



**GOVERNO DO ESTADO
DE SÃO PAULO**

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Ricardo Milla Mota

ALTA DISPONIBILIDADE

PARA EMPRESAS DE PUBLICIDADE E PROPAGANDA

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC / Americana, sob orientação da Professora Dra. Maria Cristina Aranda.

Americana

2018

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

M871a MOTA, Ricardo Milla

Alta disponibilidade para empresas de publicidade e propaganda. / Ricardo Milla Mota. – Americana, 2018.

104f.

Monografia (Curso de Tecnologia em Segurança da Informação) - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza

Orientador: Profa. Dra. Maria Cristina Aranda

1 Redes de computadores I. ARANDA, Maria Cristina II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519

Ricardo Milla Mota

**ALTA DISPONIBILIDADE
PARA EMPRESAS DE PUBLICIDADE E PROPAGANDA**

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC / Americana, sob orientação da Professora Dra. Maria Cristina Aranda.

BANCA EXAMINADORA



Professor: Maria Cristina Aranda (orientador)

Doutora

Faculdade de Tecnologia - Fatec Americana



Professor: Renato Kraide Soffner

Doutor

Faculdade de Tecnologia - Fatec Americana



Professor: Henri Alves de Godoy

Mestre

Faculdade de Tecnologia - Fatec Americana

Americana

2018

DEDICATÓRIA

Dedico este trabalho à memória de meu pai Pedro Mota, à minha mãe Leonice P. Milla que com muito esforço possibilitou que eu estudasse e crescesse profissionalmente e especialmente à minha avó Olivia Enerstina Milla pela confiança em mim depositada e que indiretamente favoreceu para que eu concluísse o curso.

Dedico também ao Sr. Walmir Alcântara e sua esposa Sra. Josiane Alcântara na qual tenho muito orgulho de ter conhecido e que através dos ensinamentos do Karatê contribuíram para o meu crescimento pessoal e essencialmente da formação do meu caráter.

Aos amigos e familiares que estiveram comigo e que me apoiaram e incentivaram em todos os momentos desta minha caminhada.

AGRADECIMENTOS

Primeiramente a todos os professores que participaram de forma direta e indireta, no meu aprendizado e pela dedicação de cada um, no empenho por ensinar.

À Prof. Dra. Maria Cristina Aranda pela orientação, compreensão, paciência e todo o apoio para o desenvolvimento deste trabalho.

Ao Adm. Fernando Rodrigues pela amizade e companheirismo, pela oportunidade e confiança em mim depositada para que eu pudesse colocar em prática o conhecimento teórico adquirido em sala de aula, possibilitando a equivalência e o desenvolvimento do estágio obrigatório.

À Dra. Andreza Della Gracia pelo auxílio que contribuiu proativamente possibilitando que eu pudesse dar os primeiros passos no desenvolvimento deste trabalho.

Aos meus amigos pelo apoio, amizade, incentivo e paciência durante todo meu período de aprendizado.

À Secretaria de Graduação da FATEC - Americana, pelo apoio, e dedicação.

RESUMO

Partindo do consenso de que vive-se a era da informação, logo pode-se afirmar que de alguma forma as pessoas estão criando, manipulando, mantendo ou compartilhando informações, seja para uso pessoal ou profissional. Assim, persiste a ideia de que, conhecer o valor da informação tornou-se vital, principalmente para as empresas, pois estas costumam armazenar não só informações próprias, mas também informações pertencentes a seus clientes. Sendo assim, este trabalho consiste em apresentar soluções que visam assegurar a continuidade dos negócios, uma vez que a palavra indisponibilidade em uma empresa possa ser sinônimo de prejuízo. Dessa forma cabe o aprofundamento no estudo de como a disponibilidade, um dos pilares de sustentação da segurança da informação é aplicado, e se este, está presente no dia a dia das empresas. Portanto, é nessa via de raciocínio que assiste o tema deste trabalho, apresentando embasamento teórico, onde a literatura utilizada está relacionada a estudos de livros e artigos publicados na Internet, afim de conduzir o leitor especificamente para um estudo de caso de uma empresa de publicidade e propaganda, sugerindo que o uso de componentes redundantes e a implementação de um *cluster* de alta disponibilidade possa ser considerada uma solução para o problema que será apresentado. No entanto, vale ressaltar que, o uso de *cluster* não se restringe apenas a empresas de publicidade e propaganda podendo ser utilizado também em outras concepções comerciais.

Palavras chaves: Cluster, Servidores, Alta Disponibilidade

ABSTRACT

Using as consensus that we live today on the information era, we can affirm that people are creating, manipulating, maintaining or sharing information, for personal or professional use. Thus, the idea that knowing the value of information is vital, especially for companies, which store not only their own information but also ones that belongs to their clients. That way this work presents solutions to assure business continuity, once that unavailability is the same as loss of profit. For that reason deep understanding high availability, one of the pillar of information security, and how it is present on current companies is of high importance. With this line of thought this work is based, presenting theoretical founding, with specific literature, studies and publications from the Internet with the reason to guide the reader on a case study from a publicity company, suggesting that the use of redundant and deployment of a high availability cluster may be a solution for the present problem. Whoever it's wort mentioning, that using the cluster is not restricted only to this company, in a way that it is possible to be used on other application cases.

Keywords: Cluster, Servers, High Availability

SUMÁRIO

1. INTRODUÇÃO	1
2. FUNDAMENTAÇÃO TEÓRICA	3
2.1. SEGURANÇA DA INFORMAÇÃO	4
2.2. A INFORMAÇÃO NOS NEGÓCIOS	6
2.3. TI NOS NEGÓCIOS	9
3. INFRAESTRUTURA DE TI	11
3.1. HARDWARE e SOFTWARE	11
3.2. SISTEMAS OPERACIONAIS (SO)	13
3.3. LINUX DEBIAN	15
3.4. SERVIDORES.....	16
3.5. REDUNDÂNCIA.....	17
3.6. GERENCIAMENTO DE DISPONIBILIDADE.....	24
3.7. REDE DE COMPUTADORES.....	26
3.8. PROTOCOLOS DE COMUNICAÇÃO.....	28
4. ESTUDO DE CASO	30
4.1. SOBRE A EMPRESA.....	30
4.2. PROCESSO DE TRABALHO DA EMPRESA X.....	31
4.3. O PROBLEMA	33
4.4. SOLUÇÃO PROPOSTA.....	35
5. CONSIDERAÇÕES FINAIS	41
6. REFERÊNCIAS.....	42
APÊNDICE A – INSTALANDO O LINUX DEBIAN 9.....	45
APÊNDICE B – PREPARANDO O LINUX PARA O CLUSTER.....	64
APÊNDICE C – INSTALANDO E CONFIGURANDO O SAMBA	69
APÊNDICE D – INSTALANDO E CONFIGURANDO O HEARTBEAT	78

APÊNDICE E – CRIANDO RELACIONAMENTO DE CONFIANÇA VIA SSH.....	87
APÊNDICE F – INSTALANDO O RSYNC.....	90
APÊNDICE G – CONFIGURANDO O CRONTAB.....	91

LISTA DE ILUSTRAÇÕES

Figura 1 – Etapas básicas de um processamento de dados.....	3
Figura 2 – Hierarquia das necessidades de Maslow.....	7
Figura 3 – Gerenciamento de riscos.....	8
Figura 4 – Alinhamento entre objetivos de TI e de Negócios.....	9
Figura 5 – Interação do usuário com o computador.....	11
Figura 6 – Componentes básicos de um computador.....	12
Figura 7 – Estrutura de um sistema de computação (hardware e software).....	14
Figura 8 – RAID0.....	19
Figura 9 – RAID1.....	20
Figura 10 – RAID10.....	21
Figura 11 – RAID5.....	22
Figura 12 – RAID6.....	22
Figura 13 – Configuração de rede modelo cliente/servidor.....	27
Figura 14 – Protocolo de comunicação.....	29
Figura 15 – Topologia básica da Empresa X.....	31
Figura 16 – Funcionamento do Heartbeat.....	37
Figura 17 – Exemplo de cópia remotamente com o RSync.....	38
Figura 18 – Proposta para nova topologia básica da Empresa X.....	40
Figura 19 - Tela de apresentação do Debian 9.....	45
Figura 20 - Tela de definição do nome do Servidor.....	46
Figura 21 - Tela de definição do domínio.....	47
Figura 22 - Tela de definição da senha do root.....	48
Figura 23 - Tela de criação do usuário.....	49
Figura 24 - Tela de definição da senha do usuário.....	50
Figura 25 - Tela de definição do modo do particionamento.....	51
Figura 26 - Tela de definição do disco para particionamento.....	52
Figura 27 - Tela de esquema de particionamento.....	53
Figura 28 - Tela de informações de particionamento.....	54
Figura 29 - Tela de confirmação de particionamento.....	55
Figura 30 - Tela de troca de mídia de instalação.....	56
Figura 31 - Tela de definição do espelho de repositório.....	57

Figura 32 - Tela de definição do servidor de repositório	58
Figura 33 - Tela de definição do proxy	59
Figura 34 - Tela de concurso de utilização de pacotes	60
Figura 35 - Tela de seleção de software	61
Figura 36 - Tela de instalação do grub.....	62
Figura 37 - Tela de seleção do disco para instalação do grub	63
Figura 38 - Instalação do sudo	64
Figura 39 - Adicionando o usuário ao grupo sudo.....	65
Figura 40 - Configurações de rede.....	66
Figura 41 - Configurações de servidores DNS	67
Figura 42 - Configurações do Hosts.....	68
Figura 43 - Instalação do Samba	69
Figura 44 - Alteração do grupo padrão do diretório DADOS	70
Figura 45 - Alteração das permissões do diretório DADOS	71
Figura 46 - Configuração do arquivo smb.conf.....	72
Figura 47 - Comando para criação de novo usuário	73
Figura 48 - Criação de senha para usuários no Samba	74
Figura 49 - Restartando o serviço do Samba.....	75
Figura 50 - Janela do Executar do Windows	76
Figura 51 - Janela de autenticação para acesso a pasta compartilhada.....	76
Figura 52 - Janela de pastas compartilhadas.....	77
Figura 53 - Instalação do Heartbeat	78
Figura 54 - Configuração do arquivo ha.cf	79
Figura 55 - Configuração do arquivo authkeys.....	80
Figura 56 - alterando permissões do arquivo authkeys.....	81
Figura 57 - Configurações do arquivo haresources.....	82
Figura 58 - Startando o serviço do Heartbeat.....	83
Figura 59 - Ping no IP Virtual do Cluster	84
Figura 60 - Janela do Executar do Windows	85
Figura 61 - Janela de autenticação para acesso a pasta compartilhada.....	85
Figura 62 - Janela de pastas compartilhadas.....	86
Figura 63 - Criação da chave pública.....	87
Figura 64 - Copiando a chave para o SRV02.....	88
Figura 65 - Conexão via SSH sem autenticação.....	89

Figura 66 - Instalação do Rsync.....	90
Figura 67 - Configurações do Crontab	91

LISTA DE SIGLAS E ABREVIATURAS

RMC – Região Metropolitana de Campinas

TI – Tecnologia da informação

HA – High Availability

RAM – Random Access Memory

UCP – Unidade Central de Processamento

CPU – Central Processing Unit

HD – Hard Disk

SO – Sistema Operacional

RAID – Redundant Array Independent Disks

GD – Gerenciamento de Disponibilidade

ITIL – Information Technology Infrastructure Library

TCP – Transfer Control Protocol

IP – Internet Protocol

LVM – Level Volume Manager

TB – Terabyte

RSync – Remote Sync

SSH – Secure Shell

1. INTRODUÇÃO

Este trabalho tem por objetivo a implantação de alta disponibilidade em uma empresa de publicidade e propaganda Região Metropolitana de Campinas (RMC). É um estudo de caso baseado em um problema ocasionado por oscilações e falta de energia, a qual ficou inoperante por um grande período de tempo, levando à perda de informações que estavam armazenadas nos servidores da empresa e eram referentes aos serviços entregues pela mesma.

A implantação do ambiente altamente disponível foi realizada através de recursos já existentes na empresa, tentando minimizar ao máximo o custo com novos recursos. Em função do baixo custo esse processo torna-se possível, atraente e aplicável, se necessário, a outras empresas de pequeno porte.

Na linguagem de TI (Tecnologia da Informação) alta disponibilidade, do inglês *high-availability* (HA), pode ser considerada como serviços e ou aplicações que estejam sempre disponíveis quando solicitados e são configurações de múltiplos componentes que trabalham juntos e tem como objetivo manter um ou mais serviços ou aplicações no ar mesmo em caso de falhas.

O ambiente trabalhará com a sincronia de dados e informações entre dois servidores, primário e secundário, no menor tempo possível, gerando uma redundância entre eles, de modo que as informações possam ser acessadas ininterruptamente pelos usuários, caso o servidor primário sofra algum incidente.

Este trabalho está dividido em cinco capítulos e organizados a partir do segundo capítulo da seguinte forma:

O segundo capítulo tem como objetivo apresentar toda a fundamentação teórica na qual está envolvido este trabalho, apresentando inicialmente o que são dados e informações e como estes são adquiridos e qual a importância de mantê-los seguros. Composto ainda o mesmo capítulo serão apresentados o significado da informação para os negócios e uma analogia usando a teoria de Abraham Maslow sobre a pirâmide das necessidades humanas voltadas à esfera empresarial como gestão de riscos para a obtenção dos resultados esperados. A fim de introduzir a importância do departamento de TI para os negócios.

O terceiro capítulo apresenta os componentes básicos existentes em ambientes de Tecnologia da Informação que podem potencializar a geração, manutenção, armazenamento e a segurança de informações dentro das empresas durante seu ciclo de vida, de forma que se forem otimizados podem garantir a continuidade dos negócios em casos de falhas. Assim, serão abordados o que são hardware, software e sistemas operacionais (SO). Explica ainda, o que são redes de computadores e como é efetuada a comunicação entre os computadores.

O quarto capítulo trata-se da apresentação do estudo de caso em que falhas, como, quedas e oscilações de energias foram cruciais para a paralização total de uma empresa durante cerca de 15% do tempo da sua produção semanal. Este capítulo mostra ainda que uma empresa do ramo de publicidade e propaganda localizada na Região Metropolitana de Campinas (RMC), poderia, com baixo custo e através de recursos próprios diminuir consideravelmente o tempo de inatividade e até mesmo evitar problemas mais sérios.

Quanto ao último capítulo, revela sobre a possibilidade e a viabilidade da implantação do Cluster de Alta Disponibilidade na empresa estudada envolvendo baixo custo, otimizando principalmente os recursos de TI já existentes.

2. FUNDAMENTAÇÃO TEÓRICA

Nos dias atuais comumente ouve-se falar em dados e informações. Seja em algum tipo de cadastro na *web*, onde um usuário digita seus dados pessoais para assinar um serviço de *e-mail*. Ou, em alguma pesquisa, por exemplo, para saber qual time de futebol brasileiro tem a maior torcida, onde o pesquisador necessita colher os dados referente às respostas dos entrevistados ou até mesmo em uma fatura mensal fornecida por uma empresa de serviços de Internet, telefone ou TV a cabo, onde serão exibidos os dados detalhados sobre o consumo dos serviços prestados. E, em uma infinidade de outras situações.

De acordo com Elias (2013), dados são considerados unidade básica de uma informação, os dados necessitam estarem aglomerados em um contexto para que então seja adquirida uma informação ou para que sejam contabilizados e conseqüentemente obter-se um resultado, ou seja, utiliza-se certa quantidade de dados para gerar uma determinada informação. Em outras palavras, dados nada mais são que o conteúdo quantitativo, algo expressado somente em quantidade e que graças ao seu valor, por si só, não é capaz de causar entendimento sobre algum assunto ou situação.

A Figura 1 demonstra as etapas básicas do processamento de dados que tem como resultado final a obtenção de uma informação.

Figura 1 – Etapas básicas de um processamento de dados



Fonte: Monteiro (2007, p.2)

Dessa forma, entende-se como informação qualquer conteúdo que eventualmente possa ser utilizado por um indivíduo ou uma organização que seja capaz de transmitir entendimento e expressar uma situação (ELIAS, 2013).

Após a obtenção de informação através do processamento, manipulação e/ou organização dos dados, é pertinente que se conheça o valor que essa informação

possui. O que não é uma tarefa muito fácil, uma vez que o valor da informação pode variar de acordo com o contexto em que é produzida e entre as pessoas que compartilham da mesma, podendo possuir significados diferentes para cada indivíduo.

Muitas pessoas fazem uso de computadores, *smartphones*, *tablets* e *notebooks* para as mais variadas tarefas, gerando com isso um grande fluxo de informações, sejam elas locais, na rede em que trabalham ou na Internet. Porém, muitas dessas informações acabam sendo perdidas, por erros de sistemas, não conhecimento do valor da informação, acesso indevido, fraude, sabotagem, roubo e até mesmo causas da natureza. Graças à grande utilização desses equipamentos, tanto para uso pessoal quanto para uso profissional, acabam fazendo com que os dados se multipliquem a cada instante. Contudo, a segurança desses dados em alguns casos, são baixíssimas ou até mesmo nulas por parte dos usuários ou até mesmo por gestores, em alguns casos por falta de conhecimento, desinteresse ou indisponibilidade financeira, deixando-os vulneráveis.

2.1. SEGURANÇA DA INFORMAÇÃO

Segundo Santos (2009, p.3) normalmente quando o assunto é Segurança da Informação as pessoas rapidamente direcionam o assunto aos sistemas de computadores. Porém, a Segurança da Informação não está relacionada apenas à proteção de equipamentos que armazenam e processam dados, mas também consiste em preservar desde a segurança física até a segurança pessoal, tanto no meio corporativo como individual, por existir dentro de cada uma dessas situações os riscos e ameaças próprios e as soluções capazes de evitar e/ou minimizar os prejuízos e as consideráveis perdas envolvendo a informação.

O que sustenta a ideia de que a TI (Tecnologia da Informação) faz parte do cotidiano da maioria das pessoas, e que com o decorrer dos dias, essas pessoas estão cada vez mais dependentes dos computadores. Isso faz com que as expressões do tipo: *firewall*, invasões, vírus, antivírus, sistema fora do ar, *backup*, políticas de segurança, etc. tornarem-se comuns. Logo essas expressões encontram-se ligadas à Segurança da Informação.

Preservando ainda o ponto de vista do Santos (2009), quando se fala em segurança na área de TI, dá-se ênfase à questão de como proteger os computadores e outros recursos físicos, tirando, às vezes, o foco do que seria mais importante nessa questão, as informações armazenadas nesses equipamentos. Muitas pessoas ainda não se deram conta de que o *hardware* pode ser substituído em um eventual caso de perda. No entanto a perda das informações contidas nesses equipamentos pode ser em alguns casos, irrecuperável.

Diariamente computadores são invadidos e dispositivos portáteis de comunicação e armazenamento são perdidos ou roubados, gerando assim uma grande perda de informações. Nesses casos é imprescindível que se conheça por quem e como são usados os equipamentos que armazenam dados e informações e que se entenda do que, e de quem devem se proteger. Só assim será possível definir as políticas necessárias a fim de garantir um bom nível de segurança.

Isso implica em ações que venham atingir os principais pilares de sustentação da Segurança da Informação, que são: disponibilidade, integridade e confidencialidade. Porém, Segurança da Informação vai muito além do aspecto tecnológico, abrangendo também aspectos gerenciais, educacionais e não menos importante, o fator humano.

De acordo com Sêmola (2014, p.41) segurança da informação trata-se da área de conhecimento que tem como propósito a aplicação de processos de proteção de informações e ativos digitais armazenados em computadores e/ou redes de processamentos de dados contra acessos não autorizados, alterações indevidas ou indisponibilidade. Ou seja, processos que visam conservar os três pilares que sustentam a segurança da informação: disponibilidade, integridade e confidencialidade.

Sêmola (2014, p.43) aponta os fundamentos principais da segurança da informação: disponibilidade, integridade e confidencialidade citados anteriormente da seguinte maneira:

A Disponibilidade tem como objetivo garantir que a informação esteja disponível quando solicitada, e para acessá-la deve-se ter autorização.

Integridade, essa propriedade visa garantir que a informação seja correta e verdadeira de maneira que suas características originais sejam mantidas após a manipulação da mesma, ou seja, da maneira que foram estabelecidas pelo seu criador.

E por fim Confidencialidade, garante que a informação seja acessada somente por quem tem autorização para acessá-la, podendo haver limitações ao acesso, como por exemplo, estabelecer qual o tipo de privilégio um determinado indivíduo terá ao acessar uma informação.

2.2. A INFORMAÇÃO NOS NEGÓCIOS

Sêmola (2014, p.1) explica que a informação cada dia mais tem sido valorizada e sempre esteve presente nas principais mudanças no mundo dos negócios como na reengenharia de processos, na terceirização, na virtualização e atualmente dentro da Tecnologia da Informação apresentando sua importância quanto à gestão dos negócios tendo como alvo a melhoria da produtividade, redução de custos, agilidade e competitividade e principalmente auxiliando nos processos de tomada de decisão.

Dessa forma entende-se implicitamente que, é necessário que as organizações tenham segurança dos seus ativos, ou seja, precisam assegurar tudo que a mesma possui e que são utilizados para alcançar seus objetivos. Por exemplo: dinheiro, saldo em conta corrente, títulos financeiros e ações, mercadorias, direitos autorais e patentes, pesquisas, pessoas, tecnologias, etc. Estabelecendo uma relação entre as informações e os negócios, uma vez que as informações representam a base dos negócios e podem possuir valor significativo para a sua continuidade, transformando as informações em um dos ativos mais importantes para a empresa.

Isso acaba gerando um grande mercado competitivo, as empresas necessitam fazer mais investimentos e cada vez mais sistemas informatizados são implantados para melhorarem seus processos organizacionais, buscando obter melhores resultados, além de mais precisos em menor tempo. Visando, é claro, estar sempre um passo à frente dos seus concorrentes. E conseqüentemente, isso aumenta a importância da segurança da Informação dentro das empresas.

Antes de ingressar no assunto Segurança da Informação na esfera empresarial, é importante hierarquizar os níveis de necessidades, apresentando indispensavelmente algumas informações básicas sobre a teoria de Maslow datada de 1954. Essa teoria pode ser utilizada a fim de ilustrar e associar os seus indicadores aos níveis de necessidades voltados à gestão de risco e necessidades empresariais para obtenção dos resultados.

Segundo Costa (1980, p.60) a teoria de Maslow sugere que para atingir o mais alto nível de realização pessoal, é necessário que se atenda os níveis mais básicos de um ser humano, obviamente estar vivo e cuidar das necessidades básicas do corpo e posteriormente atender aos níveis de segurança. Em seguida amor/relacionamento, gradativamente, nível a nível até atingir os níveis mais altos.

A Figura 2 ilustra a hierarquia das necessidades da teoria de Abraham Maslow, mostrando as necessidades humanas organizadas em cinco níveis, sendo eles:

Figura 2 – Hierarquia das necessidades de Maslow

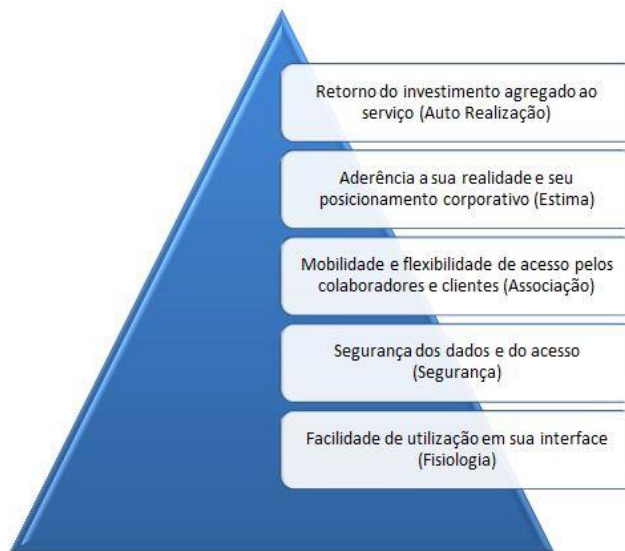


Fonte: Borges; Rodrigues (2010)

Usando-se o mesmo raciocínio, porém, voltado à esfera empresarial, é necessário que uma determinada empresa possua um planejamento estratégico que vise direcioná-la e prepará-la para melhor enfrentar seus desafios, de forma que se estabeleça as prioridades a serem cumpridas gradativamente a fim de atingir os seus objetivos. Assim como a hierarquia das necessidades proposta na teoria de Maslow, Popovici (2011) propõe na Figura 3 uma nova visão hierárquica, na qual uma empresa

precisa seguir para chegar a sua autorrealização, podendo ser lucro, retorno dos investimentos, captação de novos clientes, etc.

Figura 3 – Gerenciamento de riscos



Fonte: Popovici (2011)

Semelhante à primeira teoria, assim como um indivíduo, para uma empresa atingir os níveis mais elevados, afim de garantir a sua evolução, também é necessário que se cumpra inicialmente as etapas inferiores e posteriormente as superiores.

Baseando-se nas duas teorias, nota-se que há certa analogia na forma usada para atingir o sucesso a partir das necessidades, seja pessoal ou empresarial/profissional. Com isso conclui-se que segurança pode não ser apenas uma questão de escolha por parte de uma organização, mas sim uma questão de necessidade, uma vez que esta deve prezar por sua missão, visão e valores.

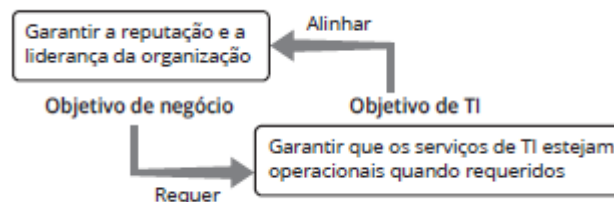
2.3. TI NOS NEGÓCIOS

De acordo com Gasetta (2012, p.7) atualmente, graças a TI, cada vez mais empresas estão transformando seus bens físicos em bens lógicos. Deixando-as mais dependentes dos recursos de TI, o que acaba exigindo maiores cuidados voltados à sua infraestrutura, pois sem ela, não seria possível atender os seus processos de negócio mais básicos. Por sua vez, negócio é tratado como sendo algo tangível ou não, como, por exemplo, um produto ou um serviço entregue por uma organização a seus clientes que esperam assim satisfazer uma necessidade qualquer.

Para isso é necessário haver um alinhamento entre a TI e os negócios da empresa (Figura 4), de forma que sejam entregues valor aos seus clientes e os resultados esperados pela mesma, sejam obtidos.

"A TI tem papel fundamental em manter os recursos de TI necessários para que o objetivo do negócio seja alcançado" (GASETA, 2012, p.6)

Figura 4 – Alinhamento entre objetivos de TI e de Negócios



Fonte: Gasetta (2012, p.7)

O autor ressalta ainda que, assim como a TI, os negócios também estão em constantes mudanças, isso consiste eventualmente em tomadas de decisões que podem ser cruciais e que podem causar intercessão no alinhamento entre os negócios e a tecnologia da informação. Salientando então, que, a TI tem a missão de fornecer os serviços na qual são esperados pelo negócio e, que estes, possam de maneira eficaz, evidenciar os retornos do investimento que foi feito, resultando na valorização do departamento de TI.

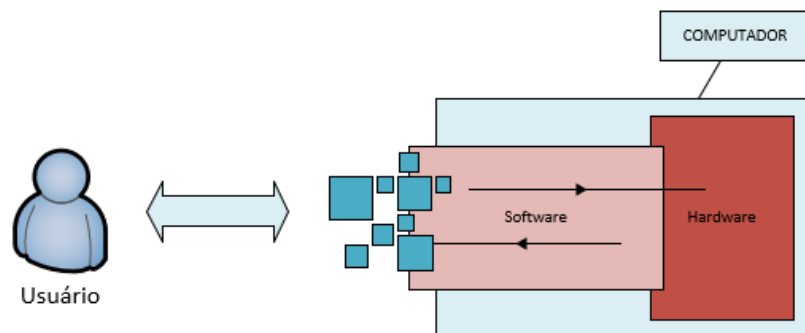
Após o alinhamento da TI com as estratégias do negócio, Gasetta (2012, p.8) explica que possuir um bom gerenciamento de risco é relevante para o negócio, pois assim é possível identificar e classificar os riscos potenciais e assim, prover os mecanismos de defesa antecipadamente para cada risco existente podendo diminuir ou até mesmo mitigar os prejuízos que um determinado risco apresenta. Preservando, com isso a reputação da empresa.

3. INFRAESTRUTURA DE TI

3.1. HARDWARE e SOFTWARE

Monteiro (2007, p.3) trata computador como sendo uma máquina composta de diversos componentes eletrônicos de tamanhos variados que corresponde à parte física do equipamento, denominado como *hardware*. Alega ainda que o *hardware* de uma máquina não possui capacidade própria, pois necessita de alguma instrução ou comando para realização de atividades. Instruções essas que podem ser organizadas de forma diferente com o propósito de originar os resultados esperados e são apresentadas por ele como *software*. Tornando mais simples e intuitiva a ideia de *hardware* e *software*, o *hardware* seria a *interface* física de comunicação entre o usuário e o computador, enquanto que o *software* corresponde à interface lógica de comunicação entre o usuário e o computador. Assim, pode-se dizer que o usuário é capaz de interagir indiretamente com o *hardware* através do *software*, cujo assunto será ainda melhor abordado neste trabalho. A Figura 5 ilustra como funciona a interação do usuário com o *hardware* através do *software* (programas) seguida ainda da explicação dos componentes básicos de um sistema de computação apresentados por esse autor (MONTEIRO, 2007).

Figura 5 – Interação do usuário com o computador



Fonte: Autoria própria

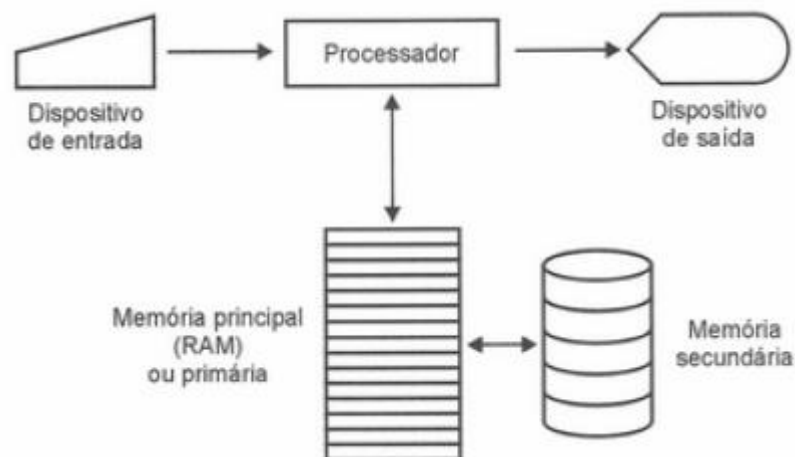
Processador, memória RAM (*Random Access Memory*), ou memória primária, disco rígido (ou memória secundária) e dispositivos de entrada/saída,

respectivamente como teclado/*mouse* e monitor são apenas alguns exemplos de componentes de *hardware* básicos que compõe um sistema de computação.

Conhecida também como UCP (Unidade Central de Processamento) ou do inglês CPU (*Central Processing Unit*) é um *chip* formado basicamente por circuitos e componentes eletrônicos com a responsabilidade de ler e interpretar instruções de máquina para a realização qualquer operação de computador (MONTEIRO, p.153).

A memória RAM (MONTEIRO, p.79) é considerada memória primária de um sistema de computação, como sugere a Figura 6, a memória RAM, tem a finalidade armazenamento e recuperação de dados utilizados durante os processos da CPU. Sua gravação é efetuada de forma randômica, por isso o nome RAM. Apesar de muito rápida, tanto para gravação quanto para acesso e recuperação de dados pelo processador, a mesma não possui capacidade de armazenamento permanente o que implica na perda dos dados quando o computador é desligado. Ainda para o autor, diferentemente da memória RAM os discos rígidos do inglês HD's (*hard disk*) são considerados dispositivos de memória secundária, não possuem a mesma velocidade de gravação e recuperação de dados quanto a memória RAM, porém os discos rígidos não perdem suas informações quando o computador é desligado. É neste dispositivo que ficam armazenados o sistema operacional e demais programas e aplicativos instalados no computador além ainda de armazenar arquivos pessoais de usuários como, fotos, músicas, documentos, vídeos, etc.

Figura 6 – Componentes básicos de um computador



Entende-se como software os sistemas operacionais (SO) e aplicativos desenvolvidos em determinadas linguagens de programação. Na sequência serão apresentados mais detalhadamente a hierarquia básica de softwares existentes em um computador e suas respectivas funções. De forma a facilitar o entendimento deste trabalho.

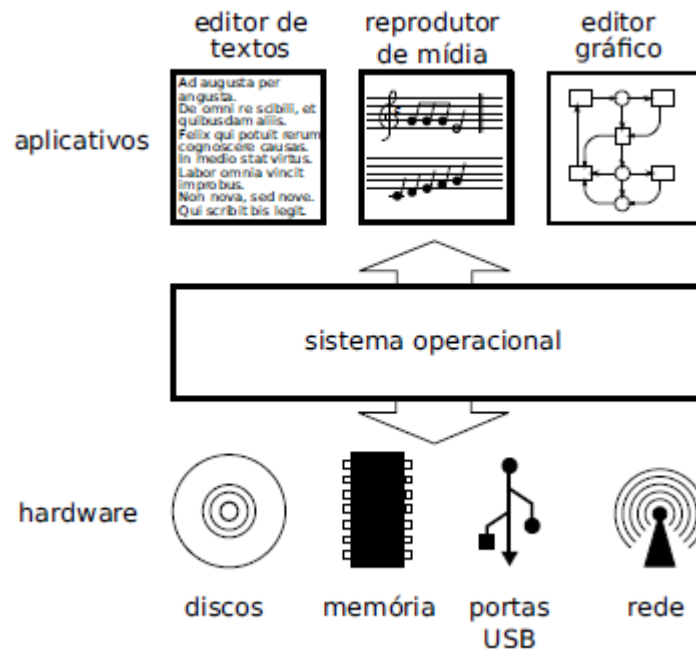
3.2. SISTEMAS OPERACIONAIS (SO)

Assim como Monteiro (2007), Maziero (2017) também demonstra que o *hardware* e *software* constituem um sistema de computação. Porém, sobre o *software*, Maziero (2017, p.1) apresenta que este pode ser dividido basicamente em duas camadas, sendo elas, uma camada de nível mais baixo e a outra de nível mais alto. A camada de baixo nível seria a camada mais próxima do *hardware* onde atua o SO e a camada de alto nível seria a camada mais “próxima” do usuário, essa no caso, é a camada que possui os aplicativos como editor de textos, reproduzidor de mídia, editor gráfico, jogos, entre outros.

Maziero (2017, p.1), explica que o SO é uma camada de *software* que opera logo acima do *hardware* e conseqüentemente abaixo dos aplicativos que são utilizados pelo usuário e sua função basicamente consiste em utilizar os dispositivos de *hardware*, gerenciando-os para que os objetivos de um usuário ao usar o computador sejam concretizados, ou seja, garantir que um usuário possa navegar na Internet, criar e editar textos e imagens, armazenar e recuperar informações em um banco de dados e muito mais (Figura 7).

Em outras palavras, o sistema operacional proporciona uma forma mais amigável, através de uma interface gráfica, a possibilidade do usuário ter uma experiência mais adequada quanto ao uso de recursos de *hardware* presentes num sistema computacional.

Figura 7 – Estrutura de um sistema de computação (hardware e software)



Fonte: Maziero (2007, p.2)

De acordo com Delfino (2017) existem várias opções, mas há três tipos de sistemas operacionais disponíveis no mercado que são predominantemente mais utilizados em computadores, devido ao fato de já virem instalados nos mesmos. Estes são, o Windows da Microsoft, OS X da Apple e GNU/Linux que é um tipo sistema operacional considerado de código aberto, o que quer dizer que qualquer indivíduo pode desenvolvê-lo ou modificá-lo de acordo com as suas necessidades. E mesmo que, com pelo menos três sistemas operacionais diferentes no mercado, estes costumam trazer consigo as funcionalidades mais básicas para gerenciamento do *hardware*, porém com diferenciais em nível de aplicações e *interface* gráfica, isso acaba trazendo novas experiências aos usuários, que normalmente o adquire baseando-se também nas suas necessidades e assim definem qual seria a melhor opção.

Delfino (2017) ressalta ainda que existe um certo ponto de equilíbrio entre os três SO's mais utilizados, já que não é possível determinar o melhor entre eles sem antes conhecer as necessidades na qual cada um deles se adequaria melhor. Dessa forma, o autor aponta alguns exemplos de necessidades que podem ser primordiais na escolha de um sistema operacional. Se a necessidade for praticidade e

entretenimento, como jogos por exemplo, uma boa opção seria o Windows, se o que importa é a interface e recursos gráficos, então OSX deve ser considerado, contudo quando o assunto é desempenho e segurança, o GNU/Linux sai na frente perante os outros, inclusive, é muito usado para funções de servidores em muitas empresas.

Morimoto (2011, p15) explica que após a década de 1980 houve um grande crescimento no uso de computadores de mesa, causando a queda na utilização dos *mainframes*, que eram computadores de grande porte utilizados nas décadas 1960 e 1970. Após a disseminação da Internet, as aplicações que antes eram usadas diretamente nesses computadores passaram a dar lugar às aplicações *online*, por exemplo, acessos de *e-mails*, armazenamento e para troca de mensagens instantâneas. Tudo a partir da *interface web*. Em função desse crescimento, resultou-se na utilização dos servidores, pois além de serem atualmente de baixo custo, possuem estruturas físicas semelhantes aos computadores de mesa e ainda possibilitam a admiração remota, no caso, via Internet.

Referente ao GNU/Linux, Morimoto (2011, p.16) afirma que no início de sua criação os sistemas operacionais de código aberto não haviam sido desenvolvidos para serem utilizados no uso doméstico, mas sim para uso em servidores, que na sua forma convencional, trata-se de uma máquina que fica ligada o tempo todo desempenhando a mesma função. Porém, não necessariamente uma única função, por exemplo com um servidor web, ou um servidor de arquivos, mas sim uma única máquina ligada o tempo todo provendo os dois serviços ao mesmo tempo. Levando em consideração é claro se os recursos de *hardware* existente nessa máquina são suficientes para suportar essas aplicações simultaneamente.

Na esfera dos sistemas operacionais de códigos aberto existe uma grande variedade de tipos de sistemas, essas são chamadas de distribuições Linux. A seguir será abordada a distribuição Linux Debian.

3.3. LINUX DEBIAN

Segundo o próprio site oficial (debian.org) Debian é um projeto, que conta com a associação de mais de mil indivíduos espalhados pelo mundo todo com o objetivo

comum de desenvolver um sistema operacional livre para os usuários de computador, ou seja, sem custo.

Com 25 anos após o seu início por Ian Murdock, a comunidade do Debian cresceu consideravelmente transformando-a em um exemplo de organização de desenvolvedores e usuários que a mantêm cuidadosamente.

O seu núcleo conta com um conjunto de aplicativos básicos necessários para o funcionamento do computador, possibilitando que um usuário o desfrute da melhor maneira possível. Tal sistema operacional possui um arsenal com mais de 51000 aplicações que podem ser instaladas que vão desde edições simples de documentos até jogos e *softwares* para desenvolvimento de outros *softwares*.

O Debian é amplamente usado por organizações de todos os portes, tanto em estações de trabalho como em servidores, incluindo instituições educacionais, governamentais, sem fins lucrativos ou até comerciais em todo mundo.

3.4. SERVIDORES

Morimoto (2011, p. 683), explica de forma resumida, que um servidor tem como função básica disponibilizar serviços para um, ou mais usuários de uma rede ao mesmo tempo. E que cada situação determina qual o tipo de máquina componente deverá ser usado.

Dependendo da aplicação que se deseja rodar, não precisa-se de muito desempenho, no que se refere a configuração de máquina para se ter um bom servidor, até mesmo máquinas que não foram desenvolvidas para esse tipo de emprego/situação podem ser configuradas para tal.

Obviamente, não são em todos os casos em que o uso de qualquer máquina se torna viavelmente proposto, tudo depende da demanda de acessos e do tipo de aplicação que um determinado servidor irá rodar, nesse caso, o porte da empresa deve ser indispensavelmente levado em consideração na hora de configurar uma máquina qualquer como servidor, pois esta, irá implicar diretamente no tipo de *hardware* que será necessário para atender as demandas que a empresa necessita,

analisando a fundo e fazendo um levantamento de requisitos de *hardware* necessário para a questão.

Os *hardwares* de servidores são componentes que foram desenvolvidos para trabalharem com diversas aplicações rodando simultaneamente e muitas vezes aplicações pesadas. O que justifica o porquê de serem otimizados e capazes de funcionar por muito tempo sem apresentar problemas, até mesmo, em alguns casos, sem a necessidade, sequer, de manutenção. Isso certamente tende a proporcionar uma maior confiabilidade como também oferecer o suporte necessário para que as empresas possam com o seu auxílio sustentar as aplicações que movem os seus negócios.

Os servidores, por guardarem, na maioria das vezes grande quantidade de dados e informações, ou por rodarem aplicações críticas ou serviços importantes, necessitam de atenção especial pelos seus administradores, pois, muitas vezes estes costumam ser um dos principais ativos tangíveis das empresas. Nesse caso, conhecer a forma como eles trabalham, quais aplicações são críticas, o que ele armazena é pertinente para qualquer organização, visto que qualquer interrupção dos seus serviços pode ser definitiva para um enorme prejuízo empresarial.

Ao sincronizar as ideias de Morimoto (2011) à de McLian e Thomas (2008, p. 587) é praticável a afirmação de que os requisitos de negócio é que vão determinar quais aplicativos serão considerados críticos. Sendo assim, torna-se possível classificar o grau de importância de um servidor para o negócio e conseqüentemente estabelecer quanto tempo é aceitável para a sua inatividade caso ocorra algum problema.

3.5. REDUNDÂNCIA

Embora o tempo de inatividade de um determinado serviço ou aplicação possa ser em alguns casos imensurável, é possível que isso seja evitado ou minimizado usando recursos disponibilizados dentro de um ambiente de TI, é capaz de garantir a continuidade dos negócios nos momentos em que ocorram a inatividade de serviços, de aplicações e até mesmo de servidores principais por completo.

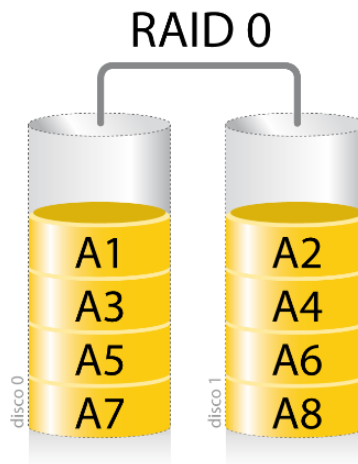
Morimoto (2011, p.687) alega que é importante expressar alguns dos componentes que podem fazer parte de um servidor e que podem perfeitamente trabalhar em paralelo, ou seja de forma redundante, afim de tentar impedir que o mesmo pare por algum motivo, garantindo que seus serviços continuem atendendo as demandas da empresa. Algumas delas são fonte de energia, discos com configuração RAID (*Redundant Array of Independent/Inexpensive Drives*), em português, Conjunto Redundante de Discos Independentes/Econômicos, conceito este que será apresentado neste trabalho. Existem outros componentes externos que também possuem a capacidade de gerar redundância para manter um servidor, seus serviços e suas aplicações disponíveis por mais tempo, são os casos dos geradores de energia, *nobreaks*, *switches*, conexões de Internet, etc.

Assim como mencionado anteriormente, o tipo de sistema operacional, as aplicações críticas para o negócio de uma empresa é que vai definir qual o tipo de RAID deve ser usada em cada situação. Se o objetivo é obter mais velocidade de acesso ao armazenamento, o RAID0 (*stripping*) é o mais indicado, porém, se o objetivo é aumentar a segurança, é aconselhável que se use RAID1 (*mirroring*).

Morimoto (2011) apresenta os tipos RAID existentes e em quais situações serão adotados, conforme segue:

RAID0 (*stripping*) - Os discos são vistos como um único sistema, aumentando sua capacidade de armazenamento e desempenho de leitura e escrita. Os dados são fragmentados antes da gravação, assim os fragmentos podem ser gravados simultaneamente em vários discos. No entanto, não há segurança nenhuma nesse modo de utilização, caso haja algum problema com um dos discos, faltará informações para reconstituir as informações perdidas e logo todo o conteúdo armazenado será perdido.

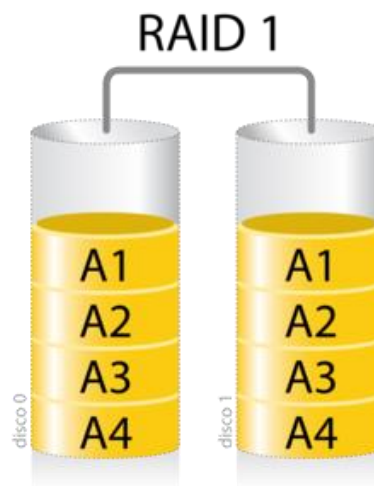
Figura 8 – RAID0



Fonte: Infotrend Brasil (2016)

RAID1 (*mirroring*) – Considerado seguro se comparado ao RAID0. Necessita de pelo menos dois discos ou qualquer outro número par de discos e trabalha fazendo o espelhamento de conteúdo de um disco para o outro. Em caso de falha do disco principal, o sistema automaticamente transfere as leituras e gravações para o segundo disco. Se houver substituição do disco danificado, é possível a recuperação automatizada das informações, pois estas estarão integras ainda no segundo disco. Porém, ao ligar concomitantemente dois discos de mesma capacidade de armazenamento, apenas a capacidade de um disco será disponibilizada pelo sistema para gravação.

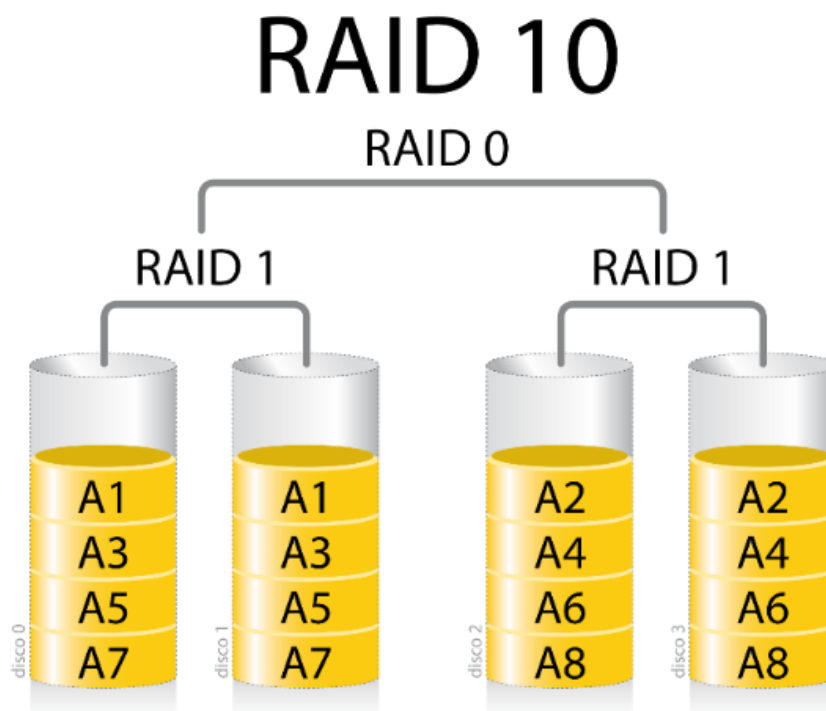
Figura 9 – RAID1



Fonte: Infotrend Brasil (2016)

RAID10 (*mirror/strip*) – Uma combinação dos dois modos citados anteriormente, RAID0 e RAID1. Necessita no mínimo de 4 discos, ou qualquer outro número par de discos. Seu esquema de funcionamento define-se da seguinte maneira, metade dos discos trabalham no modo RAID0 (*striping*) enquanto a outra metade trabalha fazendo o espelhamento RAID1 (*mirroring*) de dados entre os discos.

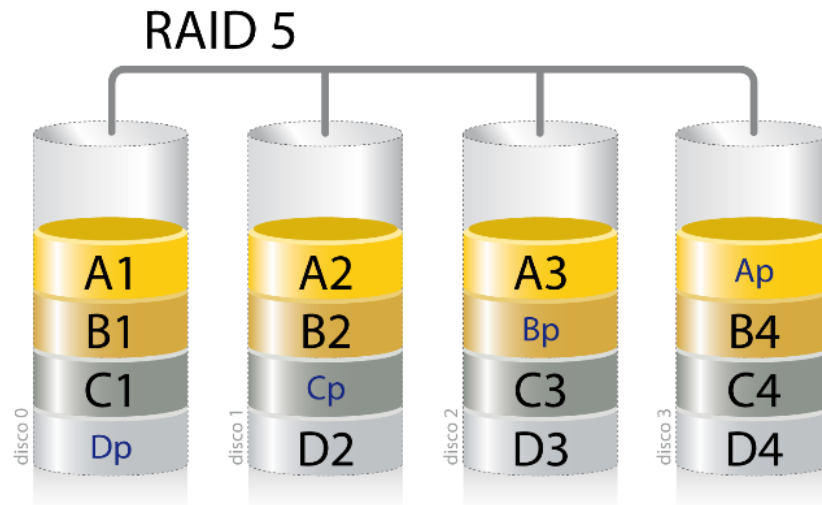
Figura 10 – RAID10



Fonte: Infotrend Brasil (2016)

RAID5 – Comumente mais utilizado em servidores com grande número de discos. Esse sistema trabalha com a fragmentação de dados, e para cada fragmento cria-se um código de paridade e esses são gravados em todos os discos que compõe o sistema para que haja integridade e recuperação dos dados em caso de falha em um dos discos. Além disso melhora o desempenho, uma vez que os fragmentos podem ser gravados simultaneamente em todos os discos. Esse processo necessita no mínimo três discos e o espaço equivalente a um dos discos é desperdiçado para o armazenamento. Caso um segundo disco falhe enquanto o primeiro não é substituído a recuperação dos dados será impossível.

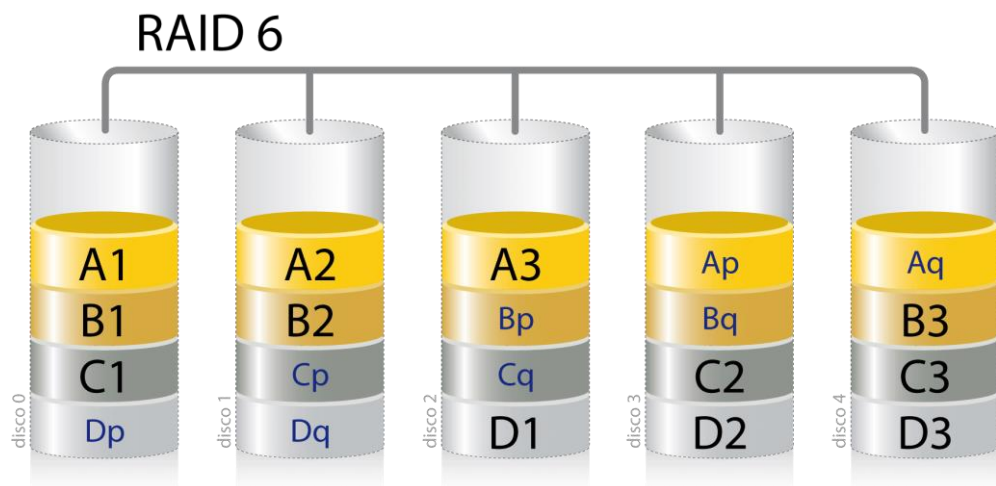
Figura 11 – RAID5



Fonte: Infotrend Brasil (2016)

RAID6 – Esse modo de operação visa “corrigir” o ponto fraco do modo anterior, que seria a perda de dados em caso de perda de dois discos. Possui duplicidade nos fragmentos dos dados, tornando-o mais seguro com relação à perda de dados com a parada de dois discos simultaneamente. Ideal para servidores com grande quantidade de discos e o espaço inutilizado por conta da paridade, diminui à medida que mais discos são adicionados ao sistema.

Figura 12 – RAID6



Fonte: Infotrend Brasil (2016)

Da mesma forma que se usa equipamentos externos ou componentes internos para gerar redundância em um servidor, também é possível usar vários servidores para criar redundância de serviços, são os chamados *clusters* e que são classificados por Morimoto (2011, p. 690) de duas maneiras:

1. *Cluster* com balanceamento de carga – deve conter dois servidores ou mais e são considerados (ativo/ativo). Normalmente são configurados para trabalharem simultaneamente com o intuito de dividirem as tarefas e requisições.
2. *Cluster* de *failover* (ou tolerante a falha em português) – também necessita de dois ou mais servidores, no entanto, este trabalha no modo (ativo/passivo), ou seja, num ambiente onde possuem dois servidores, um é considerado primário e o outro secundário. Sendo assim o secundário assumirá as tarefas e atenderá as requisições caso o primário pare de responder.

McLian e Thomas (2008, p. 587) expõem, que existem ambientes de negócios que necessitam que suas aplicações, base de dados, *sites*, entre outros, estejam disponíveis aos seus usuários vinte e quatro horas por dia, durante os sete dias da semana, e são elas que determinam qual o tempo de indisponibilidade pode ser considerado aceitável ou não, pois isto pode impactar consideravelmente na continuidade dos negócios. Logicamente isso não é uma regra para todos os ambientes, por isso, é necessário e indispensável que a TI esteja alinhada aos processos de negócio, assim a identificação do tempo de indisponibilidade aceitável será muito mais fácil.

3.6. GERENCIAMENTO DE DISPONIBILIDADE

Para Cestari (2012, p.54), trata-se como disponibilidade o aspecto crítico da garantia de um serviço, que propõe a obtenção de garantia de disponibilidade na qual serão entregues nos serviços TI, de forma a atender eficazmente às necessidades de disponibilidade dos serviços. Para tal, apresenta então o gerenciamento de disponibilidade que por sua vez tem a função de definir, planejar e melhorar os aspectos de disponibilidade garantindo que todos os processos, infraestruturas, ferramentas e papéis de TI sejam adequados para que as metas dos negócios sejam atingidas.

Dentro do gerenciamento de disponibilidade descritos por Cestari (2012), torna-se indispensável a apresentação de dois pontos importantes acerca deste trabalho, o objetivo, que sugere construir um mapeamento claro dos requisitos do negócio relacionados com a disponibilidade dos serviços de TI, com o intuito de aperfeiçoar a capacidade da infraestrutura para se alinhar a estas necessidades de negócios e a disponibilidade que é habilidade de um serviço, componente ou item de configuração executar sua função sempre quando necessário.

O gerenciamento de disponibilidade (GD) de acordo com Cestari (2012, p.54) cabe ainda apresentar a sustentabilidade que representa a capacidade que um sistema, serviço ou componente da infraestrutura responder as aquisições quando necessário, logo, quanto mais rápido o tempo de restauração desses sistemas, serviços ou componentes, maior o tempo de disponibilidade, chamado em Tecnologia da Informação de *uptime*.

Corroborando com Cestari (2012) sobre o gerenciamento da disponibilidade, Dorow (2009) explica que segundo a ITIL (*Information Technology Infrastructure Library*) o gerenciamento da disponibilidade visa fornecer disponibilidade dos serviços e infraestrutura de TI de acordo com a exigência das necessidades apresentadas pelas organizações. Porém Dorow (2009) salienta que uma das responsabilidades GD é definir através de uma fórmula qual o tempo de disponibilidade que uma empresa precisa para atingir seus objetivos, sendo ela definida por: $D = (TS-DT) / TS \times 100$.

Onde D = Disponibilidade, TS = Tempo de Serviço acordado e DT = *Downtime* (ou tempo de indisponibilidade).

Portanto, se através de um acordo a empresa e seu fornecedor de hardware, o servidor poderá ficar disponível durante 12 horas por dia, durante 7 dias da semana. Deverá ser usada a fórmula apresentada para saber se as eventuais indisponibilidades estão dentro do acordado ou não. Abaixo segue dois exemplos dos cálculos, o primeiro, mostra que não houve incidentes de indisponibilidade, garantindo 100% de disponibilidade e o outro levando em consideração que uma empresa teve uma parada de 3 horas no servidor de produção.

1. Exemplo:

$$TS = 12h \times 7d = 84h/\text{semana}$$

$$DT = 0$$

$$D = (84-0) / 84 \times 100 = 100\% \text{ de Disponibilidade na semana}$$

2. Exemplo:

$$TS = 12h \times 7d = 84h/\text{semana}$$

$$DT = 3$$

$$D = (84-3) / 84 \times 100 = 96,43\% \text{ de Disponibilidade na semana}$$

3.7. REDE DE COMPUTADORES

Segundo Tanenbaum (2003, p.18) uma das principais conquistas do século XX, foi a capacidade em se obter, processar e distribuir informações. Pois possibilitou que muitas empresas mantivessem suas filiais mais próximas, no que diz respeito a sincronia de informações independentemente da localização geográfica. O autor alega ainda que graças a interação entre os computadores e a comunicação, os antigos centros de computação que eram usados pelas organizações, onde um único modelo de computador ficava encarregado de processar os trabalhos dos seus usuários, perdessem espaço para o que atualmente é chamado de redes de computadores.

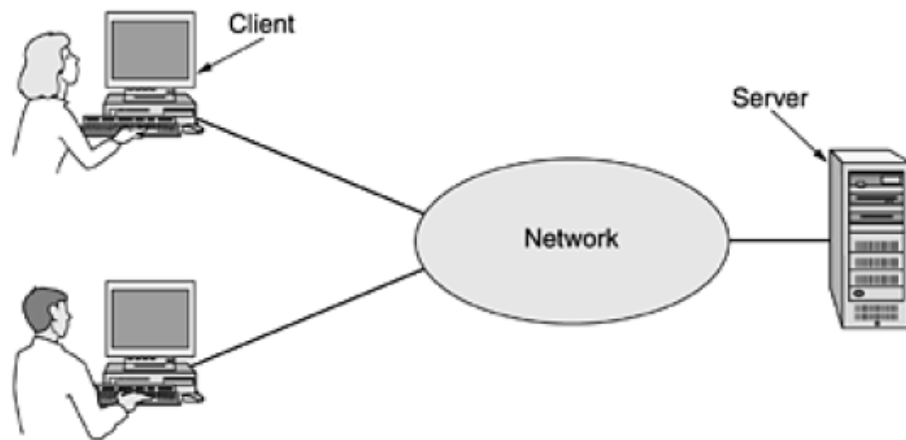
Ainda ele (Tanenbaum, 2003, p.18) explica que as redes de computadores são constituídas basicamente de dois ou mais computadores capazes de trabalhar individualmente, no entanto, interconectados, de maneira que seja possível a comunicação entre eles, e logo, seus respectivos usuários. Ressalta ainda que os meios físicos que conectam esses computadores podem ser de várias formas, por exemplo, fio de cobre, fibras ópticas, micro-ondas, ondas de infravermelho e satélite de comunicações.

Para Tanenbaum (2003, p.19) as redes de computadores são utilizadas principalmente em duas esferas, para as aplicações comerciais e para aplicações domésticas. Em ambas esferas, o objetivo final é o mesmo, extração e/ou correlação de informações armazenadas em computadores, que para o autor compreende-se como compartilhamento de recursos.

Compartilhamento de recursos a que o autor se refere, dá-se pela capacidade de, através de uma rede de computadores disponibilizar desde dados e informações até programas e equipamentos para todos os usuários que utilizam da mesma, mesmo que estes não estejam presentes no local.

Para um melhor entendimento, a Figura 13 trata da exemplificação de como pode ser configurada uma rede onde os usuários de computadores, estes denominados clientes, acessam as informações armazenadas em um servidor através da rede (*network*). Esse modelo é conhecido como cliente/servidor.

Figura 13 – Configuração de rede modelo cliente/servidor



Fonte: Tanenbaum (2003, p.20)

Findando sobre os objetivos na qual uma rede de computadores pode ser utilizada tanto na esfera comercial quanto na esfera doméstica:

Para aplicações na esfera comercial:

1. Comunicação entre funcionários;
2. Videoconferência para realização de reuniões;
3. Negócios entre empresas;
4. Comércio eletrônico.

Para aplicações na esfera doméstica:

1. Acesso a informações remotas;
2. Comunicação entre pessoas;
3. Entretenimento interativo;
4. Comércio eletrônico.

3.8. PROTOCOLOS DE COMUNICAÇÃO

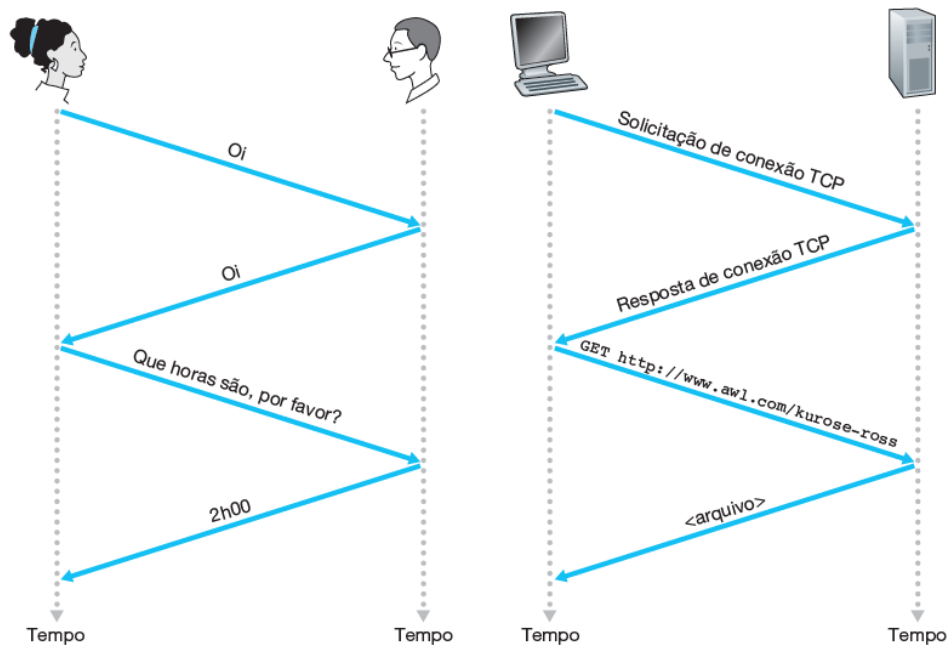
De acordo com Kurose e Ross (2013, p.3) as redes interligam os computadores (*hosts*) através de enlaces (*links*) de comunicação que são constituídos de diferentes meios físicos, podendo ser via fios de cobre, fibras ópticas, micro-ondas, entre outros, como também já citado anteriormente (Tanenbaum, 2003, p.18), roteadores e comutadores (*switches*) de pacotes.

As redes de computadores, referenciadas por eles (Kurose; Ross, 2013) como rede comutadas por pacotes, se mostram muito parecidas com as rodovias de transportes. De forma que estas representariam os meios físicos (*links*), os cruzamentos representam os comutadores (*switches* e roteadores), a origem e o destino seriam os computadores (*hosts*) e os veículos que trafegam nessas rodovias se apresentam como sendo os pacotes, ou seja, os dados e informações.

Para maior controle das trocas de informações que são feitas através da rede de computadores, existem vários tipos de protocolos que são utilizados em diferentes situações de comunicação. Para o desenvolvimento deste trabalho será apresentado o TCP (Transmission Control Protocol), em português, Protocolo de controle de transmissão e o protocolo IP (Internet Protocol) ou protocolo da Internet que especifica o formato dos pacotes que são enviados e recebidos entre os comutadores e *hosts*.

Usando uma analogia humana (Kurose; Ross, 2013, p.5) mostra como dá-se a comunicação entre computadores interligados em rede através de protocolos. Primeiramente, imagina-se duas pessoas dialogando, uma delas diz "Oi", a outra responde com outro "Oi", assim estabelecendo o diálogo, em seguida a primeira pessoa pergunta: "que horas são, por favor?" e a segunda responde: "2h00". Baseando-se nesse diálogo entre duas pessoas, pode-se demonstrar com mais clareza como é efetivada a comunicação entre um cliente e um servidor, por exemplo quando um usuário tenta acessar uma página *web*. Veja na figura a seguir (Figura 14).

Figura 14 – Protocolo de comunicação



Fonte: Kurose e Ross (2013, p.6)

Dessa forma pode-se dizer que um protocolo de rede é a linguagem e como de se dará a "conversa" entre dois ou mais computadores interligados numa rede.

4. ESTUDO DE CASO

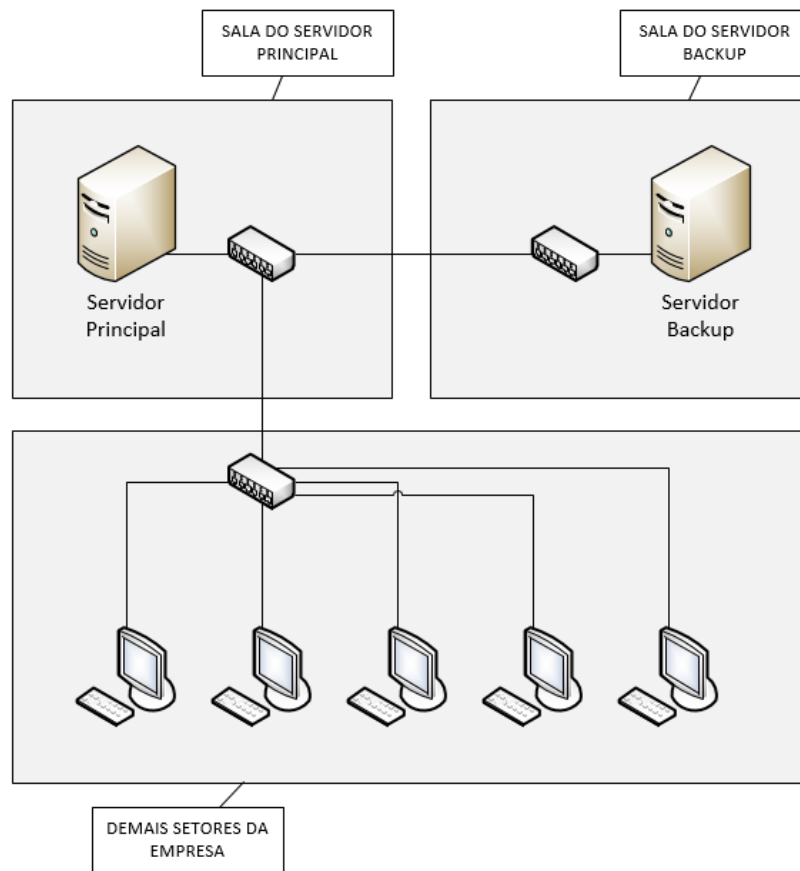
4.1. SOBRE A EMPRESA

Seguido pelo princípio da confidencialidade entre empresa e prestador de serviços, a divulgação do nome da empresa em questão será mantida em sigilo. E será referenciada no decorrer do mesmo, quando necessário, como "Empresa X". Empresa de pequeno porte, com 20 funcionários, divididos em seis departamentos, sendo eles direção/administrativo, atendimento, criação, redação/produção/mídia, planejamento/programação e revisão/finalização. E por fim o departamento de TI que é interno, porém, administrado por terceiros. Considerada uma das principais agências da região, a empresa X atua há mais de 15 anos na Região Metropolitana de Campinas (RMC) no ramo de publicidade e propaganda e também como agência de notícias, coletando, sintetizando e difundindo meios de comunicação. Além ainda de realizar atividades de produção cinematográfica, de vídeos e de programas de televisão e produção de filmes para publicidade.

A Empresa X contém cerca de 28 equipamentos ativos que são utilizados para os desenvolvimentos dos seus serviços, a Figura 15 exemplifica a topologia da empresa. Estes estão distribuídos entre os seus treze setores da seguinte maneira:

- Direção, administrativo, atendimento, redação, produção, mídia, planejamento, programação, finalização e revisão – 15 computadores;
- Criação – 6 computadores Apple;
- Departamento de TI - 02 computadores utilizados como servidores, 1 computador estacionado, 3 switches, 1 roteador e 1 link de Internet.

Figura 15 – Topologia básica da Empresa X



Fonte: Autoria própria

4.2. PROCESSO DE TRABALHO DA EMPRESA X

Após o cliente chegar à mesma através de indicação, Internet, ou prospecção segue-se uma série de procedimentos padronizados para que então seja iniciado, processado e concluído um determinado contrato. O cliente demanda o que precisa, em alguns casos é apresentado o portfólio da empresa ou então o cliente apenas solicita o que já possui em mente e que esteja dentro das possibilidades da agência.

Depois de entender as necessidades do cliente, é efetuado o cadastramento do cliente no sistema. Com isso é definido o *job* que deverá ser desenvolvido. Neste caso o *job* é constituído das tarefas delegadas para cada responsável no processo (criação, redação, produção, etc)

Nessa etapa torna-se indispensável que os servidores e a infraestrutura de TI estejam funcionando corretamente para que tudo ocorra de maneira satisfatória. A partir daí os acessos aos recursos de TI se tornam mais intensos. A partir do momento em que é definido o *job* a ser realizado, usa-se o código gerado com o mesmo, juntamente com o nome do cliente para criação e nomeação de um diretório no servidor principal e nele são armazenados todos os conteúdos referentes ao desenvolvimento do mesmo.

Com o *job* previamente concluído, o mesmo é avaliado pelo departamento de atendimento e, em seguida, se estiver de acordo com os parâmetros estabelecidos inicialmente é encaminhado para o cliente, caso não esteja volta para o responsável que por sua vez deve realizar os ajustes necessários.

Uma vez que o cliente recebe o *job* previamente concluído, o departamento de atendimento fica no aguardo do retorno com a aprovação ou alteração. No caso de alterações, é lançado novamente no sistema para que o responsável em questão possa realizá-las até que então, seja classificado como aprovado, sendo assim o mesmo é encaminhado para finalização.

Por fim, depois que dado como aprovado pelo cliente, o *job* é dado como encerrado e passivo de emissão de nota fiscal.

Todo o processo de trabalho descrito acima ressalta a importância dos servidor de arquivos no cotidiano desta empresa, pois a sua utilização acontece em todas as etapas de desenvolvimento do processo, independente dos indivíduos envolvidos, pois, por menor que seja o acesso deste servidor, como por exemplo, um indivíduo do setor de atendimento que necessita acessá-lo para verificar se um *job* está sendo desenvolvido dentro do prazo estabelecido, ou encontra-se de acordo com o que foi combinado com o cliente, está de fato sendo cumprido. Qualquer incidente envolvendo este servidor pode acarretar em sérios problemas para a empresa uma vez que isto pode ameaçar a entrega dos seus serviços.

4.3. O PROBLEMA

Como já exposto anteriormente, a Empresa X possui em sua infraestrutura de TI dois computadores comuns que são utilizados como servidores, rodando o sistema operacional Linux Debian 9. Um deles é configurado como servidor principal, que é acessado frequentemente em todo o horário de expediente da empresa, pois contém todos os diretórios e arquivos referente aos seus clientes e *jobs* correspondentes. O segundo servidor é acessado uma vez por dia, pelo servidor principal, após o horário de expediente para guardar um *backup*¹ de tudo que foi alterado ou gerado no servidor principal, ou seja, um *backup* diferencial².

Apesar de serem computadores que foram utilizados como servidores e possuírem configurações e componentes de *hardware* como processador e memórias mais potentes e discos de maior capacidade em relação às estações de trabalho encontradas nos demais setores da empresa, e apesar de serem bem semelhantes entre si, existe uma diferença, que são a quantidade e forma que os discos trabalham em cada servidor, pois o servidor principal possui dois discos de 2TB cada um. Enquanto que, no servidor de *backup*, são três discos de 1TB cada, aglomerados numa LVM³ (*Logical Volume Manager*), totalizando assim 3TB para armazenamento.

Num determinado dia, aparentemente, uma queda de energia fora do horário de expediente fez com alguns equipamentos desligassem e/ou reiniciassem, dentre eles o servidor de *backup*. Isso acabou danificando no servidor *backup*, um dos discos que compunha a LVM, fazendo com que toda a LVM parasse de funcionar, dessa forma todos os dias subsequentes, após o expediente, quando o servidor principal se conectava ao servidor de *backup* para efetuar a sua rotina de cópia diferencial, os arquivos não eram copiados, devido ao volume de destino para cópia não encontrar-se mais ativo. Como não havia sinais do ocorrido, já que o servidor de *backup* não era de responsabilidade dos funcionários e que não conheciam a gravidade que esse

¹ Backup é a cópia de segurança de dados para um ou mais dispositivos de armazenamento, afim de protegê-los. (MORIMOTO, 2005)

² Backup diferencial, consiste na cópia de todos os dados que foram modificados desde o último backup executado. (ALIANÇATI, 2015)

³ LVM é um recurso para gerenciamento de volume lógico no Linux que cria uma camada de abstração entre o sistema operacional e os discos. (OLIVEIRA, 2013)

incidente poderia causar, sendo assim, evidentemente a informação não foi passada ao responsável pelo departamento de TI da empresa.

Alguns dias depois uma forte oscilação de energia na região, ocasionou a parada total da empresa por alguns minutos, e, em seguida, ao ser reestabelecida a energia, notaram que o servidor principal da empresa não estava acessível e imediatamente o responsável pela TI foi acionado. Após diagnósticos, foram detectados que a fonte de alimentação e um dos discos que armazenavam os arquivos no servidor principal foram danificados.

Após efetuada as trocas da fonte de energia e do disco danificado tentou-se a restauração do *backup*. Foi então detectado de fato, que o *backup* não estava sendo executado a mais de quinze dias, pois a LVM do servidor de *backup* já havia sido comprometida anteriormente com o incidente com o servidor principal.

Perante essas dificuldades por conta das oscilações e queda de energia elétrica, a empresa ficou paralisada em seus processos por um período de quase oito horas, ou seja, praticamente um dia inteiro de expediente sem produção. Esse foi o menor problema se comparado à perda das informações que estavam armazenadas em dois discos que continham informações relevantes e aos prazos que não foram cumpridos graças ao primeiro incidente. A ocorrência desses incidentes gerou insatisfação por parte de vários clientes, além de uma grande dor de cabeça para os responsáveis, ainda podendo comprometer a reputação da empresa, por não passar mais credibilidade aos clientes que contratam os seus serviços. A falta de redundância e uma alta garantia de disponibilidade para esse tipo de empresa, pode gerar graves impactos nos negócios e, conseqüentemente nos objetivos que a mesma pretende atingir.

Este acontecimento não foi tornado público por se tratar de informações confidenciais, ficando só para a alta administração. Mesmo assim os prejuízos e/ou quanto a empresa deixou de lucrar após a paralização foram altos em função do longo período produtivo que a empresa ficou parada.

Contudo, utilizando-se a fórmula do cálculo para ilustrar qual foi a porcentagem de disponibilidade durante a semana do incidente. Pode-se notar que, de acordo com as necessidades de utilização do servidor da empresa que são de 8 horas durante 5 dias da semana (TS), mais de 15% do tempo de produtividade foi afetado.

$$TS = 8h \times 5d = 40h/\text{semana}$$

$$DT = 7$$

$$D = (40-7) / 40 \times 100 = 82,5\% \text{ de Disponibilidade na semana}$$

4.4. SOLUÇÃO PROPOSTA

Levando em consideração todo o embasamento teórico levantado para entendimento geral no que tange o desenvolvimento deste trabalho, do quão importante deve ser a sincronia entre o departamento de TI e o de negócios de uma empresa para a obtenção dos seus objetivos, será apresentado a seguir uma solução baseada no problema encontrado na Empresa X como estudo de caso, com o intuito de mostrar que com baixo custo e o correto uso dos recursos já presentes no ambiente em questão, seriam potencialmente minimizados ou até mesmo eliminados os riscos causados por oscilações e quedas de energia.

Partindo do princípio de que todo o problema foi gerado em torno de oscilações e quedas de energia em pelo menos duas ocasiões, e estas foram cruciais para a parada da empresa, é importante ressaltar que a Empresa X necessita primeiramente de *nobreaks*, de preferência gerenciáveis, instalados nos dois servidores. Esses nobreaks possuem recursos interessantes, como por exemplo, podendo enviar *e-mails* ou SMS automáticos com alertas sobre quedas de energia ao administrador, ou ainda serem configurados para desligar o servidores de maneira segura, no tempo determinado em situações de falhas de energia, caso a mesma não se estabeleça, além de contar com painéis de controle, onde é possível monitorar, inclusive remotamente todo o sistema de baterias e voltagens de entrada e saída do *nobreak*.

No servidor principal é interessante que os discos estejam configurados em RAID1, para que todo o conteúdo armazenado no disco1 seja espelhado no disco2, assim mesmo que um disco venha a falhar o outro continuará mantendo os serviços e os arquivos ativos até que seja possível a substituição do disco danificado e com espaço de armazenamento de 2TB.

No servidor de *backup*, por possuir três discos de 1TB cada, é essencial que tenha em nível de capacidade de armazenamento, pelo menos a mesma quantidade que o servidor principal, ou seja, 2TB. No entanto, a única forma de igualar esse espaço de armazenamento e ainda ter um ponto contra falhas de discos neste servidor, seria configurar os discos em RAID5, de forma que eles contenham em si, as informações suficientes para manter as informações em caso de falha de um dos discos e ainda com capacidade para reconstruir o sistema de RAID5, após substituição do disco danificado.

Embora, esses dois equipamentos tenham funcionado por muito tempo como servidores de forma adaptada e suprimindo as necessidades da empresa, trata-se de uma composição de *hardware* não confiável para este fim, sendo insuficiente, quando o assunto é a salvaguardar informações importantes.

Por isso, a sugestão oferecida à empresa é a transformação dos servidores principal e de *backup*, respectivamente em servidores primário e secundário, de maneira em que os dois tivessem, as informações sincronizadas em um período de tempo mais curto, afim de criar um espelhamento entre eles e que caso haja uma interrupção que impossibilite o acesso ao servidor primário, o secundário possa assumir de maneira automática a função do servidor primário, pois este já estaria pronto para fornecer os serviços necessários aos usuários.

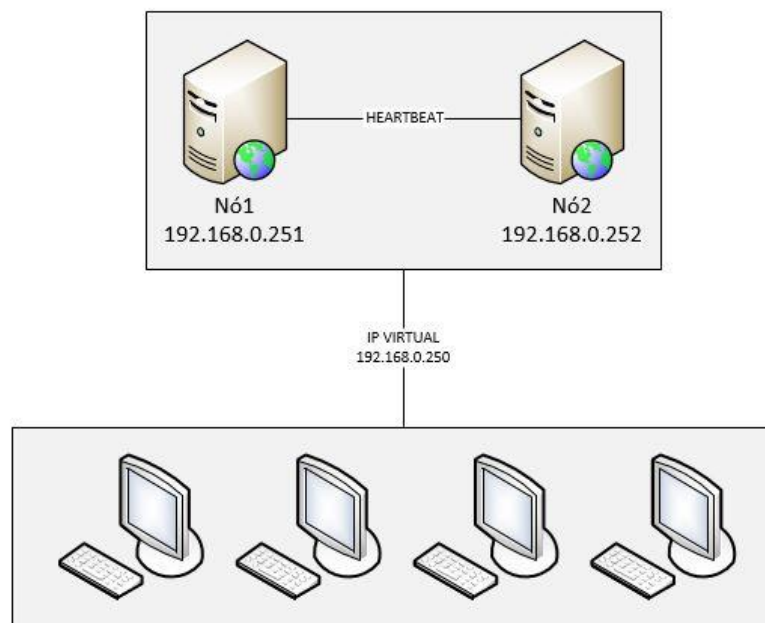
Usando o conceito de alta disponibilidade, o sistema proposto implica em fornecer um endereço de IP virtual único para os dois servidores, onde os usuários não acessariam mais pelo IP de um ou outro servidor, mas sim por esse IP virtual, e se eventualmente o servidor primário parasse de responder por algum motivo, todas as solicitações seriam automaticamente enviadas ao servidor secundário.

Para melhor entendimento do sistema proposto, torna-se pertinente a apresentação das ferramentas utilizadas para sua implementação. São elas o *Heartbeat* e o *RSync*. Controles esses que podem ser instalados no sistema Linux e podem ser baixados através do comando "*apt-get install heartbeat*" ou "*apt-get install rsync*", no caso do Linux Debian 9.

O *Heartbeat* (Figura 16) de acordo o site oficial (2010) é um controle que fornece serviços de infraestrutura de *cluster* para sistemas Linux a partir de dois equipamentos, denominado "nós", a partir de um IP virtual. Para exemplificação, serão

denominados, nó1 e nó2. Após a configuração adequada do *Heartbeat* nos dois nós, sua função mais básica é monitorar os batimentos cardíacos (*heartbeat*) de ambos os nós em duplo sentido, tanto do nó1 para o nó2, quanto do nó2 para o nó1, para então estabelecer qual ação deverá ser tomada em caso de um determinado nó deixar de responder por um determinado período de tempo. Por exemplo, para dois servidores *web* o nó2 fica em *standby* monitorando os batimentos cardíacos do nó1, através de uma porta específica configurada e se por algum motivo, o nó1 que estaria rodando o Apache que é o serviço responsável por páginas *web*, pare de responder por um tempo, o nó2 automaticamente sobe o serviço de controle do Apache, e, a partir daí, responderá a todas as requisições *web* que serão feitas através do IP virtual. Veja na Figura 16.

Figura 16 – Funcionamento do Heartbeat

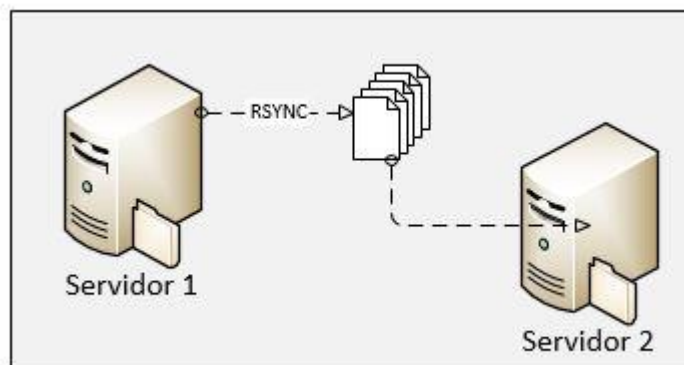


Fonte: Autoria própria

Já o *RSync* (Figura 17) de acordo com o site oficial (2014) é uma ferramenta utilizada para efetuar cópia de arquivos tanto localmente quanto remotamente. Além

de muito ágil, o *RSync* permite ainda que seja feita a comparação entre arquivos de dois diretórios, a fim de garantir a cópia de somente informações que for diferente entre eles, reduzindo uso de banda de rede em casos de cópias entre *hosts* remotos de forma compactada, evitando assim que um determinado arquivo seja copiado inteiramente inúmeras vezes após cada alteração. Essa ferramenta foi desenvolvida pela *samba.org* que também desenvolve uma ferramenta para controle de compartilhamentos no Linux de acordo com o site oficial (2009). O *RSync* Possibilita ainda a comunicação segura através de *SSH*, e é amplamente usada para efetuar *backups* e espelhamento entre *hosts*, preservando ainda propriedades de arquivos de diretórios, como: dono, grupo padrão e permissões.

Figura 17 – Exemplo de cópia remotamente com o RSync



Fonte: Autoria própria

Como o objetivo deste trabalho é a implantação de alta disponibilidade na Empresa X, após a reconfiguração dos discos nos servidores da mesma, será necessário a configuração dos grupos e usuários que acessam os arquivos igualmente nos dois servidores para que não haja impossibilidade por algum usuário da rede em acessar algum arquivo ou informação em qualquer que seja o servidor ativo no momento. Nota-se que, os grupos e usuários cadastrados no sistema Linux, não são necessariamente os mesmos que irão acessar as informações compartilhadas, para isso cabe a configuração de permissão de cada usuário no arquivo de configuração do samba.

Portanto, ao serem aplicadas todas as alterações descritas anteriormente para obtenção do ambiente com alta disponibilidade na Empresa X, o sistema funcionaria da seguinte maneira:

O servidor primário com o samba e suas respectivas configurações de acesso de diretórios, grupos e usuários e permissões ativo, receberá diretamente através do IP virtual, todas as requisições feitas pelos *hosts* clientes, quanto ao acesso aos compartilhamentos de arquivos. Por sua vez, todo conteúdo gerado e/ou alterado será copiado, mantendo as propriedades de diretórios e arquivos para o servidor secundário que estará monitorando o servidor primário e se encontrará pronto para assumir as requisições vindas dos *hosts* cliente, caso aconteça algum imprevisto com o servidor primário.

Uma vez que o servidor primário torna-se inacessível, seja por estar desligado ou a placa de rede com falha, o servidor secundário, automaticamente iniciará o serviço de compartilhamento do samba e passará a receber as requisições dos *hosts* cliente, sem que esses clientes “notem” a mudança de servidor.

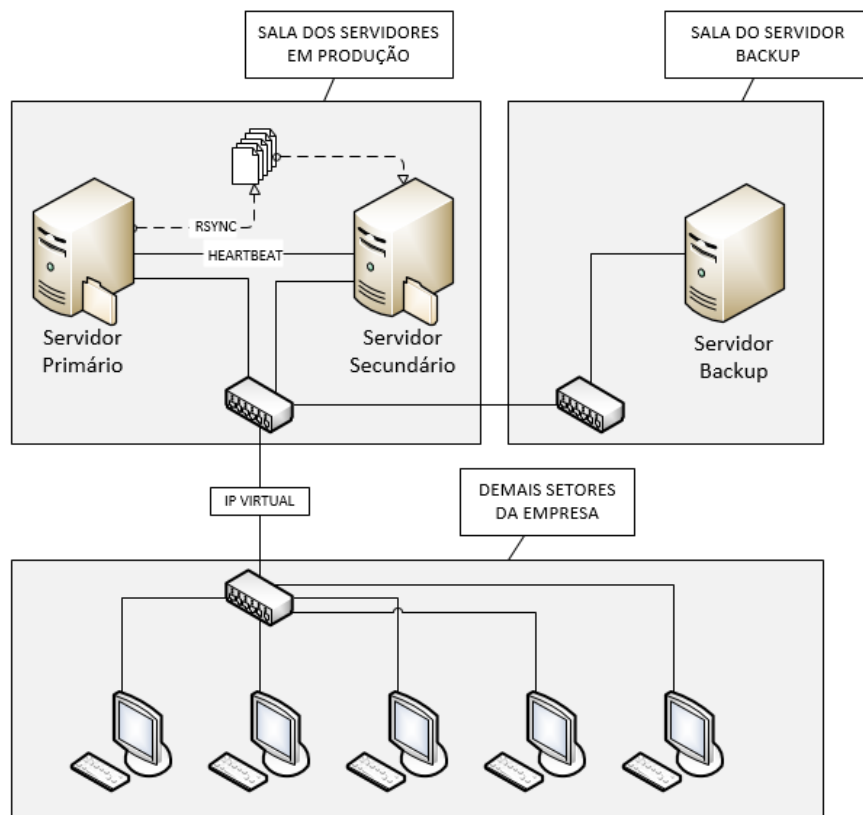
Para assegurar os dados, no que diz respeito a tempo de retenção, ou seja, backup, poderá ser usado o equipamento estacionado no departamento de TI. Sendo necessário, é claro, antecipadamente aquisição de novos discos, devido a necessidade de se garantir maior segurança e confiabilidade, preferencialmente com o dobro de capacidade que os servidores em produção possuem naquele momento, no caso, 4TB, a fim de prepará-lo para desempenhar essa função.

Seria pertinente a implementação de uma rotina de *backup* diferencial, para que assim o processo de cópia seja efetuado de maneira mais ágil, uma vez que esta rotina será executada após o expediente, sugerindo ainda a criação de um script que desligue o servidor de *backup* automaticamente ao fim da execução da rotina.

Como a referida empresa não possui um responsável especialista pela infraestrutura de TI, seria interessante a exibição de painéis com a sinalização do status do cluster através de páginas web armazenadas em cada servidor. Esse procedimento seria fácil de ser implantado pois a transição entre um servidor e outro ocorre de forma transparente. Sendo assim, o painel indicaria qual servidor está ativo no momento, para que a administração possa tomar as devidas providências e solicitar o suporte técnico o mais rápido possível.

Com o intuito de minimizar custos e reorganizar os recursos existentes na Empresa X, aproveitando-os da melhor maneira possível, a solução proposta, possivelmente, diminuiria os problemas encontrados, evitando, consideravelmente o tempo de ociosidade por parte da produção da empresa com eventuais falhas do servidor principal, garantindo ainda, a segurança das informações nele armazenadas. A seguir a Figura 18 exibe a nova topologia após todas as alterações aplicadas.

Figura 18 – Proposta para nova topologia básica da Empresa X



Fonte: Autoria própria

5. CONSIDERAÇÕES FINAIS

Baseando-se nas informações levantadas no decorrer deste trabalho, é possível evidenciar que a cada dia, a TI se torna mais importante para as empresas. Bem como sistemas automatizados são capazes de potencializar e otimizar consideravelmente os recursos utilizados para obtenção de resultados, auxiliando no crescimento da organização e favorecendo a ascensão de patamares mais altos em relação às suas concorrentes, seja na captação de novos clientes, melhorias nos processos ou nos prazos e até mesmo na entrega de melhores produtos.

Dessa forma a implantação do Cluster de Alta Disponibilidade contingenciará de forma eficiente a produtividade, proporcionando eficazmente a continuidade do negócio, além ainda de reduzir os impactos motivados por incidentes e aumentando o nível de segurança das informações armazenadas. Agregando assim valor aos seus negócios passando maior credibilidade aos seus clientes.

Contextualizando sobre o estudo de caso apresentado, a implantação do cluster maximizara o uso de recursos existentes, trazendo consigo o alinhamento necessário entre o departamento de TI e as necessidades de negócios apresentados na empresa X. Gerando uma melhoria na qualidade também da administração dos servidores e serviços de armazenamentos e *backups*.

Finalizando, não sendo possível a aplicação literal do Cluster de Alta Disponibilidade na empresa analisada, devido ao fato de que a empresa possui contrato com a prestadora de serviços de TI, tornou-se necessário a implantação em ambiente simulado, através de máquinas virtuais. No entanto, o projeto se mostrou plausível e viavelmente bem-sucedido conforme pode ser visualizado nos Apêndices a seguir, elaborados para fins explicativos dos passos percorridos para a implementação do cluster de alta disponibilidade.

6. REFERÊNCIAS

ALIANÇATI. **Quatro tipos de backup**. 27 de maio 2015. Disponível em: <<http://www.aliancatecnologia.com/conteudo/2015/05/quatro-tipos-de-backup/>>. Acesso em 31 maio 2018.

BORGES, F.M, RODRIGUES, C.L.P. Pontos passíveis de melhoria no método de projeto de produto de Pahl e Beitz. **Gestão & Produção**; V.17, n.2, 2010. São Carlos. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-530X2010000200005 >. Acesso em 30 mai. 2018.

CESTARI, Felício. **ITIL V3: fundamentos**. Rio de Janeiro: Editora RNP/ESR, 2012.

ELIAS, Diego. **Dados vs. informação**. 11 de dez 2017. Disponível em: <<https://www.binapratca.com.br/dados-x-informacao/>>. Acesso em 31 maio 2018.

DEBIAN, Linux. **Sobre o debian**. 06 de jun. 2017. Disponível em: <<https://www.debian.org/intro/about>>. Acesso em 09 maio 2018.

DELFINO, Pedro. **Sistemas operacionais: conheça os melhores do mercado e tenha outras opções**: 02 de jun. 2017. Disponível em: <<http://e-tinet.com/linux/sistemas-operacionais-os-melhores/>>. Acesso em 09 maio 2018.

DOROW, Emerson. **ITIL – gerenciamento da disponibilidade**: 23 de nov. 2009. Disponível em: <<https://www.profissionaisiti.com.br/2009/11/itil-gerenciamento-da-disponibilidade/>>. Acesso em 23 maio 2018.

GASETA, E.R. **Fundamentos de governança de TI**. 2ª ed. Rio de Janeiro: Editora RNP/ESR, 2012.

HARDWARE, Guia. **Backup**. 26 de jun. 2005. Disponível em: <<https://www.hardware.com.br/termos/backup/>>. Acesso em 31 maio 2018.

HESKETH, José Luiz; COSTA, Maria T. P. M. Construção de um instrumento para medida de satisfação no trabalho. **Revista. Administração de Empresas**; v. 20, n. 3, p. 59-68, set. 1980. São Paulo. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-75901980000300005>. Acesso em: 16 jun. 2017.

BRASIL, Infortrend. **O que é RAID e como ele funciona**. 29 de setembro 2016. Disponível em: <<http://www.infortrendbrasil.com.br/tecnologia/o-que-e-raid-e-como-ele-funciona/>>. Acesso em 05 jun. 2018.

KUROSE, J. F; ROSS, K. W. **Redes de computadores e a internet**: uma abordagem top-down. 6ª ed. São Paulo: Editora Pearson, 2013.

HA, Linux. **Heartbeat**. 20 de fevereiro 2010. Disponível em: <<http://linux-ha.org/wiki/Heartbeat>>. Acesso em 31 maio 2018.

MAZIERO, Carlos. **Sistemas operacionais**: conceitos e mecanismos. Curitiba: Editora DINF-UFPR, 2017.

MCLEAN, Ian; THOMAS, Orin. Windows server administration: training kit. **MCITP EXAM**. p. 70-646. Washington: Editora Microsoft Press, 2008.

MONTEIRO, M.A. **Introdução à organização de computadores**. 5ª ed. Rio de Janeiro: Editora LTC, 2007.

MORIMOTO, Carlos E. **Servidores Linux**: guia prático. 3º ed. Porto Alegre: Editora SUL Editores, 2011.

OLIVEIRA, E.F. **LVM - Introdução**. 03 de maio 2013. Disponível em: <<https://www.vivaolinux.com.br/dica/LVM-Logical-Volume-Manager>>. Acesso em 31 maio 2018.

SAMBA. **Rsync**. 23 de dez. 2014. Disponível em: <<https://rsync.samba.org/>>. Acesso em 31 maio 2018.

SAMBA. **About Samba**. 17 de jul. 2009. Disponível em: <<https://www.samba.org/>>. Acesso em 31 maio 2018.

SANTOS, L.A.F. **Segurança da informação: introdução**, 2009. Disponível em: <http://pt.slideshare.net/luiz_arthur/seguranca-da-informao-introduo>. Acesso em 30 maio 2016.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. 2ª ed. Rio de Janeiro: Editora Elsevier, 2014.

TANEMBAUM, A. S. **Redes de computadores**. 4º ed. Rio de Janeiro: Editora Campus, 2003.

TANEMBAUM, A. S. **Sistemas operacionais modernos**. 3º ed. São Paulo: Editora Pearson, 2009.

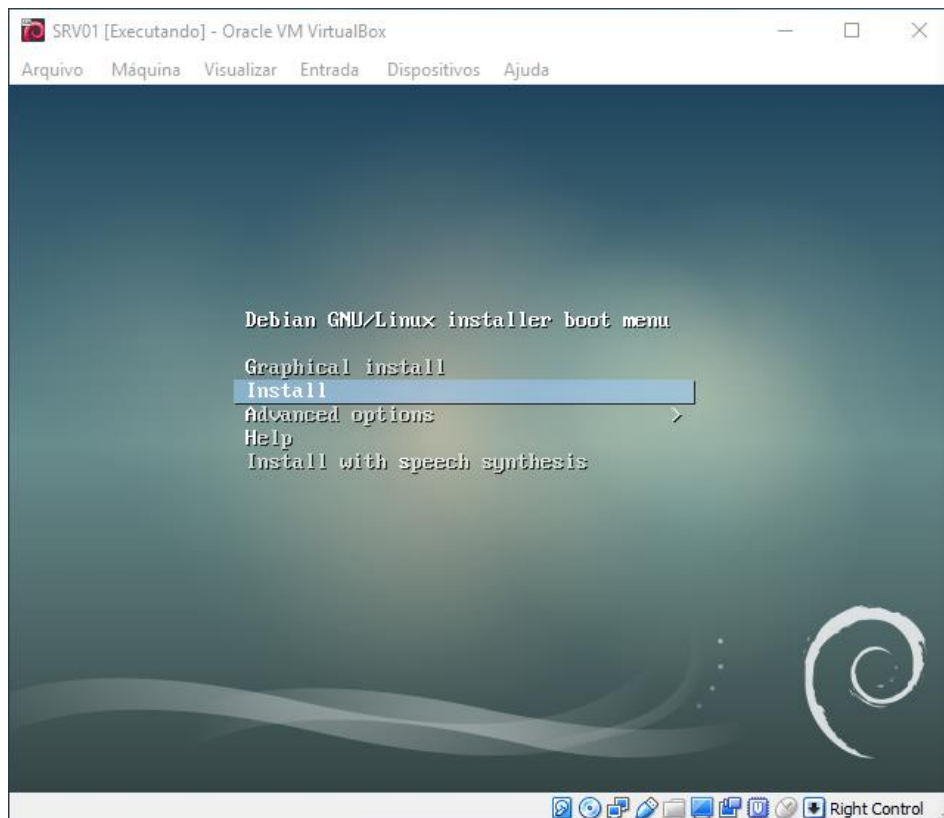
APÊNDICE A – INSTALANDO O LINUX DEBIAN 9

A instalação foi executada simultaneamente nos dois servidores de forma simples e objetiva com as funcionalidades mais básicas, porém suficientes para o funcionamento do cluster de alta disponibilidade.

A mídia de instalação da instalação do Linux Debian 9 foi baixada no seguinte link: <https://cdimage.debian.org/debian-cd/current/amd64/iso-cd/debian-9.4.0-amd64-netinst.iso>

Na tela de apresentação da instalação do **Debian 9**, foi selecionado a opção **Install** para iniciar a instalação sem os recursos gráficos.

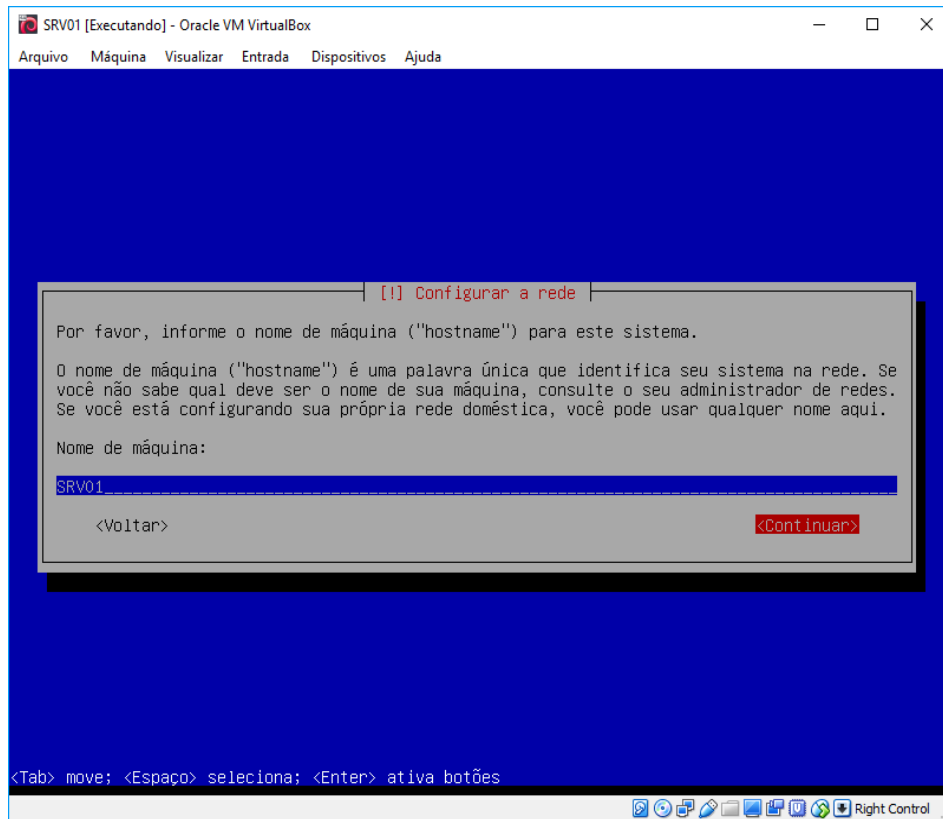
Figura 19 - Tela de apresentação do Debian 9



Fonte: Autoria própria

E em seguida definido o nome **SRV01** para o servidor primário e **SRV02** para secundário.

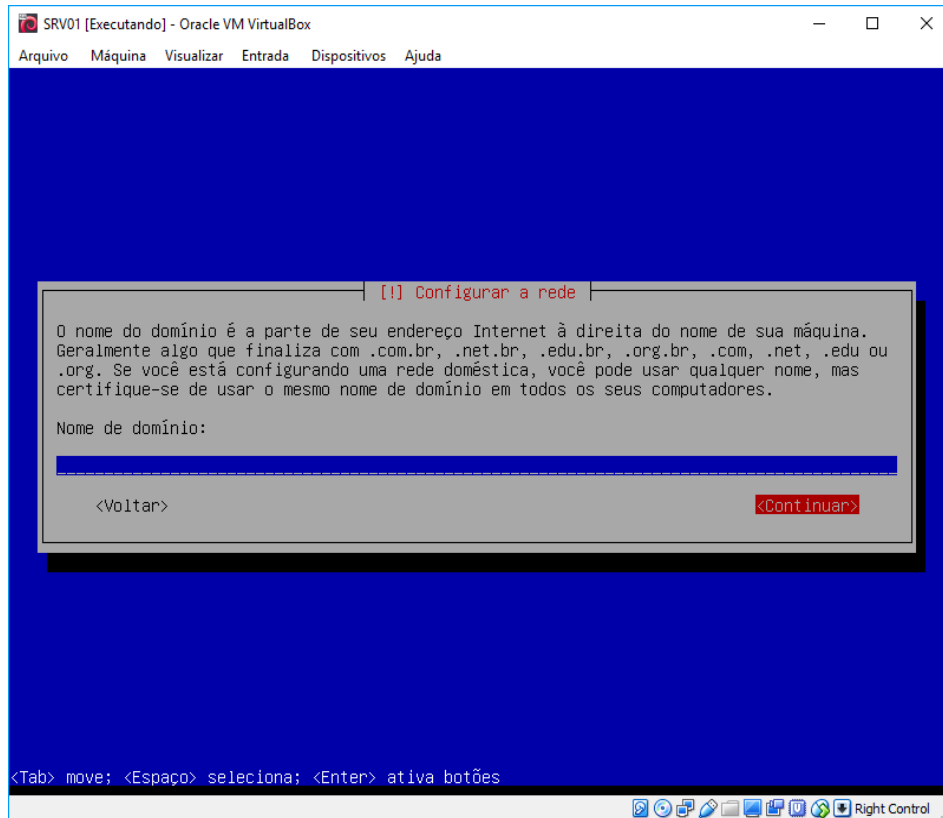
Figura 20 - Tela de definição do nome do Servidor



Fonte: Autoria própria

O nome de domínio não foi definido por não ser necessário.

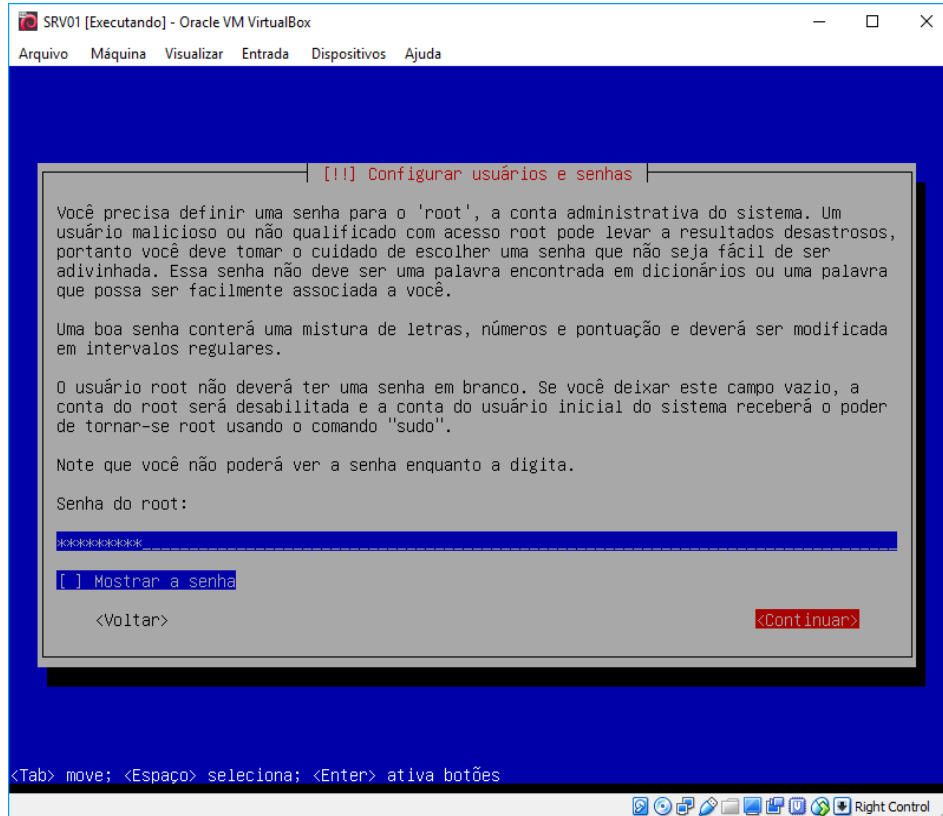
Figura 21 - Tela de definição do domínio



Fonte: Autoria própria

Em seguida foi definido a senha do **root** (administrador do Linux).

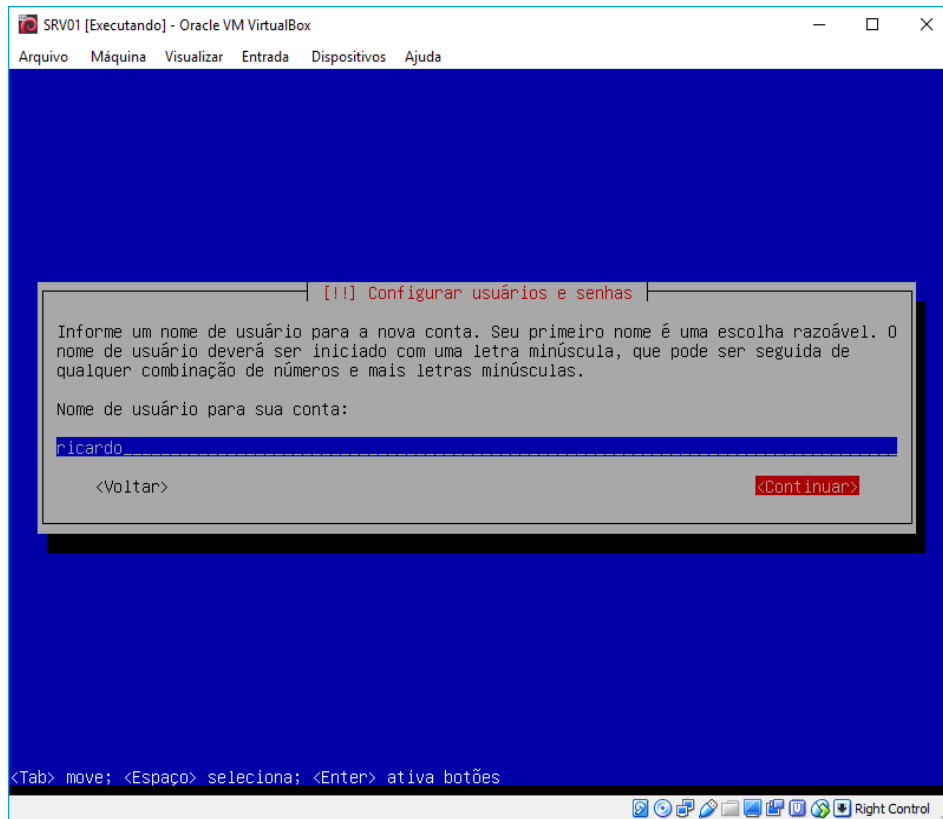
Figura 22 - Tela de definição da senha do root



Fonte: Autoria própria

Foi criado um usuário como **ricardo** e que posteriormente foi utilizado para efetuar as configurações do Linux.

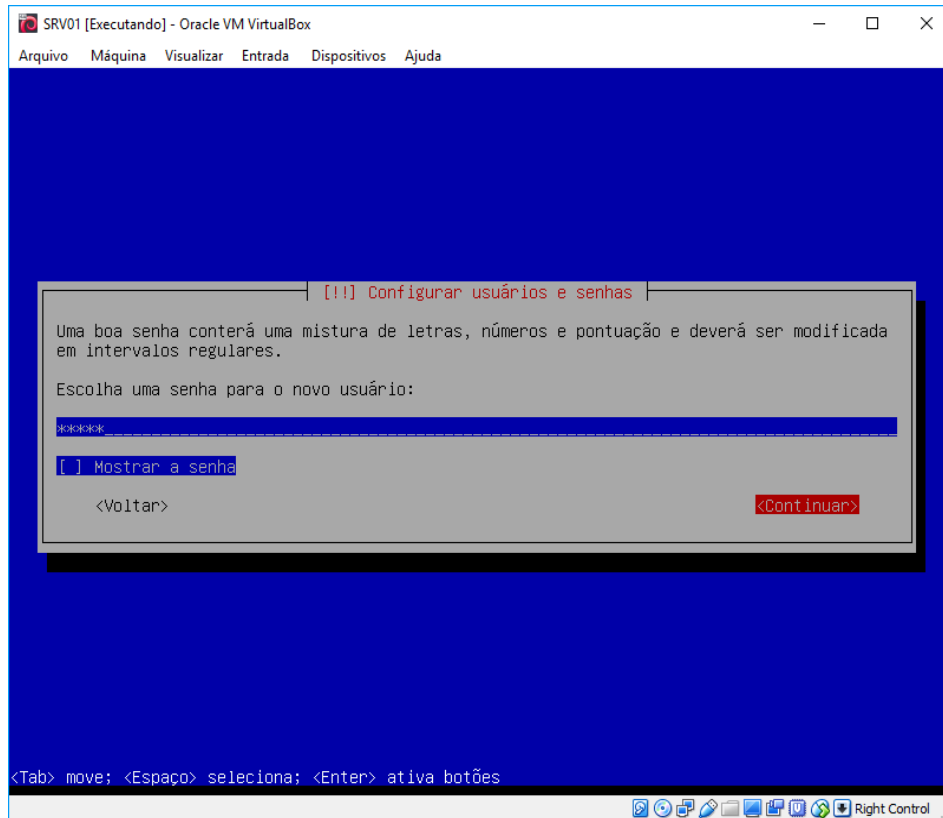
Figura 23 - Tela de criação do usuário



Fonte: Autoria própria

Com o usuário **ricardo** criado, foi definido então a senha.

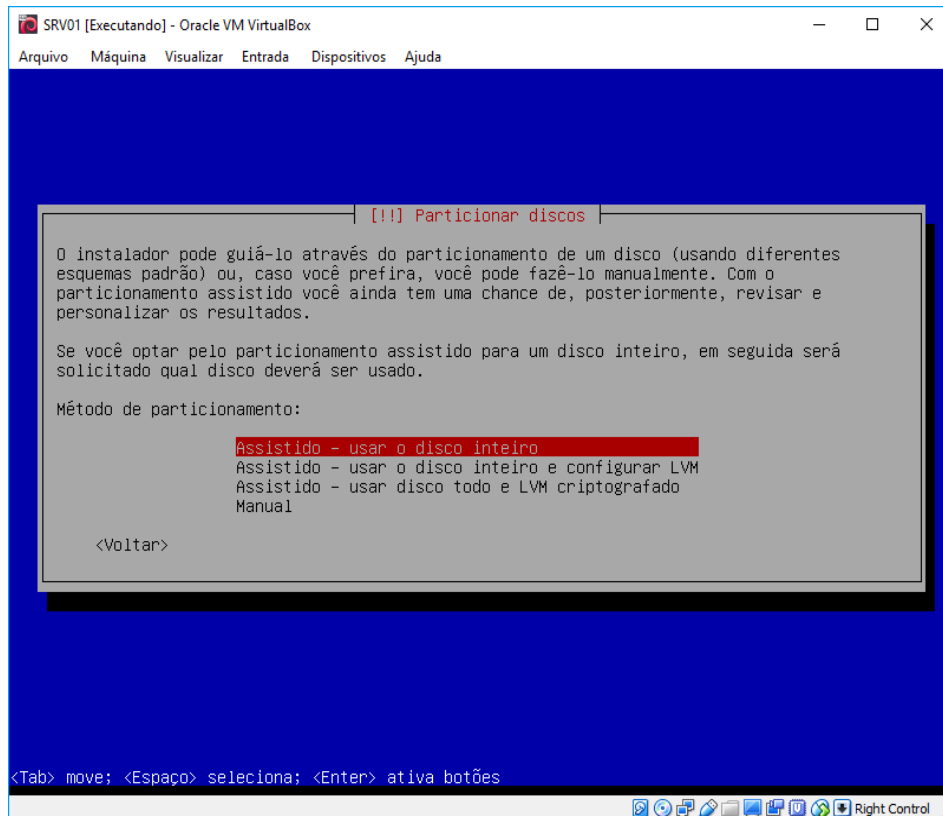
Figura 24 - Tela de definição da senha do usuário



Fonte: Autoria própria

Foi selecionado o método de particionamento **Assistido – usar o disco inteiro** para simplificar a instalação.

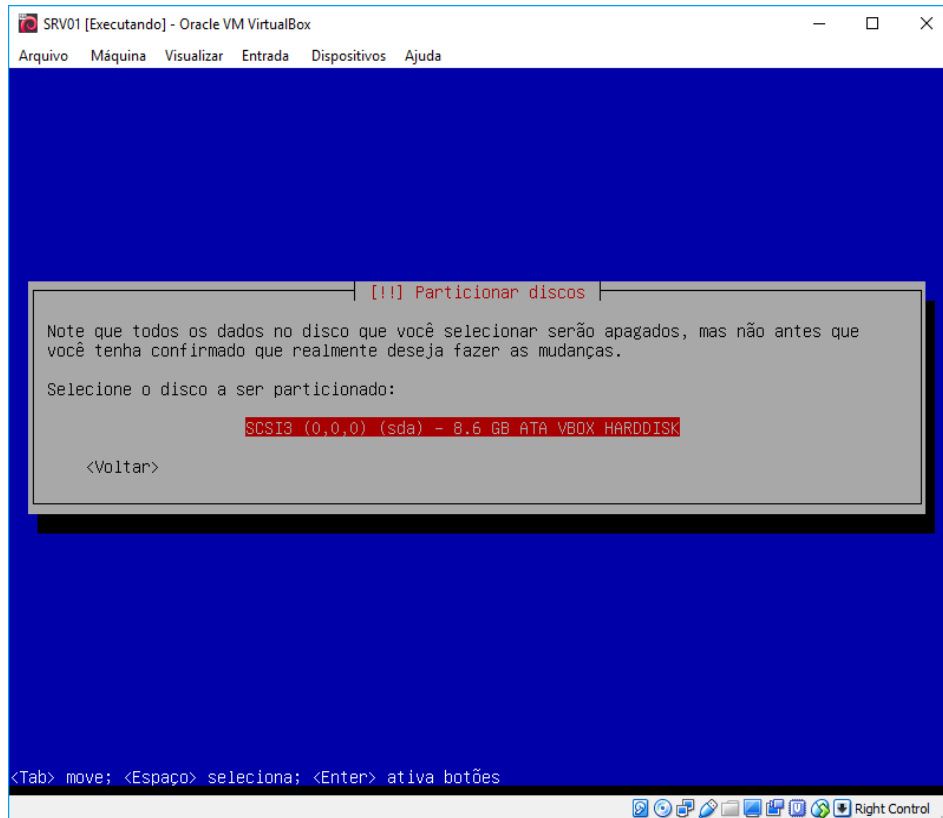
Figura 25 - Tela de definição do modo do particionamento



Fonte: Autoria própria

Foi selecionado então o disco a ser particionado, no caso (**sda**).

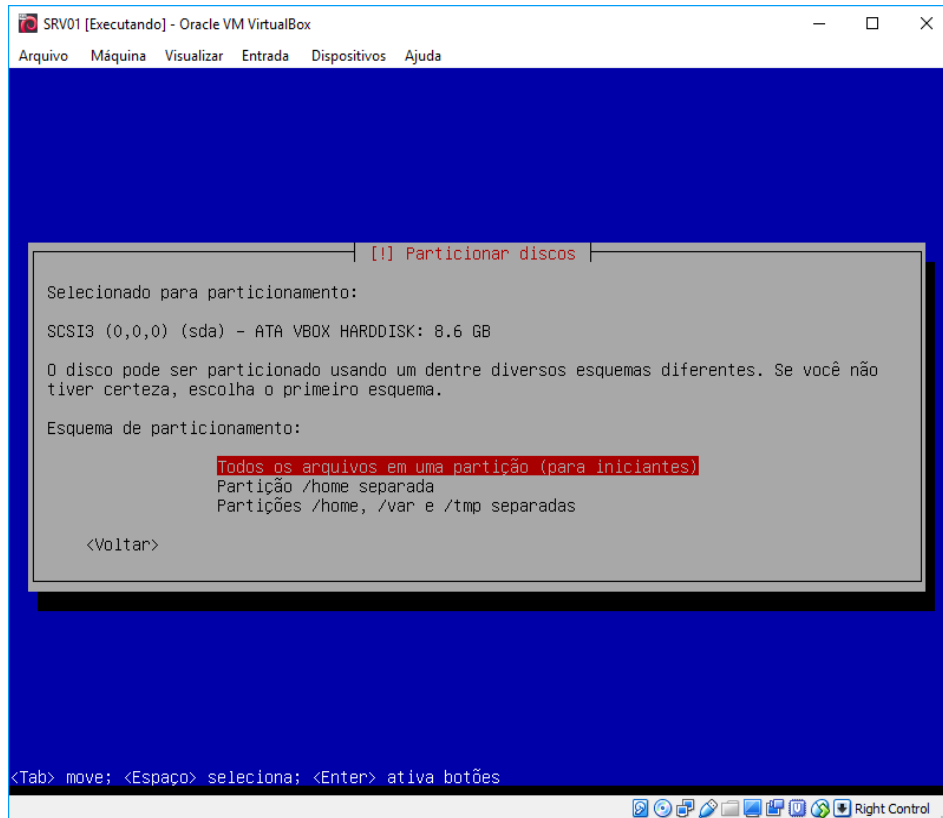
Figura 26 - Tela de definição do disco para particionamento



Fonte: Autoria própria

Foi selecionado a opção **Todos os arquivos em uma partição (para iniciantes)**

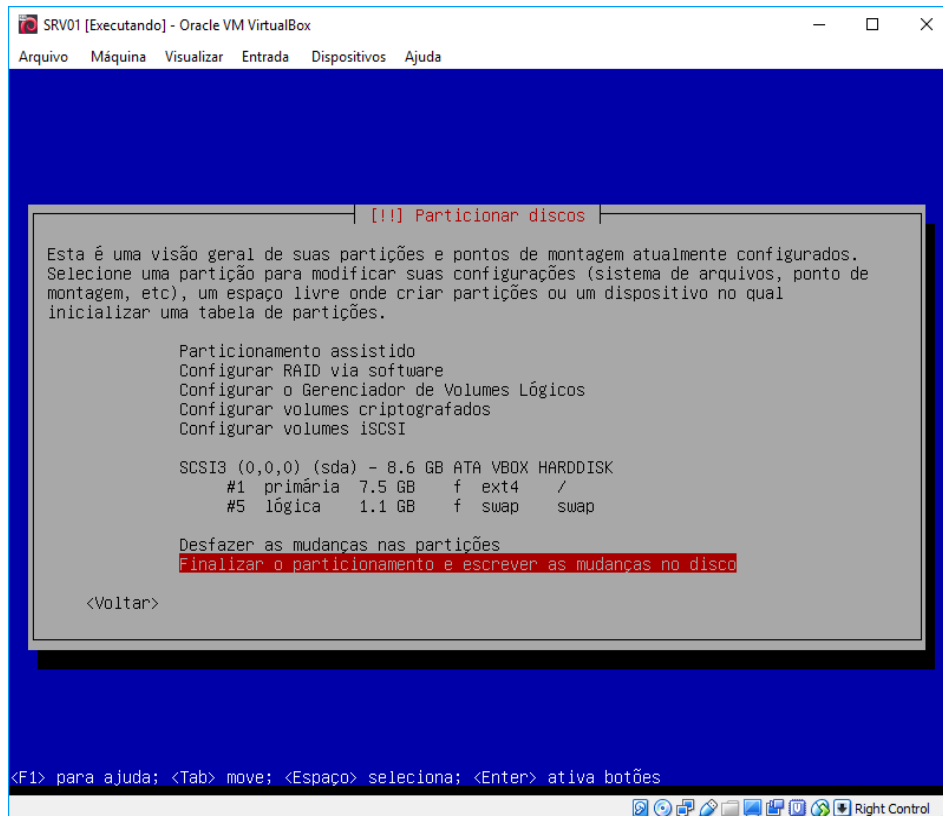
Figura 27 - Tela de esquema de particionamento



Fonte: Autoria própria

Após verificação do particionamento foi selecionado a opção **Finalizar o particionamento e escrever mudanças no disco.**

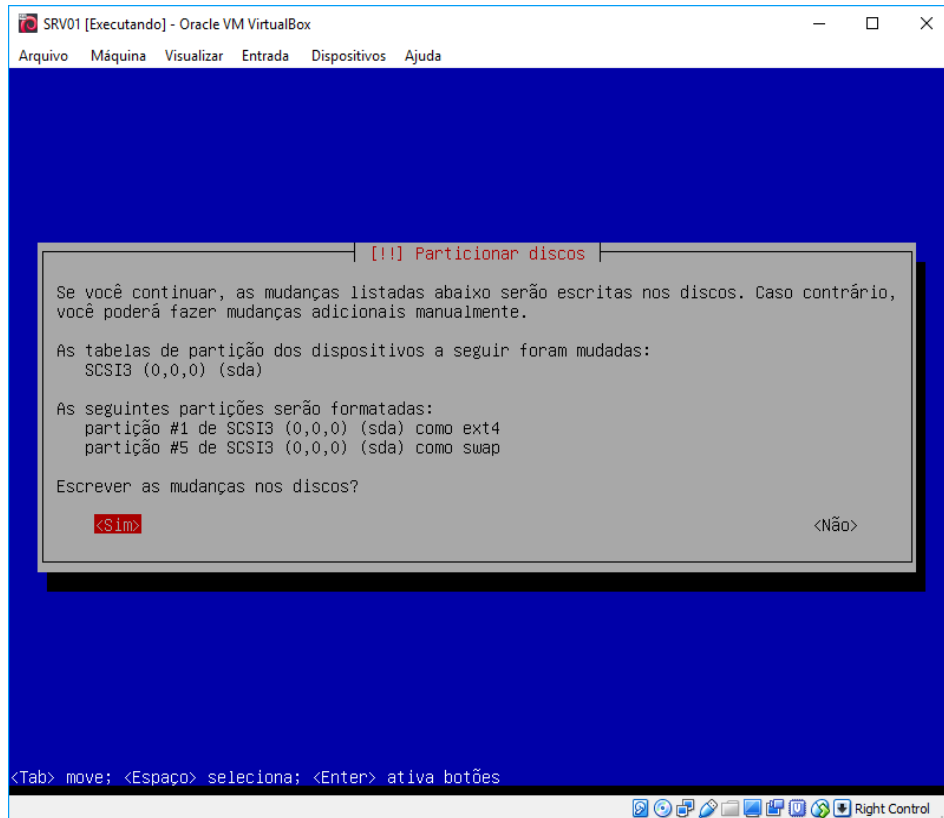
Figura 28 - Tela de informações de particionamento



Fonte: Autoria própria

Em seguida foi confirmado selecionando a opção **Sim**.

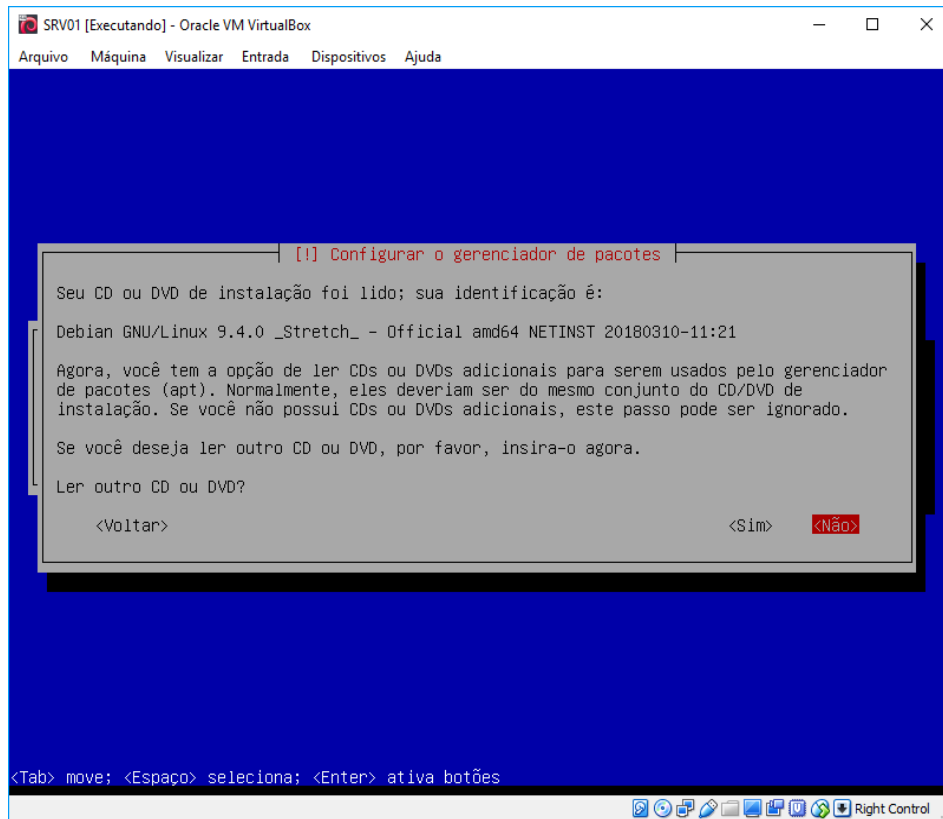
Figura 29 - Tela de confirmação de particionamento



Fonte: Autoria própria

Quando solicitado sobre o desejo de inserir outra mídia de instalação, foi selecionado a opção **Não**.

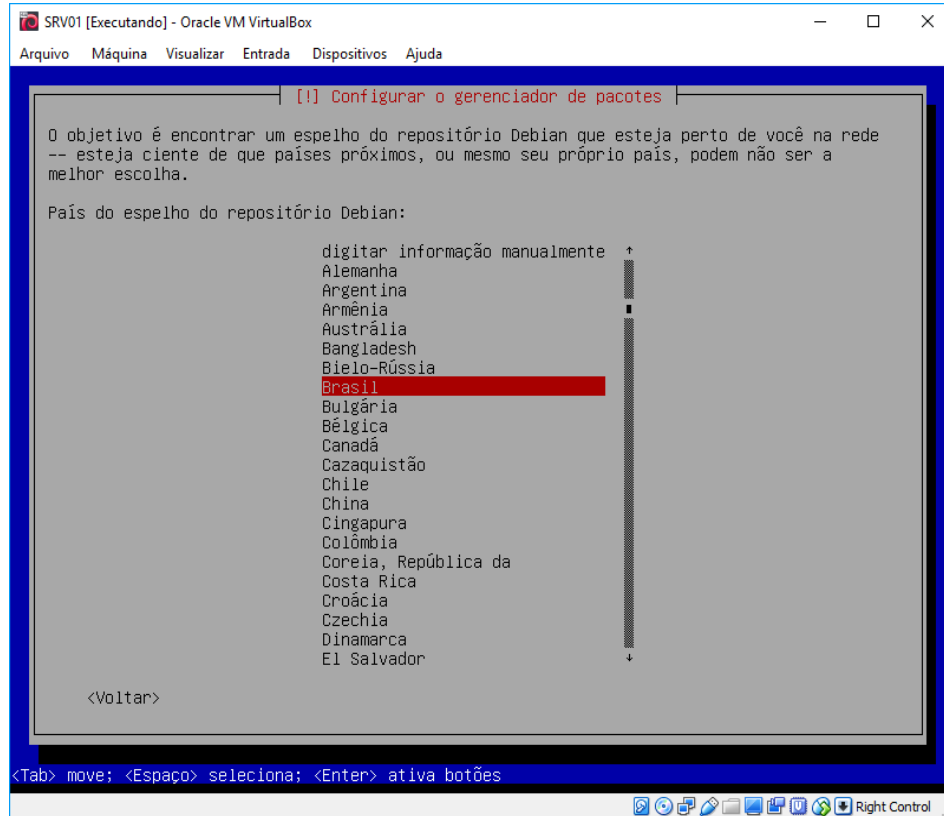
Figura 30 - Tela de troca de mídia de instalação



Fonte: Autoria própria

Na configuração de gerenciador de pacotes, foi selecionado **Brasil**.

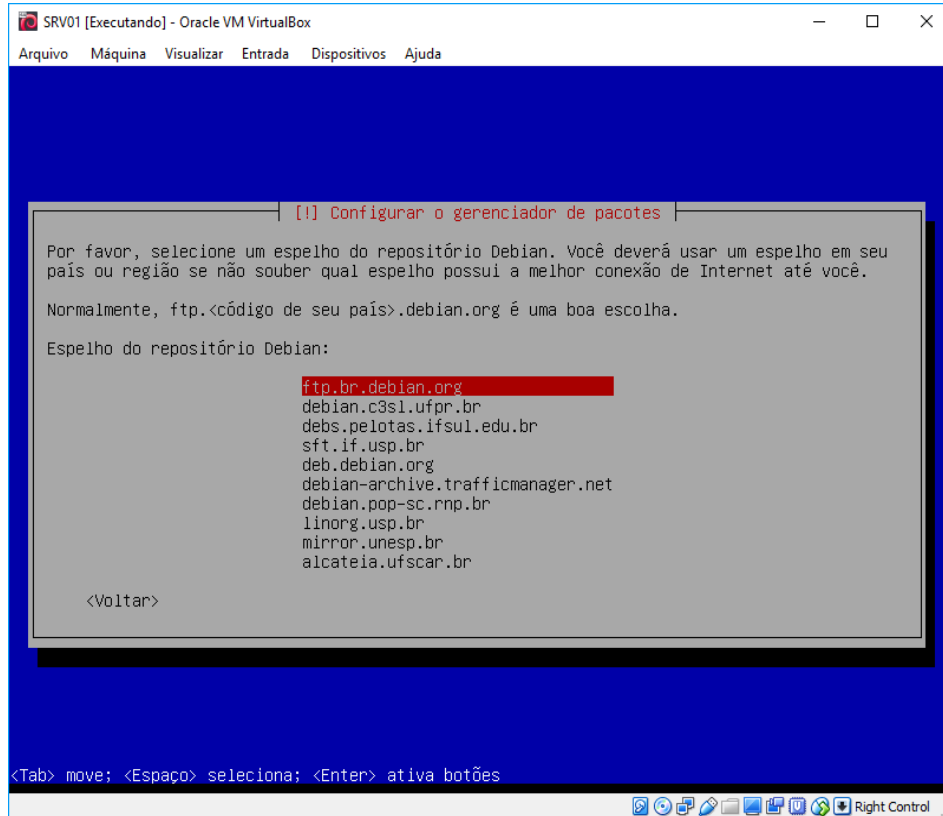
Figura 31 - Tela de definição do espelho de repositório



Fonte: Autoria própria

Sobre o espelho do repositório, foi selecionado a opção **ftp.br.debian.org**.

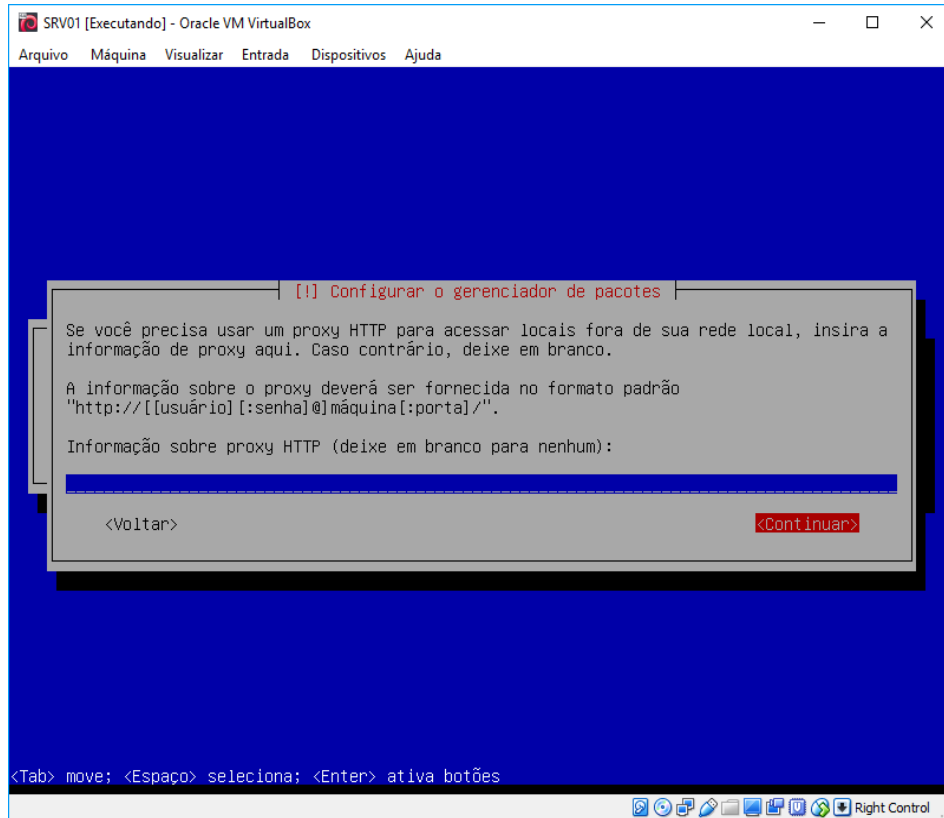
Figura 32 - Tela de definição do servidor de repositório



Fonte: Autoria própria

Não foi necessário configuração de **proxy HTTP**.

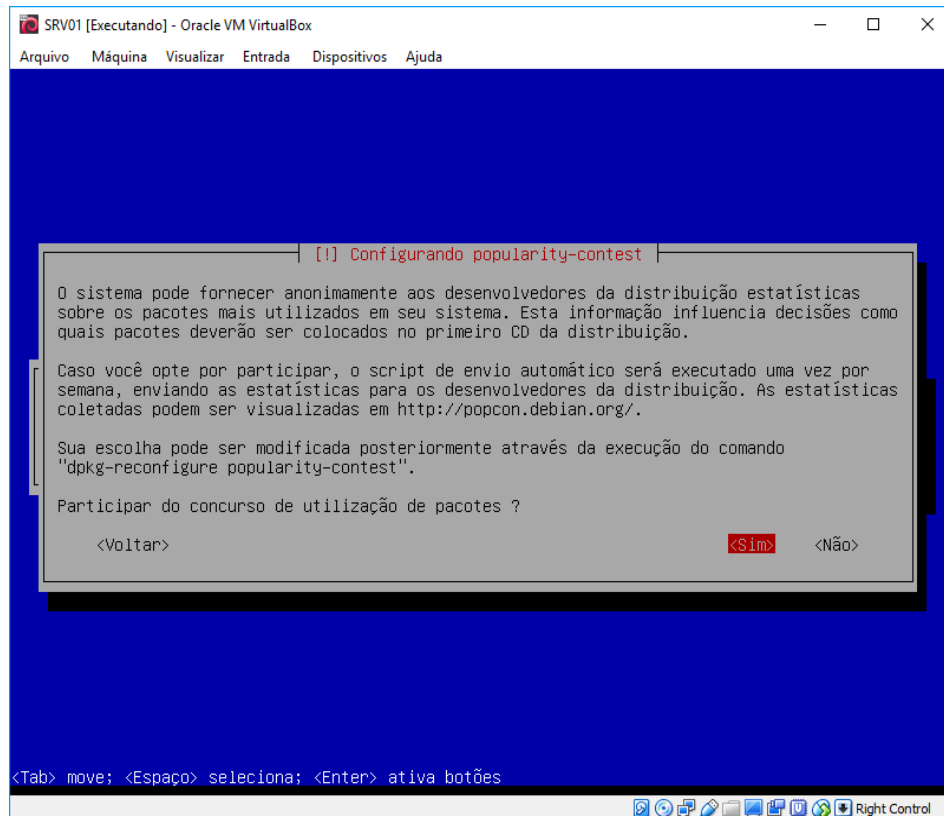
Figura 33 - Tela de definição do proxy



Fonte: Autoria própria

Quando solicitado para participar do concurso de utilização de pacotes, foi selecionado **Sim**.

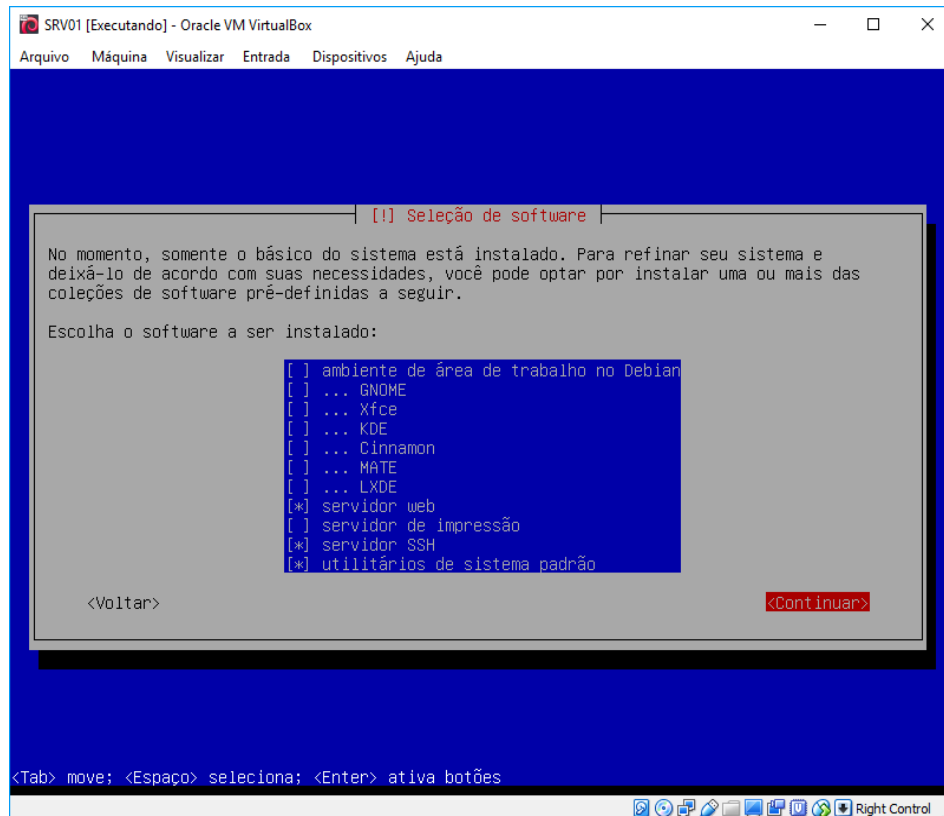
Figura 34 - Tela de concurso de utilização de pacotes



Fonte: Autoria própria

E em seleção de software, foram marcados **servidor web**, **servidor ssh** e **utilitários de sistema padrão**.

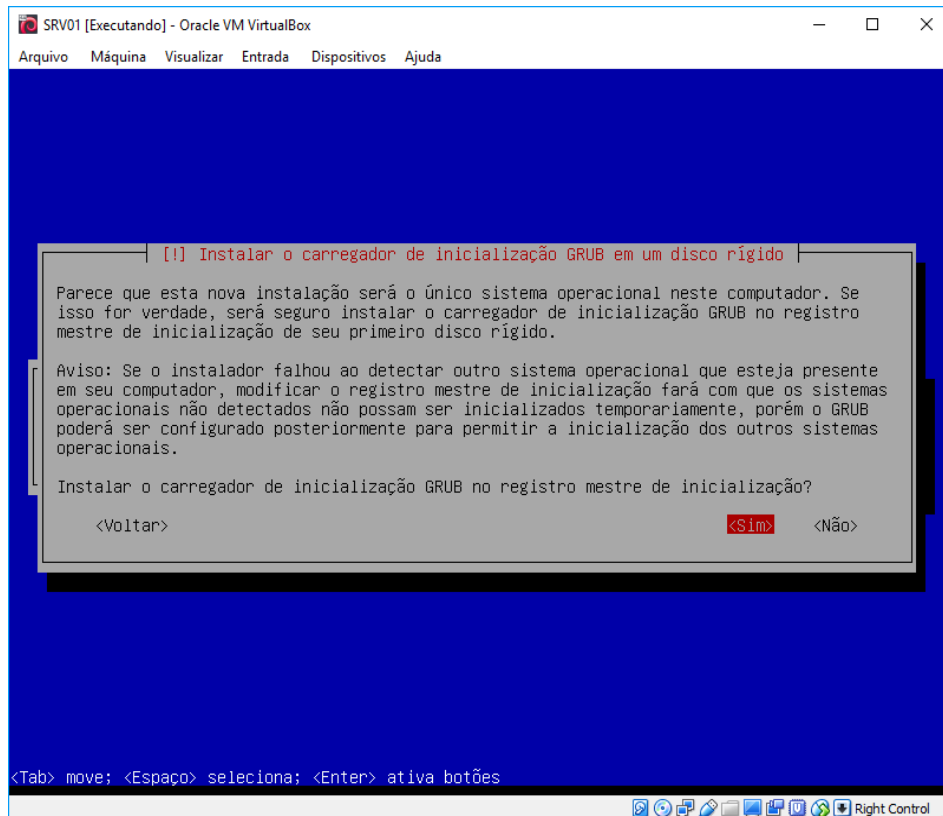
Figura 35 - Tela de seleção de software



Fonte: Autoria própria

Após instalado os softwares selecionados junto com o sistema, restaria a instalação do carregador de inicialização **GRUB** do Linux, foi selecionado **Sim**.

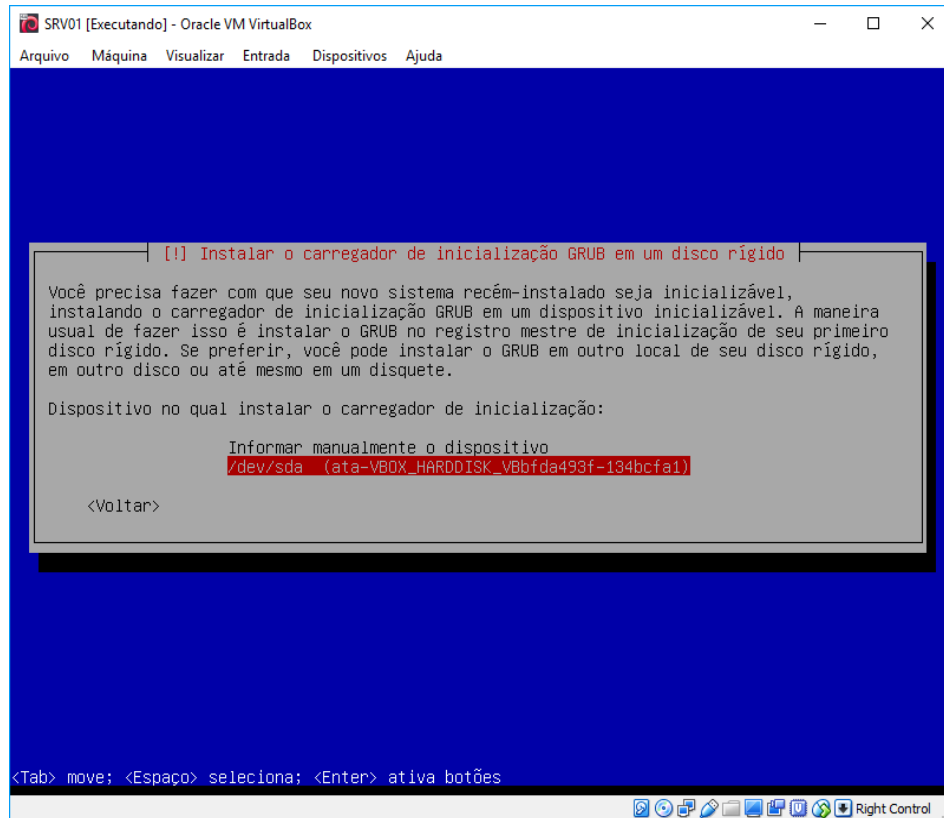
Figura 36 - Tela de instalação do grub



Fonte: Autoria própria

E então selecionado o dispositivo (**/dev/sda**) para instalação do **GRUB**.

Figura 37 - Tela de seleção do disco para instalação do grub

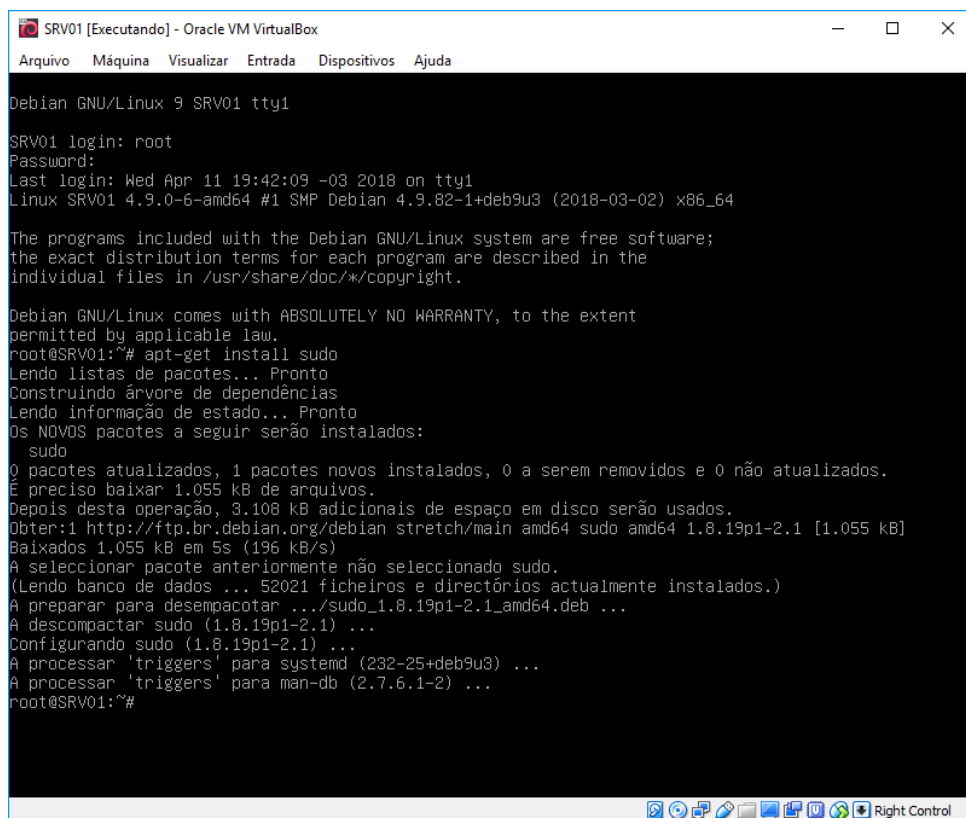


Fonte: Autoria própria

APÊNDICE B – PREPARANDO O LINUX PARA O CLUSTER

Todas as configurações apresentadas no APÊNDICE B foram efetuadas simultaneamente e igualmente nos dois servidores. Sendo assim, para que fosse possível a configuração do Linux através do usuário **ricardo** criado anteriormente na instalação, foi necessário adicioná-lo ao grupo **sudo**, que por sua vez, não vem habilitado no Linux Debian. Foi executado então o comando ***apt-get install sudo***.

Figura 38 - Instalação do sudo



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

Debian GNU/Linux 9 SRV01 tty1
SRV01 login: root
Password:
Last login: Wed Apr 11 19:42:09 -03 2018 on tty1
Linux SRV01 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) x86_64

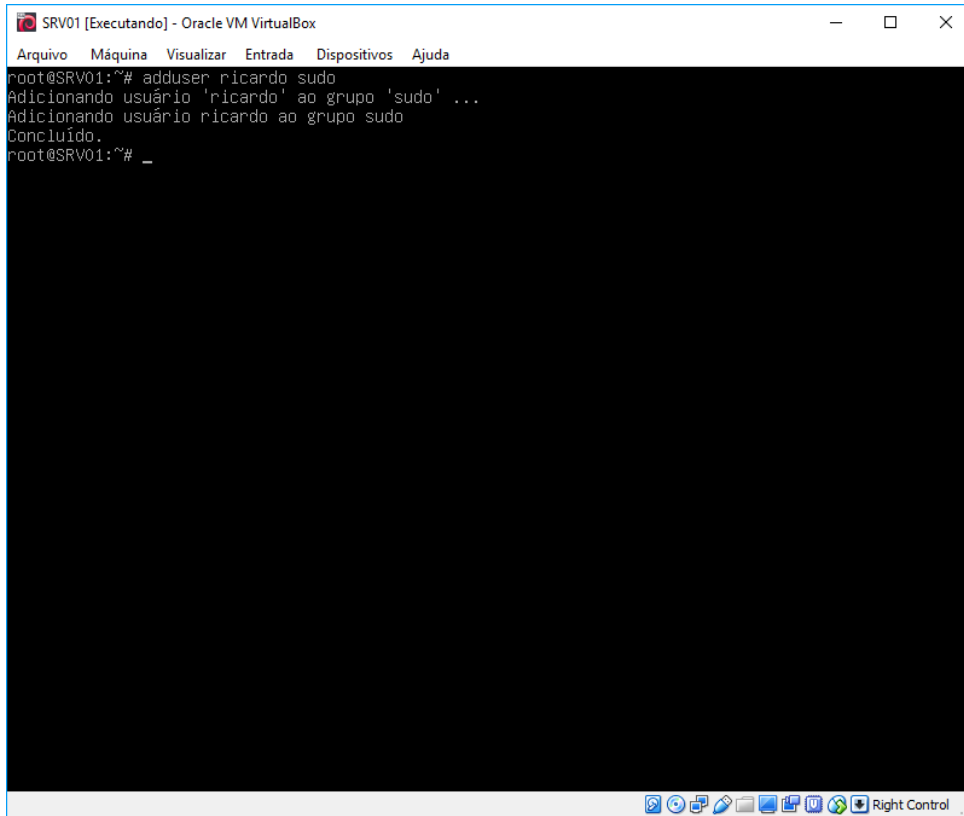
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@SRV01:~# apt-get install sudo
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Os NOVOS pacotes a seguir serão instalados:
  sudo
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso baixar 1.055 kB de arquivos.
Depois desta operação, 3.108 kB adicionais de espaço em disco serão usados.
Obter:1 http://ftp.br.debian.org/debian stretch/main amd64 sudo amd64 1.8.19p1-2.1 [1.055 kB]
Baixados 1.055 kB em 5s (196 kB/s)
A seleccionar pacote anteriormente não seleccionado sudo.
(Lendo banco de dados ... 52021 ficheiros e directórios actualmente instalados.)
A preparar para desempacotar ../sudo_1.8.19p1-2.1_amd64.deb ...
A descompactar sudo (1.8.19p1-2.1) ...
Configurando sudo (1.8.19p1-2.1) ...
A processar 'triggers' para systemd (232-25+deb9u3) ...
A processar 'triggers' para man-db (2.7.6.1-2) ...
root@SRV01:~#
```

Fonte: Autoria própria

Após instalação dos pacotes, o usuário ricardo foi adicionado ao grupo **sudo** executando o comando ***adduser ricardo sudo***.

Figura 39 - Adicionando o usuário ao grupo sudo



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
root@SRV01:~# adduser ricardo sudo
Adicionando usuário 'ricardo' ao grupo 'sudo' ...
Adicionando usuário ricardo ao grupo sudo
Concluído.
root@SRV01:~# _
```

Fonte: Autoria própria

As configurações de rede, foram feitas manualmente para comunicação entre os servidores editando o arquivo `/etc/network/interfaces`.

SRV01

```
auto enp0s3

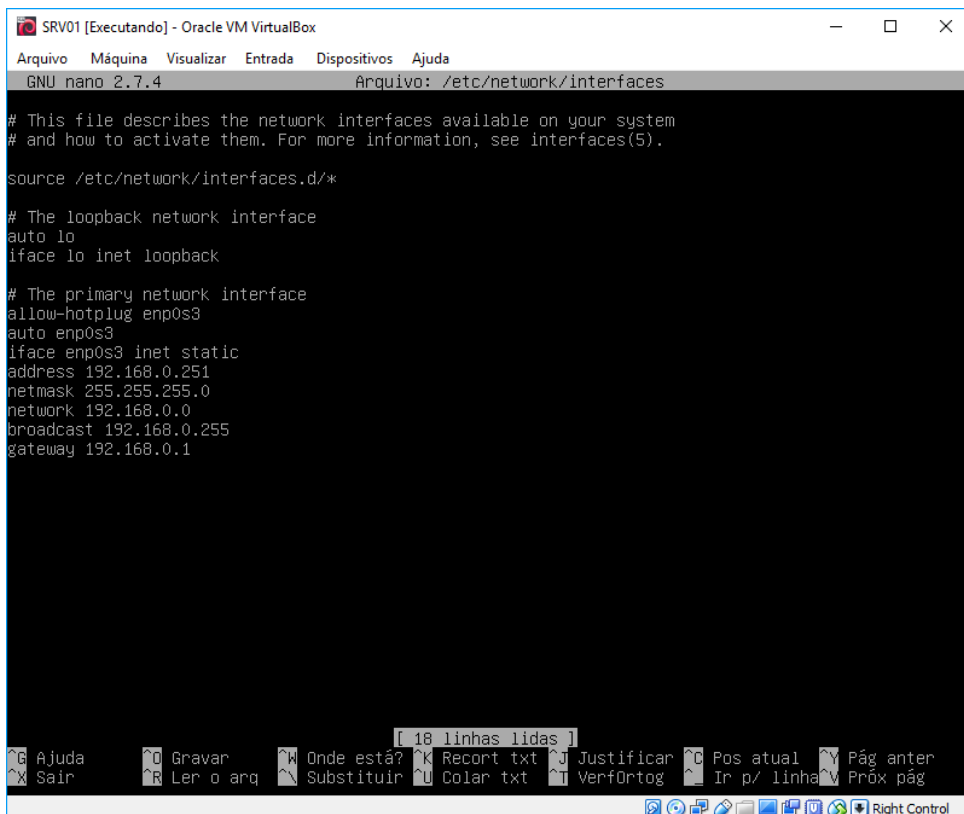
iface enp0s3 inet static
address 192.168.0.251
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.1
```

SRV02

```
auto enp0s3

iface enp0s3 inet static
address 192.168.0.252
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.1
```

Figura 40 - Configurações de rede



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
GNU nano 2.7.4      Arquivo: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
auto enp0s3
iface enp0s3 inet static
address 192.168.0.251
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.1

[ 18 linhas lidas ]
Ajuda  Gravar  Onde está?  Recort txt  Justificar  Pos atual  Pág anter
Sair  Ler o arq  Substituir  Colar txt  VerifOrtog  Ir p/ linha  Próx pag
Right Control
```

Fonte: Autoria própria

Foram configurados manualmente como servidores DNS, os servidores do Google editando o arquivo */etc/resolv.conf*.

```
nameserver 8.8.8.8
```

```
nameserver 8.8.4.4
```

Figura 41 - Configurações de servidores DNS



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
GNU nano 2.7.4                               Arquivo: /etc/resolv.conf

nameserver 8.8.8.8
nameserver 8.8.4.4

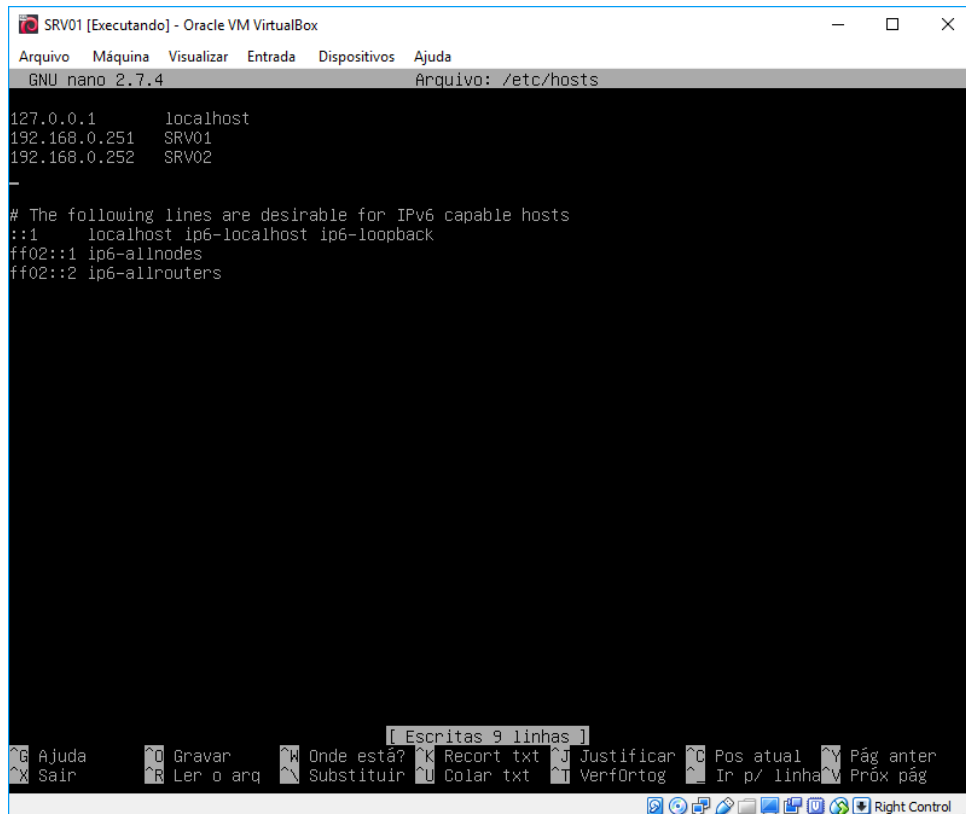
[ Escritas 3 linhas ]
Ajuda  Gravar  Onde está?  Recort txt  Justificar  Pos atual  Pág anter
Sair  Ler o arq  Substituir  Colar txt  Verf0rtog  Ir p/ linha  Próx pág
Right Control
```

Fonte: Autoria própria

Foi configurado o arquivo hosts editando o arquivo */etc/hosts*.

```
127.0.0.1          localhost
192.168.0.251     SRV01
192.168.0.252     SRV02
```

Figura 42 - Configurações do Hosts



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
GNU nano 2.7.4  Arquivo: /etc/hosts

127.0.0.1          localhost
192.168.0.251     SRV01
192.168.0.252     SRV02
-
# The following lines are desirable for IPv6 capable hosts
::1      localhost ip6-localhost ip6-loopback
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters

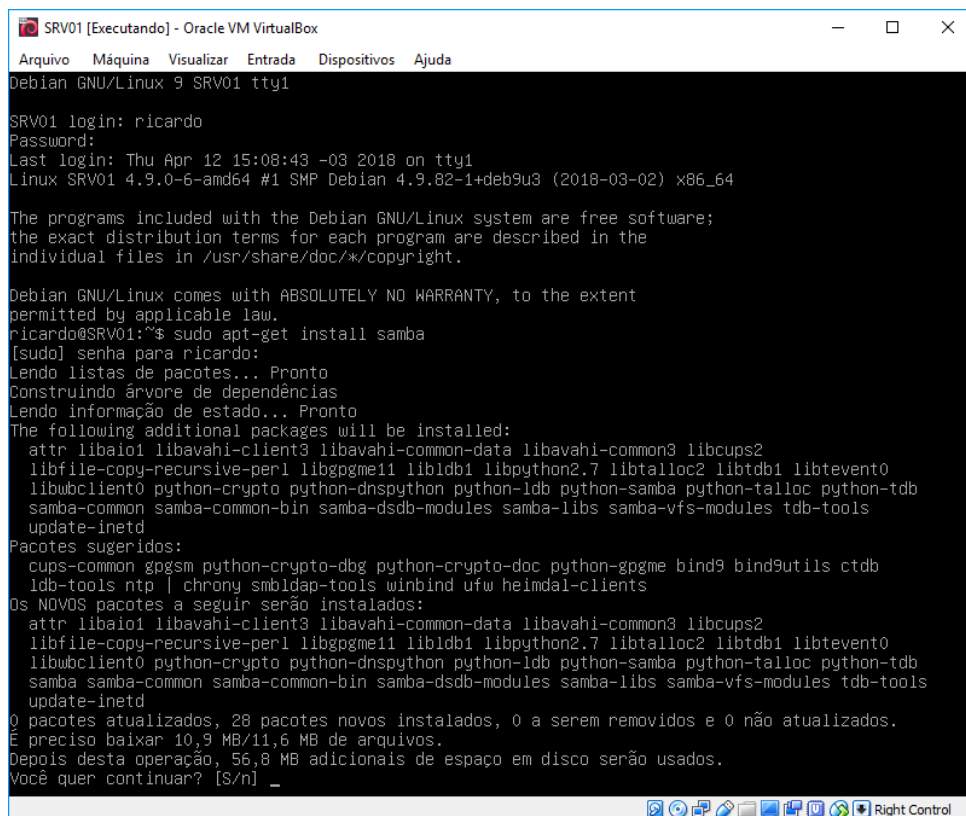
[ Escritas 9 linhas ]
Ajuda  Gravar  Onde está?  Record txt  Justificar  Pos atual  Pág anter
Sair   Ler o arq  Substituir  Colar txt   VerfOrtog  Ir p/ linha  Próx pág
Right Control
```

Fonte: Autoria própria

APÊNDICE C – INSTALANDO E CONFIGURANDO O SAMBA

Todas as configurações apresentadas no APÊNDICE C foram efetuadas simultaneamente e igualmente nos dois servidores. Uma vez que o usuário **ricardo** havia sido cadastrado e posteriormente adquirido permissões administrativas dentro do Linux, todas as demais configurações puderam ser através dele. Primeiramente foi instalado o **samba** através do comando **sudo apt-get install samba**.

Figura 43 - Instalação do Samba



```

SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
Debian GNU/Linux 9 SRV01 tty1

SRV01 login: ricardo
Password:
Last login: Thu Apr 12 15:08:43 -03 2018 on tty1
Linux SRV01 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
ricardo@SRV01:~$ sudo apt-get install samba
[sudo] senha para ricardo:
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
The following additional packages will be installed:
  attr libaio1 libavahi-client3 libavahi-common-data libavahi-common3 libcups2
  libfile-copy-recursive-perl libgpgme11 libldb1 libpython2.7 libtalloc2 libtdb1 libtevent0
  libwbclient0 python-crypto python-dnspython python-ldb python-samba python-talloc python-tdb
  samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
  update-inetd
Pacotes sugeridos:
  cups-common gpgsm python-crypto-dbg python-crypto-doc python-gpgme bind9 bind9utils ctdb
  ldb-tools ntp | chrony smbldap-tools winbind ufw heimdal-clients
Os NOVOS pacotes a seguir serão instalados:
  attr libaio1 libavahi-client3 libavahi-common-data libavahi-common3 libcups2
  libfile-copy-recursive-perl libgpgme11 libldb1 libpython2.7 libtalloc2 libtdb1 libtevent0
  libwbclient0 python-crypto python-dnspython python-ldb python-samba python-talloc python-tdb
  samba samba-common samba-common-bin samba-dsdb-modules samba-libs samba-vfs-modules tdb-tools
  update-inetd
0 pacotes atualizados, 28 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso baixar 10,9 MB/11,6 MB de arquivos.
Depois desta operação, 56,8 MB adicionais de espaço em disco serão usados.
Você quer continuar? [S/n] _

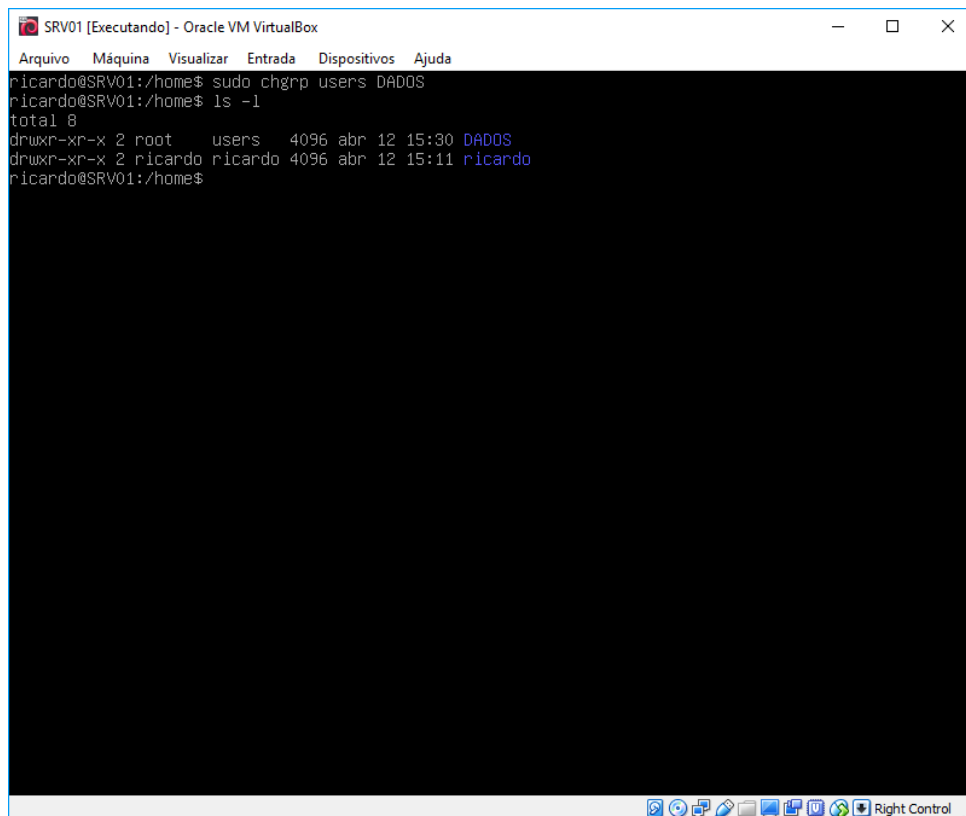
```

Fonte: Autoria própria

Foi criado o diretório **DADOS** em **/etc/home** para posteriormente ser compartilhado na rede. Utilizou-se então o comando **mkdir /home/DADOS**.

Em seguida foi alterado o grupo padrão do diretório **DADOS** criado anteriormente para que todos os usuários que pertencentes ao grupo **users** tenham acesso. Para isso foi executado o comando **sudo chgrp users /home/DADOS**.

Figura 44 - Alteração do grupo padrão do diretório DADOS

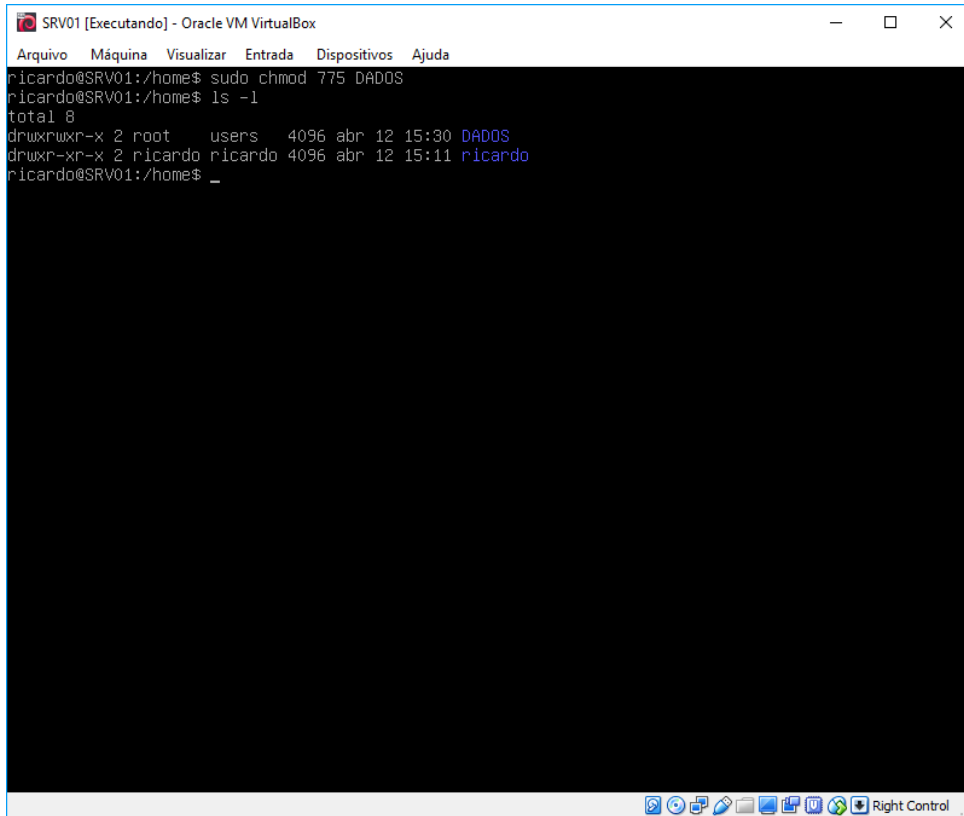


```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
ricardo@SRV01:/home$ sudo chgrp users DADOS
ricardo@SRV01:/home$ ls -l
total 8
drwxr-xr-x 2 root  users  4096 abr 12 15:30 DADOS
drwxr-xr-x 2 ricardo ricardo 4096 abr 12 15:11 ricardo
ricardo@SRV01:/home$
```

Fonte: Autoria própria

Após alterar o grupo padrão do diretório **DADOS** foi necessário alterar também as permissões do diretório para que todos os usuários pertencentes ao grupo **users** possam gravar arquivos. Executando o comando **sudo chmod 775 DADOS**.

Figura 45 - Alteração das permissões do diretório DADOS



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
ricardo@SRV01:/home$ sudo chmod 775 DADOS
ricardo@SRV01:/home$ ls -l
total 8
drwxrwxr-x 2 root  users  4096 abr 12 15:30 DADOS
drwxr-xr-x 2 ricardo ricardo 4096 abr 12 15:11 ricardo
ricardo@SRV01:/home$ _
```

Fonte: Autoria própria

Após as devidas permissões configuradas para o diretório **DADOS**, foi necessário editar o arquivo de configurações do samba para que então o diretório fosse compartilhado. Para isso foi editado o arquivo **smb.conf** no diretório **/etc/samba**.

[DADOS]

path = /home/DADOS

valid users = @users

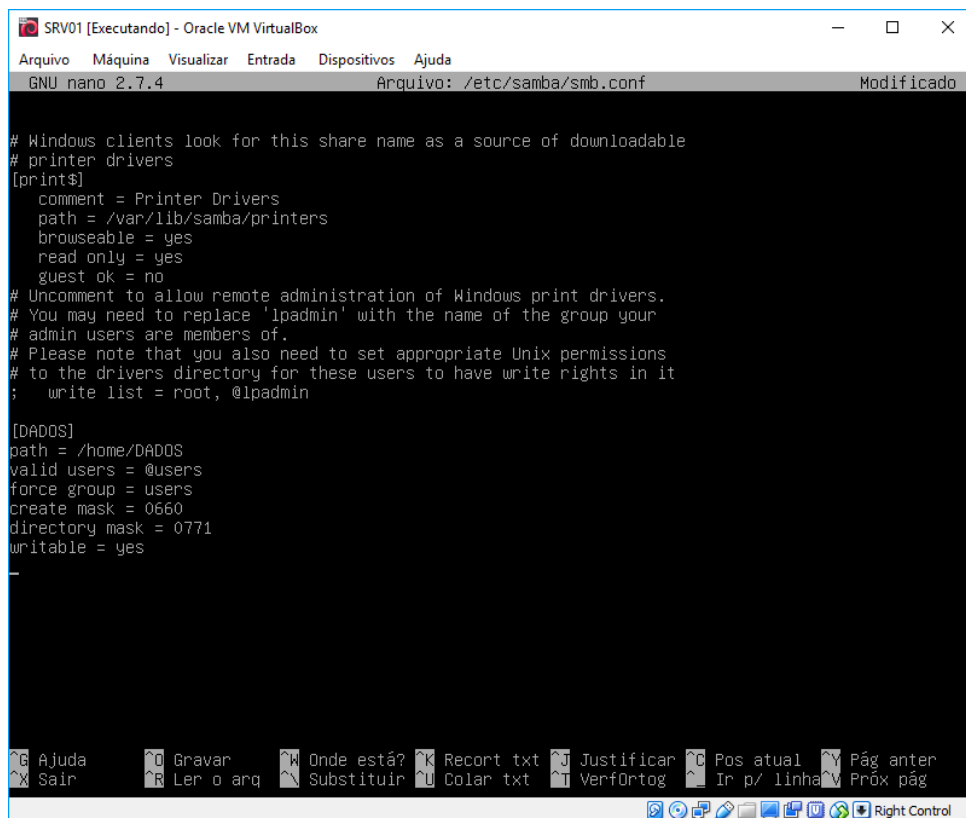
force group = users

create mask = 0660

directory mask = 0771

writable = yes

Figura 46 - Configuração do arquivo smb.conf



```

SRV01 [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
GNU nano 2.7.4 Arquivo: /etc/samba/smb.conf Modificado

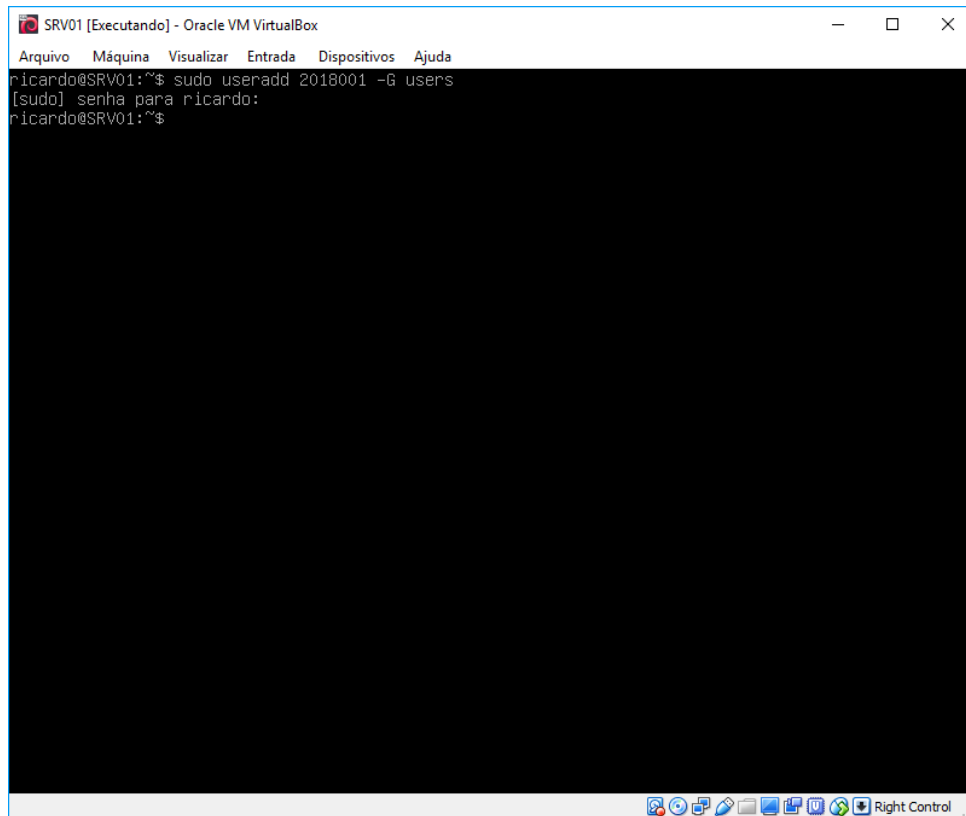
# Windows clients look for this share name as a source of downloadable
# printer drivers
[print$]
  comment = Printer Drivers
  path = /var/lib/samba/printers
  browseable = yes
  read only = yes
  guest ok = no
# Uncomment to allow remote administration of Windows print drivers.
# You may need to replace 'lpadmin' with the name of the group your
# admin users are members of.
# Please note that you also need to set appropriate Unix permissions
# to the drivers directory for these users to have write rights in it
; write list = root, @lpadmin

[DADOS]
path = /home/DADOS
valid users = @users
force group = users
create mask = 0660
directory mask = 0771
writable = yes
-
G Ajuda      O Gravar    W Onde está?  K Recort txt  J Justificar  C Pos atual  Y Pág anter
X Sair      R Ler o arq  Substituir  U Colar txt  T VerfOrtog  Ir p/ linha  V Próx pág
  
```

Fonte: Autoria própria

Uma vez configurado as permissões e efetuado o compartilhamento do diretório **DADOS**, foi necessário definir quais usuários teriam acesso ao compartilhamento. Para fins de testes foi criado um novo usuário com o login **2018001** e adicionado ao grupo **users**, que é o grupo padrão do diretório e que possui as permissões de acesso e gravação de arquivos. Executou-se o comando ***sudo adduser 2018001 -G users***.

Figura 47 - Comando para criação de novo usuário

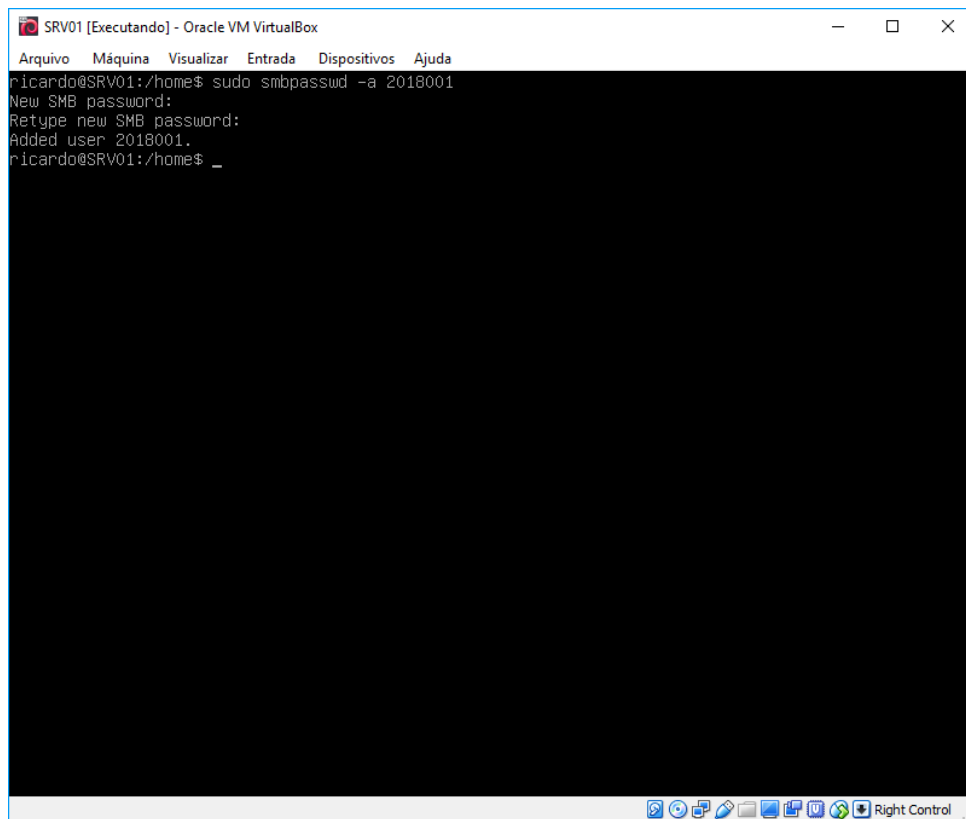


```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
ricardo@SRV01:~$ sudo useradd 2018001 -G users
[sudo] senha para ricardo:
ricardo@SRV01:~$
```

Fonte: Autoria própria

Porém, o samba difere as permissões entre usuários locais e remotos, por exemplo, mesmo que um determinado usuário tenha permissões para acessar e gravar arquivos no diretório **DADOS** localmente, ou seja, logados no servidor, não significa que através de outro computador da rede isso seja possível. Para isso foi necessário definir a um usuário já existente no grupo **users** uma nova senha para acesso ao compartilhamento através do comando ***sudo smbpasswd -a 2018001***.

Figura 48 - Criação de senha para usuários no Samba



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
ricardo@SRV01:/home$ sudo smbpasswd -a 2018001
New SMB password:
Retype new SMB password:
Added user 2018001.
ricardo@SRV01:/home$ _
```

Fonte: Autoria própria

Após todas as configurações efetuadas foi necessário a reinicialização do serviço do samba para que as alterações tivessem efeito. Para isso foi executado o comando ***sudo /etc/init.d/smbd restart***.

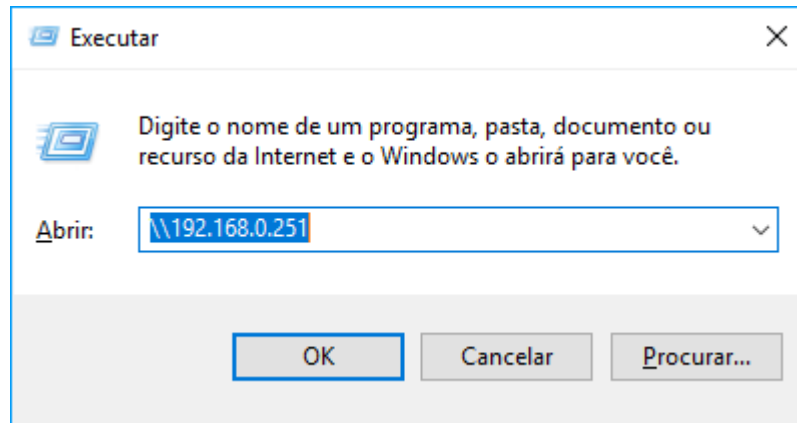
Figura 49 - Restartando o serviço do Samba

A screenshot of a terminal window titled "SRV01 [Executando] - Oracle VM VirtualBox". The window has a menu bar with "Arquivo", "Máquina", "Visualizar", "Entrada", "Dispositivos", and "Ajuda". The terminal content shows the user "ricardo@SRV01" at the "/home" directory. The command "sudo /etc/init.d/smbd restart" is entered, and the output is "[ok] Restarting smbd (via systemctl): smbd.service.". The prompt returns to "ricardo@SRV01:/home\$ _". The terminal window has a standard Linux desktop environment at the bottom with various icons and a "Right Control" button.

Fonte: Autoria própria

Para testar, foi utilizada uma máquina com sistema operacional Windows para acessar o compartilhamento. Foi digitado no **Executar (logotipo do Windows + R)**: \\192.168.0.251.

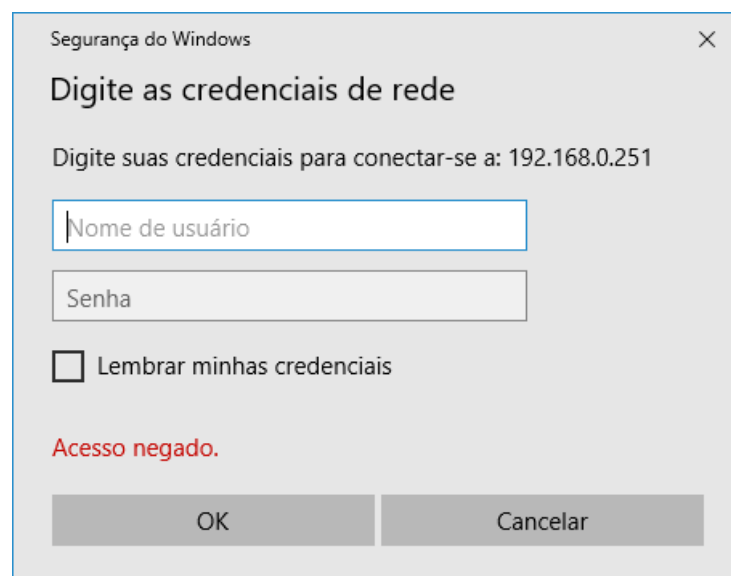
Figura 50 - Janela do Executar do Windows



Fonte: Autoria própria

Em seguida uma janela solicitando usuário e senha apareceu. Foi utilizado login e senha do usuário **2018001** cadastrado no samba anteriormente.

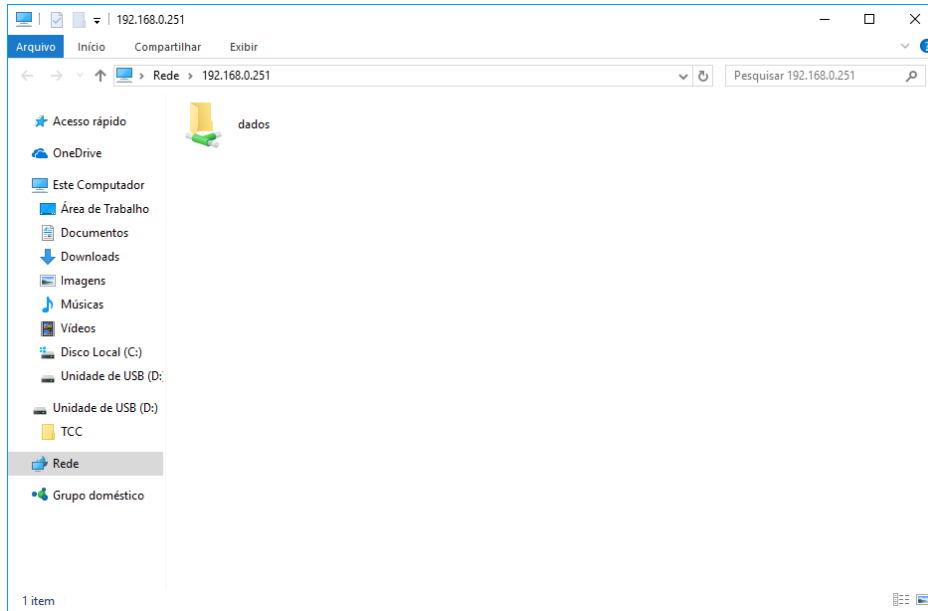
Figura 51 - Janela de autenticação para acesso a pasta compartilhada



Fonte: Autoria própria

Após fornecidos usuário e senha corretos, tornou-se disponível o diretório criado e compartilhado no Linux.

Figura 52 - Janela de pastas compartilhadas

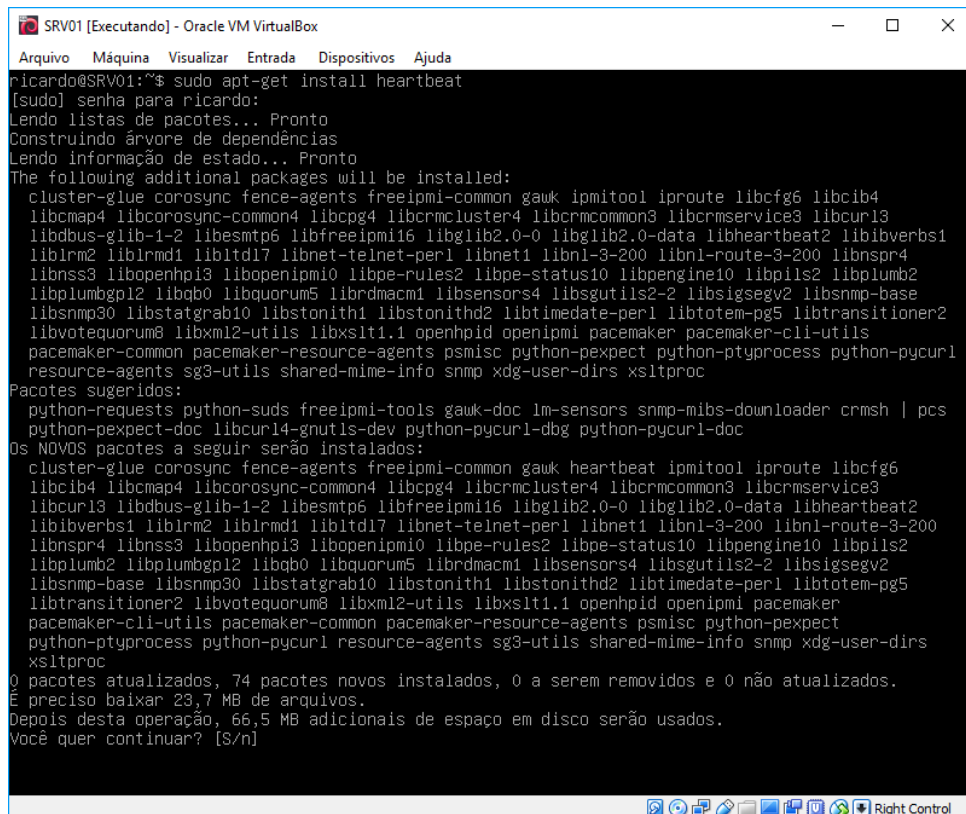


Fonte: Autoria própria

APÊNDICE D – INSTALANDO E CONFIGURANDO O HEARTBEAT

Todas as configurações apresentadas no APÊNDICE D foram efetuadas simultaneamente e igualmente nos dois servidores. Para instalação do **HEARTBEAT** executou-se o comando **sudo apt-get install heartbeat**.

Figura 53 - Instalação do Heartbeat



```

SRV01 [Executando] - Oracle VM VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda
ricardo@SRV01:~$ sudo apt-get install heartbeat
[sudo] senha para ricardo:
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
The following additional packages will be installed:
 cluster-glue corosync fence-agents freeipmi-common gawk ipmitool iproute libcfg6 libcid4
 libcm4 libcorosync-common4 libcp4 libcrmcluster4 libcrmcommon3 libcrmservice3 libcur13
 libdbus-glib-1-2 libesmt6 libfreeipmi16 libglib2.0-0 libglib2.0-data libheartbeat2 libibverbs1
 liblrm2 liblrm1 libltd17 libnet-telnet-perl libnet1 libnl-3-200 libnl-route-3-200 libnspr4
 libnss3 libopenhpi3 libopenipmi0 libpe-rules2 libpe-status10 libpengine10 libpils2 libplumb2
 libplumbgp12 libqb0 libquorum5 librdmac1 libsensors4 libsgutils2-2 libsigsegv2 libsnmp-base
 libsnmp30 libstatgrab10 libstonith1 libstonithd2 libtimedate-perl libtotem-pg5 libtransitioner2
 libvotequorum8 libxml2-utils libxslt1.1 openhpid openipmi pacemaker pacemaker-cli-utils
 pacemaker-common pacemaker-resource-agents psmisc python-pexpect python-ptyprocess python-pycurl
 resource-agents sg3-utils shared-mime-info snmp xdg-user-dirs xsltproc
Pacotes sugeridos:
 python-requests python-suds freeipmi-tools gawk-doc lm-sensors snmp-mibs-downloader crmsh | pcs
 python-pexpect-doc libcurl4-gnutls-dev python-pycurl-dbg python-pycurl-doc
Os NOVOS pacotes a seguir serão instalados:
 cluster-glue corosync fence-agents freeipmi-common gawk heartbeat ipmitool iproute libcfg6
 libcid4 libcm4 libcorosync-common4 libcp4 libcrmcluster4 libcrmcommon3 libcrmservice3
 libcur13 libdbus-glib-1-2 libesmt6 libfreeipmi16 libglib2.0-0 libglib2.0-data libheartbeat2
 libibverbs1 liblrm2 liblrm1 libltd17 libnet-telnet-perl libnet1 libnl-3-200 libnl-route-3-200
 libnspr4 libnss3 libopenhpi3 libopenipmi0 libpe-rules2 libpe-status10 libpengine10 libpils2
 libplumb2 libplumbgp12 libqb0 libquorum5 librdmac1 libsensors4 libsgutils2-2 libsigsegv2
 libsnmp-base libsnmp30 libstatgrab10 libstonith1 libstonithd2 libtimedate-perl libtotem-pg5
 libtransitioner2 libvotequorum8 libxml2-utils libxslt1.1 openhpid openipmi pacemaker
 pacemaker-cli-utils pacemaker-common pacemaker-resource-agents psmisc python-pexpect
 python-ptyprocess python-pycurl resource-agents sg3-utils shared-mime-info snmp xdg-user-dirs
 xsltproc
0 pacotes atualizados, 74 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso baixar 23,7 MB de arquivos.
Depois desta operação, 66,5 MB adicionais de espaço em disco serão usados.
Você quer continuar? [S/n]

```

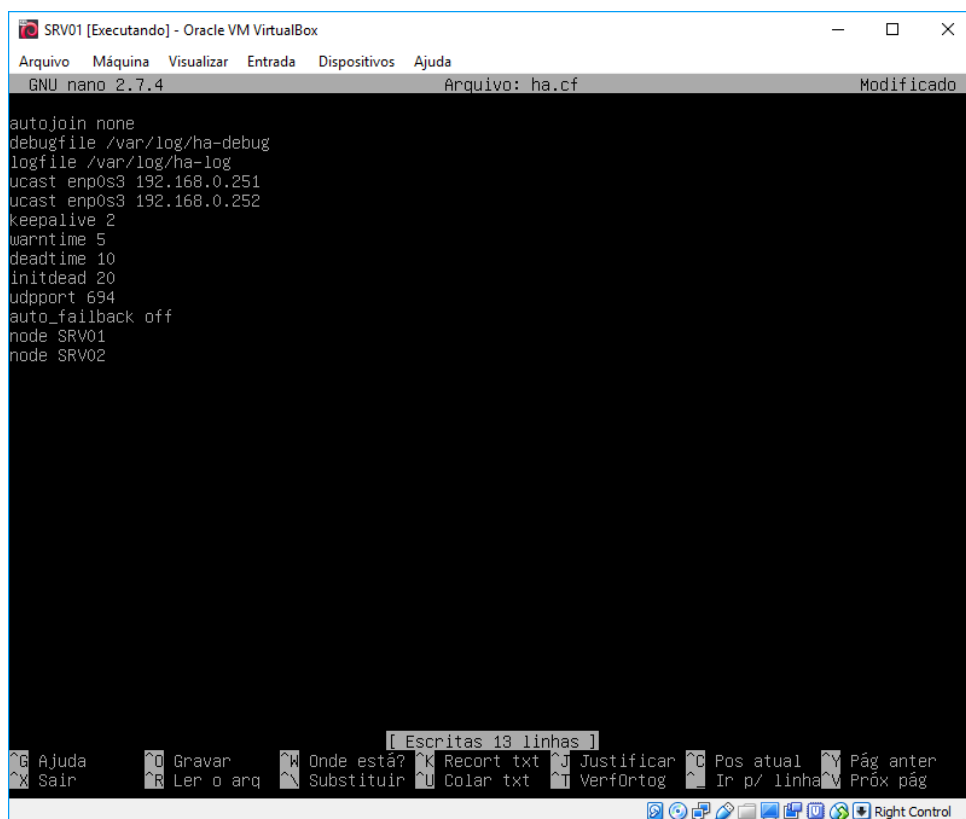
Fonte: Autoria própria

Usando o comando **cd /etc/ha.d** para acessar o diretório do **HEARTBEAT**, antes de iniciar a configuração foram necessário a criação de três arquivos importantes. São eles **ha.cf**, **authkeys** e **haresources**. Para isso foi utilizado o comando **sudo touch ha.cf authkeys haresources**.

O **ha.cf**, é um dos arquivos mais importantes, ele é responsável por armazenar as informações referentes ao cluster, por exemplo, quais são servidores e quais os recursos estarão ativos. Então, foi editado com as seguintes configurações.

```
autojoin none
debugfile /var/log/ha-debug
logfile /var/log/ha-log
ucast enp0s3 192.168.0.251
ucast enp0s3 192.168.0.252
keepalive 2
warntime 5
deadtime 10
initdead 30
udpport 694
auto_failback off
node SRV01
node SRV02
```

Figura 54 - Configuração do arquivo ha.cf



The image shows a screenshot of a terminal window titled "SRV01 [Executando] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.7.4 editor, editing the file "ha.cf". The content of the file is as follows:

```
autojoin none
debugfile /var/log/ha-debug
logfile /var/log/ha-log
ucast enp0s3 192.168.0.251
ucast enp0s3 192.168.0.252
keepalive 2
warntime 5
deadtime 10
initdead 20
udpport 694
auto_failback off
node SRV01
node SRV02
```

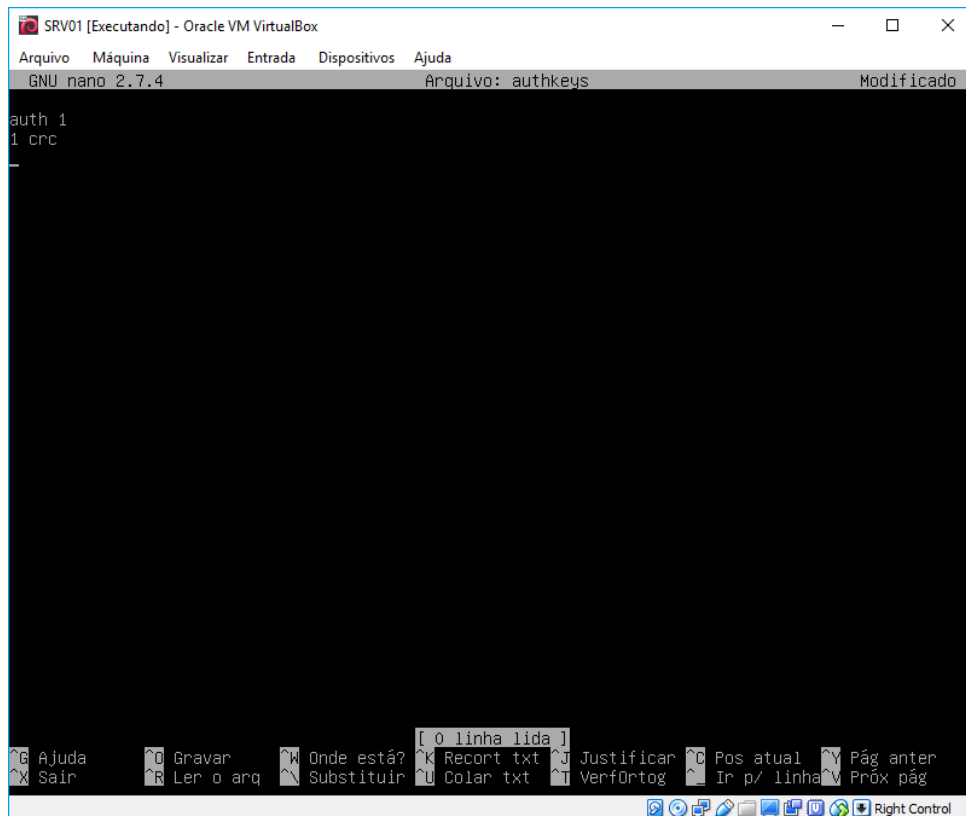
The terminal window also shows a status bar at the bottom with the text "[Escritas 13 linhas]" and various keyboard shortcuts for editing and navigation.

Fonte: Autoria própria

No arquivo **authkeys**, são definidos a forma de autenticação entre os membros do cluster, normalmente possui apenas duas linhas, uma diz qual chave a ser usada na assinatura de pacotes de saída e a outra definindo quais pacotes de entrada podem ser assinados. Este foi editado com as seguintes configurações.

```
auth 1  
1 crc
```

Figura 55 - Configuração do arquivo authkeys



The image shows a screenshot of a terminal window titled "SRV01 [Executando] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.7.4 editor, editing the file "authkeys". The content of the file is:

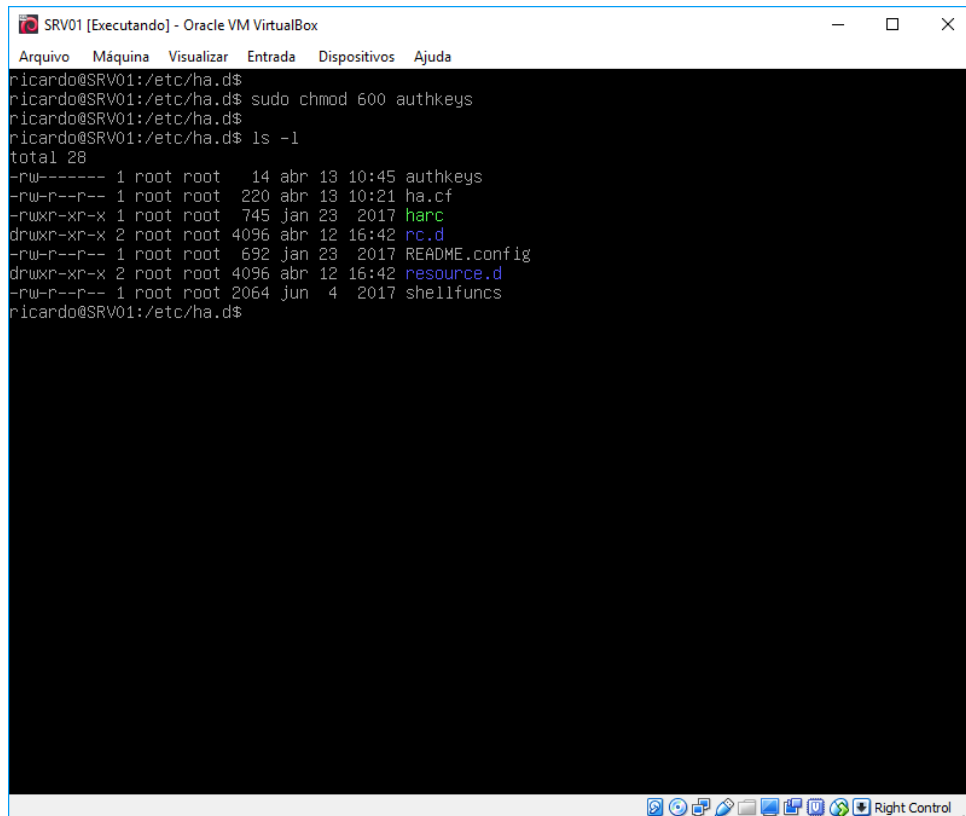
```
auth 1  
1 crc
```

The terminal window includes a menu bar with options: Arquivo, Máquina, Visualizar, Entrada, Dispositivos, Ajuda. At the bottom, there is a status bar with various keyboard shortcuts and a "Right Control" button.

Fonte: Autoria própria

Contudo, de acordo com o site oficial, por questões de segurança, somente o criador root do sistema pode ler e gravar no arquivo. Para garantir isso, foi necessário alterar as permissões do arquivo, executando o comando ***sudo chmod 600 authkey***.

Figura 56 - alterando permissões do arquivo authkeys



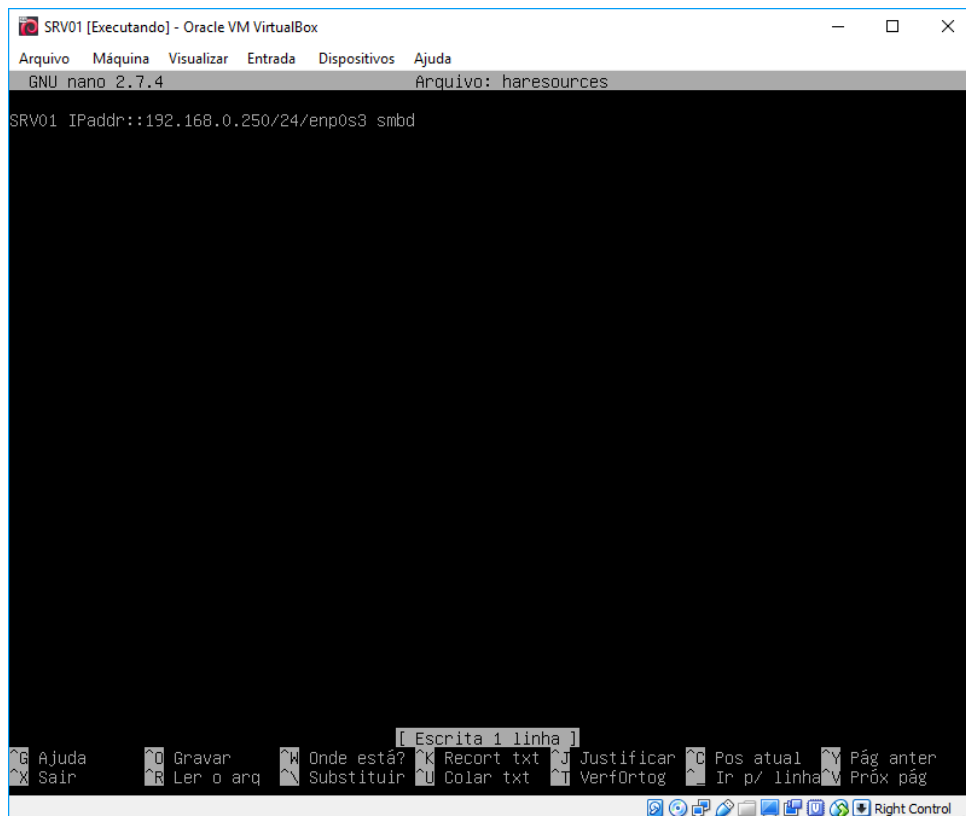
```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
ricardo@SRV01:/etc/ha.d$
ricardo@SRV01:/etc/ha.d$ sudo chmod 600 authkeys
ricardo@SRV01:/etc/ha.d$
ricardo@SRV01:/etc/ha.d$ ls -l
total 28
-rw----- 1 root root  14 abr 13 10:45 authkeys
-rw-r--r-- 1 root root 220 abr 13 10:21 ha.cf
-rwxr-xr-x 1 root root 745 jan 23  2017 harc
drwxr-xr-x 2 root root 4096 abr 12 16:42 rc.d
-rw-r--r-- 1 root root  692 jan 23  2017 README.config
drwxr-xr-x 2 root root 4096 abr 12 16:42 resource.d
-rw-r--r-- 1 root root 2064 jun  4  2017 shellfuncs
ricardo@SRV01:/etc/ha.d$
```

Fonte: Autoria própria

E o terceiro arquivo, **haresources**, armazena informações de quem é o servidor primário, qual endereço IP virtual será atribuído ao cluster, em qual interface de rede se dará a comunicação entre os servidores envolvidos, e qual será o serviço monitorado pelo **HEARTBEAT**. E foi editado com as seguintes configurações.

```
SRV01 IPaddr::192.168.0.250/24/enp0s3 smbd
```

Figura 57 - Configurações do arquivo haresources

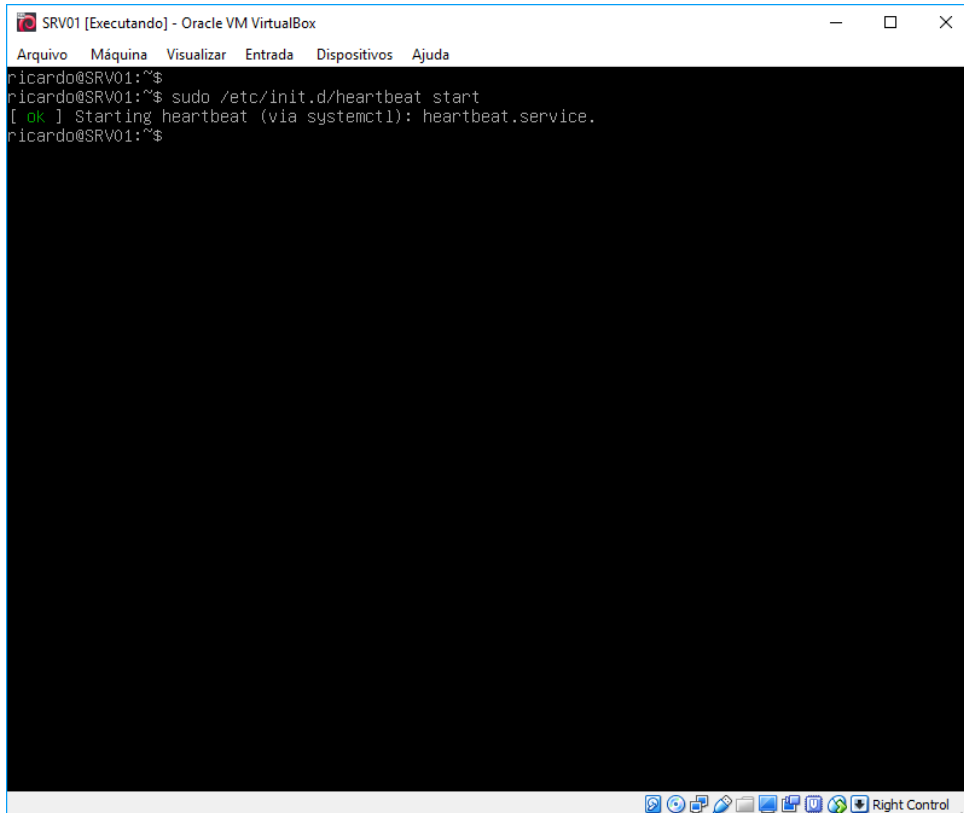


```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
GNU nano 2.7.4      Arquivo: haresources
SRV01 IPaddr::192.168.0.250/24/enp0s3 smbd
Escrita 1 linha 1
^G Ajuda      ^O Gravar      ^W Onde está?  ^K Recort txt  ^J Justificar  ^C Pos atual  ^Y Pág anter
^X Sair      ^R Ler o arq  ^N Substituir  ^U Colar txt  ^I VerfOrtog  ^_ Ir p/ linha  ^V Próx pag
Right Control
```

Fonte: Autoria própria

Após todas as configurações efetuadas, o serviço do **HEARTBEAT** foi inicializado através do comando ***sudo /etc/init.d/heartbeat start***.

Figura 58 - Startando o serviço do Heartbeat



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
ricardo@SRV01:~$
ricardo@SRV01:~$ sudo /etc/init.d/heartbeat start
[ ok ] Starting heartbeat (via systemctl): heartbeat.service.
ricardo@SRV01:~$
```

Fonte: Autoria própria

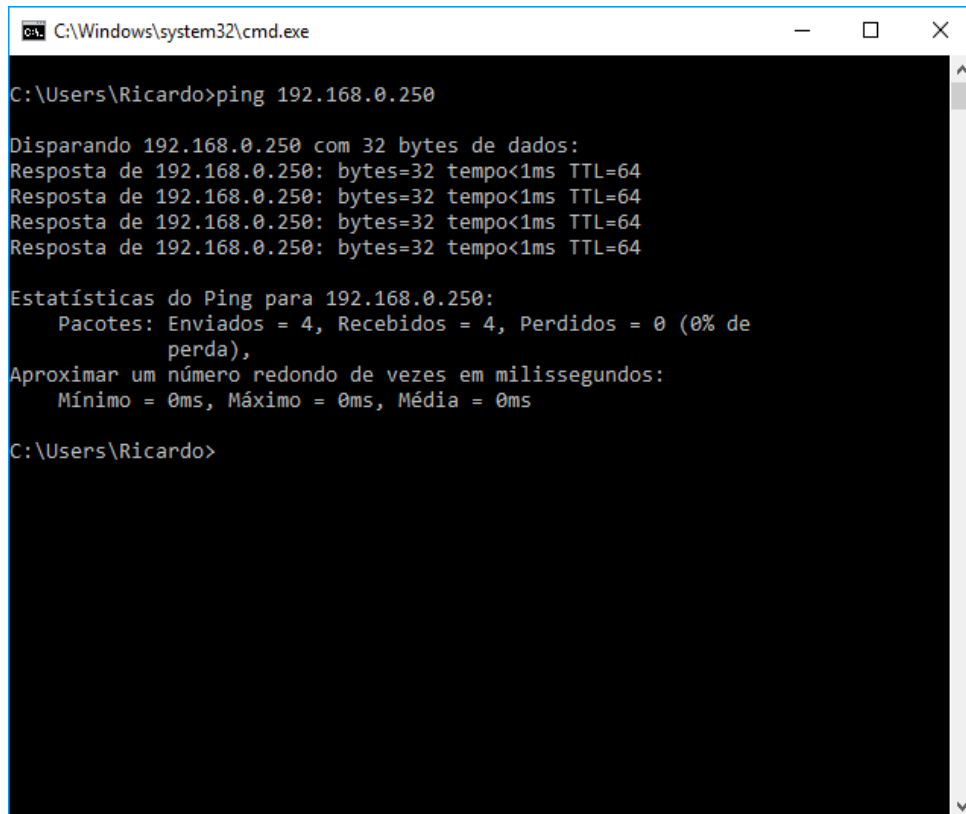
Uma vez que o serviço do samba seria monitorado pelo HEARTBEAT foi necessário desabilitá-lo da inicialização do Linux. Dessa forma, após efetuado acesso ao diretório ***/etc/init.d*** foi executado o comando ***sudo update-rc.d smbdisable***.

E para fazer com que o serviço do HEARTBEAT fosse inicializado com o Linux, ainda no mesmo diretório foi executado o comando ***sudo update-rc.d heartbeat enable***.

Feito isso, o serviço do HEARTBEAT precisou ser reiniciado. Para isso foi utilizado o comando ***sudo service heartbeat restart***.

Depois efetuado todas as configurações apresentadas, tornou-se possível efetuar os testes através do IP virtual utilizado pelo cluster. No primeiro teste foi executado o comando **ping 192.168.0.250**.

Figura 59 - Ping no IP Virtual do Cluster

A screenshot of a Windows command prompt window titled "C:\Windows\system32\cmd.exe". The window shows the execution of the command "ping 192.168.0.250". The output displays four successful responses, each with a response time of less than 1ms and a TTL of 64. Below the responses, it shows ping statistics: 4 packets sent, 4 received, and 0 lost (0% loss). The average response time is 0ms, with a minimum of 0ms and a maximum of 0ms. The prompt returns to "C:\Users\Ricardo>".

```
C:\Windows\system32\cmd.exe
C:\Users\Ricardo>ping 192.168.0.250

Disparando 192.168.0.250 com 32 bytes de dados:
Resposta de 192.168.0.250: bytes=32 tempo<1ms TTL=64
Resposta de 192.168.0.250: bytes=32 tempo<1ms TTL=64
Resposta de 192.168.0.250: bytes=32 tempo<1ms TTL=64
Resposta de 192.168.0.250: bytes=32 tempo<1ms TTL=64

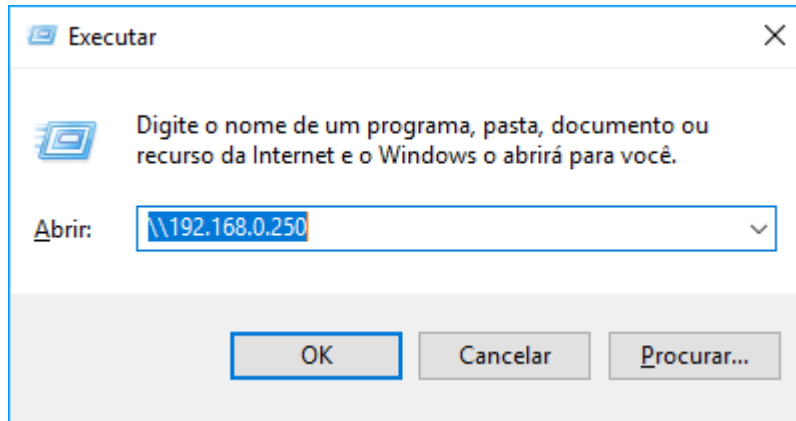
Estatísticas do Ping para 192.168.0.250:
    Pacotes: Enviados = 4, Recebidos = 4, Perdidos = 0 (0% de
    perda),
Aproximar um número redondo de vezes em milissegundos:
    Mínimo = 0ms, Máximo = 0ms, Média = 0ms

C:\Users\Ricardo>
```

Fonte: Autoria própria

Em seguida, através do serviço **Executar** do Windows. Foi efetuada tentativa de acesso ao diretório compartilhado do Linux, porém, através do endereço IP virtual atribuído ao cluster **\\192.168.0.250**.

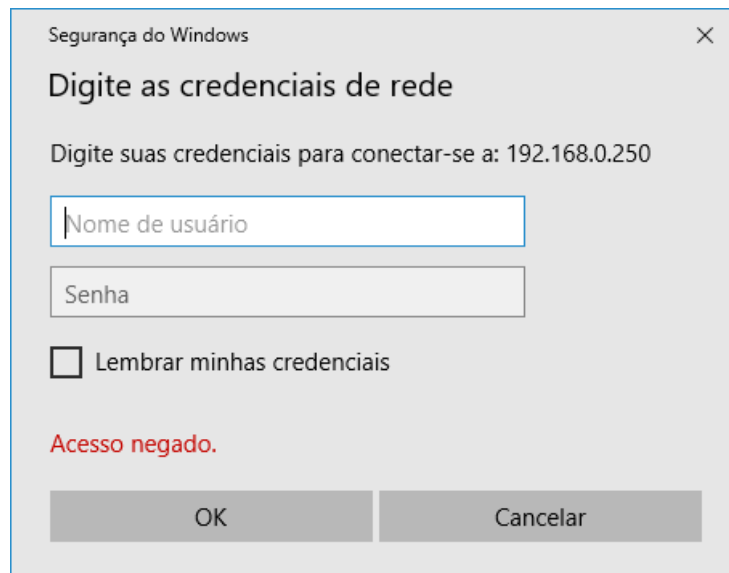
Figura 60 - Janela do Executar do Windows



Fonte: Autoria própria

A janela solicitando as credenciais surgiu, onde foram informados login e senha do usuário **2018001** cadastrado no samba.

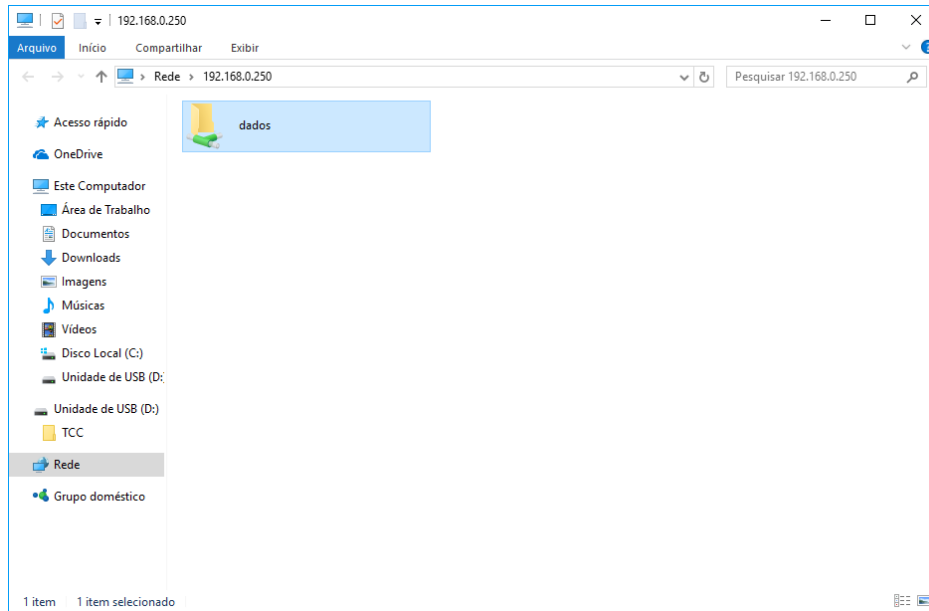
Figura 61 - Janela de autenticação para acesso a pasta compartilhada



Fonte: Autoria própria

E seguida foi possível acessar o diretório compartilhado no Linux.

Figura 62 - Janela de pastas compartilhadas



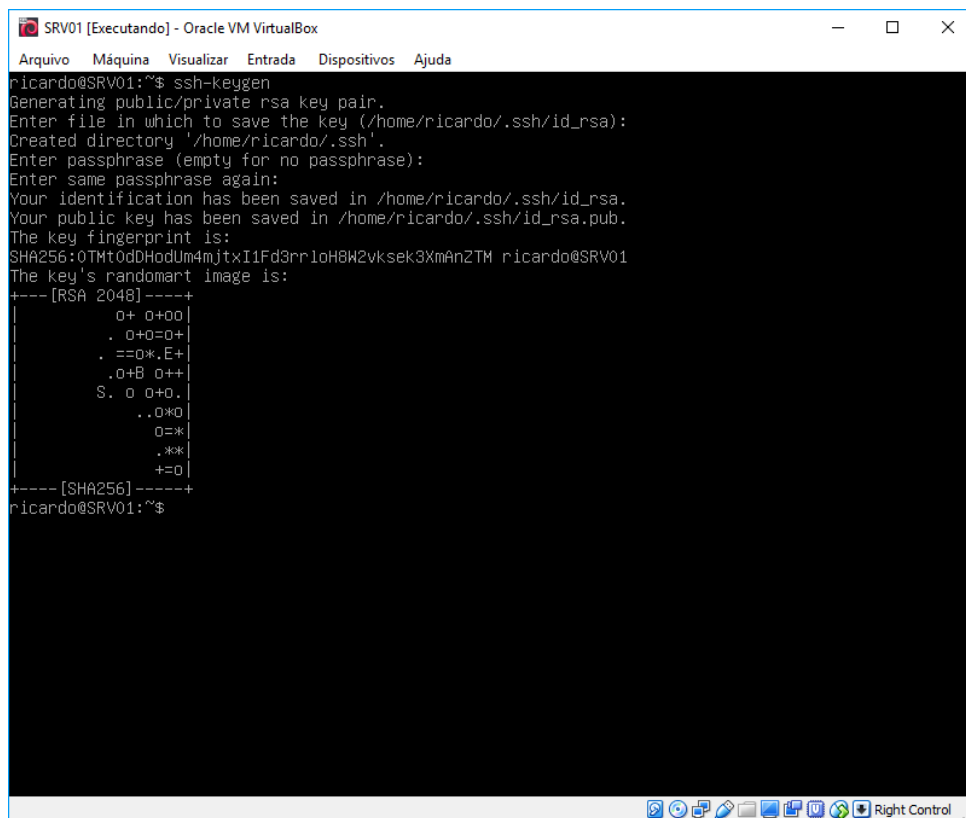
Fonte: Autoria própria

APÊNDICE E – CRIANDO RELACIONAMENTO DE CONFIANÇA VIA SSH

Todas as configurações apresentadas no APÊNDICE E foram efetuadas igualmente nos dois servidores. Para que fosse possível a sincronização automática de arquivos usando o RSYNC e sem a exigência de autenticação, era importante que houvesse um relacionamento seguro de confiança entre os dois servidores, ou seja, os acessos ao diretório DADOS existentes nos dois servidores seriam feitos através de conexão criptografada SSH a qualquer momento e sem a necessidade da inserção de senha.

Em ambos servidores, foi executado o comando **ssh-keygen**. Esse comando consiste na criação da chave pública de criptografia para as conexões via SSH.

Figura 63 - Criação da chave pública



```

SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
ricardo@SRV01:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ricardo/.ssh/id_rsa):
Created directory '/home/ricardo/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ricardo/.ssh/id_rsa.
Your public key has been saved in /home/ricardo/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:0TMT0d0HodUm4mjtXII1Fd3rr1oH8W2vksek3XmAn2TM ricardo@SRV01
The key's randomart image is:
+----[RSA 2048]-----+
|          o+  o+o+ |
|         . o+o=0+ |
|        . ==o*.E+ |
|       .o+B  o++ |
|      S. o  o+o. |
|         ..O*O |
|          o=* |
|         .** |
|          +=0 |
+----[SHA256]-----+
ricardo@SRV01:~$

```

Fonte: A autoria própria

A chave foi gerada em cada servidor com o nome **id_rsa.pub** no diretório **.ssh**, um diretório oculto dentro da pasta do usuário **ricardo**, para acessá-la usou-se o comando **cd /home/ricardo/.ssh/**.

Com as chaves gerada em cada um dos servidores, foi necessário para copia-la do servidor primário para o servidor secundário e do secundário para o primário. Usando-se o seguinte comando.

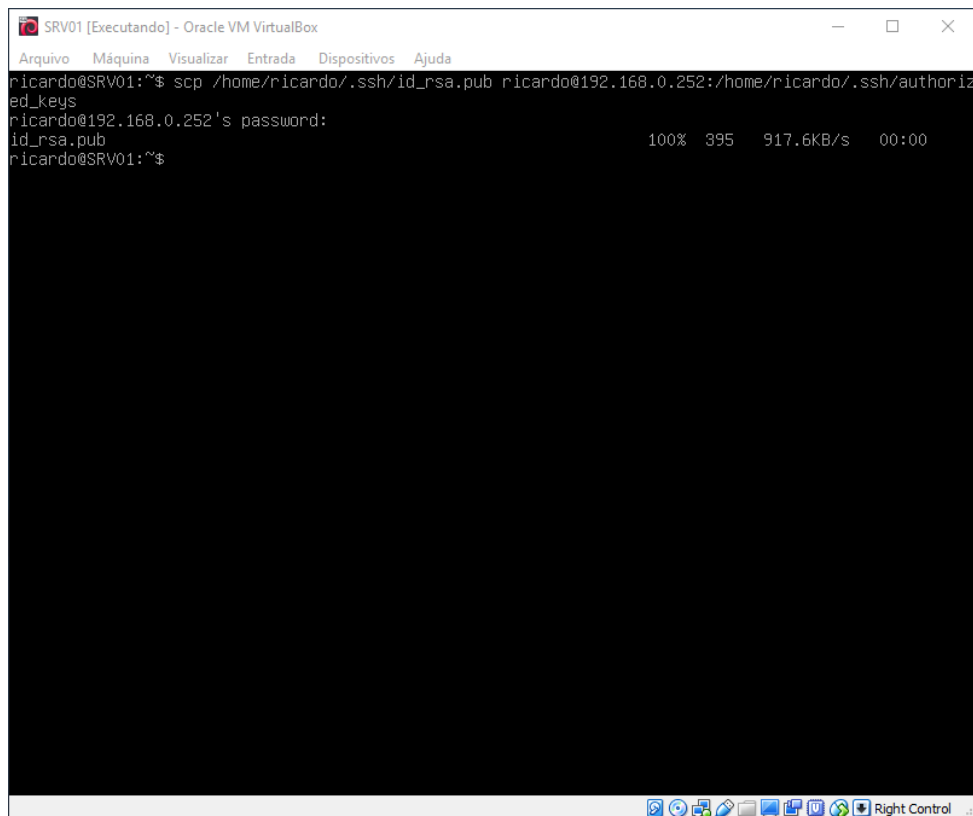
Do SRV01 para o SRV02

```
scp /home/ricardo/.ssh/id_rsa.pub  
ricardo@192.168.0.252:/home/ricardo/.ssh/authorized_keys
```

Do SRV02 para o SRV01

```
scp /home/ricardo/.ssh/id_rsa.pub  
ricardo@192.168.0.251:/home/ricardo/.ssh/authorized_keys
```

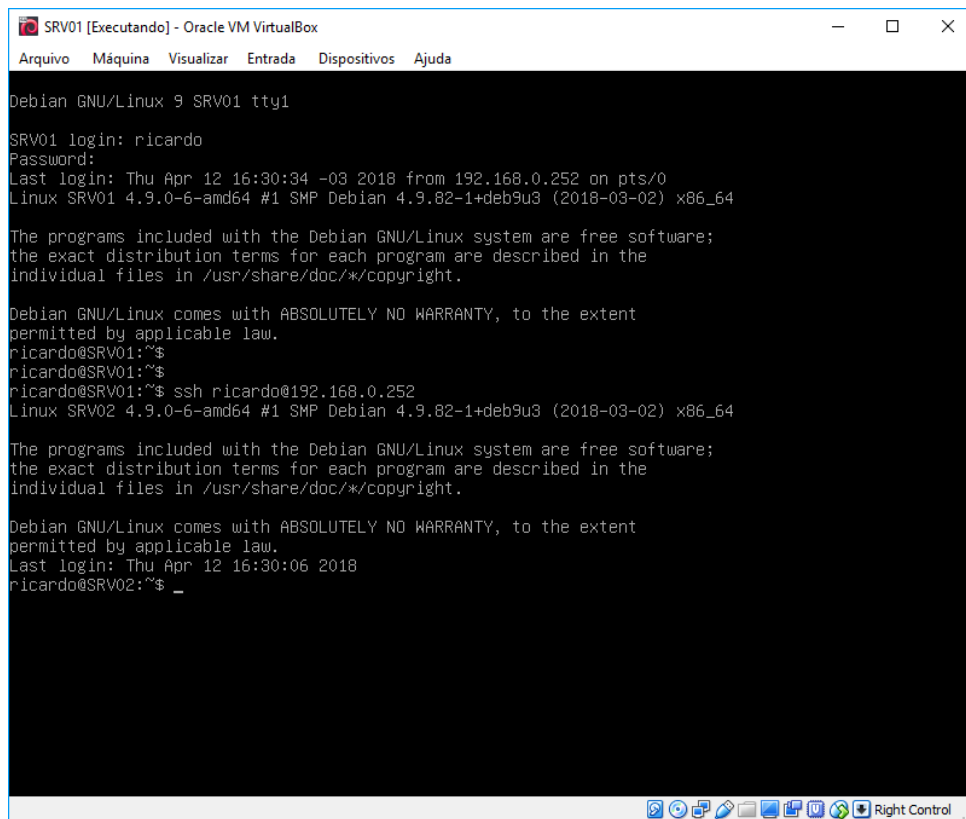
Figura 64 - Copiando a chave para o SRV02



Fonte: Autoria própria

Após a troca de chaves, as conexões efetuadas entre os dois servidores através de SSH não exigiram mais a autenticação. Efetuado os testes após a reinicialização dos dois servidores e os mesmos mostrou que o relacionamento de confiança entre os dois servidores estava estabelecido.

Figura 65 - Conexão via SSH sem autenticação



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda

Debian GNU/Linux 9 SRV01 tty1
SRV01 login: ricardo
Password:
Last login: Thu Apr 12 16:30:34 -03 2018 from 192.168.0.252 on pts/0
Linux SRV01 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
ricardo@SRV01:~$
ricardo@SRV01:~$ ssh ricardo@192.168.0.252
Linux SRV02 4.9.0-6-amd64 #1 SMP Debian 4.9.82-1+deb9u3 (2018-03-02) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

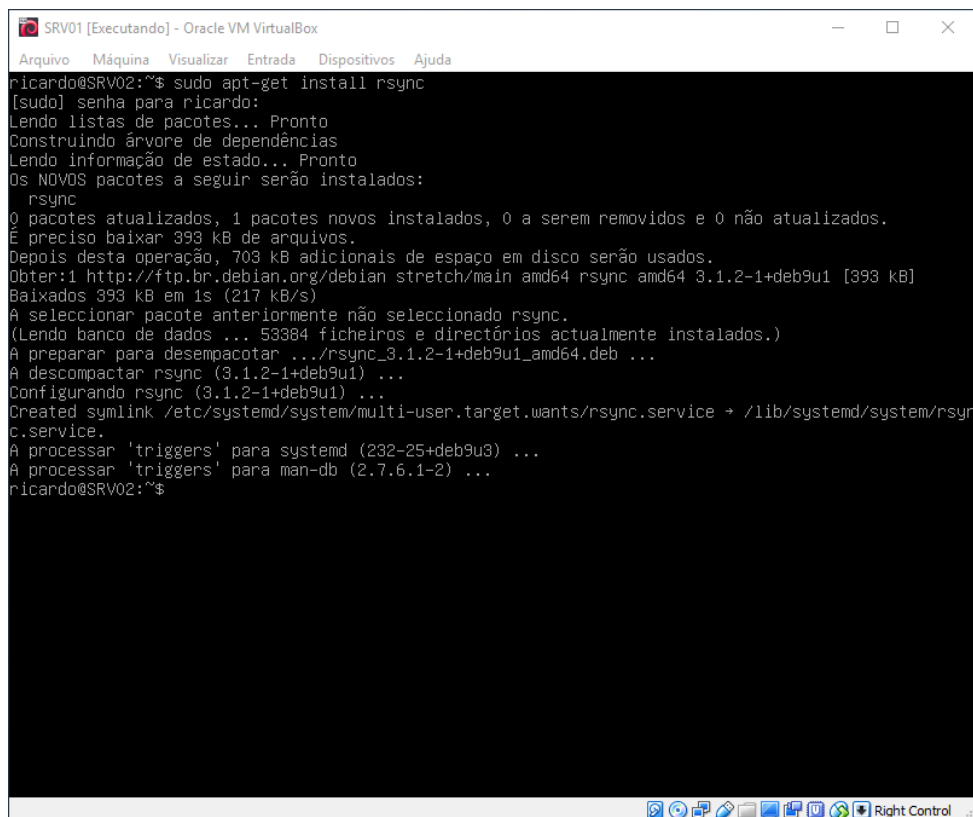
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 12 16:30:06 2018
ricardo@SRV02:~$ _
```

Fonte: Autoria própria

APÊNDICE F – INSTALANDO O RSYNC

Durante os processos de desenvolvimento deste trabalho não se mostrou necessário a instalação do RSYNC nos dois servidores, uma vez que o mesmo possui capacidade de efetuar cópias tanto enviando, quanto recebendo arquivos através da rede. Para a sua instalação utilizou-se o comando ***sudo apt-get install rsync***.

Figura 66 - Instalação do Rsync



```

SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
ricardo@SRV02:~$ sudo apt-get install rsync
[sudo] senha para ricardo:
Lendo listas de pacotes... Pronto
Construindo árvore de dependências
Lendo informação de estado... Pronto
Os NOVOS pacotes a seguir serão instalados:
 rsync
0 pacotes atualizados, 1 pacotes novos instalados, 0 a serem removidos e 0 não atualizados.
É preciso baixar 393 kB de arquivos.
Depois desta operação, 703 kB adicionais de espaço em disco serão usados.
Obter:1 http://ftp.br.debian.org/debian stretch/main amd64 rsync amd64 3.1.2-1+deb9u1 [393 kB]
Baixados 393 kB em 1s (217 kB/s)
A seleccionar pacote anteriormente não seleccionado rsync.
(Lendo banco de dados ... 53384 ficheiros e directórios actualmente instalados.)
A preparar para desempacotar .../rsync_3.1.2-1+deb9u1_amd64.deb ...
A descompactar rsync (3.1.2-1+deb9u1) ...
Configurando rsync (3.1.2-1+deb9u1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/rsync.service → /lib/systemd/system/rsync.service.
A processar 'triggers' para systemd (232-25+deb9u3) ...
A processar 'triggers' para man-db (2.7.6.1-2) ...
ricardo@SRV02:~$
  
```

Fonte: Autoria própria

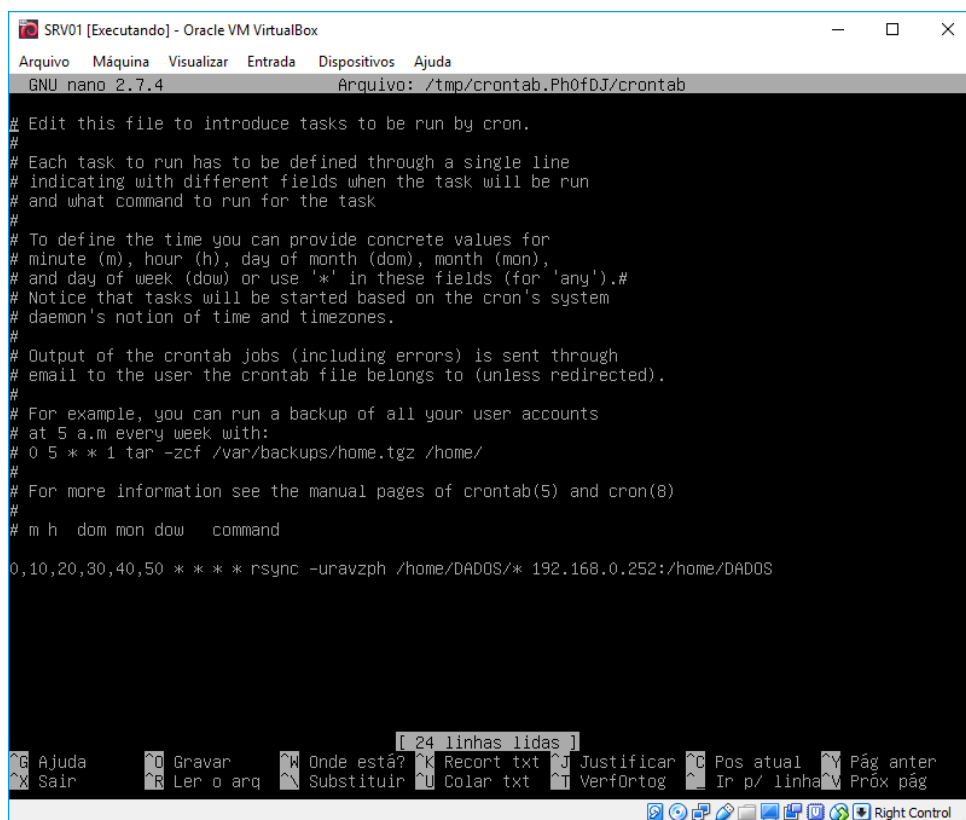
Após a instalação do RSYNC não houve necessidade de configurações. Bastando apenas adicionar o usuário **ricardo** no grupo **users**, através do comando ***adduser ricardo users*** nos dois servidores e depois executar o comando de cópia informando os parâmetros desejados, origem e destino. Sendo assim, para fins de testes foi efetuado a sincronia de arquivos do diretório DADOS em SRV01 para o diretório DADOS em SRV02. Lembrando que estes estão compartilhados para acesso na rede nos dois servidores. Através do comando ***rsync -aghoprtuvzOP --del --timeout=5 /home/DADOS/ 192.168.0.252:/home/DADOS***

APÊNDICE G – CONFIGURANDO O CRONTAB

Usado para agendar tarefas no Linux, o CRONTAB pode ser configurado para agendar a sincronia de informações entre os servidores do cluster, executando no tempo programado o comando juntamente com os parâmetros necessário do RSYNC. Para editar o arquivo de configuração do CRONTAB foi executado o comando **crontab -e**, e em seguida selecionado a opção 1 para abrir com o editor de texto nano do Linux. Foi então acrescentado as seguintes configurações necessárias para efetuar a sincronização a cada 20 minutos.

```
0,10,20,30,40,50 * * * * rsync -aghoprtuvzOP --del --timeout=5 /home/DADOS/
192.168.0.252:/home/DADOS
```

Figura 67 - Configurações do Crontab



```
SRV01 [Executando] - Oracle VM VirtualBox
Arquivo  Máquina  Visualizar  Entrada  Dispositivos  Ajuda
GNU nano 2.7.4      Arquivo: /tmp/crontab.Ph0fDJ/crontab

# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow  command
0,10,20,30,40,50 * * * * rsync -uravzph /home/DADOS/* 192.168.0.252:/home/DADOS

[ 24 linhas lidas ]
^G Ajuda      ^O Gravar     ^W Onde está? ^K Recort txt ^J Justificar  ^C Pos atual  ^Y Pág anter
^X Sair       ^R Ler o arq  ^_ Substituir  ^U Colar txt  ^T VerfOrtog ^_ Ir p/ linha ^V Próx pág
Right Control
```

Fonte: Autoria própria