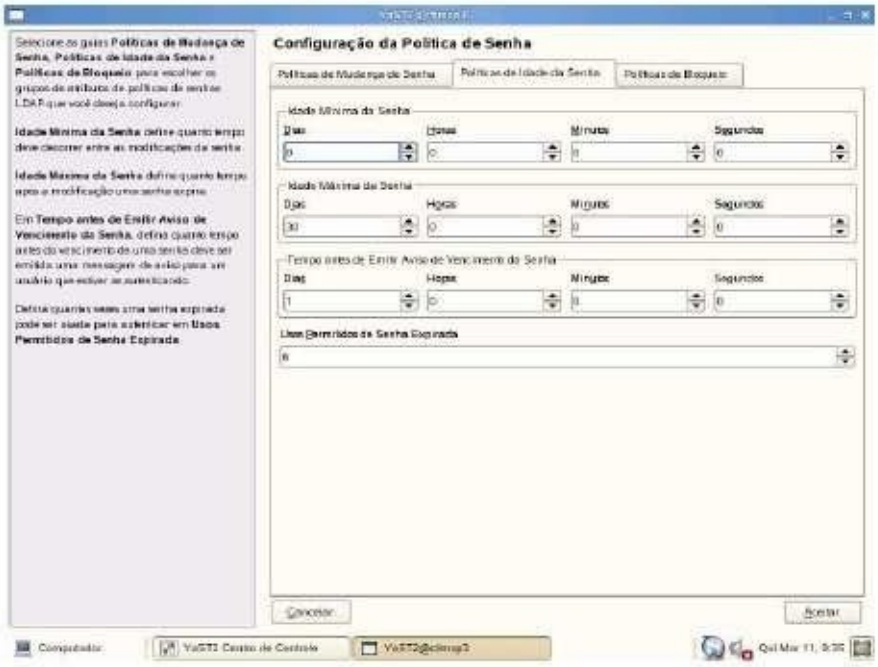


Na primeira tela de configuração das Políticas de Senha, há os seguintes campos:

- ✔ Número máximo de senhas armazenadas no histórico: Essas senhas não poderão ser repetidas.
- ✔ O usuário deverá mudar a senha após a redefinição: Quando o administrador mudar a senha de um usuário este será solicitado no próximo login a alterar sua senha.
- ✔ O usuário pode mudar a senha: permite que o usuário altere sua senha quando desejar.
- ✔ Senha antiga obrigatória para mudança de senha: funciona em conjunto com a opção anterior, fazendo com que o usuário deva digitar a senha antiga para poder inserir uma nova.
- ✔ Verificar qualidade da senha: Define se a quantidade da senha que será testada quando o usuário tentar trocá-la. É recomendável selecionar “Aceitar somente senhas verificadas”

✔ Tamanho minimo da senha: Define o número mínimo de caracteres que a senha deverá ter para ser considerada válida.

A tela seguinte refere-se aos períodos de validade da senha.



Seus campos podem ser descritos como:

✔ Idade mínima da senha: tempo mínimo em que o usuário deverá utilizar a senha. Recomenda-se manter este tempo em 0 para que o usuário possa trocar sua senha a qualquer momento.

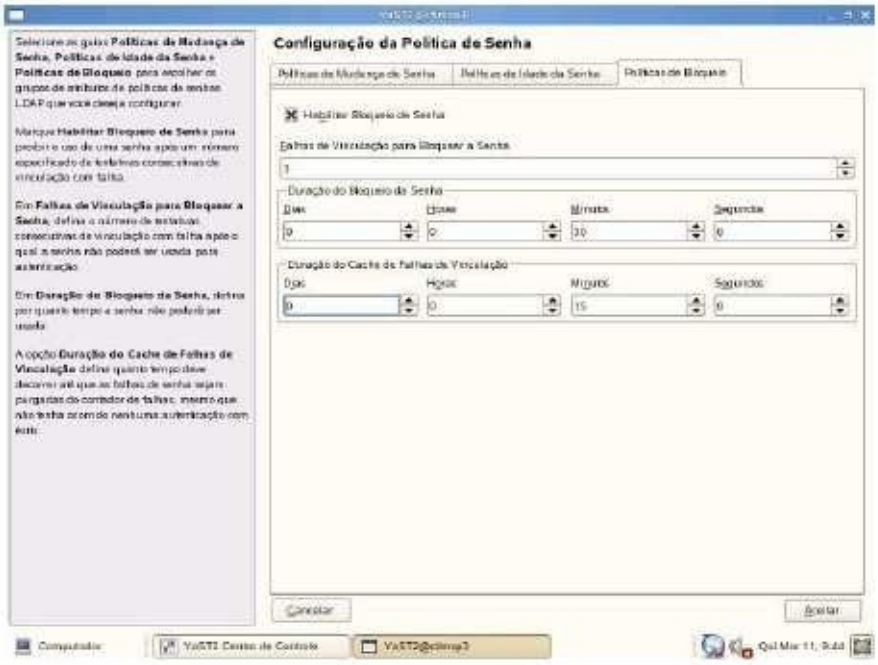
✔ Idade máxima da senha: período em que a senha poderá ser utilizada.

✔ Tempo antes de emitir aviso de vencimento de senha: Número de dias antes da data da expiração da senha em que o usuário será avisado de que ela está por vencer.

✔ Uso permitido de senhas expiradas: número de vezes que o usuário poderá logar mesmo após sua senha ter vencido.

A última tela da Política de senha trata do bloqueio em caso de tentativas de invasão.

Clique em “Habilitar bloqueio de senha”.



Seus campos devem ser descritos como:

- ✔ Falhas de vinculação: número de erros que quando ultrapassado ativará a política de bloqueio.
- ✔ Duração do bloqueio: tempo em que a conta ficará bloqueada caso a política de bloqueio seja ativada.
- ✔ Duração do cache de falhas: é o tempo em que caso as falhas excedam o número previsto a política de bloqueio será ativada.

A tela acima pode ser lida da seguinte maneira: “Se a senha for informada erroneamente mais de 3 vezes no intervalo de 15 minutos a conta ficará bloqueada por 30 minutos.”

Clique em “Aceitar” para encerrar a configuração e feche o YaST.

Parabéns ! a instalação e configuração inicial foi concluída com sucesso.

9. CONFIGURANDO O FIREWALL

O Firewall é um dispositivo que impõe uma política de segurança com o objetivo de regular o tráfego de dados entre hosts (servidores e estações de trabalho) e/ou redes, impedindo dessa forma a transmissão e/ou recepção de acessos nocivos ou não autorizados entre esses elementos.

O Suse 10 SP3 vem configurado por padrão com o firewall habilitado. Pode-se habilitar ou desabilitar o firewall utilizando a ferramenta YaST, contudo não é recomendável desabilitá-lo, e sim disponibilizar, quando houver necessidade, portas de acesso para um determinado serviço a um ou mais usuários. Neste caso, o procedimento consiste em criar filtros usando comandos do Iptables, o firewall padrão do linux.

Antes de qualquer intervenção, o serviço precisa estar habilitado pelo firewall. Para conferir e/ou habilitá-lo basta acessar o yaST > Segurança e Usuários > Firewall > Serviços Permitidos. Os serviços listados como permitidos são aqueles que poderão ser utilizados através do host, caso contrário não haverá possibilidade de se acessar tal serviço. Através das Figuras 1, 2, 3 e 4 pode-se visualizar essas opções por meio da ferramenta yaST.

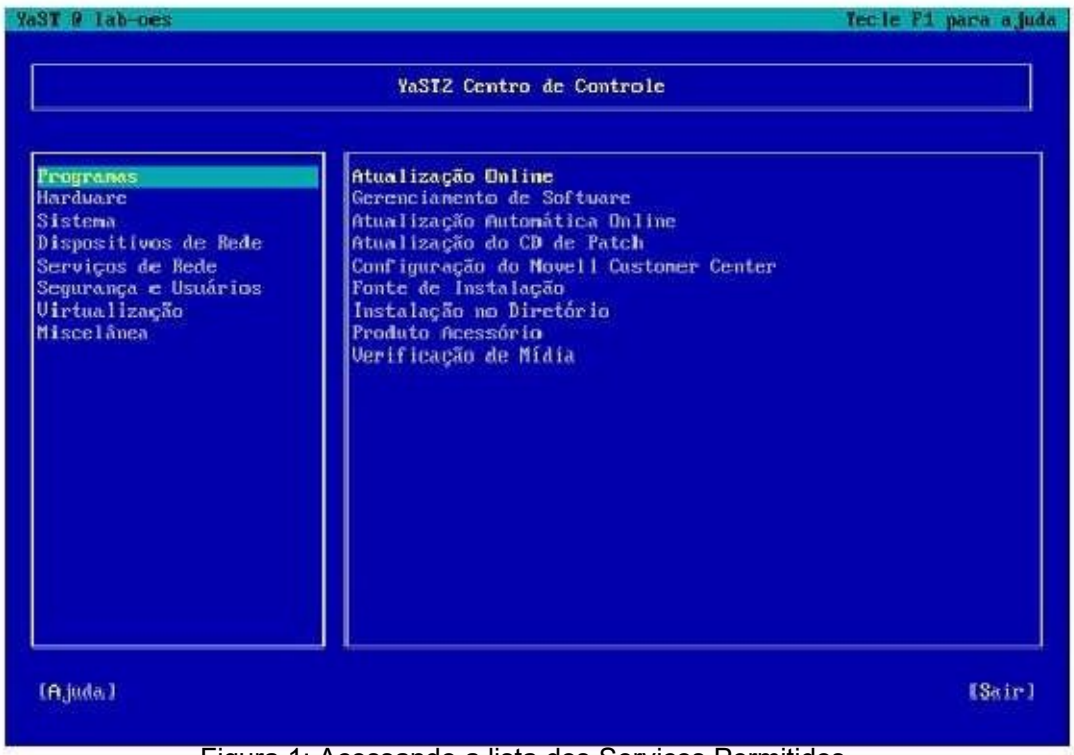


Figura 1: Acessando a lista dos Serviços Permitidos

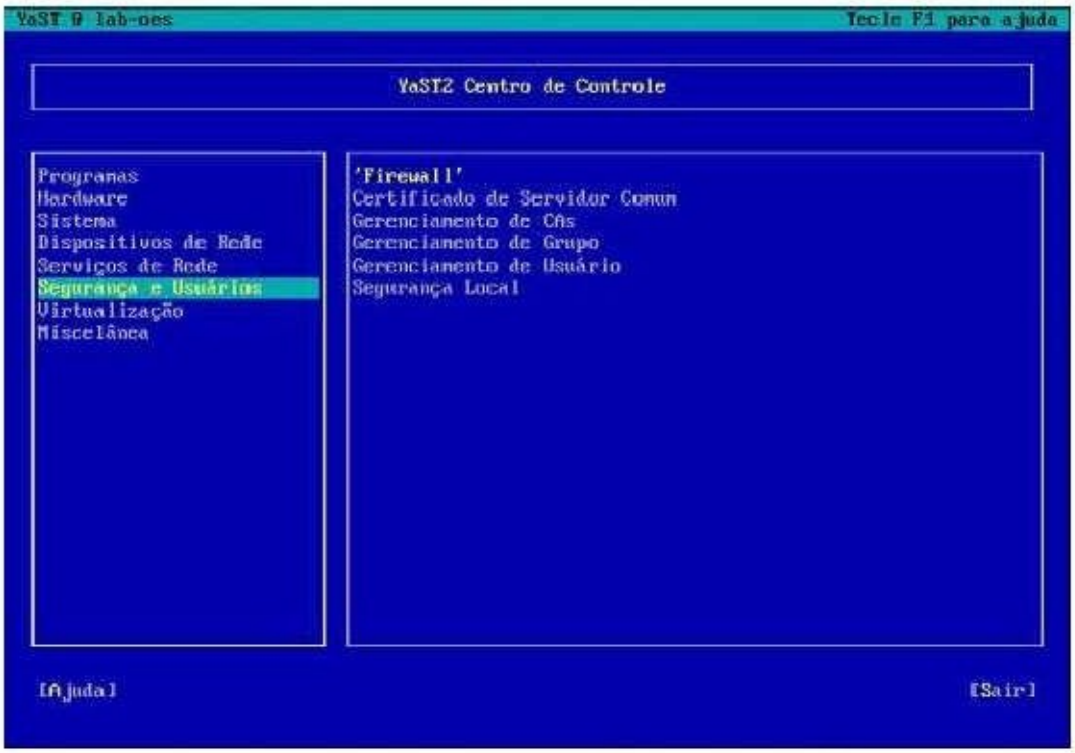


Figura 2: Acessando a lista de Serviços Permitidos

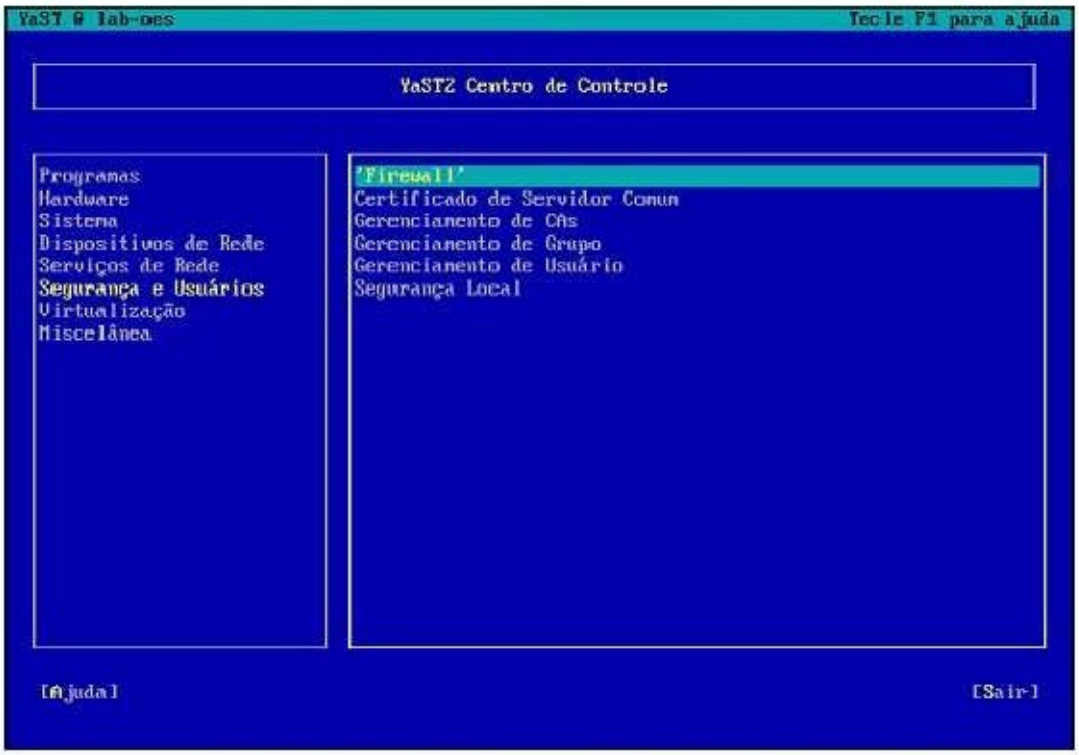


Figura 3: Acessando a lista dos Serviços Permitidos

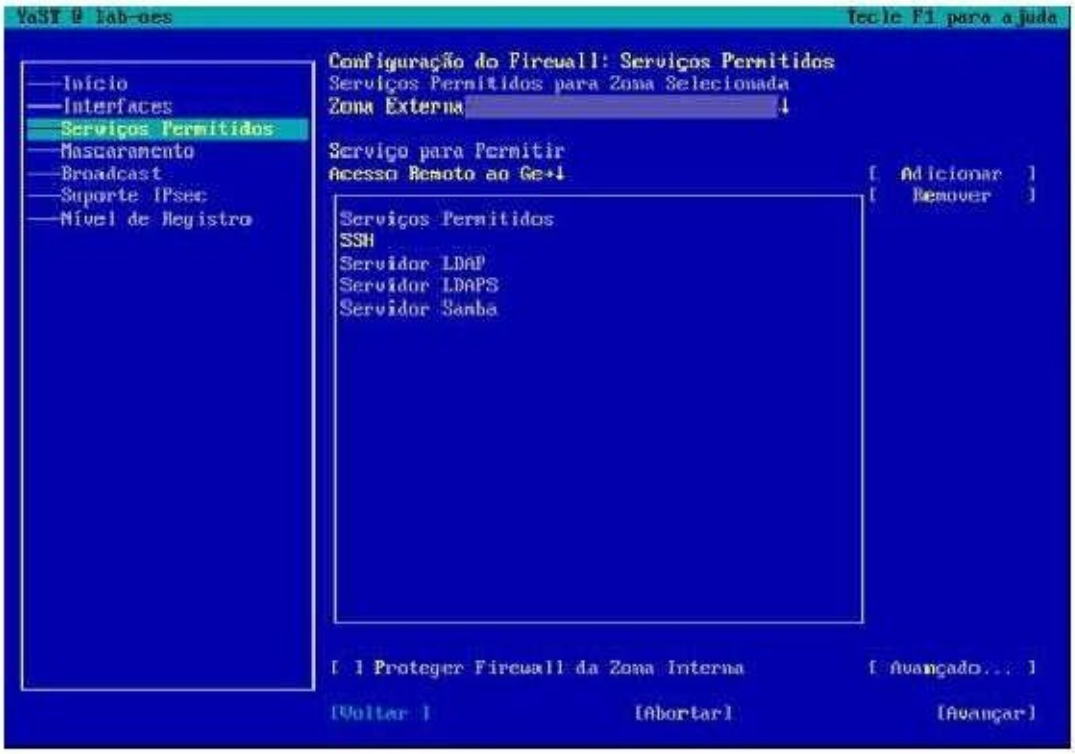


Figura 4: Acessando a lista dos Serviços Permitidos. Observe que o serviço SSH está devidamente habilitado no host.

Os serviços listados na Figura 4 são aqueles que estão disponíveis para serem utilizados, nesse mesmo ambiente da ferramenta pode-se adicionar mais serviços ou remover alguns dos que já estão habilitados. **Cabe ao administrador da rede definir quais serviços ficarão habilitados e quem terá acesso a cada um deles**. Observe que o **serviço SSH (Secure Shell), para aceso remoto a outros hosts**, que será mais adiante utilizado como exemplo no presente capítulo, está devidamente habilitado naquele host.

Apresenta-se abaixo (Tabela 1), a título de exemplo, a sequencia de comandos para habilitar o acesso ao serviço de ssh de um servidor para dois endereços ip fictícios xxx.xxx.xxx.xxx e yyy.yyy.yyy.yyy.

LinhasComandos
iptables -t filter -I INPUT -p tcp --dport 22 -j DROP
iptables -t filter -I INPUT -s xxx.xxx.xxx.xxx -p tcp --dport 22 -j ACCEPT
iptables -t filter -I INPUT -s yyy.yyy.yyy.yyy -p tcp --dport 22 -j ACCEPT [3,...,n]Idem

Tabela 1: Linhas de comando para configuração do firewal através do iptables

O comando (-I INPUT) do iptables é utilizado para inserir novas regras no topo da cadeia (no caso a cadeia INPUT), dessa forma cada nova regra inserida irá ocupar o topo da lista de regras da cadeia INPUT, impedindo que a mesma seja rejeitada por causa de alguma outra regra que possa ter maior precedência.

Por essa razão, o comando da primeira linha da Tabela 1, que bloqueia (-j DROP) o tráfego ssh (protocolo tcp) pela porta 22 para todos os ip's, será o primeiro a ser inserido a fim de que possa ser deslocado ao final da cadeia a medida em que outras regras de exceção estão sendo incluídas. Ou seja, sempre que uma nova regra for inserida na cadeia INPUT via comando (-I) essa terá maior precedência em relação às que haviam anteriormente.

Na segunda linha em diante, começam a ser lançadas as exceções de acesso. Na linha dois, o ip xxx.xxx.xxx.xxx terá acesso (-j ACCEPT) através da porta de destino 22 (--dport) que usa protocolo tcp (-p tcp) para o serviço de ssh. Na terceira linha, o procedimento é o mesmo para o ip yyy.yyy.yyy.yyy e assim sucessivamente.

Ao final das inserções das regras, pode-se visualizar como elas ficaram dispostas ao longo da cadeia INPUT através do comando “iptables -L INPUT” que irá listar todas as regras da cadeia INPUT, conforme visualizado na Tabela 2.

lab-oes:~ # iptables -L INPUT					
Chain INPUT (policy DROP) targetprot opt source					
				destination	
ACCEPT tcp ACCEPT tcp DROPtcp ACCEPT all ACCEPT all input_ext all					
input_ext all	--	--	yyy.yyy.yyy.yyy anywhere tcp dpt:ssh xxx.xxx.xxx.xxx anywhere tcp dpt:ssh		
	anywhere tcp dpt:ssh anywhere				
		--			
	anywhere state RELATED,ESTABLISHED anywhere				
	anywhere				
	anywhere limit: avg 3/min burst 5 LOG level warning tcp-options				
	all--anywhere				
LOGall					
DROP					

Tabela 2: Exemplo do comando para listar as regras da cadeia INPUT

Percebe-se que a exceção lançada para o ip yyy.yyy.yyy.yyy foi a ultima a ser inserida dentre as regras da cadeia INPUT segundo a Tabela 1, no entanto ela se encontra na primeira linha das regras. Isso é uma característica do comando (-I) que insere a regra mais nova no topo da cadeia, a fim de que essa regra não seja bloqueada por alguma outra mais abrangente, como por exemplo uma regra padrão de bloqueio de todos os acessos.

De acordo com a necessidade, pode-se remover alguma regra inserida bastando escrever o mesmo comando para inserção trocando o (-I) de inserir pelo (-R) de remover, por exemplo: “iptables -t filter -R INPUT -s yyy.yyy.yyy.yyy -p tcp --dport 22 -j ACCEPT”.

Dessa forma, o administrador da rede poderá liberar acesso ao servidor para algumas estações de trabalho na rede, restrito à determinados serviços, lançando exceções no firewall ao invés de desabilitá-lo.

Entre os serviços que podem ser disponibilizados no servidor, existem aqueles destinados ao compartilhamento de arquivos. Não é recomendável, para estes casos o uso do FTP. **O SUSE Linux dispõe de alternativas mais seguras para o compartilhamento de arquivos, tais como o protocolo SSH e o SMB, utilizados no contexto de um serviço de diretório**. Em ambos os casos, **o tráfego de dados e senhas se dá por meio de uma conexão criptografada**, o que não ocorre com o FTP.

10. BIBLIOGRAFIA

Os livros utilizados como base para a implementação deste projeto:

Negus, Christopher e Caen, Francois. **Suse Linux Toolbox: 1000+ Commands For Opensuse And Suse Linux Enterprise**, Editora John Wiley & Sons. 2007;

ROSS, Keith W.e KUROSE, James F. **Redes de Computadores e a Internet - Uma Abordagem Top-down - 3ª Ed.** Editora Pearson Education. 2007; e

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**, Editora Axcel Books. 2000.