

**FACULDADE DE TECNOLOGIA ALCIDES MAYA - AMTEC
CURSO TECNOLÓGICO EM REDES DE COMPUTADORES**

GUILHERME MACIEL FEIJÓ

**IMPLEMENTAÇÃO DE NUVEM PRIVADA EM EMPRESAS PARA A SEGURANÇA
DE DADOS USANDO O OWNCLOUD**

Porto Alegre

2019

GUILHERME MACIEL FEIJÓ

IMPLEMENTAÇÃO DE NUVEM PRIVADA EM EMPRESAS PARA A SEGURANÇA
DE DADOS USANDO O OWNCLOUD

Projeto de Pesquisa apresentado como
requisito parcial para obtenção do título de
Tecnólogo em Redes de Computadores,
pelo Curso Superior de Tecnologia em
Redes de Computadores da Faculdade de
Tecnologia Alcides Maya - AMTEC

Orientador: Prof. Anderson Silva

Porto Alegre

2019

GUILHERME MACIEL FEIJÓ

IMPLEMENTAÇÃO DE NUVEM PRIVADA EM EMPRESAS PARA A SEGURANÇA
DE DADOS USANDO O OWNCLOUD

Projeto de Pesquisa apresentado como
requisito parcial para obtenção do título de
Tecnólogo em Redes de Computadores,
pelo Curso Superior de Tecnologia em
Redes de Computadores da Faculdade de
Tecnologia Alcides Maya - AMTEC

Orientador: Prof. Anderson Silva

Porto Alegre

2019

LISTA DE TABELAS

Tabela 1 - Testes	33
Tabela 2 - Máquinas.....	38
Tabela 3 – Download e Upload	43

LISTA DE FIGURAS

Figura 1– Nuvem Pública	15
Figura 2 – Nuvem Privada.....	16
Figura 3 – Nuvem Híbrida	18
Figura 4– Collabora.....	22
Figura 5– Login da segurança de duas vias.....	24
Figura 6 - Topologia de Rede.....	29
Figura 7 - Plataforma de nuvem	30
Figura 8 - QRcode.....	32
Figura 9 - Passos para criar a nuvem	34
Figura 10 – Configuração do OwnCloud	35
Figura 11 - Topologia	37
Figura 12 – Usuários	39
Figura 13 - Autenticação de duplo fator	39
Figura 14 – Teste de Download com 5 Usuários.....	40
Figura 15 – Teste de Download com 10 Usuários.....	41
Figura 16 – Teste de Upload com 5 Usuários	41
Figura 17 – Teste de Upload com 10 Usuários	42
Figura 18 - Ataque de Força Bruta (hydra).....	44
Figura 19 – Teste de carga	45

LISTA DE SIGLAS

APT	Advanced Package Tool
Brasscom	Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação
BSD	Berkeley Software Distribution
BSD	Berkeley Software Distribution
CRLs	Certificate Revocation List System
CSC	Cloud Services Customer
CSP	Cloud Services Providers
CSRs	Civil Service Retirement System
DDR	Double Data Rate
DDoS	Distributed Denial of Service
DFSG	Debian Free Software Guidelines
GPL	General Public License
HD	Disco Rígido
HTML	HyperText Markup Language
IP	Internet Protocol
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
LXC	Linux Containers
NIST	National Institute of Standards and Technology
NT	New Technology
NVM	Non-Volatile memory
RAM	Random Access Memory
SO	Sistema operativo
SQL	Structured Query Language
TI	Tecnologia da Informação

SUMÁRIO

1 INTRODUÇÃO	8
1.1 Definição do Tema ou Problema	9
1.2 Delimitações do Trabalho	10
1.3 Objetivos	10
1.3.1 Objetivo Geral	10
1.3.2 Objetivos Específicos	10
1.4 Justificativa	10
2 REVISÃO BIBLIOGRÁFICA	12
2.1 Computação em Nuvem	12
2.1.1 Características:	12
2.2 NUVEM PÚBLICA	13
2.3 NUVEM PRIVADA	15
2.4 NUVEM HÍBRIDA	17
2.5 NUVEM COMUNITÁRIA	19
2.6 OWNCLOUD	20
2.7 OPENSSE	21
2.8 COLLABORA	21
2.9 DOCKER	22
2.10 AUTENTICAÇÃO DE DUPLO FATOR	23
2.11 FAIL2BAN	24
2.12 KALI LINUX	25
2.13 APACHE JMETER	25
3 DESCRIÇÃO DA SOLUÇÃO	27
3.1 TOPOLOGIAS DE MÁQUINAS E REDE	28
3.2 PLATAFORMA DE NUVEM	29
3.3 APLICATIVOS	31
3.4 TESTES QUE SERÃO REALIZADOS	32
4 METODOLOGIA	34
4.1 TESTES	36
5 VALIDAÇÃO	37

5.1 CONFIGURAÇÕES DE USUARIOS E FERRAMENTAS	38
5.2 TESTES DE DOWNLOAD E UPLOAD.....	40
5.2 TESTE DE INVASÃO E DDOS.....	43
7 CRONOGRAMA	48
8 REFERÊNCIAS BIBLIOGRÁFICA	49

1 INTRODUÇÃO

Ao longo do tempo as empresas vêm acumulando informações sobre o seu negócio. Com isso as empresas têm que aumentar a qualidade de seus equipamentos e de seus servidores para a prevenção de ataques, pois segundo a Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação (Brasscom) "o Brasil é um dos países que mais sofre ataques cibernéticos, principalmente com o Phishing (fraude eletrônica). Esta forma de ato ilícito cresceu 59% entre 2013 e 2012". Com esses ataques as empresas podem ficar vulneráveis à perda de seus dados.

Segundo a ISO 20.000-2 (2005) "Information security is the result of a system of policies and procedures designed to identify, control and protect information and any equipment used in connection with its storage, transmission and processing." Com isso podemos ver que para se proteger os dados é necessário ter uma política de segurança com os dados da empresa.

Por isso este projeto foi proposto, para poder apresentar uma forma de inovar e de melhorar o nível de segurança de seus dados. Este projeto tem como prioridade manter os dados do cliente seguros em uma nuvem privada, que será criada em um ambiente seguro. Neste projeto será criada uma nuvem privada, para demonstrar suas funções, tais como escalabilidade, backup, segurança do usuário, disponibilidade sem internet, entre outros.

Para poder alcançar estes objetivos o projeto terá que passar por algumas etapas que poderão comprovar este estudo. No primeiro Capítulo será apresentado o projeto, mostrando o problema que o projeto pretende resolver, seus objetivos e justificar o motivo do porque deste estudo. Já no segundo Capítulo teremos a revisão bibliográfica, que falara sobre as nuvens que existem, será falado da plataforma de nuvem privada escolhida (OwnCloud) e das ferramentas que serão necessárias para seu funcionamento.

No terceiro Capítulo deste projeto teremos a descrição da solução, que tem como objetivo explicar o porquê foi escolhido a plataforma do OwnCloud, ferramentas e as funções do OwnCloud. Já no quarto Capítulo poderemos ver como

foi feito para fazer funcionar toda esta estrutura de nuvem e configurações de suas ferramentas, para que o leitor possa ter uma experiência própria desta plataforma.

Em seguida no quinto Capítulo será apresentado a Validação, esta parte mostrara os testes realizados, esses testes consistem em ataque de força bruta, ataque DDoS, Download e Upload. Estes testes têm como objetivo, verificar integridade da nuvem, verificar a disponibilidade, desempenho e funcionabilidade. E por fim será apresentada a conclusão deste projeto, que apresentara os pontos finais deste projeto.

1.1 Definição do Tema ou Problema

Para não perderem suas informações e não gastarem tanto com equipamentos. Segundo Papo (2013) "A maioria das organizações está gastando 80% do seu investimento e tempo de TI com manutenção, sustentação de projetos e DATACENTERS em vez de investirem em inovação.", com isso muitas empresas acabam partindo para a nuvem pública.

Segundo Taurion (2009) "O que vemos são as empresas mais inovadoras buscando experimentar o conceito. Na nuvem da Amazon, já vemos mais de 400.000 usuários, a maioria pequenas empresas e start-ups ou pesquisadores."

Contudo a mudança para a nuvem pública vem com alguns riscos. Segundo a Fecomercio-SP "Muitos provedores de nuvem pública possuem cláusulas em seus contratos afirmando que os dados armazenados pertencem a ele, provedor - e não ao cliente. Este é um risco que costuma pegar os clientes de surpresa[...]", com isso a propriedade dos dados da empresa acaba sendo não a penas da empresa, mas também do provedor da nuvem.

O documento sobre considerações de segurança na computação em nuvem da ISACA aponta mais alguns exemplos de fatores de risco de uma implementação de nuvem pública:

1. Partilha total da "nuvem" – incorpora riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação - a infraestrutura de "nuvem" é partilhada por vários tenants, por vários CSC (Cloud Services Customer), sem relação, interesses comuns, ou o mesmo nível de preocupações com a segurança, sendo isso um risco potencial acrescido para os CSC que deve ser analisado e mitigado;

2. Danos colaterais – inclui riscos de Indisponibilidade, Perda, Roubo e/ou Divulgação- numa infraestrutura partilhada se um dado cliente for atacado poderá haver impacto noutros clientes do mesmo CSP(Cloud Services Providers), mesmo que não sejam o objetivo do alvo a atingir (por exemplo DDoSAttack). (CLOUD COMPUTING 2012).

Conforme a citação acima se percebe que a nuvem pública pode apresentar problemas no que se refere à segurança e privacidade dos dados de empresas que venham a utilizá-la. Nesse sentido, o presente projeto visa oferecer uma alternativa de implantação de nuvem privada, como forma de prover maior segurança e privacidade nos dados corporativos.

1.2 Delimitações do Trabalho

Este projeto irá apresentar uma proposta de nuvem privada interna na empresa. Logo, será realizada a demonstração da nuvem privada, de seus benefícios e de suas funções. Não será objetivo desse projeto o monitoramento dos usuários da nuvem proposta, segurança interna de seus servidores nem a, manutenção de seus equipamentos. O projeto delimitar-se-á somente em demonstrar a nuvem privada como um meio viável de proteção e de segurança de dados.

1.3 Objetivos

Os objetivos dividem-se em: geral e específicos.

1.3.1 Objetivo Geral

Propor uma solução de ambiente com o máximo de seguro e controle possível para armazenamento de dados das empresas.

1.3.2 Objetivos Específicos

- a) Apontar os benefícios e funções da nuvem privada;
- b) Apresentar uma solução de nuvem privada usando o OwnCloud.

1.4 Justificativa

Este projeto tem o intuito de apresentar a nuvem privada para as empresas como uma forma de inovação tecnológica, buscando melhorar o nível de proteção e

segurança dos dados corporativos. Justifica-se esse projeto, como uma forma de apresentar parte dos riscos aos quais as empresas estão expostas ao não investirem em inovações de plataformas de nuvem privada, ao mesmo tempo em que busca razões para não migrar para a nuvem pública, apontando suas falhas e seus riscos.

O projeto visa demonstrar os benefícios fazendo uma demonstração de seu uso prático utilizando o Owncloud como servidor da nuvem privada.

Com essa plataforma de nuvem instalada e configurada pode-se demonstrar suas funcionalidades, tais como alta escalabilidade, alta disponibilidade, maior segurança entre outros benefícios. Este projeto servirá como base para empresas que querem investir em nuvem privada, mas não tem o conhecimento necessário sobre o que é ou como funciona a plataforma.

2 REVISÃO BIBLIOGRÁFICA

Nas seções abaixo, serão explorados conceitos inerentes às tecnologias que envolvem a computação em nuvens públicas e privadas, elencado seus recursos, problemas e soluções relacionadas a segurança.

2.1 Computação em Nuvem

Segundo Taurion [...]a Computação em Nuvem é uma evolução natural da convergência de várias tecnologias e conceitos, como o Grid, mais o conceito de Utility Computing(que são serviços computacionais comercializados como os serviços utilitários, como energia elétrica)[...] (2009).Conforme foi dito acima a computação em nuvem é uma junção de tecnologias que serve para facilitar e apoiar o desenvolvimento de novas tecnologias.

A computação em nuvem é uma plataforma que permite acesso à rede de nuvem, que demanda uma rede de computadores compartilhada que disponibiliza recursos computacionais (por exemplo: redes, servidores, armazenamento, aplicativos e serviços) ,que podem ser disponibilizados rapidamente e liberados com pouco esforço de interação e monitoramento (National Institute of Standards and Technology, 2011).

2.1.1 Características:

Self-Service(Auto-atendimento):Uma empresa ou pessoa física pode sublocar recursos de computação, como serviços de armazenamento ou serviços de servidores na rede, conforme necessário, sem a necessidade de interação com técnicos de informática com cada serviço solicitado (NIST p6 2011).Para suprir este tipo de nuvem ela deve conter o auto-atendimento, pois o usuário deve solicitar, personalizar, pagar e usufruir dos serviços solicitados sem a interferência de técnicos (Pedrosa e Nogueira p 2 2011).

Ampla acesso à rede: As ferramentas estão disponíveis na rede e são acessados por mecanismos padroes que servem para promover o uso por plataformas

heterogêneas de thin ou thick client (por exemplo, telefones celulares, tablets, laptops e estações de trabalho) (NIST p6 2011).

Elasticidade e Escalonamento: Os dados podem ser disponibilizados e liberados de forma ágil, em determinados casos automaticamente, para buscar informações ou levar informações de acordo com a demanda. Para o consumidor, muitas vezes os recursos disponíveis para uso parecem ilimitados e podem ser apropriados em qualquer quantidade e a qualquer momento(NIST p6 2011).

Medição de serviços:A plataforma em nuvem controla e otimiza automaticamente o uso da capacidade dos recursos aproveitando um recurso para cada tipo de situação sendo dividido por nível de abstração apropriado ao tipo de serviço (por exemplo, armazenamento, processamento, largura de banda e contas de usuário ativas)(NIST p6 2011). Segundo Pedrosa e Nogueira “Por esta razão, as nuvens devem implementar recursos que garantam um eficiente comércio de serviços, tais como tarifação adequada, contabilidade, faturamento, monitoramento e otimização do uso (Pedrosa e Nogueira p 2 2011).” com isso o usuário pode sempre estar a par do que esta sendo cobrado.

2.2 NUVEM PÚBLICA

A nuvem pública é uma infraestrutura provisionada para uso aberto pelas pessoas em geral (Peter e Timothy 2011). Segundo Torquato “Neste modelo, a nuvem é disponibilizada para usuários em geral, para os mais variados propósitos. A infraestrutura que aloca a nuvem é de propriedade de organizações de grande porte, dotadas de robusto aparato computacional.”(p,35 2014).Conforme foi dito a nuvem pública é na grande maioria de grandes empresas que sub alocam seus espaços para empresas e usuários.

Com isso é criado uma ilusão de computadores com recursos ilimitados, mas assim proporcionando um ambiente controlado e adequado para seus clientes poderem fazer diversos tipos de cenários.Com tudo esse tipo de recurso de nuvem somente é disponibilizado via internet (Torquato p,35 2014).

Segundo os professores Luís Henrique Costa e Otto Duarte da universidade federal do Rio de Janeiro do curso de redes de computadores II a nuvem:

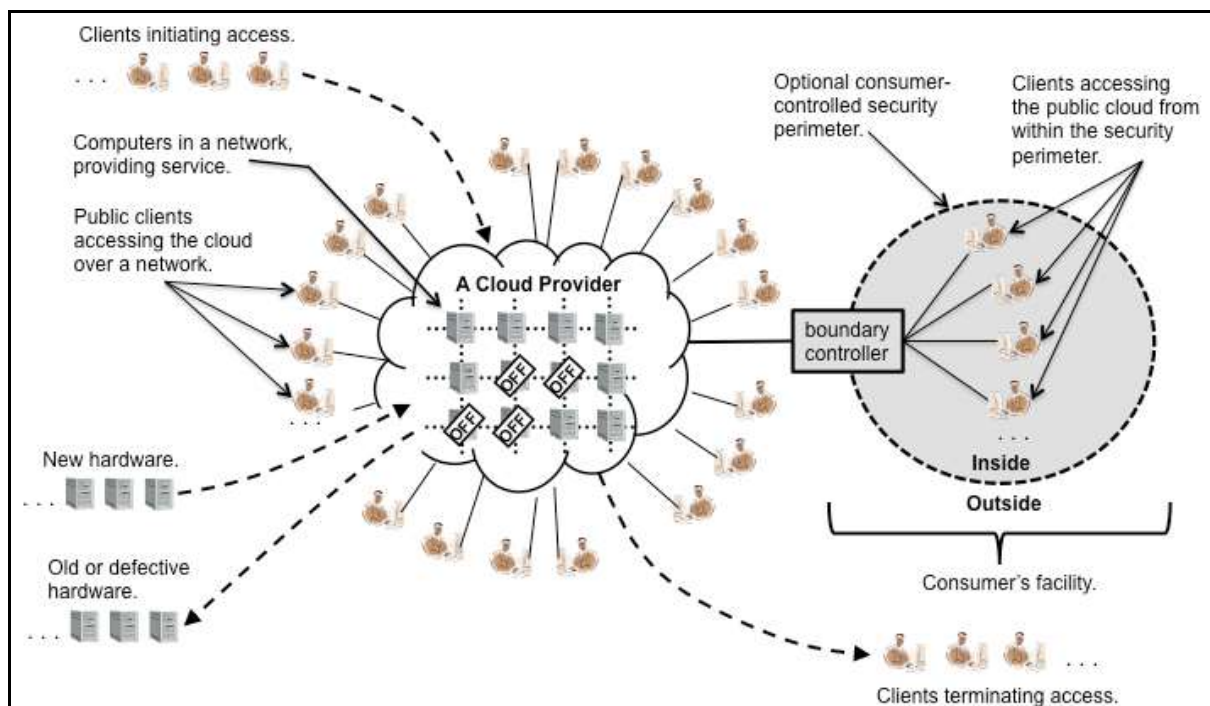
As nuvens públicas são aquelas que são executadas por terceiros. As aplicações de diversos usuários ficam misturadas nos sistemas de armazenamento, o que pode parecer ineficiente a princípio. Porém, se a implementação de uma nuvem pública considera questões fundamentais, como desempenho e segurança, a existência de outras aplicações sendo executadas na mesma nuvem permanece transparente tanto para os prestadores de serviços como para os usuários.(2009).

Conforme a citação acima, este tipo de nuvem é mais recomendado para o uso de pessoas físicas, pois esta "mistura" de usuários na nuvem pública pode aumentar o risco de perda de informações ou o risco de expor informações da empresa é grande. Um dos grandes exemplos que a nuvem pública pode vazear informações para rede é a própria Google Drive que tem na sua cláusula 3. Proteção à privacidade que é:

A Política de privacidade do Google explica como tratamos seus dados pessoais e protegemos sua privacidade quando você usa o Google Drive. Ao acessar o Google Drive, você permite que o Google use esses dados de acordo com nossas políticas de privacidade.(Site do Google 2018).

As ofertas disponibilizadas pelos provedores de nuvem pública ocasionalmente não proporcionam as necessidades específicas de segurança e privacidade de uma empresa. Os riscos são determinados e adequados conforme o uso da nuvem. A adequação dos serviços em nuvem requer uma análise do risco, o contexto no qual a organização opera e as consequências das ameaças plausíveis que enfrentam. Certos ajustes são necessários nas empresas para o ambiente de computação em nuvem pública. As organizações devem exigir que qualquer solução de computação em nuvem pública selecionada seja configurada, implantada e gerenciada para atender sua segurança, privacidade e outros requisitos. (Wayne e Timothy 2011).

Figura 1– Nuvem Pública



Fonte: NIST SpecialPublication 800-146

A figura acima representa o que é uma nuvem pública. Nesta nuvem pública tem um perímetro de segurança para proteger seus usuários de ataques externos. Esta imagem demonstra também os recursos de computação e armazenagem que podem ser expandidos de acordo com a necessidade do cliente.

2.3 NUVEM PRIVADA

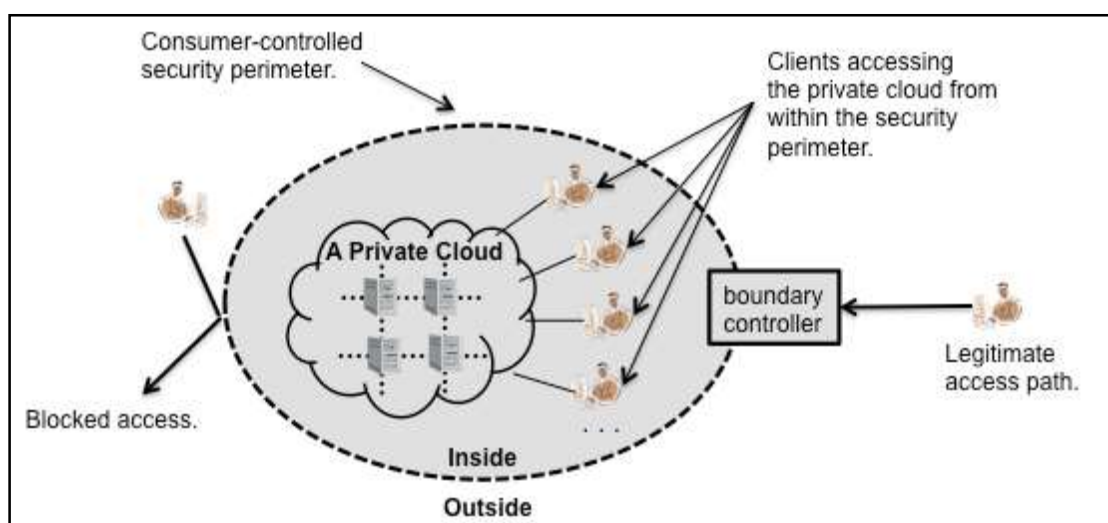
A nuvem privada é uma infraestrutura que provisiona para seus usuários exclusividade no acesso por uma única organização. Esta nuvem pode ser propriedade, gerenciada e operada pela própria empresa, por terceiros ou por ambos, e pode ser localizada dentro ou fora do ambiente de trabalho (Peter; Timothy 2011).

Com uma nuvem privada as empresas podem compartilhar informações e recursos operacionais com todos os funcionários, mas seguindo ordens de

hierarquia de uso. Segundo Buyya et. "establishing a private cloud means restructuring an existing infrastructure by adding virtualization and cloud-like interfaces (2011)". O modo de virtualização de uma nuvem privada visa interligar as informações e diminuir custos de hardware. Como é dito pelos autores do artigo Systems and methods for private cloud computing:

Through virtualization, a private cloud gives an enterprise the ability to host applications on virtual machines enterprise-wide. This provides benefits of shared hardware costs, better service recovery, and the ability to scale up or scale down depending on demand. (McCarthy et al. 2013)

Figura 2 – Nuvem Privada



Fonte: NIST Special Publication 800-146

Nesta imagem é apresentada uma demonstração simples de uma nuvem privada. Conforme é demonstrado na imagem, tem um perímetro de segurança em volta dos recursos do usuário e da nuvem privada (Badger et. 2012).

Segundo Paper:

Núvens privadas oferecem muitos benefícios para a empresa. Esses benefícios incluem o fornecimento de auto-atendimento que é igual ou superior ao de provedores de terceiros; aplicativos e serviços feitos especialmente para as necessidades comerciais; segurança confiável e conformidade indisponível para provedores de núvens públicas no momento; a habilidade de escalar recursos com fornecimento automático para permitir alta utilização e agilidade. (2012 Cisco)

Conforme foi dito por Paper, a nuvem privada possui benefícios que agregam as empresas. Com a nuvem privada feita especialmente para a

necessidade do cliente. Ela pode proteger, inovar seus aplicativos e melhorar a troca de dados na empresa.

Na nuvem privada a escalabilidade e desempenho são algo crucial para a sua melhor qualidade de desempenho, mesmo mantendo um alto nível de segurança. A inovação tecnológica de segurança em nuvem está sempre evoluindo para poder manter um ambiente seguro e controlados para seus usuários. Conforme diz Paper:

- Escalabilidade e desempenho: Os requisitos de segurança em nuvem estão estreitamente ligados à automação, escalabilidade e desempenho devido às cargas de trabalho potencialmente volumosas e aos severos requisitos de segurança envolvidos. Tecnologias inovadoras capazes de ajudar a melhorar o desempenho mantendo, ao mesmo tempo, um alto padrão de segurança são cruciais para a implementação da segurança em nuvem.
- Autenticação e controle de acesso: Como foi discutido anteriormente, o controle de acesso à nuvens privadas depende dos atributos com consciência do contexto e da identidade, dispositivo e local do usuário. Para autenticar e fornecer acesso seguro ao ambiente de nuvem privada de diversos dispositivos e locais, é importante implantar a segurança dentro da rede e possuir diversos pontos de execução (como firewalls, IPS e VPN). (2012 Cisco)

Como foi dito a cima o controle de acesso na nuvem privada tem que ter um rigoroso cuidado, pois se um usuário acessar de um local onde possa ter algum risco de invasão o sistema de proteção pode ser comprometido. Devido a isso os usuários devem possuir dispositivos com proteção para manter um ambiente controlado.

2.4 NUVEM HÍBRIDA

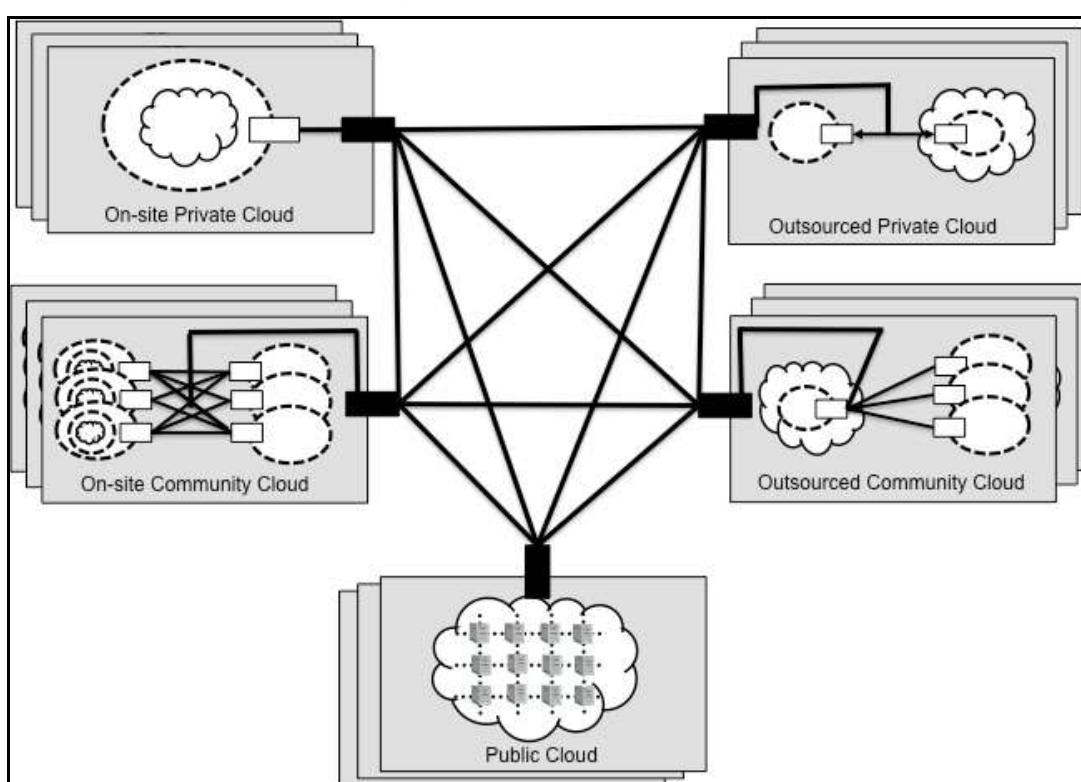
A estrutura de uma nuvem híbrida é formada por duas ou mais plataformas de nuvens (privada, comunitária ou pública), que continuam sendo plataformas diferentes, com isso unidas por meios de tecnologias padronizadas ou proprietárias que se interligam assim formando a nuvem híbrida (Peter;Timothy 2011).

Com essa plataforma vem algumas complicações como dito por Matheus "Devido ao hibridismo de sua composição pode ser particularmente difícil de gerenciar estruturas de nuvem híbrida. É necessário, portanto, delimitar bem as

premissas de cada aplicação que será alocada em nuvem híbrida (2014)".Com isso o monitoramento e controle de usuários tem que ser bem cuidado.

Uma Nuvem Híbrida, é uma junção de nuvens que cada nuvem faz parte de uma variante de cinco partes. Com isso existem diversas configurações possíveis de nuvem híbrida e não é realista enumerá-las. Porém, a capacidade de potencial dessa ferramenta podem ser ilustrados conforme a figura 3.(Badger ;Grance ;Patt; Jeff Voas 2012)

Figura 3 – Nuvem Híbrida



Fonte:NISTSpecialPublication 800-146

A nuvem híbrida pode ser de uso diversificado, pois algumas empresas podem compartilhar seus espaços em nuvem com outras empresas que necessitem de grande poder computacional. Conforme é dito pelo Matheus D'Eça em seu projeto de mestrado modelos de disponibilidade para nuvens privadas: rejuvenescimento de software habilitado por agendamento de migração de VMS (Virtual Machine) :

As motivações para uso de nuvens híbridas são diversas. Organizações com propósitos semelhantes podem compartilhar seus recursos em nuvem. Empresas que necessitam de grande poder computacional apenas em picos de requisição podem criar um canal para unir sua nuvem com um provedor de nuvem pública externo a fim de balancear cargas.(2014)

Com essa uniam as empresas podem ter funcionários trabalhando de outros locais no mundo, acessando os dados da empresa sem precisar estar no ambiente físico da empresa.

2.5 NUVEM COMUNITÁRIA

A nuvem comunitária é parecida com a nuvem híbrida, pois pode estar tanto internamente quanto externamente, mas a diferença é que a nuvem comunitária é compartilhada entre varias empresas. Como é dito por Veras (2012) “a infraestrutura da nuvem comunitária é compartilhada por diversas organizações e suporta uma comunidade que possui interesses comuns, sendo possível existir tanto fora como dentro das organizações.”

Mas como existe mais que uma organização tomando conta desta nuvem, pode se ter diferentes tipos de políticas de gerenciamento entre elas, com essa união políticas o sistema poderá se mostrar complexo (Henrique p 5 2016).

Como é dito por Henrique:

As instituições podem ter normas diferentes a respeito da aquisição de equipamentos, procedimentos distintos para a utilização desses equipamentos, horários de funcionamento diferentes, políticas de segurança diferentes, entre outras peculiaridades que qualquer uma das instituições mantenedoras da nuvem comunitária pode ter. Essas diferenças criam necessidades particulares a cada instituição que devem ser atendidas pelo sistema que prove o serviço de computação em nuvem, mantendo as características importantes ao serviço(Henrique p 5 2016).

Como foi dito a cima esse tipo de nuvem tem que ser feito visando todas as partes compradoras do serviço, pois com algumas empresas juntas na mesma nuvem pode se ter divergências no modo como a nuvem é administrada.

2.6 OWNCLOUD

O Owncloud é uma aplicação que serve para criar nuvem privada, com essa nuvem é possível compartilhar informações com diversos usuários. Com essa plataforma é possível fazer sincronismo de arquivos e com isso a velocidade de acesso aumenta. Segundo Marco, Gláucio e Evandro que escreveram em seu artigo Implementação de uma nuvem de armazenamento privada usando Owncloud e Raspberry PI o Owncloud é:

O Owncloud é uma aplicação web escrita usando a linguagem PHP. Sua primeira versão foi lançada em 2012 com o propósito de fazer sincronização de arquivos entre vários dispositivos. Tal característica é útil quando se quer compartilhar arquivos com outros usuários e/ou até mesmo fazer backups dos dados. As principais vantagens de se utilizar essa ferramenta são: gratuita e código fonte é open source, permitindo que o usuário altere o código conforme sua necessidade e possibilita a criação de uma nuvem de armazenamento privada sendo uma alternativa as nuvens públicas.(2015)

O Owncloud é uma ferramenta que é dividida em duas partes: cliente e servidor, ambas com funções específicas. O cliente esta responsável pelos dados que serão enviados para o servidor e de quando serão baixados. O servidor é a parte que lida com os dados que o cliente envia e manter todos os usuários , que estejam relacionados, com os mesmos dados. Conforme dito por Antoni et.

Ele é dividido em duas partes: i) Cliente: é a parte responsável por decidir quando os dados devem ser enviados e fazer o download dos arquivos atualizados do servidor. O cliente está disponível para as versões desktop (Linux, Mac e Windows) e mobile (Android, BlackBerry e IOS). Ainda é possível acessar os arquivos diretamente do browser através de uma interface web. ii) Servidor: é o ponto de armazenamento centralizado dos dados sendo responsável por enviar os novos arquivos para todos os clientes relacionados aquela conta de usuário. Por ser uma aplicação escrita em PHP, é necessário ter o interpretador PHP instalado no servidor. Além disso é necessário ter um gerenciador de banco de dados para armazenamento dos metadados dos arquivos (atualmente) e um servidor web onde a instância do Owncloud estará disponível.(2015)

O OwnCloud oferece para as empresas ou usuários físicos uma plataforma onde seus usuários possam compartilhar arquivos corporativos ou não simultaneamente. Conforme dito em seu site:

ownCloud offers enterprise fileshare capabilities while it is hosted on your servers, using your storage, under the control of your IT. With ownCloud, you provide users file access to data wherever it lives, supported by your enterprise security systems, management tools and governance policies.(2018)

Com o OwnCloud, os clientes usam apenas uma interface da qual podem acessar a plataforma de nuvem privada, também podem sincronizar e compartilhar arquivo em qualquer tipo de aparelho, em qualquer hora e lugar. Os usuários podem localizar arquivos e compartilhar eles rapidamente, sendo ou não do próprio usuário. Com recursos como proteção por senha, expiração de link , compartilhamento de acesso anônimo e completo, os arquivos podem ser melhor monitorados.(OwnCloud 2018)

2.7 OPENSLL

Este *software* cria uma biblioteca de códigos criptografados, como é dito por Nelson e David “Openssl é uma biblioteca criptográfica de código aberto disponibilizada sob uma licença do tipo BSD (Berkeley Software Distribution)(2005)”. Com isso é criado um ambiente seguro conforme a necessidade, assim como diz Aranha et. “A biblioteca de software OpenSSL se apresenta através de uma implementação segura e eficiente de código aberto dos algoritmos criptográficos que provém aquelas necessidades (2017)”

O OpenSSL vem com uma vasta quantidade de recursos inclusos nele, como dito por Edward et.;

As características mais marcantes da biblioteca OpenSSL são: Criação, gestão de chaves públicas e privadas, administração de operações de criptografia avançados, criando o tipo de certificados X.509, CSRs e CRLs.(2015)

Isso acaba ajudando os usuários na hora de manter o controle sobre seus *softwares* e também faz com que tenha menos funções para se preocupar.

2.8 COLLABORA

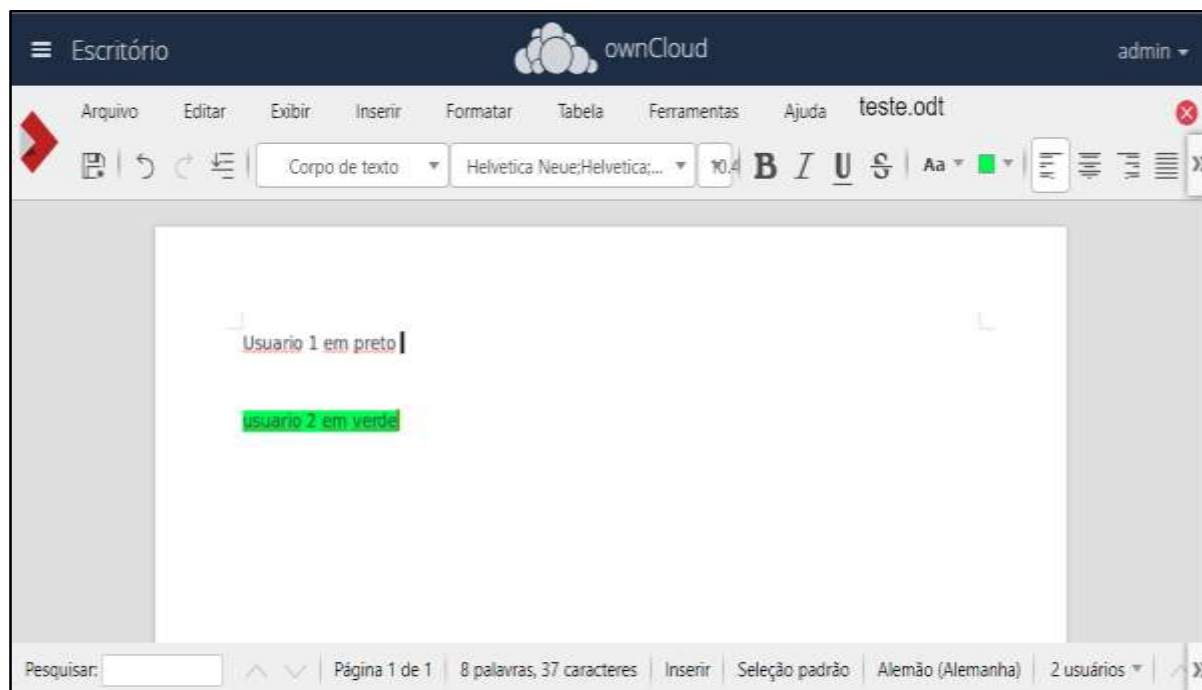
O Collabora é uma ferramenta de edição e criação de arquivos online, que é baseada no LibreOffice. Esta ferramenta é de grande ajuda em meios corporativos, pois os documentos sempre estão a disposição em qualquer lugar da empresa. Conforme é dito no seu site:

O Collabora Online é um poderoso escritório on-line baseado no LibreOffice que suporta todos os principais formatos de arquivo de documentos,

planilhas e apresentações, que você pode integrar em sua própria infraestrutura(2018).

O Collabora assim como o LibreOffice é compatível com quase todos os tipos de Sistemas Operacionais (Linux, Windows e Unix).

Figura 4– Collabora



Fonte: Produzida pelo Autor

Esta ferramenta também possui modo de colaboração, que disponibiliza a função de edição de documentos entre dois ou mais usuários ao mesmo tempo assim como é demonstrado na figura 4.

2.9 DOCKER

Esta ferramenta é baseada em criar container, conforme dito por Fernando e André (2016) “*Container* é, em português claro, o agrupamento de uma aplicação junto com suas dependências, que compartilham o *kernel* do sistema operacional do *host*, ou seja, da máquina (seja ele virtual ou física) onde está rodando.”

Docker é uma ferramenta que cria containeres conforme é dito no seu site “Docker provides container software that is ideal for developers and teams looking to get started and experimenting with container-based applications(2018)”. Esta

ferramenta permite criar, gerenciar e proteger aplicativos assim como é dito em seu site “Docker unlocks the potential of your organization by giving developers and IT the freedom to build, manage and secure business-critical applications without the fear of technology or infrastructure lock-in(2018)”.

O Docker é uma plataforma de virtualização, mas, contudo ele monta sistema operacional isolado que utilizam funções do kernel em comum. Conforme é dito por Cristiano Diedrich :

Docker não é um sistema de virtualização tradicional. Enquanto em um ambiente de virtualização tradicional nós temos um S.O. completo e isolado, dentro do Docker nós temos recursos isolados que utilizando bibliotecas de kernel em comum (entre host e container), isso é possível pois o Docker utiliza como backend o nosso conhecido LXC.(2017)

Com isso é possível fazer ligações entres sistemas dentro do próprio sistema operacional para assim poder ter mais agilidade.

2.10 AUTENTICAÇÃO DE DUPLO FATOR

A segurança de dados é uma das coisas mais priorizadas tanto em cli"entes quanto em quem provê serviços de nuvem. Assim como é dito por Cavalcanti: "Data security and confidentiality can be considered one of main reasons that affect both sides, clients and cloud providers". (2017).

Esta forma de autenticação de duplo fator da uma segurança a mais, serve para criar mais uma barreira de invasão, pois somente o usuário que tiver acesso a segunda senha poderá ter controle sobre o local acessado. Como é dito pelo site da Kaspersky;

A autenticação de dois fatores é um recurso oferecido por vários prestadores de serviços online que acrescentam uma camada adicional de segurança para o processo de login da conta, exigindo que o usuário forneça duas formas de autenticação. A primeira forma – em geral – é a sua senha. O segundo fator pode ser qualquer coisa, dependendo do serviço.(2018)

Esta ferramenta foi criada com o intuito de proteger a privacidade dos usuários de diversas plataformas. Assim como é dito por Camurça (2018) “Facebook, Twitter, Google, LinkedIn e Dropbox, entre outros serviços, já oferecem esse recurso“. A iPhone é uma das empresas que usam a dupla autenticação para proteger seus clientes. Como é dito pelo site da Apple;

A autenticação de dois fatores é uma camada adicional de segurança do ID Apple criada para garantir que você seja a única pessoa que consiga acessar sua conta, mesmo que alguém saiba sua senha. (2018)

Figura 5– Login da segurança de duas vias



Fonte: Produzida pelo Autor

A figura 5 mostra uma das formas de ter segurança de duas vias. Na imagem pode se observar um QRcode, que precisa ser lido por um aplicativo (O Aplicativo usado neste projeto foi Authy, mas pode ser usado qualquer aplicativo que leia ou gere senhas atrás do QRcode) de celular para poder gerar uma senha de seis dígitos, que a cada trinta segundo é modificada.

2.11 FAIL2BAN

Fail2Ban é uma ferramenta que monitora logs e monitora tentativas de acessos de um único Ip, como é dito por Nascimento “O aplicativo fail2ban é um agente que monitora os logs, e verifica a quantidade de tentativas de conexão sem sucesso, bloqueando o IP suspeito, após determinado número de insucessos.” (2011)

Segundo Rodrigo e Paulino;

O aplicativo monitora a tentativa de acesso em diversos serviços, e bloqueia o possível ataque adicionando regras no Firewall instalado. Ele também bloqueia ataques de força bruta, comuns quando se tem conexão com a internet, de forma confiável, sem prejudicar usuários autênticos. (softwares para criação de mecanismo de segurança baseado na plataforma linux 2013)

Como foi dito a cima o Fail2Ban é uma ferramenta que auxilia na prevenção de ataques externos e também internos. Esta ferramenta não prejudica a utilização

do sistema operacional assim mantendo o usuário seguro e mantendo o desempenho.

2.12 KALI LINUX

O Kali Linux é uma ferramenta de teste de invasão, como dito em seu site “Kali Linux é uma avançada distribuição Linux especializado em Testes de Intrusão e Auditoria de Segurança. (Kali 2019)”. Esta ferramenta é utilizada para fazer testes de invasão, o que ajuda a verificar os pontos fracos de uma rede ou servidor”.

Segundo deu site;

Kali Linux incorpora mais de 300 testes de penetração e programas de auditoria de segurança com um sistema operacional Linux, oferecendo uma solução completa que permite aos administradores de TI e profissionais de segurança testar a eficácia das estratégias de mitigação de riscos. (2019)

Conforme é mencionado acima esta ferramenta tem diversas ferramentas de invasão, que servem para auxiliar os administradores de segurança e TI. Com essas ferramentas os admins podem saber como proteger servidores, CPU, sites, entre outros.

2.13 APACHE JMETER

O Apache JMeter é uma ferramenta de teste de aplicativos como e dito por Nevedrov “Apache JMeter is a tool that can be used to test applications utilizing HTTP or FTP servers.” (2007). Esta ferramenta serve para comprovar o funcionamento dos servidores.

Segundo Chandel et.;

The Apache Jmeter desktop application is open source software, a 100% pure Java application designed to load test functional behavior and measure performance. It was originally designed for testing Web Applications but has since expanded to other test functions.(Comparative Study of Testing Tools: Apache JMeter and Load Runner 2013)”

O Apache JMeter é uma aplicação Java que é uma ferramenta de código aberto. Como foi dito acima essa ferramenta serve para fazer testes de desempenho e mostrar o comportamento funcional de teste de sistemas WEB.

3 DESCRIÇÃO DA SOLUÇÃO

A solução proposta por este projeto é baseada na montagem de uma nuvem privada em uma máquina Virtual, que tem como prioridade manter os dados da empresa ou do cliente seguros.

Pois algumas nuvens públicas como a Google acabam se apropriando dos dados do cliente, como é descrito no seu contrato de uso. Tanto a Google como a Amazon tem serviços de nuvem pública que tem infraestruturas interligadas, que acaba sendo um risco para os outros usuários, pois se um cliente mal intencionado derrubar o servidor os outros clientes acabam perdendo o serviço, com isso gerando as falhas em disponibilidade.

Deste modo, a solução proposta possui as seguintes vantagens: disponibilidade, pois esta nuvem fica alocada dentro da empresa, e não se beneficia dos dados do cliente, pois os dados são exclusivos do usuário e a infraestrutura da nuvem é feita para cada cliente.

A escolha da plataforma de nuvem privada para este projeto foi a OwnCloud, pois foi feita uma pesquisa das empresas que já usam este serviço. Uma das empresas que usam este serviço é a Datto, que é uma empresa que faz segurança cibernética e backups de dados, se uma empresa que é voltada para segurança de dados confia nesta plataforma quer dizer que é algo segura. Por isso o autor deste projeto optou pela OwnCloud e por que esta plataformas pode ser usada de acordo com os objetivos do projeto.

A nuvem privada que será apresentada neste projeto é a OwnCloud, que é uma plataforma gratuita e de fácil manuseio. O OwnCloud é uma plataforma que permite que seu usuário tenham total liberdade na hora de criar usuários e dar-lhes permissões de acesso. Esta plataforma cria um ambiente onde somente o cliente tem acesso a seus dados, assim evitando a apropriação dos dados do cliente.

A OwnCloud é uma nuvem que não precisa de internet para ser utilizada internamente na empresa, pois o servidor fica alocado dentro da empresa. Com isso a disponibilidade de acesso é mais rápida (dependendo da quantidade de usuários e da capacidade do servidor), pois o usuário faz o uso ponto a ponto com o servidor

da nuvem. Sendo uma nuvem criada para cada cliente, o risco de usuários externos terem acesso a ela fica mais restringido. Com isso o OwnCloud fica um pouco mais protegido de ataques externos.

Para se criar o servidor deste projeto foi utilizado o VirtualBox, pois esta ferramenta é gratuita e supre as necessidades do projeto, tais como economia de espaço físico, manutenção simples e compatibilidade com outras plataformas. O VirtualBox será utilizado para criar uma máquina virtual que servirá de base para a instalação do Debian 9, que será o servidor do OwnCloud.

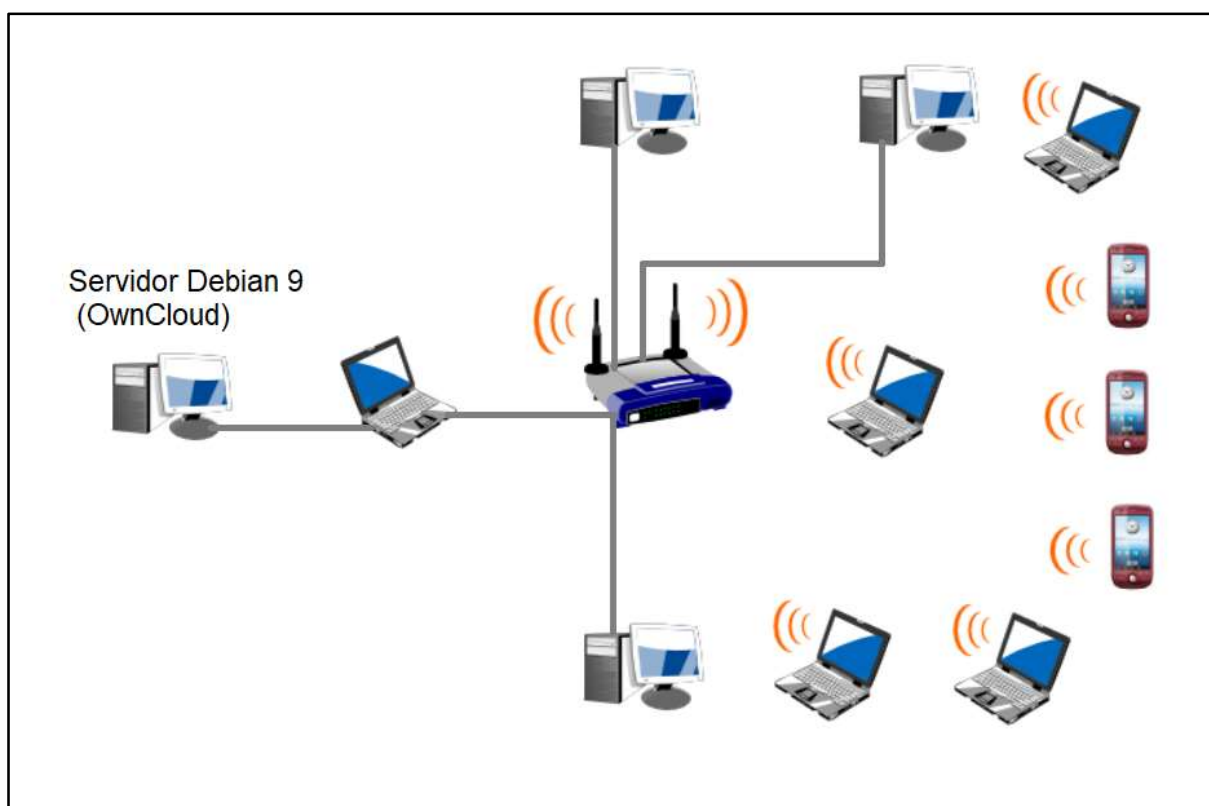
A solução proposta neste projeto necessita de velocidade de transmissão, pois quanto mais rápido os dados saírem do servidor maior será o desempenho do OwnCloud. O Debian 9 é leve e rápido o que facilita muito na hora de utilizar a nuvem, pois quanto mais velocidade há no servidor maior será a transmissão de dados. Este SO também possui compatibilidade com os pacotes PHP, MySQL, Apache, entre outros, que são a base do OwnCloud.

3.1 TOPOLOGIAS DE MÁQUINAS E REDE

O VirtualBox foi instalado em um Notebook Acer que tem um processador Core i5 da sétima geração, 1 Terabyte de HD, 8G (gigabytes) de memória RAM DDR 4 e uma placa de vídeo dedicada Nvidia Geforce GTX 1050 de 4G DDR5. Nesta máquina será criada uma máquina virtual para armazenar o servidor Debian 9. Esta máquina virtual utilizada tem a capacidade de armazenamento de 20G (gigabytes) de memória e 2 giga de memória RAM.

A rede utilizada neste ambiente de teste foi criada através de um roteador D-Link, que foi o responsável por gerar os Ips para os dispositivos. Esta rede não terá acesso à internet, para não haver acesso de terceiros. A rede contará com 11 dispositivos conectados, sendo um deles o servidor da máquina virtual. Conforme é apresentada na figura 6.

Figura 6 - Topologia de Rede



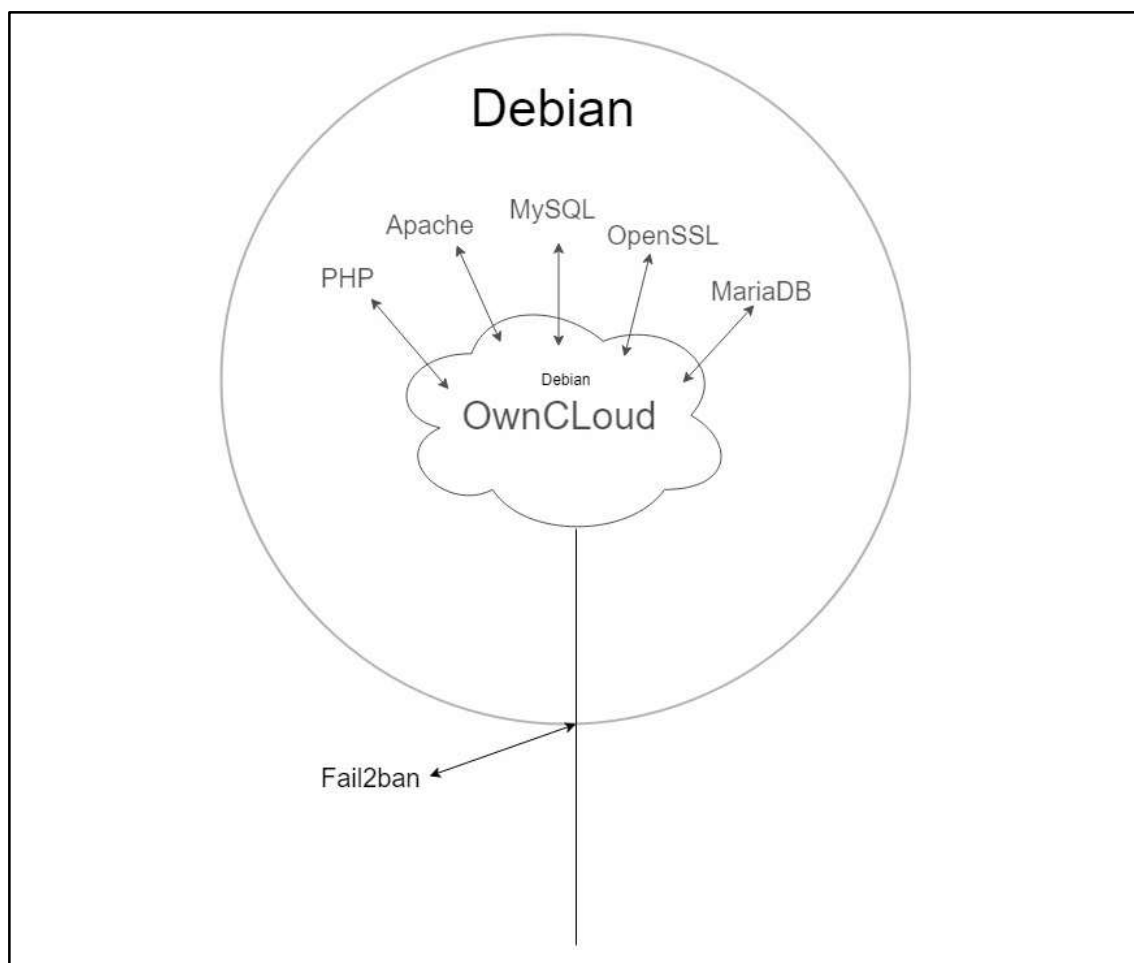
Fonte: Produzida pelo Autor

Os dispositivos apresentados na figura 6 foram utilizados na implementação deste projeto, sendo um dos Notebooks o provedor do OwnCloud. Os dispositivos têm as seguintes configurações 3 CPU processador Core i3, 4G de memória RAM e 500G de HD, 2 Notebook: Pentium, 2G de memória RAM e 360G de HD, 1 Notebook: Quad core, 6G de memória RAM e 750G de HD e 3 celulares Samsung.

3.2 PLATAFORMA DE NUVEM

Após a instalação do Debian é necessário fazer algumas instalações de pacotes que o OwnCloud precisa para funcionar. Os pacotes são: Apache, MariaDB, MySQL, PHP e OpenSSL. Com esses pacotes instalados corretamente é preciso configurá-los como será mostrado no Apêndice do projeto. Neste servidor será instalado também o Fail2ban para bloquear ataques DDOS, pois esta ferramenta monitora e bloqueia o IP de usuários maliciosos.

Figura 7 - Plataforma de nuvem



Fonte: Produzida pelo Autor

A figura 7 mostra como o OwnCloud utiliza os pacotes PHP, Apache, MariaDB, MySQL e OpenSSL. O OwnCloud precisa destas ferramentas instaladas, pois ele é uma plataforma baseada em PHP, por causa disto é necessário a instalação desta ferramenta, para o OwnCloud poder fazer uso de suas ferramentas. A função do MariaDB e MySQL é criar o banco de dados do OwnCloud. O Apache é uma ferramenta Web que auxiliará a plataforma em sua pagina de acesso e o OpenSSL serve para criptografar e descriptografar as informações que passem por ele. O Fail2ban ficará encarregado de monitorar os logs dos usuários, para verificar as tentativas de acesso dos usuários ao servidor. Se houver mais de três tentativas ininterruptas de um mesmo usuário o Fail2ban bloqueia o endereço Ip para não comprometer o servidor.

Esta plataforma será utilizada pois ela tem uma vasta capacidade de interação com os usuários, fácil interação com seus aplicativos e é uma plataforma totalmente gratuita. Esta plataforma permite que seu usuário crie, defina permissões para cada membro da sua nuvem e monte grupos de usuários.

Os usuários têm acesso individual de suas informações na nuvem privada, mas podem ser criado um documento ou arquivos compartilhado com outros usuários do mesmo grupo. Em vista a internet das coisas esta plataforma criou uma forma de poder usar diversos tipos de plataformas como computadores, Notebooks, Tablets e celulares.

3.3 APLICATIVOS

O OwnCloud tem suporte para editores de texto com o Collabora, que é uma ferramenta baseada em LibrsOffice. O Collabora permite criar e editar documentos, tabelas e slides diretamente na plataforma da nuvem, com isso é possível fazer alterações em documentos sem a necessidade de baixá-los. Esta plataforma também vem com o modo cooperativo, que serve para dois ou mais usuários editarem o documento ou arquivo ao mesmo tempo. A figura 4 comprova esse uso.

Para esta ferramenta funcionar é necessário a configuração que será apresentada na metodologia, que será a instalação do Docker. O Aplicativo do Collabora precisa ser configurado em um contêiner dentro do Docker para que assim possa gerar os documentos diretamente na nuvem.

Esta nuvem privada também conta com editor de txt diretamente na nuvem através do Collabora. Pode-se abrir arquivos em PDF sem a necessidade de fazer o download, ver imagens, é possível escutar musicas diretamente da nuvem, sincronizar o email corporativo na nuvem, fazer gráfico, entre diversos outros tipos de funções que são disponibilizados em seus aplicativos.

Esta ferramenta foi adicionada no projeto, pois ela da ao usuário a segurança na qual para acessar sua conta será necessária uma segunda senha e com isso acaba cria mais uma camada de segurança dos dados do cliente. A ferramenta de dupla autenticação funciona através de um QRcode que tem que ser lido por um aparelho celular, assim como é mostrado na figura 8.

Figura 8 - QRcode



Fonte: Produzida pelo Autor

Após a leitura deste QRcode terá que ser colocado o código de autenticação de leitura, assim será criado um gerador de senhas no celular. Estas senhas que serão geradas são trocadas a cada 30 segundos e só podem ser usadas no usuário que foi feito a leitura do QRcode. Com isso somente o usuário que tiver a chave de duplo fator poderá acessar a conta da usuária, assim podendo dar uma segurança a mais para os dados pessoais do cliente.

Alem da ferramenta de autenticação de duplo fator o OwnCloud também possui um aplicativo que limita os erros de login e senha por Ip. Esse aplicativo serve para evitar os ataque DDoS, pois limitando a quantidade de erros, o ataque de força bruta acaba sendo neutralizado.

3.4 TESTES QUE SERÃO REALIZADOS

Este projeto tem a premissa de apresentar um ambiente seguro e controlado. Para comprovar estas funções serão necessários alguns testes que vão ser apresentados na validação.

Tabela 1 - Testes

Teste	Objetivo	Resultado esperado
Ataque DDoS	Testar proteção do servidor	Bloquear o ataque de DDoS após a terceira tentativa
Ataque de Força Bruta	Testar proteção do servidor	Bloquear o ataque de Força Bruta depois do teste
Upload e Download	Verificar a capacidade do servidor fazendo ambos os serviços	Ver quantos usuários pode fazer esta função ao mesmo tempo

Fonte: Produzida pelo Autor

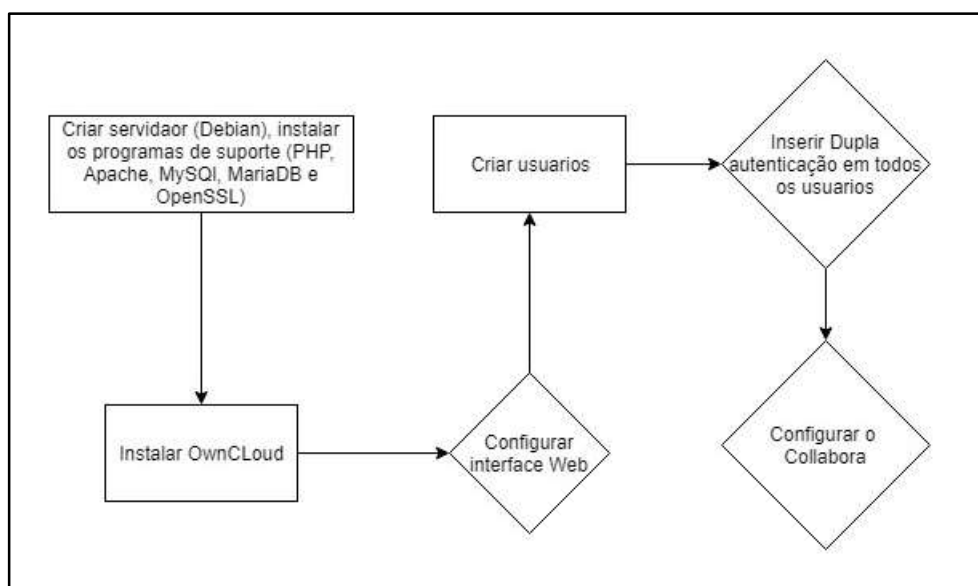
Conforme mostra a tabela 1 um dos testes que será feito é o ataques DDOS para ver o quanto esta nuvem suportara, lembrando que no servidor existe uma ferramenta que bloqueia este tipo de ação e também a nuvem privada.

Para mostrar a eficiência da desta nuvem privada será feito testes de upload e download, para verificar o quanto o servidor agüenta. Com este teste veremos quantos usuários este servidor agüenta fazendo esta função e será apresentado ate onde ele se mantém em uso.

4 METODOLOGIA

O método usado neste projeto foi o Indutivo, pois foi criada uma nuvem privada para poder ser feito testes que comprovem os objetivos deste projeto. Para criar esta nuvem privada foram necessários alguns passos, que é apresentado da figura 9.

Figura 9 - Passos para criar a nuvem



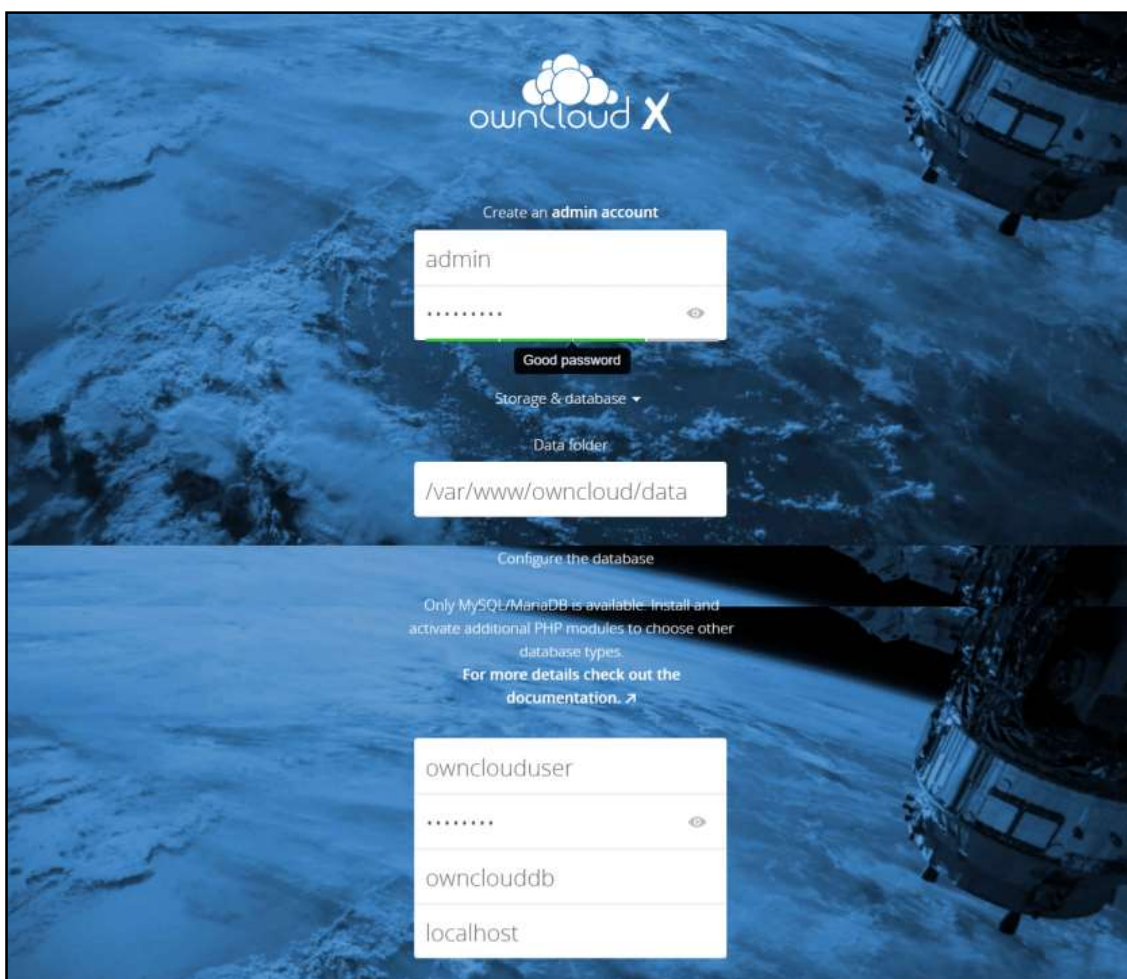
Fonte: Produzida pelo Autor

O primeiro procedimento necessário para a aplicação do projeto foi a instalação de um SO (Debian 9) no VirtualBox. Considera-se que para a execução desse projeto, que o servidor esteja instalado e com sua rede configurada no modo Bridge, pois é necessário um Ip que esteja fora do VirtualBox, também será necessário o uso de internet para baixar e atualizar os programas necessários para o funcionamento da nuvem.

Após a instalação do Debian é necessário instalar os pacotes PHP, Apache, MySQL, MariaDB e OpenSSL. Esses pacotes serviram de base para o OwnCloud funcionar corretamente, pois o mesmo é baseado em PHP e utiliza os bancos de dados do MySQL e MariaDB. O OwnCloud utiliza também a linguagem Web do Apache, e o OpenSSL cria um canal criptografado entre o servidor e o OwnCloud.

Efetuada todas estas instalações será possível acessar a página web do OwnCloud. Para acessar a nuvem deve-se acessar uma interface web e colocar o Ip e o nome da nuvem conforme este exemplo: "<http://192.168.0.20/owncloud>". Quando entrar no URL o OwnCloud, precisará ser configurado os dados de usuário, que foram criados no MySQL conforme mostra a figura 10.

Figura 10 – Configuração do OwnCloud



Fonte: Produzida pelo Autor

Depois de configurado o Admin será pedido para entrar com o Login e senha, que foi configurado na figura 10, após isto o OwnCloud está configurado no seu básico.

4.1 TESTES

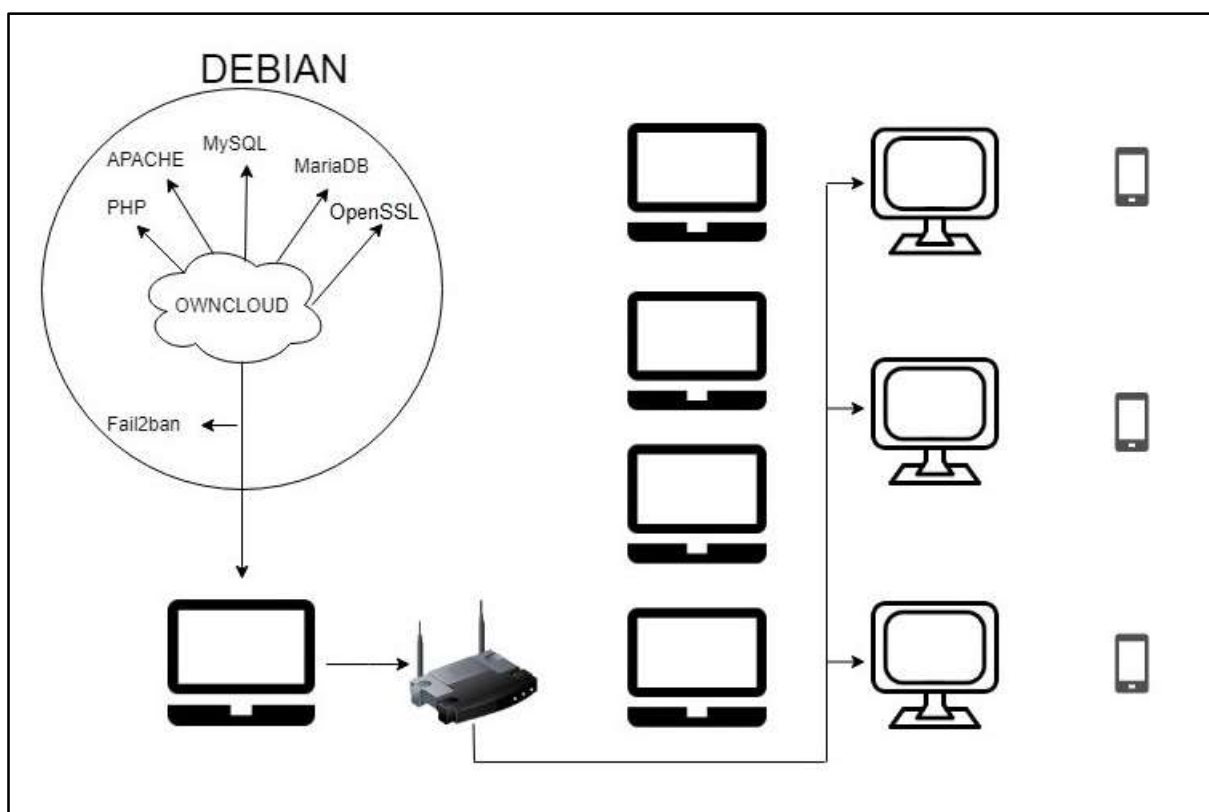
Para fazer os testes foram criados alguns usuários, com o intuito de ver a sua performance do servidor da nuvem privada. Foi feito um teste de carga que será demonstrado e dirão quantos usuários o servidor pode agüentar simultaneamente.

O segundo teste será de DDoS que demonstrara se a nuvem privada e segura contra este tipo de ataque. Este ataque será feito diretamente ao servidor da nuvem privada, pois a nuvem privada já possui um sistema que protege de ataque DDoS e também possui a dupla autenticação, que com isso restringe ainda mais os ataques.

5 VALIDAÇÃO

Para poder fazer a validação deste projeto foi necessário criar uma nuvem privada (OwnCloud), onde foi testado seu uso e seus benefícios. Esta plataforma de nuvem foi criada em um ambiente controlado com a topologia de redes que é demonstrado na figura 13.

Figura 11 - Topologia



Fonte: Produzida pelo Autor

Esta topologia consiste em um notebook Acer Nitro 5 com um processador core I5 da sétima geração, 8gb de memória RAM, 4gb de placa de vídeo dedicada e 1Tb de HD. Este notebook servirá de base para ser instalado o VirtualBox, onde estará instalado o servidor Debian com o OwnCloud dentro. A máquina virtual que foi criada para instalar a nuvem tem o processador Pentium com um núcleo de processamento, 2Gb de memória RAM e 20Gb de HD. As máquinas que foram utilizadas nos testes estão detalhadas na Tabela a baixo.

Tabela 2 - Máquinas

Modelo	Processador	Memória RAM	HD
Notebook Acer	Processador AMD 4 core	6 Gb RAM	750Gb de HD
Notebook Acer	Processador Core I3 quarta geração	4 Gb RAM	500Gb de HD
Notebook Acer	Processador Core I3 quarta geração	6 Gb RAM	500Gb de HD
Notebook CCE	Processador Pentium	4 Gb RAM	320Gb de HD
CPU	Processador Core I3 quarta geração	4 Gb RAM	500Gb de HD
CPU	Processador Core I3 quarta geração	4 Gb RAM	500Gb de HD
CPU	Processador Core I3 quarta geração	4 Gb RAM	500Gb de HD
Celular Samsung	J7	2 Gb RAM	32 Gb de HD
Celular Samsung	J7	2 Gb RAM	32 Gb de HD
Celular Samsung	J5	1 Gb RAM	16 Gb de HD

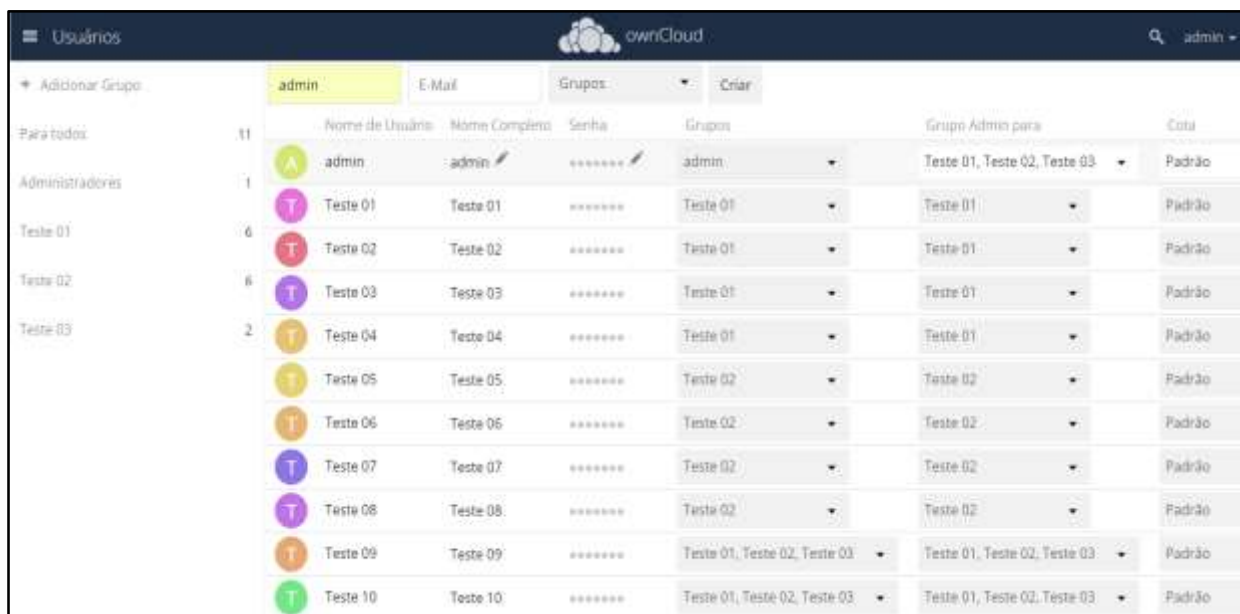
Fonte: Produzida pelo Autor

Na tabela 2 é mostrada a capacidade de hardware de cada dispositivo utilizado no ambiente de teste. O roteador D-Link foi utilizado para criar os Ips, este roteador tem 4 porta 100Mbps e Wireless 2.4 Hz. Não foi definido um Ip fixo para cada dispositivo com exceção da máquina virtual da nuvem, pois se for trocado o endereço de Ip o serviço ficará indisponível.

5.1 CONFIGURAÇÕES DE USUARIOS E FERRAMENTAS

Para criar os usuários é necessário estar logado como administrador, pois somente o admin tem a liberação de criar usuários. Quando se é criado um novo usuário o administrador escolhe o grupo, senha e capacidade de armazenamento que cada usuário pode utilizar. Estas contas podem ser divididos por grupo que podem compartilhar arquivos entre eles e grupos de Administração, que tem as mesmas liberações do admin assim como é mostrado na figura 12. O admin pode escolher também quanto de memória cada usuário pode usar.

Figura 12 – Usuários



	Nome de Usuário	Nome Completo	Senha	Grupos	Grupo Admin para	Cota
11	admin	admin	*****	admin	Teste 01, Teste 02, Teste 03	Padrão
1	Teste 01	Teste 01	*****	Teste 01	Teste 01	Padrão
6	Teste 02	Teste 02	*****	Teste 01	Teste 01	Padrão
6	Teste 03	Teste 03	*****	Teste 01	Teste 01	Padrão
2	Teste 04	Teste 04	*****	Teste 01	Teste 01	Padrão
	Teste 05	Teste 05	*****	Teste 02	Teste 02	Padrão
	Teste 06	Teste 06	*****	Teste 02	Teste 02	Padrão
	Teste 07	Teste 07	*****	Teste 02	Teste 02	Padrão
	Teste 08	Teste 08	*****	Teste 02	Teste 02	Padrão
	Teste 09	Teste 09	*****	Teste 01, Teste 02, Teste 03	Teste 01, Teste 02, Teste 03	Padrão
	Teste 10	Teste 10	*****	Teste 01, Teste 02, Teste 03	Teste 01, Teste 02, Teste 03	Padrão

Fonte: Produzida pelo Autor

Para fazer a configuração da autenticação de duplo fator é necessário que esteja logado como administrador, pois será necessário instalar o aplicativo do duplo fator. O usuário deve ir até o Market e procurar pelo aplicativo TOTP Segundo-fator Auto e clicar nele e no botão de instalação.

Figura 13 - Autenticação de duplo fator



Fonte: Produzida pelo Autor

Após fazer a instalação é necessário ir em configurações, segurança e marcar a opção TOTP que vai mostrar o QRcode assim como é mostrado na figura 12. A leitura deste QRcode pode ser feito com qualquer tipo de aplicativo que gere códigos através desta leitura. O aplicativo utilizado deste projeto será o Authy que está disponível gratuitamente na AppStore, em seguida deverá ser lido o QRcode

para ser gerado um código. Com a leitura deste código o Admin tem que colocar o código de autenticação para validar e cadastrar o celular, depois disso a dupla autenticação esta configurada.

5.2 TESTES DE DOWNLOAD E UPLOAD

Para fazer os testes de desempenho do OwnCloud foi necessário um arquivo 50mb que foi escolhido pelo autor, pois arquivos maiores que esse sendo feito upload ou download podem trancar o trafego de rede, pois a rede é toda em 100Mbps. O teste teve como base inicial 5 usuários baixando ao mesmo tempo este arquivo. Como podemos ver na figura 14.

Figura 14 – Teste de Download com 5 Usuários



Fonte: Produzida pelo Autor

Esta figura mostra o processados do servidor do OwnCloud no momento que estava baixando os arquivos de 5 usuários. Este gráfico mostra os Context switches per second e interrupts per second, isso mostra o tempo de comutação por segundo e tempo de interrupção por segundo. Podem-se ver no gráfico que o tempo de interrupção mínimo é de 80 ips e o Maximo de 1,02 Kips quando atinge o ápice do Download. A comutação permanece quase estável ao longo do processo, mas como podemos ver na figura 15 os gráficos mudam.

Figura 15 – Teste de Download com 10 Usuários



Fonte: Produzida pelo Autor

Nesta figura é mostrado o teste com 10 usuários baixando este mesmo arquivo. Podem-se ver no gráfico que o tempo de interrupção mínimo mudou de 80 ips para 69 ips e o Máximo de 1,02 Kips para 2,17 Kips quando atinge o ápice do Download. A comutação permanece quase estável ao longo do processo, mas quando passamos para o Upload isso é diferente como é mostrado na figura 16.

Figura 16 – Teste de Upload com 5 Usuários



Fonte: Produzida pelo Autor

Pode-se ver que os números mudam quando é feito o Upload a comutação mínima é de 232 sps e a máxima de 1,81 Ksp/s e a interrupção mínima 90 ips e o Maximo de 1,23 Kips quando atinge o ápice do Upload. Vemos que quando subimos alguma coisa para a nuvem exige mais do processador.

Figura 17 – Teste de Upload com 10 Usuários



Fonte: Produzida pelo Autor

Na figura 17 mostra que o processador já está quase utilizando sua capacidade máxima por segundo. A comutação mínima do Upload de 10 usuários é de 261 sps e a máxima de 3,02 Ksp/s e a interrupção mínima 89 ips e o Maximo de 1,99 Kips quando atinge o ápice do Upload. Esta figura mostra que o processador já está quase em capacidade máxima. Se usarmos mais algum usuário o serviço vai começar a ficar cada vez mais lento até o ponto de parar. Por isso é recomendado utilizar somente 10 usuários com esta configuração de servidor.

Tabela 3 – Download e Upload

Teste de Download e Upload com 10 usuários baixando 50mb	
Download	Upload
0,264 sps 2,17 Kips	0
0	3,02 Ksps 1,99 Kips
0,264 sps 2,17 Kips	3,02 Ksps 1,99 Kips
0,528 sps 4,34 Kips	6,04 Ksps 3,98 Kips

Fonte: Produzida pelo Autor

A tabela 3 mostra a relação entre os dois testes para ver qual deles é mais importante e qual deve ser mais cuidado. Foi feito uma comparação de uso de um de cada vez e dos dois ao mesmo tempo, com isso é possível ver que o Upload consome mais capacidade do processador do que o Download. Com o Upload consumindo 6,04 Ksps de comutação e 3,98 de interrupção enquanto o Download consome 0,528 sps de comutação e 4,34 Kips de interrupção.

5.2 TESTE DE INVASÃO E DDOS

O teste de ataque foi feito com um servidor Kali Linus. A ferramenta utilizada para fazer o ataque de força bruta foi o hydra, que utiliza um usuário e uma lista de combinações de senhas para fazer a invasão de um servidor ou computador testando as senhas uma a uma. Como o OwnColud vai ficar internamente na empresa e somente os usuários locais tem acesso a nuvem, a lista de senhas foi criado com caracteres específicos do administrador. Como o Owncloud já tem duas maneiras de bloquear o ataque de força bruta (Duplo fator e Limitador de erros de senha). O autor deste projeto decidiu atacar o próprio servidor, pois se o servidor for derrubado o serviço da nuvem parara de funcionar. A figura 18 mostra o ataque feito ao servidor.

Figura 18 - Ataque de Força Bruta (hydra)

```

root@kali:~/Documents# hydra -l guilherme -P /root/Documents/teste.txt -vv 192.168.0.20 ftp
Hydra v6.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-06-05 16:15:04
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1679616 login tries (1:lp:1679616), ~104976 tries per task
[DATA] attacking ftp://192.168.0.20:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000000' - 1 of 1679616 [child 0] (0/0)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000001' - 2 of 1679616 [child 1] (0/0)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000002' - 3 of 1679616 [child 2] (0/0)
Process 2303: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2302: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2301: Can not connect [unreachable], retrying (1 of 1 retries)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000005' - 4 of 1679616 [child 3] (0/0)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000008' - 5 of 1679616 [child 4] (0/0)
Process 2304: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2305: Can not connect [unreachable], retrying (1 of 1 retries)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000009' - 6 of 1679616 [child 5] (0/0)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000010' - 7 of 1679616 [child 6] (0/0)
Process 2306: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2307: Can not connect [unreachable], retrying (1 of 1 retries)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000011' - 8 of 1679616 [child 7] (0/0)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000012' - 9 of 1679616 [child 8] (0/0)
Process 2308: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2309: Can not connect [unreachable], retrying (1 of 1 retries)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000015' - 10 of 1679616 [child 9] (0/0)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000018' - 11 of 1679616 [child 10] (0/0)
Process 2310: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2311: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2312: Can not connect [unreachable], retrying (1 of 1 retries)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000019' - 12 of 1679616 [child 11] (0/0)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000020' - 13 of 1679616 [child 12] (0/0)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000021' - 14 of 1679616 [child 13] (0/0)
Process 2313: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2314: Can not connect [unreachable], retrying (1 of 1 retries)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000022' - 15 of 1679616 [child 14] (0/0)
[ATTEMPT] target 192.168.0.20 - login 'guilherme' - pass '00000025' - 16 of 1679616 [child 15] (0/0)
Process 2315: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2316: Can not connect [unreachable], retrying (1 of 1 retries)
Process 2301: Can not connect [unreachable]
[ERROR] Child with pid 2301 terminating, can not connect
Process 2302: Can not connect [unreachable]
[ERROR] Child with pid 2302 terminating, can not connect
Process 2305: Can not connect [unreachable]
[ERROR] Child with pid 2305 terminating, can not connect
Process 2304: Can not connect [unreachable]
[ERROR] Child with pid 2304 terminating, can not connect

```

Fonte: Produzida pelo Autor

Como é mostrado na figura 18 o ataque foi bloqueado com sucesso, pois no servidor foi instalada uma ferramenta chamada Fail2ban. Esta ferramenta é responsável pelo monitoramento de tentativas de login e quando um usuário tenta logar mais de 3 vezes sem êxito o Fail2ban bloqueia o Ip e não deixa mais o usuário tentar entrar por 24h.

O ataque DDoS foi feito através de uma ferramenta chamada JMeter que é do Apache. Esta ferramenta faz testes de carga em dispositivos web para ver o funcionamento dos serviços. Na figura 19 é mostrado o teste que foi efetuado no OnwCloud.

Figura 19 – Teste de carga

Amostra #	Tempo de início	Nome do Usuário Virt...	Rótulo	Tempo da amostra (ms)	Estado	Bytes	Latency
1	10:37:25.403	Grupo de Usuários 1-5	Requisição HTTP	293		11012	293
2	10:37:25.403	Grupo de Usuários 1-6	Requisição HTTP	294		11012	294
3	10:37:25.403	Grupo de Usuários 1-10	Requisição HTTP	294		11012	294
4	10:37:25.406	Grupo de Usuários 1-1	Requisição HTTP	292		11012	292
5	10:37:25.698	Grupo de Usuários 1-5	Requisição HTTP	12		11011	12
6	10:37:25.403	Grupo de Usuários 1-7	Requisição HTTP	303		11012	303
7	10:37:25.718	Grupo de Usuários 1-6	Requisição HTTP	6		11011	5
8	10:37:25.727	Grupo de Usuários 1-10	Requisição HTTP	2		11011	2
9	10:37:25.731	Grupo de Usuários 1-1	Requisição HTTP	3		11011	3
10	10:37:25.737	Grupo de Usuários 1-5	Requisição HTTP	5		11011	5
11	10:37:25.750	Grupo de Usuários 1-7	Requisição HTTP	3		11011	3
12	10:37:25.752	Grupo de Usuários 1-6	Requisição HTTP	2		11011	2
13	10:37:25.754	Grupo de Usuários 1-10	Requisição HTTP	3		11011	3
14	10:37:25.755	Grupo de Usuários 1-1	Requisição HTTP	3		11011	3
15	10:37:25.781	Grupo de Usuários 1-5	Requisição HTTP	3		11011	3
16	10:37:25.785	Grupo de Usuários 1-6	Requisição HTTP	7		11011	6
17	10:37:25.786	Grupo de Usuários 1-10	Requisição HTTP	6		11011	6
18	10:37:25.787	Grupo de Usuários 1-1	Requisição HTTP	5		11011	5
19	10:37:25.784	Grupo de Usuários 1-7	Requisição HTTP	9		11011	9
20	10:37:25.821	Grupo de Usuários 1-5	Requisição HTTP	2		11011	2
21	10:37:25.828	Grupo de Usuários 1-6	Requisição HTTP	1		11011	1
22	10:37:25.831	Grupo de Usuários 1-10	Requisição HTTP	2		11011	2
23	10:37:25.842	Grupo de Usuários 1-1	Requisição HTTP	2		11011	2
24	10:37:25.847	Grupo de Usuários 1-7	Requisição HTTP	2		11011	2
25	10:37:25.885	Grupo de Usuários 1-5	Requisição HTTP	1		11011	1
26	10:37:25.887	Grupo de Usuários 1-6	Requisição HTTP	3		11011	3
27	10:37:25.891	Grupo de Usuários 1-10	Requisição HTTP	2		11011	2
28	10:37:25.892	Grupo de Usuários 1-1	Requisição HTTP	2		11011	1
29	10:37:25.894	Grupo de Usuários 1-7	Requisição HTTP	2		11011	2

Fonte: Produzida pelo Autor

O teste mostrado na figura 19 apresenta uma falha em ataques DDoS com uma carga de 11,011Mbs/s, se este ataque for efetuado com uma carga muito alta o servidor da nuvem ficará em sobrecarga até o fim do ataque. Com este teste podemos ver que é possível derrubar a nuvem privada fazendo um ataque DDoS.

6 CONCLUSÃO

Foi observado que a nuvem privada proposta neste projeto funciona e esta operante, conforme foi apresentado no decorrer do projeto. Esta ferramenta proporcionou um ambiente onde poderá ser armazenadas informações, criar arquivos e documentos, ter interação com outros usuários, entre outras funções que o OwnCloud pode proporcionar ao cliente.

Os objetivos específicos deste projeto, que são analisar os benefícios e funções da nuvem privada e apresentar uma solução de nuvem privada usando o OwnCloud, foram alcançadas com o decorrer deste projeto. Um dos maiores benefícios que a nuvem privada proporciona ao seu cliente é a localização de seus dados, isto traz uma segurança maior para o cliente, pois o dono da nuvem sabe exatamente onde estão seus dados. A solução de nuvem com a OwnCloud funciona e esta em funcionamento, assim como é mostrado no desenvolvimento e validação do projeto.

O objetivo geral de criar um ambiente seguro e controlado não pode ser comprovado completamente, pois ambientes 100% seguros não existe, contudo este projeto apresentou um ambiente com o mínimo de chances de ser invadido por terceiros. O ambiente que foi criado sem o acesso à internet, com isso limitando a invasão por terceiros e os usuários do OwnCloud possuíram dupla autenticação e proteção contra força bruta, para ter mais uma camada de proteção para os dados, assim podendo ter o mínimo de chance de ser atacado.

Foi feito testes de DDoS e de força bruta para ver o nível de segurança desta nuvem privada. Os teste de DDoS deram resultados negativos, pois esta nuvem está vulnerável a este tipo de ataque. Contudo se o administrador da rede colocar um firewall para proteger este tipo de ataque, os resultados serão completamente diferentes. Já o ataque de força bruta foi impedido completamente, pois foi instalado uma ferramenta que bloqueia ataques maliciosos, assim como e mostrado na validação deste projeto.

Este projeto ainda tem planos futuros, como criptografia de arquivos, para proteger ainda mais os dados do cliente, acesso externo da nuvem privada,

virtualização de máquinas na nuvem privada, esta são algumas coisas que ainda podem ser aperfeiçoadas em projetos futuros.

7 CRONOGRAMA

Atividades	Meses				
	Mar.	Abr.	Mai.	Jun.	Jul.
Introdução				30.06.19	
Bibliografia		11.04.19			
Descrição da solução			11.05.19		
Metodologia				06.06.19	
Validação				13.06.19	
Conclusão				13.06.19	
Revisão final do texto e elaboração da introdução e conclusão				30.06.19	
Data limite de entrega do Projeto de Estágio					04.07.19

8 REFERÊNCIAS BIBLIOGRÁFICA

ANDRÉ, Marcus; FERNANDO, Jeferson. **Descomplicando o Docker**. eletrônica: SBNigri Artes e Textos Ltda. Rio de Janeiro, pg 6, 2016.

ÁNGEL, Miguel. **Autenticação de dois fatores: o que é e por que preciso usá-la?**. Disponível em: <<https://www.welivesecurity.com/br/2018/11/06/autenticacao-de-dois-fatores/>>. Acesso: 12 Nov 2018.

ANTONI, Marco; PREUSS, Evandro; RICARDO Gláucio. **Implementação de uma nuvem de armazenamento privada usando Owncloud e Raspberry PI**. Disponível em: <<http://eati.info/eati/2015/assets/anais/Longos/L6.pdf>>. Acesso: 29 jun 2018.

ANTONI, Marco; VIVIAN, Gláucio; PREUSS, Evandro. **Implementação de uma nuvem de armazenamento privada usando Owncloud e Raspberry PI**. Disponível em: <eati.info/eati/2015/assets/anais/Longos/L6.pdf> . Acesso em: 23 mar. 2018.

APACHE. **APACHE IS OPEN**. Disponível em: <<http://apache.org/>> Acesso 11 jun 2018.

ARANHA, Diego et al. **Estudo e Implementação do Ataque de Canal Lateral no ECDSA do OpenSSL**. Disponível em: <<http://www.ic.unicamp.br/~reltech/PFG/2017/PFG-17-24.pdf>>. Acesso: 12 Nov 2018.

BADGER, Lee; GRANCE, Tim; PATT, Robert; VOAS, Corner. **Cloud Computing Synopsis and Recommendations**. Disponível em: <<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf>> Acesso 16 jun 2018

BRASSCOM.**Segurança de Dados.** Disponível em:<<https://brasscom.org.br/seguranca/>>. Acesso em: 16 mar. 2018.

BROBERG, James; BUYYA, Rajkumar; GOSCINSKI, Andrzej. **CloudcomputingPrinciplesandParadigms**.ed Copyright, 2011.

BROBERG, James; BUYYA, Rajkumar; GOSCINSKI, Andrzej. **CLOUD COMPUTING Principles and Paradigms**.Disponível em:<http://dphoto.lecturer.pens.ac.id/lecture_notes/internet_of_things/CLOUD%20COMPUTING%20Principles%20and%20Paradigms.pdf> . Acesso: 26 jun 2018.

Cavalcanti, JORGE. MULTI-FACTOR AUTHENTICATION WITH OPENID IN VIRTUALIZED ENVIRONMENTS.**Disponível em:**<<https://ieeexplore.ieee.org/abstract/document/7867604/authors>>.Acesso: 29 Out 2018.

CHANDEL, Vandana; GULERIA, Sonal; PATIAL, Shilpa; **Comparative Study of Testing Tools: Apache JMeter and Load Runner**, 2013. Disponível em: <<http://www.ijccr.com/May2013/3.pdf>> . Acesso: 10 Mai 2019.

CHOPRA,Nitish;SINGH,Sarbjeet.**Deadline and cost based workflow scheduling in hybrid cloud**.Disponível em:<<https://ieeexplore.ieee.org/abstract/document/6637285/>>. Acesso: 26 jun 2018.

CLOUD COMPUTING. 2012. *Security Considerations for Cloud Computing.* 2012.

Costa, Luís; Duarte, Otto.**Computação em nuvem.** Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/seabra/index.html>. Acesso em: 12 mai 2018.

D'EÇA, Matheus. **Modelos de disponibilidade para nuvens privadas: rejuvenescimento de software habilitado por agendamento de migração de VMS.** Disponível

em:<https://www.researchgate.net/publication/280318186_Modelos_de_Disponibilida_de_para_Nuvens_Privadas_Rejuvenescimento_de_Software_Habilitado_por_Agendamento_de_Migracao_de_VMs>. Acesso em: 16 jun. 2018.

DE PAULA, Fábio Berbert. **O que são distribuições.** Disponível em: <<https://www.vivaolinux.com.br/artigo/O-que-sao-distribuicoes/>>. Acesso: 16 jun 2018.

DOCKER.**Docker Simplifies the Developer Experience.** Disponível em:<<https://www.docker.com/>>. Acesso: 17 Out 2018.

DUARTE, Otto; HENRIQUE, Luís. **Redes de Computadores.** Disponível em:<http://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2009_2/seabra/arquitetura.html>. Acessado em: 20 mar. 2018.

EFTAIHA, Diana. **AnIntroductionto Apache.** Disponível em:<<https://code.tutsplus.com/tutorials/an-introduction-to-apache--net-25786>>. Acesso: 01 Jul 2018.

FECOMERCIO-SP. **Armazenamento de dados em nuvem oferece riscos.** Disponível em: <www.fecomercio.com.br/noticia/armazenamento-de-dados-em-nuvem-oferece-riscos>.Acesso em: 18 mar. 2018.

GOOGLE.3. **Proteção à privacidade.**Disponível em: <https://www.google.com/intl/pt-BR_ALL/drive/terms-of-service/> Acesso 06 jun 2018.

GRANCE, Timothy; JANSEN, Wayne. **Guidelines on Security and Privacy in Public Cloud Computing.** Disponível em: <<https://dl.acm.org/citation.cfm?id=2206222>>. Acesso em: 12 mai. 2018.

HENRIQUE, Pedro. **Implementação de autenticação federada em uma nuvem comunitária geodistribuída.** Disponível em: <<http://monografias.poli.ufrj.br/monografias/monopoli10016244.pdf>>. Acesso: 03 Set 2018.

IPHONE, **Autenticação de dois fatores do ID Apple,** Disponível em: <<https://support.apple.com/pt-br/HT204915>>. Acesso: 24 Nov 2018.

ISO 20.000-2. **6.6.1 Genera.** Disponível em: <<https://law.resource.org/pub/in/bis/S04/is.iso.iec.20000.2.2005.pdf>>. Acesso: 26 Nov 2018.

KALI, **Segurança ofensiva introduz o Kali Linux,** disponível em: <<https://www.kali.org/>>. Acesso: 15 Mai 2019.

KASPERSKY, **O que é autenticação de dois fatores?** Disponível em: <<https://www.kaspersky.com.br/blog/o-que-e-a-autenticacao-de-dois-fatores-e-como-usa-la/3226/>>. Acesso: 10 Nov 2018.

KRISHNAN, Rejith; MCCARTHY, Christopher; SULLIVAN, Kevin. **SYSTEMS AND METHODS FOR PRIVATE CLOUD COMPUTING.** Disponível em: <<https://patentimages.storage.googleapis.com/0b/ec/47/86cd9e9fb4ff2d/US9137106.pdf>> Acesso: 25 jun 2018.

MARIADB, **AboutMariaDB.** Disponível em: <<https://mariadb.org/about/>>. Acesso: 09 Out 2018.

MCCARTHY, Christopher. **Systems and methods for private Cloud computing**. Disponível em: <<https://patents.google.com/patent/US20120066670/und>> . Acesso em: 30 jun. 2018.

MELL, Peter; GRANCE, Timothy. **The NIST Definition of Cloud Computing**. Disponível em:<<https://csrc.nist.gov/publications/detail/sp/800-145/final>> . Acesso em:12 mai. 2018.

MUNDODOCKER. **Mas por que que o Docker é tão legal?**. Disponível em:<<https://www.mundodocker.com.br/o-que-e-docker/>>. Acesso: 17 Out 2018.

NASCIMENTO, Ricardo B. do. Proteção utilizando fail2ban contra ataques do tipo "força bruta" or brute force. [S.l.: s.n.], 2011. Disponível em: <<https://docs.google.com/file/d/0Byq-AAimoaX-MmE4MzY0NjUtNTI4My00ZjZjLWE4MWMtNDIwOGU0NWRiMWVI/edit?hl=e>>. Acesso em: 10 mai 2019.

NEVEDROV, Dmitri. **Using JMeter to Performance Test Web Services**,2007. Disponível em: <<https://loadstorm.com/files/Using-JMeter-to-Performance-Test-Web-Services.pdf>> . Acesso em: 10 mai 2019.

OWNCLOUD, **Access your data from all your devices, on an open platform you can extend and modify**. Disponível em: <<https://owncloud.org/>>. Acesso 09 jun 2018.

PAPER , White. **Transferência para uma nuvem privada com confiança**. Disponível em: <https://www.cisco.com/c/dam/global/pt_br/assets/ofertas/securedc/pdfs/wp_privatecloud_braport.pdf>. Acesso em: 01 jul. 2018.

PAPER, White. **Transferência para uma nuvem privada com confiança.** Disponível

em:<https://www.cisco.com/c/dam/global/pt_br/assets/ofertas/securedc/pdfs/wp_privatcloud_braport.pdf>. Acesso: 28 jun 2018.

PAPO, José. **Arquitetura de Nuvem:** rompendo fronteiras. Disponível em: <<http://imasters.com.br/design-ux/arquitetura-da-informacao/arquitetura-de-nuvem-rompendo-fronteiras/>>. Acesso em: 17 mar. 2018.

REIS, David; UTO, Nelson. **Um survey sobre bibliotecas criptográficas com suporte à Criptografia de Curvas Elípticas*.** Disponível em:<http://tiagodemelo.info/aulas/uea/2012/topicos/artigo10_Uto.pdf>. Acesso: 12 Nov 2018.

RODRIGO, Leandro; PAULINO, Alexandre. **Softwares para criação de mecanismo de segurança baseado na plataforma Linux.** Disponível em: <<http://antigo.unipar.br/~seinpar/2013/artigos/Leandro%20Rodrigo%20de%20Carvalho%20Silva.pdf>>. Acesso em: 10/05/2019.

SRINIVASA, R. V.; NAGESWARA, R. N. K.; EKUSUMA, K. Cloud Computing: an overview. Journal of Theoretical and Applied Information Technology (JATIT), [S.l.], v.9, 2009.

TAURION, Cezar. **CloudComputing: computação em Nuvem - Transformando o mundo da tecnologia da informação.** Rio de Janeiro: Brasport, 2009.

VERAS, M. CloudComputing: nova Arquitetura da TI. Rio de Janeiro: Brasport, 2012.