FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"
Curso Superior de Tecnologia em Segurança da Informação

Eduardo Antônio Noronha
Gabriel Souza de Camargo

Segurança da informação em ambientes de nuvem

Americana, SP
2022

FACULDADE DE TECNOLOGIA DE AMERICANA "MINISTRO RALPH BIASI"

Curso Superior de Tecnologia em Segurança da Informação

Eduardo Antônio Noronha

Gabriel Souza de Camargo

Segurança da informação em ambientes de nuvem

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação, sob a orientação do Prof. Me. Maxwel Vitorino Da Silva

Área de concentração: Segurança em nuvem.

Americana, SP.

2022

Eduardo Antonio Noronha

Gabriel Souza de Camargo

Segurança da informação em ambientes de nuvem

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/ Americana.

Área de concentração: Segurança da Informação.

Americana, 07 de dezembro de 2022.

Banca Examinadora:

Maxwell Vitorino da Silva (Presidente)
Mestre
Fatec Americana

Eduardo Antônio Vicentini (Membro)
Mestre
Fatec Americana

Maria Elizete Luz Saes (Membro)
Mestre
Fatec Americana

AGRADECIMENTOS

Agradeço a todas as pessoas que nos ajudaram na realização desse trabalho, familiares e amigos.

DEDICATÓRIA

Aos familiares por todo o auxílio que nos deram durante essa jornada.

RESUMO

A computação em nuvem é uma forma de acessar dados pela internet e armazenar arquivos e programas. Pode-se acessar a computação em nuvem a partir de computadores e dispositivos móveis que tenham acesso à Internet. Os serviços de computação em nuvem oferecem segurança da informação com maior ênfase à medida que o serviço se expande e cresce em popularidade. Isso ocorre porque todas as partes envolvidas precisam tomar precauções para proteger os dados que passam pelo serviço. Um dos perigos da falta de segurança nesses ambientes é que as informações roubadas/hackeadas da nuvem resultam na criação de um mercado secundário onde os invasores podem comprar dados, o que tornam a segurança em ambientes de nuvem algo fundamental. Os dados na nuvem são dependentes uns dos outros, tornando os métodos tradicionais de segurança ineficazes. Isso inclui proteções como firewalls e sistemas de rede comuns. Como objetivos para o desenvolvimento do trabalho será analisada a segurança em ambientes de nuvem e como ela é mantida e gerenciada, assim como descrever a definição da computação, analisar os diferentes tipos de serviço e implementar uma exemplificação de funcionamento de ambiente de nuvem utilizando o Minukube e Kubernetes.

Palavras-Chave: Segurança; Internet; Nuvem; Invasão.

ABSTRACT

Cloud computing is a way to access data over the internet and store files and programs. Cloud computing can be accessed from computers and mobile devices that have Internet access. Cloud computing services offer information security with greater emphasis as the service expands and grows in popularity. This is because all parties involved need to take precautions to protect the data passing through the service. One of the dangers of a lack of security in these environments is that information stolen/hacked from the cloud results in the creation of a secondary market where attackers can buy data, which makes security in cloud environments paramount. Data in the cloud is dependent on each other, making traditional security methods ineffective. This includes protections such as firewalls and common networking systems. As objectives for the development of the work, security in cloud environments and how it is maintained and managed will be analyzed, as well as describing the definition of computing, analyzing the different types of service, and implementing an example of how a cloud environment works using Minukube and Kubernetes.

Keywords: *Safety; Internet; Cloud; Invasion.*

LISTA DE FIGURAS

SUMÁRIO

1. INTRODUÇÃO

Para entendermos melhor do que se trata a computação em nuvem utilizaremos dois softwares que trabalham com containers, são eles o Minikube e o Kubernetes. Com esses programas podemos ter uma visão do funcionamento de uma aplicação na nuvem e de como seria feita a sua segurança.

Segundo o *National Institute of Standards and Technology* a computação em nuvem é um modelo que permite acesso à rede de forma onipresente, conveniente e sob demanda a um conjunto compartilhado de recursos de computação configuráveis que podem ser rapidamente alocados e liberado com o mínimo de esforço de gerenciamento ou interação com o prestador de serviço. (*NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY*, s.d., apud BRASIL, 2016)

Computação em nuvem é um estilo de computação no qual recursos de TI, massivamente escaláveis, são disponibilizados sob a forma de serviços, por meio da internet, para múltiplos consumidores externos. (*GARTNER GROUP*, s.d., apud DIÓGENES; VERAS, 2014, p.6)

A segurança das informações que trafegam pelos ambientes de *Cloud Computing* é um assunto que vem ganhando espaço conforme o crescimento e a popularização desses ambientes, visto que proteger esses dados envolve os esforços dos provedores de serviço e de seus clientes.

Segundo uma pesquisa da IBM o crime cibernético aumentou o foco em ataques a Nuvem, e com isso houve também o aumento de um mercado que busca comprar essas informações vazadas, segundo o relatório 2021 *X-Force Cloud Security Threat Landscape* da IBM foram vazadas quase 30 mil contas de nuvem na *Dark Web*, e essas mesmas estão sendo vendidas a mais de 15 mil Dólares.

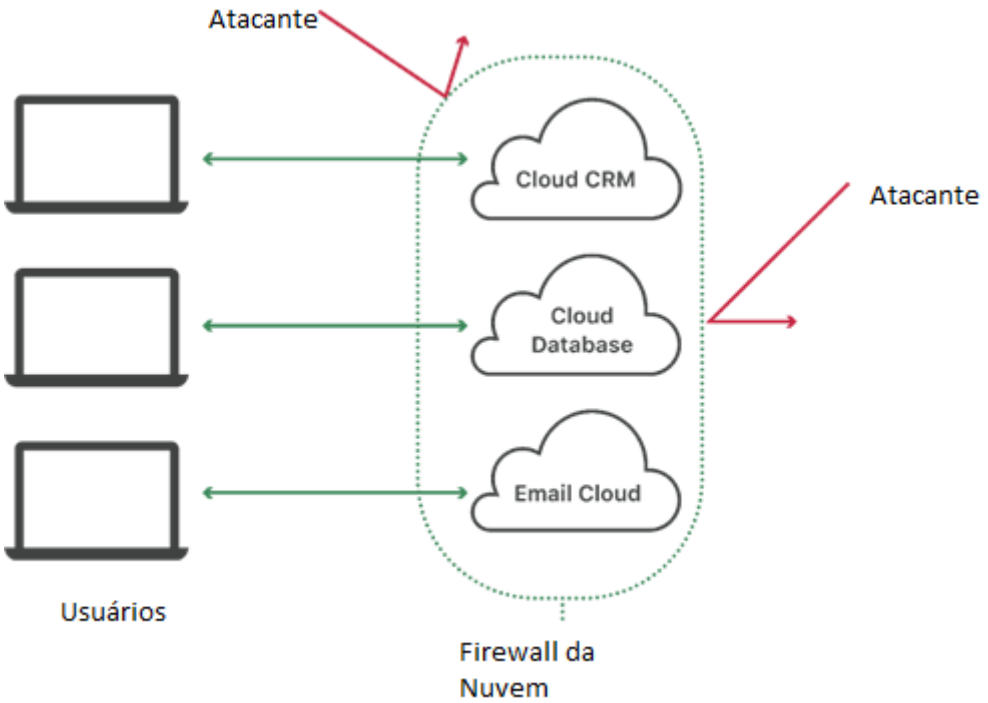
Devemos nos preocupar com a segurança dos dados em nuvem porque os seus recursos são distribuídos e são interdependentes, o que torna uma abordagem

tradicional a segurança das informações ineficiente como por exemplo os firewalls e proteções de rede comuns.

A tecnologia da computação em nuvem utiliza diversos recursos compartilhados exigindo recursos de armazenamento, rede e processamento de dados dificultando também a sua manutenção.

A segurança na nuvem inclui uma ampla variedade de ferramentas e práticas. A função mais importante da segurança na nuvem é garantir que apenas usuários autorizados acessem os dados armazenados na nuvem. As empresas utilizam uma variedade de ferramentas e estratégias para conseguir isso, como por exemplo a micros segmentação, *firewalls* de próxima geração, criptografia de dados e monitoramento e detecção para prevenção de ameaças. A figura abaixo demonstra como funciona um firewall em nuvem.

Figura 1 – *Firewall* em Nuvem



Fonte: Cloudflare.

2. CLOUD COMPUTING

2.1 O que é a *Cloud Computing?*

De acordo com Bruno Gonçalves Zanutto, autor do artigo Segurança em *Cloud Computing*, a *Cloud Computing* basicamente, é a utilização de memória, dispositivos de armazenamento e capacidade de cálculo (processamento) de computadores e servidores interligados por meio da internet de forma que isso seja o mais transparente possível para o usuário.

Com a *Cloud Computing*, um usuário pode ter acesso a recursos que se fossem executados na máquina dele, exigiriam provavelmente maior capacidade de hardware por parte do equipamento do usuário, instalação de softwares que geralmente tem licenças caras, além maior gasto de energia, aumentando custos.

Em comparação com a TI local tradicional, dependendo do serviço de nuvem escolhido, a computação em nuvem pode:

- Reduzir os custos de TI: a nuvem permite que seja aliviada parte ou a maior parte do custo e esforço de compra, instalação, configuração e gerenciamento de infraestrutura local.
- Aumentar a agilidade e o tempo de maturidade: com a nuvem, a empresa pode começar a usar aplicativos corporativos em minutos, em vez de esperar semanas ou meses para que a TI responda às solicitações
- Dimensionar facilmente: a nuvem fornece elasticidade, o que significa que não é necessário comprar excesso de capacidade que não está sendo usado durante períodos de baixa demanda, mas pode aumentar e diminuir com base em picos e quedas de tráfego.

Segundo Vinicius Durbano, escritor da Ecoit Segurança Digital o termo "computação em nuvem" também se refere à tecnologia que faz a nuvem funcionar. Isso inclui uma forma de infraestrutura de TI virtualizada, servidores, software de sistema operacional, rede e outras infraestruturas abstratas, usando software especial para que a TI possa ser agrupada e dividida independentemente dos limites do hardware físico.

Por exemplo, um único servidor de hardware pode ser dividido em vários servidores virtuais. A virtualização permite que os provedores de nuvem utilizem totalmente seus recursos de data center.

2.2 Segurança em Computação em nuvem

A Computação em Nuvem (*Cloud Computing*) é fruto da evolução e da reunião dos fundamentos técnicos de áreas como virtualização de servidores, *Grid Computing* (Computação em Grade), que também foi desenvolvido um protótipo para avaliar a proposta de arquitetura usando Grid-M, um **middleware** da pesquisa do grupo desenvolvido na Universidade Federal de Santa Catarina. Software orientado a serviços, gestão de grandes instalações (**Data Centers**), dentre outras. Trata-se de um modelo eficiente para utilizar softwares, acessar, armazenar e processar dados por meio de diferentes dispositivos e tecnologias web.

A computação em nuvem requer uma abordagem de segurança diferente dos firewalls tradicionais e medidas de segurança ao redor do perímetro da rede. Em vez disso, as empresas precisam se concentrar na implantação automática de recursos de armazenamento, rede e processamento de dados, conforme necessário. Isso ocorre porque os recursos de computação em nuvem são altamente interdependentes e distribuídos em toda a rede.

De acordo com a equipe de redação da Storm, segurança de nuvem oferece vários benefícios:

- Proteção contra-ataques.
- Segurança de dados
- Maior disponibilidade.
- Maior confiabilidade.

3. *Software as a Service* (SaaS)

O SaaS (*Software as a Service*) é uma forma de liberação de softwares e soluções de tecnologias por meio da internet. Utilizando o SaaS a empresa não

precisa instalar e realizar a manutenção de hardware e softwares, o seu acesso depende somente de uma conexão com a internet.

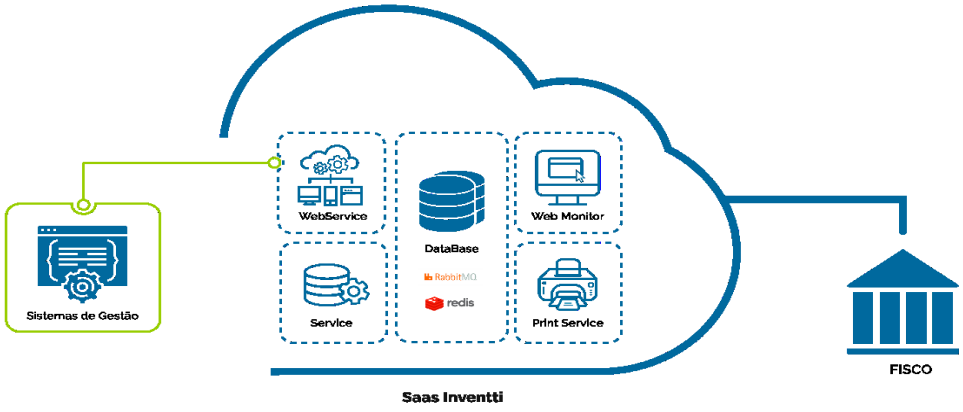
Alguns SaaS são bem comuns no nosso dia a dia como por exemplo os serviços de streaming Netflix, Disney+ etc. Também os serviços de armazenamentos em nuvem iCloud, Google Drive, Dropbox.

Esses softwares são executados nos servidores das empresas provedoras, que têm a responsabilidade de gerenciar o acesso e manter a estrutura de segurança de dados, conectividade e servidores necessários para o serviço.

As provedoras de SaaS vêm crescendo cada dia mais devido a quantidade de benefícios e facilidades que são proporcionados por essa tecnologia. Alguns benefícios são:

- Poucos obstáculos para início de uso do SaaS e baixo custo inicial;
- Alta acessibilidade;
- Facilidade na realização de upgrades;
- Integração de softwares simplificadas.

Figura 2 – Exemplo de modelo SaaS



Fonte: SaaS Inventti.

O software como serviço nasceu de uma necessidade de respostas cada vez mais rápidas, onde no mundo atual a velocidade é essencial na troca de informações. A

principal diferença entre empresas SaaS e softwares convencionais é o local da hospedagem dos dados.

No modelo convencional, o software precisava ser instalado no computador da empresa contratante. Já no SaaS, pode ser acessado através de um navegador na internet, pois os dados ficam salvos em nuvem.

4. *Infrastructure as a Service* (IaaS)

A IaaS (Infrastructure as a Service) é um método de fornecimento de computação, armazenamento, rede e outros recursos via Internet. A Infraestrutura como serviço permite que as empresas utilizem sistemas operacionais, aplicativos e armazenamentos com base na web, sem ter a necessidade de comprar e gerenciar a infraestrutura de nuvem. Algumas das plataformas mais conhecidas de IaaS são a Amazon Web Services (AWS) e a Microsoft Azure. (IBM Learn. IaaS vs. PaaS vs. SaaS. IBM)

Algumas vantagens do uso da IaaS são:

- IaaS pode ser usada para firewalls, endereços IP, servidores, roteadores, hospedagem de desktop virtual, armazenamento etc.
- A IaaS elimina todos os custos de compra, taxas e manutenção associados ao hardware.
- A IaaS permite uma fácil gestão o que elimina muitas pessoas e recursos.
- A IaaS é uma alternativa com um baixo custo.
- A infraestrutura da IaaS permite o crescimento de acordo com a necessidade da empresa.

A computação em nuvem é uma tecnologia emergente incrivelmente promissora para a TI atual e futura.

IaaS é uma versão mais flexível do serviço de nuvem, geralmente chamado de nuvem. Ele fornece instantaneamente aos usuários soluções completas para seus requisitos de computação, armazenamento e rede.

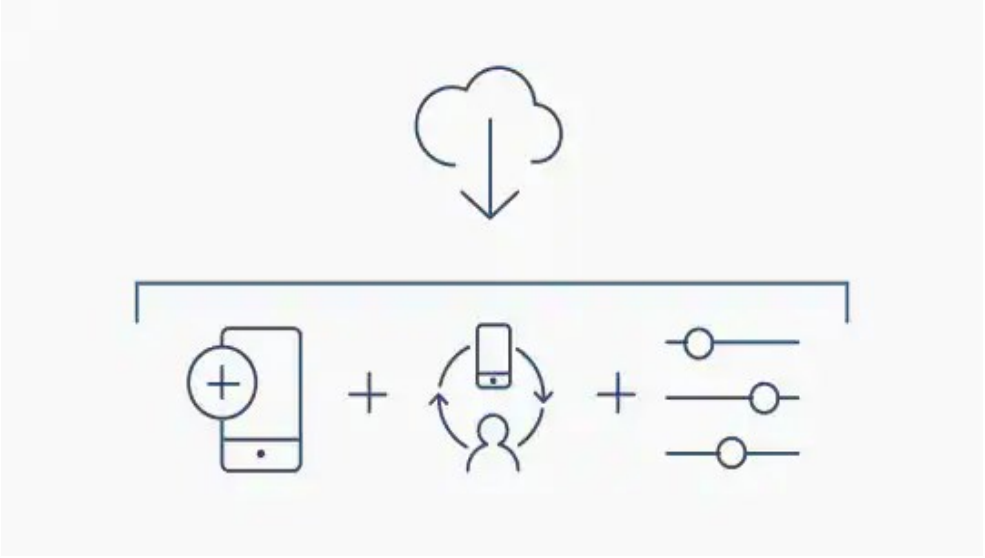
A quantidade cada vez maior de benefícios que as empresas recebem do software de RH está reduzindo as despesas, diminuindo os custos de hardware e manutenção, bem como atualizações de software e investimentos em hardware.

5. *Platform as a Service* (PaaS)

O platform as a service, também conhecido como PaaS, é um dos modos de entrega do cloud computing, onde é fornecido uma plataforma sob demanda dos desenvolvedores de software - uma solução completa de software, um hardware necessário, infraestrutura ou até mesmo ferramentas de desenvolvimento - para o desenvolvimento, execução e gerenciamento de aplicativos sem custo adicional, sem uma complexidade de alto nível e sem a inflexibilidade de manter os anteriores on-premises. (Softline Group. IaaS, PaaS e SaaS: entenda os modelos de nuvem e suas finalidades. Softline)

A imagem a seguir demonstra alguns dos recursos do PaaS, como por exemplo ser uma ferramenta que pode ser acessada remotamente através de smartphones etc.

Figura 3 – Estrutura do PaaS



Fonte: IBM Learn.

Com a PaaS, o provedor do cloud fica responsável pela hospedagem de toda infraestrutura no seu data center (servidores, redes, armazenamento, software de SO, bancos de dados). O trabalho dos desenvolvedores quanto a isso será apenas

escolher em um menu, quais ambientes serão acionados na tarefa que lhe são remetidas no momento para executar, testar, desenvolver, implementar, atualizar e escalar aplicativos.

A PaaS, nos dias de hoje, é frequentemente desenvolvida por meio de contêineres, que nada mais é que um modelo de computador virtualizado. Os contêineres virtualizam o SO, permitindo que os desenvolvedores tenham onde disponibilizar o aplicativo somente com os serviços do SO que são necessários para a tarefa, sem modificação e sem necessidade de um software que diferentes aplicações usam para se comunicar umas com as outras aplicações.

Um PaaS popular construído em torno de contêineres Docker e Kubernetes, o Red Hat OpenShift é uma solução de orquestração de contêineres de código aberto que automatiza a implantação, dimensionamento, balanceamento de carga e muito mais para aplicativos baseados em contêiner.

5.1 Benefícios do PaaS

De acordo com a IBM os benefícios de um ambiente migrado para o PaaS são muitos, alguns deles listados abaixo:

- Prazo de lançamento no mercado mais rápido - com o PaaS, a empresa pode encurtar o prazo de lançamento de um produto, pois não há a necessidade de perder tempo com a compra/instalação de um hardware/software que a empresa usa para desenvolver e manter sua plataforma de desenvolvimento de aplicativos, com isso, sobra mais tempo para as equipes se dedicarem ao que é realmente lucrativo para a empresa.

- Grande variedade de recursos financeiramente acessíveis - as plataformas PaaS, geralmente, oferecem acesso a uma variedade de opções de aplicativos, incluindo sistemas operacionais, middlewares, bancos de dados e diversas ferramentas que facilitam no desenvolvimento, de maneira prática e financeiramente acessível.

- Mais liberdade para experimentar, com menos riscos - O PaaS também permite que você experimente/teste novos sistemas operacionais, linguagens e ferramentas sem ter que fazer investimentos substanciais neles ou na infraestrutura necessária para executá-los.

- Escalabilidade e rentabilidade - com uma plataforma on-premises, o ajuste de escala é sempre muito caro e muitas vezes desgastante: você adquire capacidade adicional de computação, armazenamento e rede antes dos picos de tráfego. Após esse aumento na capacidade, grande parte fica ociosa durante os períodos de baixo tráfego e nada pode ser aumentado com exatidão caso surja necessidade de capacidade adicional, diferente do fornecido pelo PaaS.

- Maior flexibilidade para as equipes dev - os serviços PaaS fornece um ambiente de desenvolvimento de software compartilhado entre as equipes de desenvolvimento e operações, permitindo que acessem as ferramentas que necessitam a partir de qualquer local com uma conexão à internet.

- Custos mais baixos em geral - o PaaS reduz custos de modo geral, não só possibilitando que uma organização evite os gastos com equipamentos de capital associados ao desenvolvimento e ajuste de uma plataforma de aplicativos, mas também reduzindo e eliminando os custos de licenciamentos de softwares necessários para o desenvolvimento de um certo produto da empresa.

5.2 Como o PaaS funciona:

As partes principais do PaaS são divididas em 3, sendo elas:

- Infraestrutura em *cloud*, incluindo máquinas virtuais (VMs), software de sistema operacional, armazenamento, rede, firewalls,
- Software para desenvolvimento, implementação e gerenciamento de aplicativos;

- Uma interface de usuário gráfico, ou GUI, na qual as equipes de desenvolvimento ou DevOps podem fazer todo o seu trabalho ao longo de todo o ciclo de vida do aplicativo. (IBM Learn. PaaS Platform-as-a-Service. IBM)

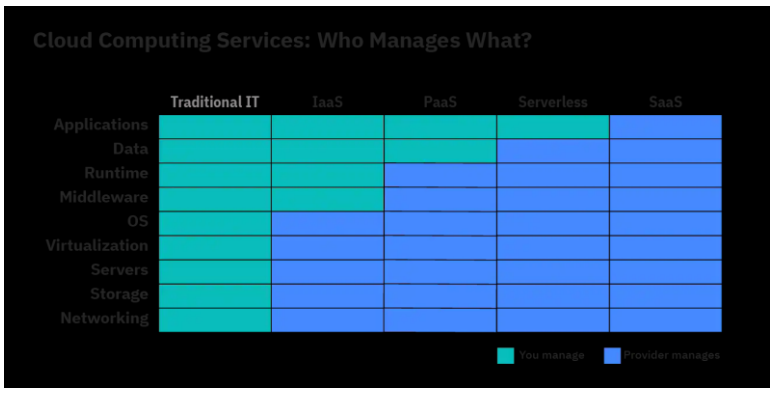
Como o PaaS faz a entrega de todas as ferramentas necessárias de desenvolvimentos padrão por meio de uma interface online, os desenvolvedores podem efetuar o login de qualquer lugar para colaborar com os projetos em desenvolvimento, permitindo testar novos aplicativos ou o lançamento de produtos já concluídos. Os aplicativos são projetados e desenvolvidos diretamente no PaaS usando middleware. Com os fluxos de trabalho simplificados, diversas equipes de desenvolvimento costumam e podem trabalhar no mesmo projeto simultaneamente.

Os provedores de PaaS, gerenciam a maior parte dos seus serviços de computação em cloud, como servidores, tempo de execução e virtualização e o cliente apenas mantém o gerenciamento de aplicativos e dados.

5.3 Casos de uso para a PaaS

O PaaS é encontrado em diversas áreas da computação em nuvem, a figura abaixo demonstra onde cada um é gerenciado e por quem é gerenciado.

Figura 4 – Onde o PaaS é usado



Fonte: IBM Learn.

- Desenvolvimento e gerenciamento API - por causa das estruturas integradas, o PaaS torna muito mais simples para as equipes o desenvolvimento,

execução, e proteção das APIs para compartilhar dados e funcionalidades entre aplicativos.

- Internet das coisas (IoT) - quando pronto para ser usado, a PaaS pode oferecer suporte a uma variedade de linguagens de programação (Java, Python etc.), ferramentas e ambientes de aplicativos usados para o desenvolvimento de aplicativos IoT e processamento em tempo real dos dados gerados por dispositivos da IoT.
- Desenvolvimento ágil e DevOps - o PaaS fornece ambientes totalmente configurados para automatizar os ciclos de vida dos aplicativos de software, incluindo integração, entrega, segurança, teste e implementação.
- Migração para a cloud e desenvolvimento nativo em cloud - Com suas ferramentas prontas para uso e recursos de integração, o PaaS pode simplificar a migração de aplicativos existentes para a nuvem, principalmente por meio da reformulação (mover aplicativos para a nuvem e modificá-los para aproveitar melhor a escalabilidade da nuvem, balanceamento de carga e outros recursos) ou fatoração.
- Estratégia de cloud híbrida - Uma nuvem híbrida integra serviços de nuvem pública, serviços de nuvem privada e infraestrutura local e fornece orquestração, gerenciamento e portabilidade de aplicativos em todos os três. O resultado é um ambiente de computação distribuído unificado e flexível, onde as organizações podem executar e dimensionar suas cargas de trabalho tradicionais (herdadas) ou nativas da nuvem com o modelo de computação mais apropriado. A solução de PaaS certa permite que os desenvolvedores criem uma vez, depois implantem e gerenciem em qualquer lugar em um ambiente de nuvem híbrida.

5.4 Tipos de PaaS desenvolvidos com propósito específico

Diversos fornecedores de cloud oferecem soluções para desenvolver tipos específicos de aplicativos ou integrações de aplicativos com tipos específicos de hardware, software ou dispositivos, por exemplo, o PaaS já foi utilizado em:

- *Artificial Intelligence:* O AIPaaS (*PaaS for Artificial Intelligence*) permite que as equipes de desenvolvimento criassem aplicativos de inteligência artificial sem

a despesa, gerenciamento e manutenção da potência de computação significativo.

- Integração como um serviço - O iPaaS (plataforma de integração como um serviço) é uma solução hospedada em cloud para integração de aplicativos.
- *Communications platform as a service* - O cPaaS (*communications platform as a service*) é um PaaS que permite aos desenvolvedores incluir recursos de voz, vídeo e mensagens dentro dos aplicativos, sem investimento adicional em hardware e software de comunicação.
- *Mobile platform as a service* - O mPaaS (*mobile platform as a service*) é um PaaS que simplifica o desenvolvimento de aplicativos mobile, fornecendo métodos de baixa necessidade de codificação para acessar recursos específicos do dispositivo, entre eles câmera, microfone, sensor de movimento etc.

6. Convenção de Budapeste

Não se pode falar sobre segurança em ambientes de nuvem sem mencionar a convenção sobre Cibercrime (Convenção de Budapeste), instrumento internacional que busca promover a cooperação entre os países signatários no combate aos crimes praticados por meio da internet e com o uso de dispositivos eletrônicos.

Existem duas modalidades de crimes cibernéticos, as próprias e as impróprias. Nas próprias existem as violações dos dados, informações ou sistemas englobando a alteração e a destruição dos dados até o acesso não autorizado dos mesmos, já nas impróprias ocorrem quando a informática é instrumento para a execução do crime, como por exemplo as fraudes eletrônicas.

A Convenção de Budapeste incentiva as empresas a considerar as muitas violações listadas ao formular suas políticas comerciais. Estes incluem os três destacados aqui. A convenção afirma que qualquer acesso ilegal a sistemas de computador, dados ou integridade é uma grande preocupação para as empresas. Além disso, a deturpação de dados em computadores é um grande problema. E o uso fraudulento de dados e propriedade intelectual online é outra questão que preocupa muitas empresas.

Não existe uma lei brasileira única que categorize os crimes cometidos no ciberespaço. Em vez disso, as leis do Brasil são incompletas e divididas em diferentes fragmentos.

O §1º do artigo 154-A criminaliza quem "produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput", sendo que agora há a causa de aumento de pena do §2º se a invasão resultar em prejuízo econômico. Contudo, sua redação é limitada em relação a alguns outros métodos comuns de controle de acesso, como os por meio da cessão ou comercialização de senhas e nomes de acesso, não previstas no tipo penal.

No §3º há a qualificação da conduta caso da invasão decorra a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas ou o controle remoto não autorizado do dispositivo invadido. Havendo divulgação, comercialização ou transmissão dos dados ou informações obtidos a terceiro, essa pena será aumentada de um a dois terços, nos termos do §4º.

A Convenção de Budapeste expande a noção de sistema de computador além de apenas um dispositivo de computador. Também impede a importação de sistemas que realizam processamento de dados mesmo quando o termo dispositivo de computador estiver incluído na convenção. A lei brasileira não diferencia entre interceptação ilegal de dados ou invasão de sistemas de computador, uma vez que estejam em conformidade com a Convenção de Budapeste.

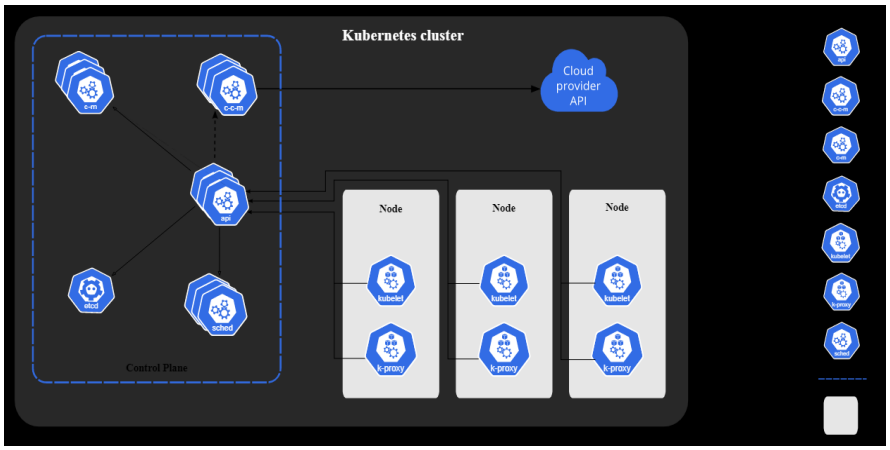
7. Kubernetes

O Kubernetes é um sistema para implantar, escalonar e gerenciar aplicativos em contêineres em qualquer lugar. Ele foi uma criação do Google e posteriormente foi feita a doação do código para a comunidade o tornando um projeto de código aberto. O Kubernetes automatiza tarefas operacionais de gerenciamento de contêineres e inclui comandos integrados para implantação de aplicativos, implementação de alterações nos seus aplicativos, escalonamento de seus aplicativos para mais e para menos para atender às necessidades de mudança, monitoramento de seus aplicativos

e muito mais, facilitando o gerenciamento de aplicativos. (Cloud Google. Quais são os benefícios do Kubernetes.)

A figura a seguir demonstra de forma sucinta como seria o funcionamento e orquestração dos contêiners.

Figura 5 – O que é Kubernetes



Fonte: Kubernetes.io.

7.1 Benefícios do Kubernetes

O Kubernetes tem comandos integrados para lidar com grande parte do trabalho pesado que envolve o gerenciamento de aplicativos, permitindo automatizar as operações diárias. (Cloud Google. Quais são os benefícios do Kubernetes.)

Quando você instala o Kubernetes, ele lida com a computação, a rede e o armazenamento em nome das suas cargas de trabalho. Isso permite que os desenvolvedores se concentrem nos aplicativos e não se preocupem com o ambiente.

O Kubernetes executa verificações de integridade continuamente nos seus serviços, reiniciando os contêineres que falharam ou pararam e só disponibiliza os serviços aos usuários quando confirma que eles estão em execução.

7.2 Funções do Kubernetes

O Kubernetes é usado para criar aplicativos fáceis de gerenciar e implantar em qualquer lugar. O Kubernetes ajuda você a criar apps baseados em micro serviços nativos da nuvem. Também suporta a conteinerização de apps existentes, tornando-se assim a base da modernização de aplicativos e permitindo que você desenvolva aplicativos mais rapidamente.

O Kubernetes foi desenvolvido para ser usado em qualquer lugar, permitindo que você execute seus aplicativos em implantações no local e em nuvens públicas; bem como em implantações híbridas entre os dois. Assim, você pode executar seus aplicativos onde precisar.

O Kubernetes pode ajustar automaticamente o tamanho de um cluster necessário para executar um serviço. Isso permite a você escalonar automaticamente seus aplicativos, para mais e para menos, com base na demanda e executá-los com eficiência.

8. KaaS (Kubernetes as a Service)

O Kubernetes as a Service (KaaS) possibilita operar o Kubernetes, o orquestrador de contêineres mais popular do mundo, como um serviço gerenciado. Os serviços KaaS geralmente são fornecidos na nuvem pública, mas algumas plataformas KaaS também podem ser implantadas no local. (Cloud Native Wiki. Kubernetes as a Service Providers. Aquasec.)

A funcionalidade básica de uma plataforma KaaS é implantar, gerenciar e manter clusters Kubernetes. Os principais recursos do Kubernetes as a Service incluem implantação de autoatendimento, atualizações do Kubernetes, escalabilidade e portabilidade em várias nuvens.

De acordo com a Aquasec as plataformas mais populares do KaaS são:

- *Google Kubernetes Engine* (GKE): O GKE foi a primeira oferta comercial do Kubernetes como serviço e é uma solução respeitada e madura, criada pelo

Google, que originalmente desenvolveu o Kubernetes. Faz parte do Google Cloud Platform (GCP).

- *Amazon Elastic Kubernetes Service* (EKS): EKS é um serviço usado para executar Kubernetes gerenciados na AWS. Ele pode implantar clusters em várias zonas de disponibilidade (AZ) com alta disponibilidade.
- *Red Hat OpenShift: OpenShift Dedicated* é um serviço gerenciado altamente personalizável que você pode usar para implantar o Kubernetes em qualquer nuvem (outras edições do serviço são específicas para AWS, Azure ou IBM Cloud).
- Docker EE: O Docker EE é um serviço de hospedagem fornecido pelo Docker, fabricante do popular mecanismo de contêiner Docker. Ele pode executar o Kubernetes e o Docker Swarm simultaneamente e oferece suporte a uma variedade de plug-ins certificados e imagens de contêiner.

Materiais e Métodos

Para esse trabalho utilizou-se o Minikube como primeiro exemplo pois ele traz uma maneira de se estudar o Kubernetes em sua própria máquina sem a necessidade de se ter mais de uma máquina para fazer um cluster, com o Minikube poderemos criar *deployments* etc.

No segundo exemplo faremos a instalação do Kubernetes em cluster e utilizaremos mais de uma máquina para demonstração dele.

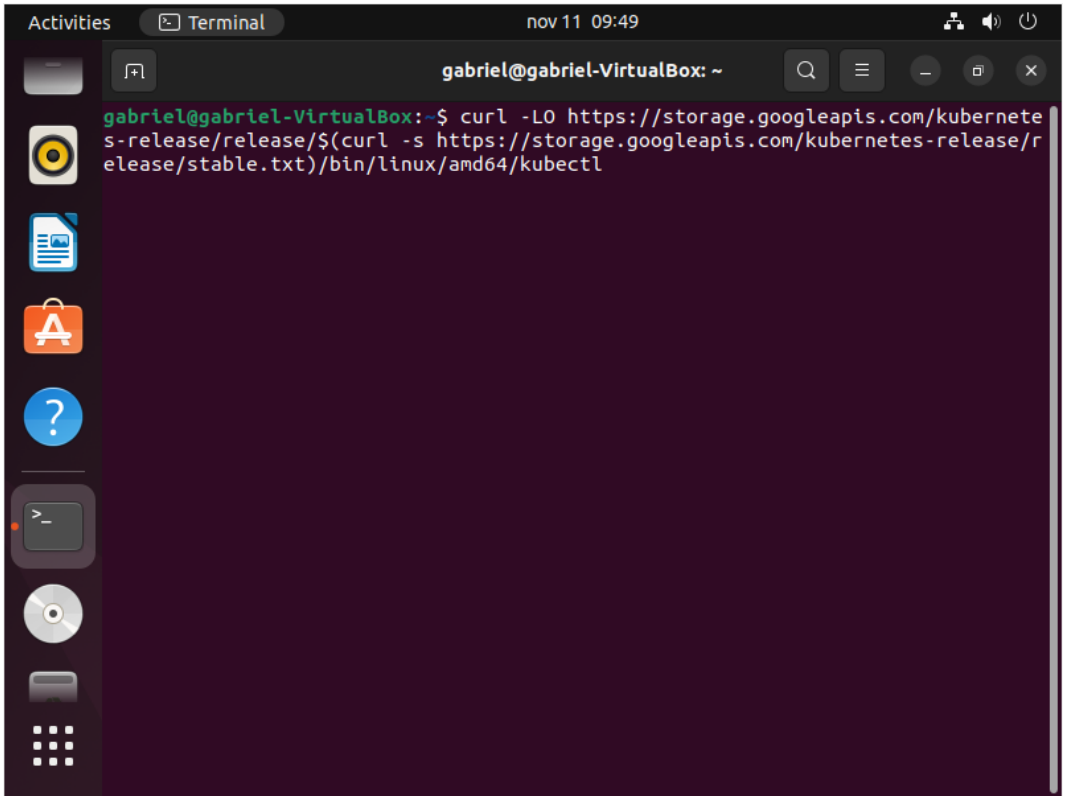
O Minikube é uma implementação do Kubernetes que cria uma VM na sua máquina física e implanta um cluster simples contendo apenas um *node*, com foco em facilitar o aprendizado e o desenvolvimento para os Kubernetes. Para iniciar o aprendizado você precisa apenas de um ambiente de máquina virtual. O Minikube pode ser instalado em sistemas Linux, MacOS e Windows. (Kubernetes. Usando Minikube para criar um cluster**.** Kubernetes IO.

Resultados

Utilizaremos uma máquina virtual Linux Ubuntu para realização da instalação e configuração do Minukube.

Antes de fazermos o download do Minukube, precisamos baixar o Kube Ctl, é o que irá fazer toda a gestão do nosso cluster e dos *deployments*.

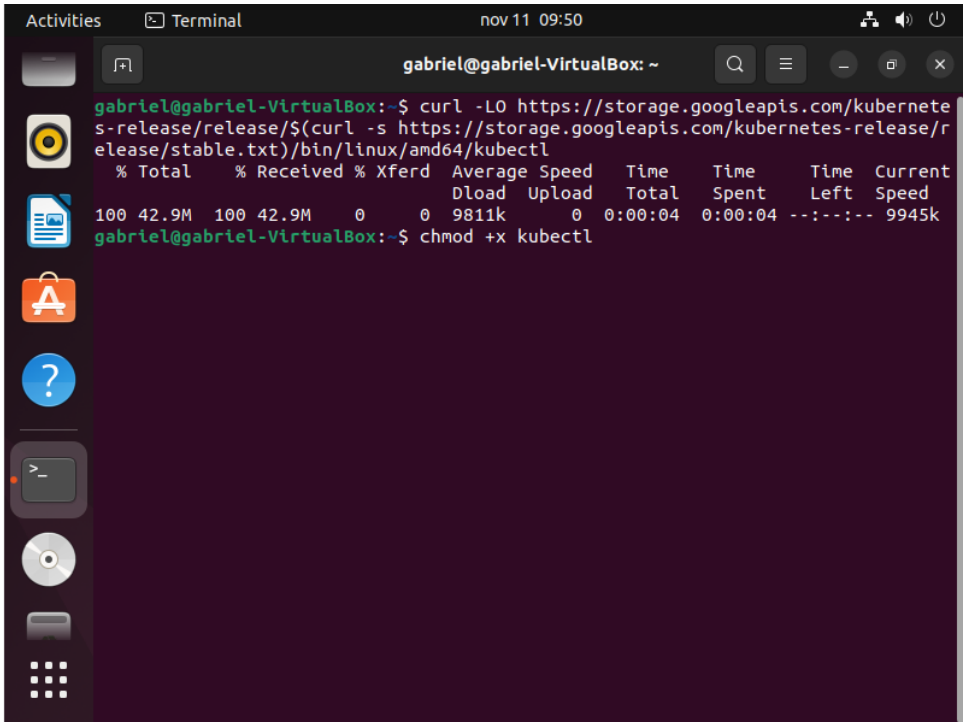
Figura 6 – Download do Kubectl



Fonte: Autores.

Após o download daremos a permissão para o Kubectl através do chmod.

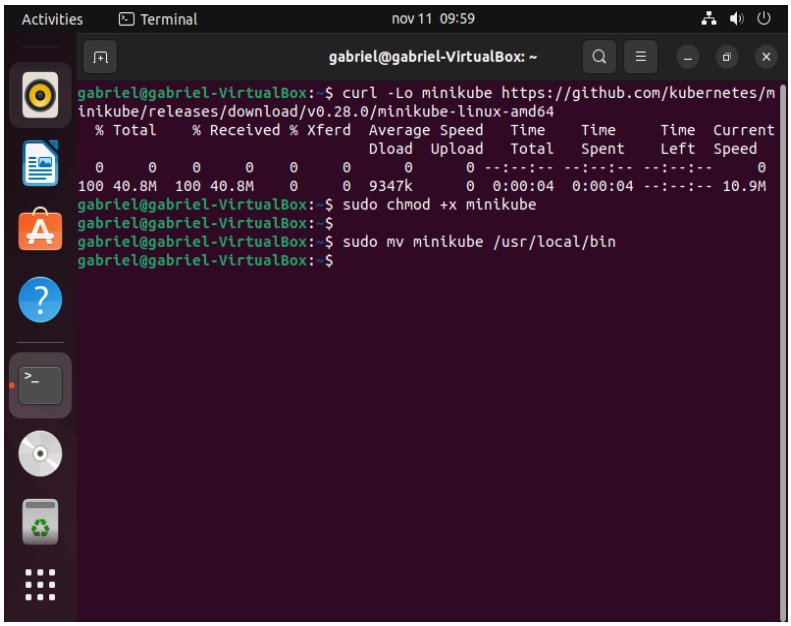
Figura 7 – Mudando permissão do Kubectl



Fonte: Autores.

Depois da mudança de permissão, movemos o Kubectl para a pasta local/bin, e em seguida fazemos o download do Minikube damos permissão a ele e mudamos para a pasta /local/bin.

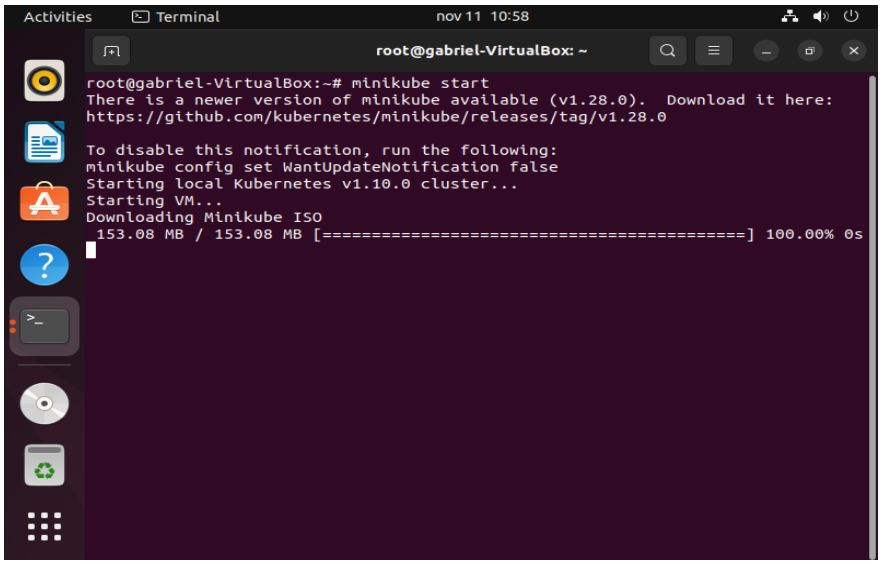
Figura 8 – Movendo Kubectl



Fonte: Autores.

Após a instalação podemos começar a iniciar o nosso Minukube, ou seja, criar a nossa estrutura de Kubernetes em um ambiente só.

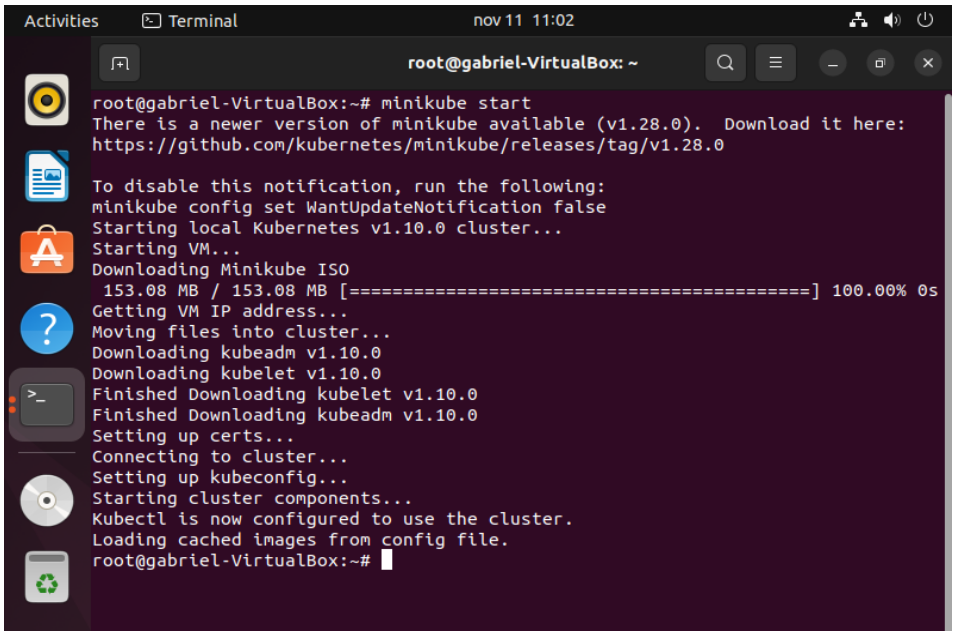
Figura 9 – Download ISO Minikube



Fonte: Autores.

Nessa etapa ela fará o download da ISO e vai rodar alguns testes que ele necessita.

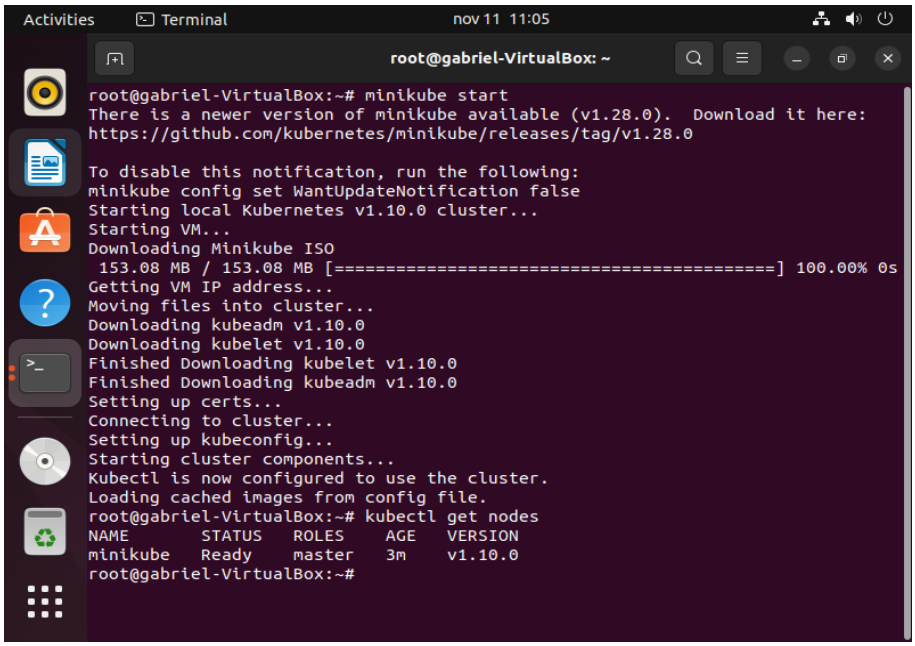
Figura 10 – Finalização da instalação do Minikube



Fonte: Autores.

Após a instalação a instalação rodaremos um comando do Kubectl (kubectl get *nodes*) para verificar se o Minukube está em funcionamento.

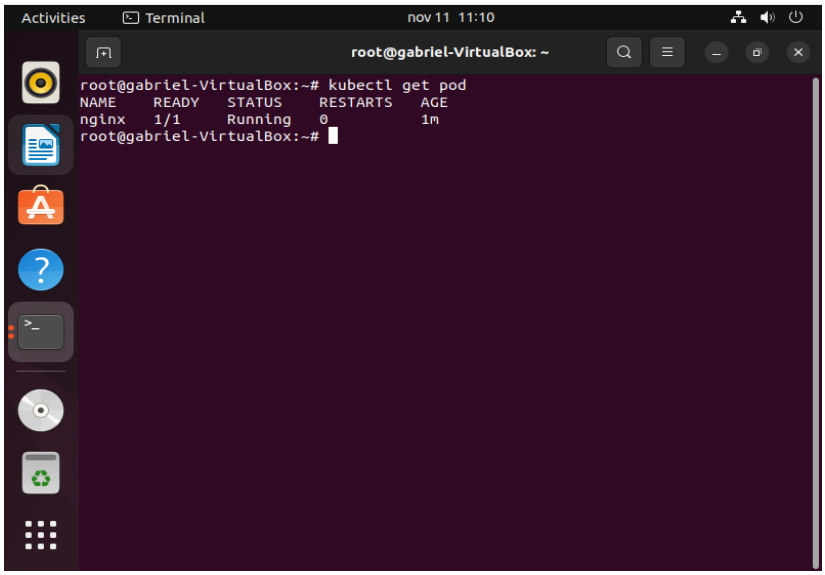
Figura 11 – Comando kubectl get *nodes*



Fonte: Autores.

Esse comando retorna todos os nós que temos no nosso cluster, como o minikube possuiu somente um ele é o único apresentado. Para o próximo teste faremos o primeiro *deployments*. O comando kubectl get pod retorna o nosso cluster.

Figura 12 – Comando kubectl get pod



Fonte: Autores.

Podemos ver na imagem acima que o primeiro *deployments* está em funcionamento com o nome de Nginx. Essa primeira configuração é apenas uma demonstração do que se pode realizar na orquestração de container utilizando apenas um *node*.

Na etapa seguinte é mostrado a instalação e configuração de um cluster Kubernetes, esse sim demonstrando o cluster com 3 *nodes*, de forma que pode ser aplicado até em ambientes empresariais de produção.

9. Cluster de Kubernetes

Um cluster de Kubernetes é um conjunto de *nodes* que executam aplicativos em contêineres, são mais leves e mais flexíveis do que máquinas virtuais, podendo ser gerenciados mais facilmente. Os clusters de Kubernetes são compostos por um *node* mestre e outros *nodes* de trabalho, sendo eles computadores físicos ou máquinas virtuais variando de acordo com o cluster. (Kubernetes. Componentes do Kubernetes. Kubernetes IO.)

De acordo com a VMWare estes são os 6 componentes principais:

Servidor de API: expõe uma interface REST para todos os recursos do Kubernetes. Este é o *front-end* do plano de controle do Kubernetes.

Programadores: insira contêineres com base em métricas e requisitos de recursos. Identifique os pods não atribuídos e selecione os nós nos quais eles são executados.

Controller Manager: Executa o processo do controlador e coordena o estado real do cluster com suas especificações desejadas. Gerencie controladores como nós, *endpoints* e replicação.

Kubelet: Garante que os contêineres estejam sendo executados em pods e interagindo com o mecanismo Docker (o programa padrão para criar e gerenciar contêineres). Selecione o conjunto de *PodSpecs* fornecido e verifique se os contêineres correspondentes estão totalmente funcionais.

Kube-proxy: gerencia a conectividade de rede e mantém as regras de rede entre os nós. Implementa o conceito de um serviço Kubernetes em cada nó de um determinado *cluster*.

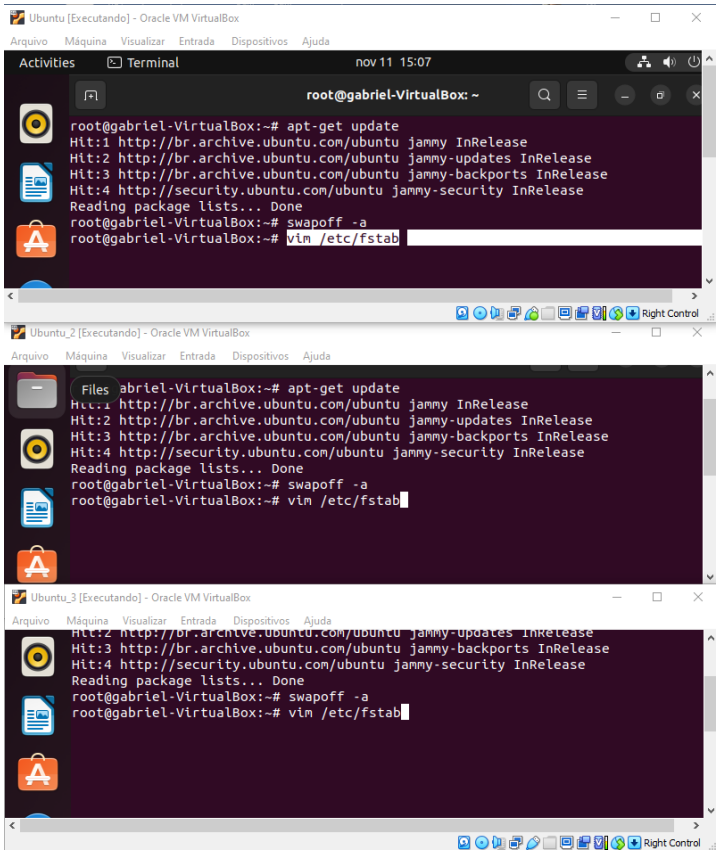
Etcd: Guarda todos os dados de cluster. Atua como um local de armazenamento de Kubernetes consistente e altamente disponível.

9.1 Instalação e configuração de um cluster Kubernetes

Faremos a instalação de um cluster Kubernetes utilizando 3 *nodes*, para isso usaremos 3 máquinas chamadas Ubuntu, Ubuntu_2 e Ubuntu_3. Antes de iniciarmos a instalação dos clusters, faremos um update nas 3 máquinas.

A figura abaixo representa as 3 máquinas utilizadas no desenvolvimento dos testes, ambas as máquinas estão executando o Linux Ubuntu versão 20.04.

Figura 13 – Máquinas virtuais Linux

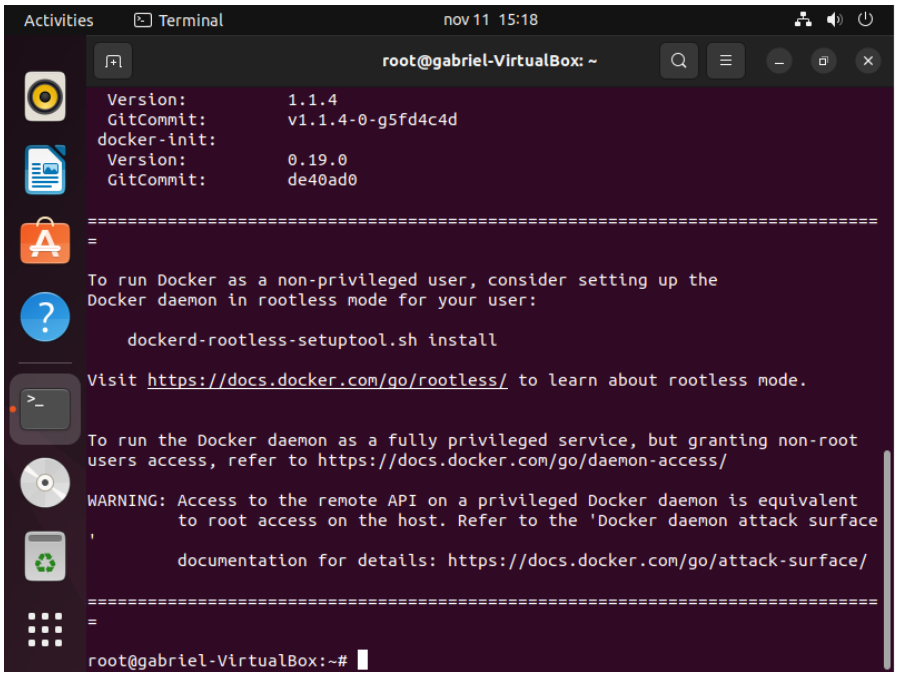


Fonte: Autores.

Fizemos o update nas 3 máquinas e desabilitamos o swap na inicialização utilizando o comando apt-get update e em seguida o swap off. Após o desligamento

do swap fazemos a instalação do Docker nas 3 máquinas Ubuntu utilizando o comando curl -fsSL https://get.docker.com | bash.

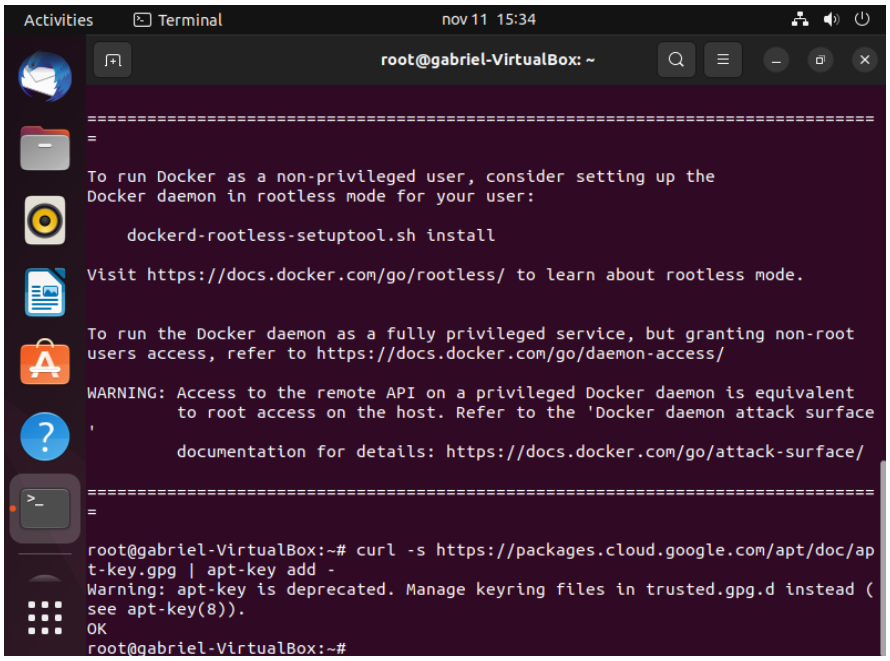
Figura 14 – Instalação do Docker



Fonte: Autores.

Depois do Docker instalado, faremos a instalação do repositório Kubernetes.

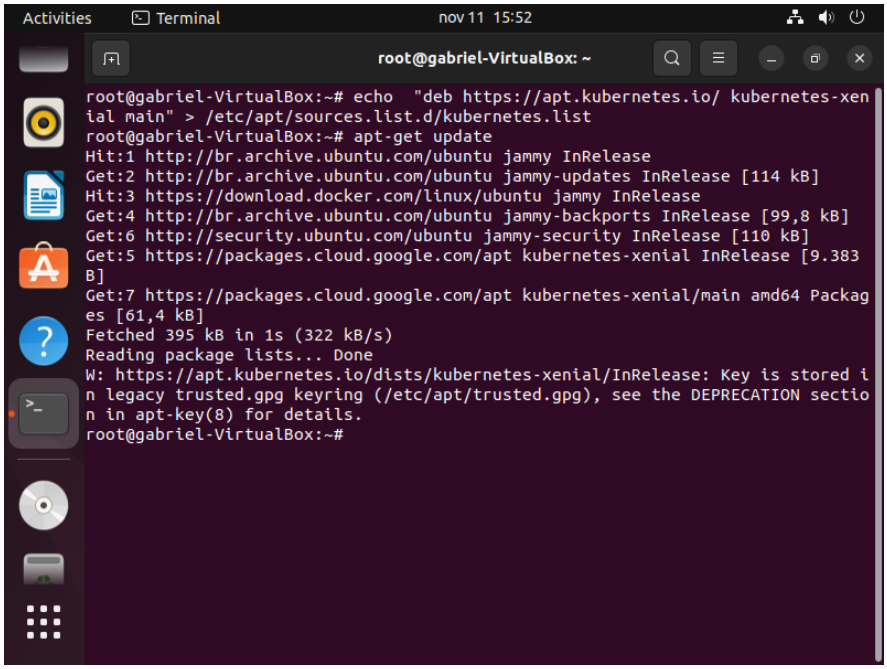
Figura 15 – Instalação do repositório Kubernetes



Fonte: Autores.

O repositório é adicionado usando o comando echo, que redireciona o repositório para o caminho colocado, em seguida devemos rodar o comando apt-get update para atualizar o local que foi salvo o repositório

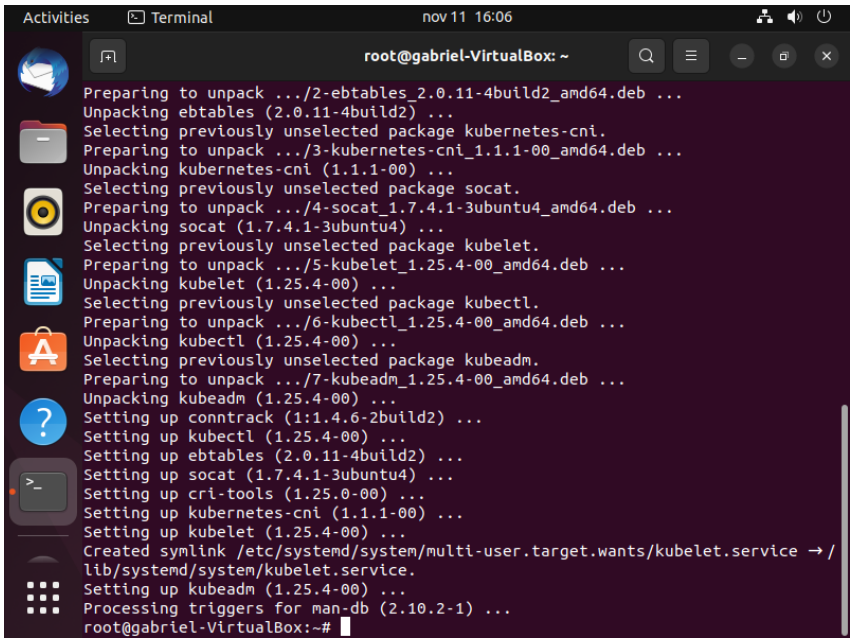
Figura 16 – Redirecionamento do repositório



Fonte: Autores.

Feito isso instalamos o kubelet, o kubectl e o kubeadm, o kubeadm fará a montagem do nosso cluster, já o kubectl opera o cluster, se queremos criar um *deployments* etc. utilizaremos o kubectl, e o kubelet é um agente do Kubernetes que é responsável por se comunicar com a api da versão master do Kubernetes.

Figura 17 – Instalando kubelet, kubectl e kubeadm

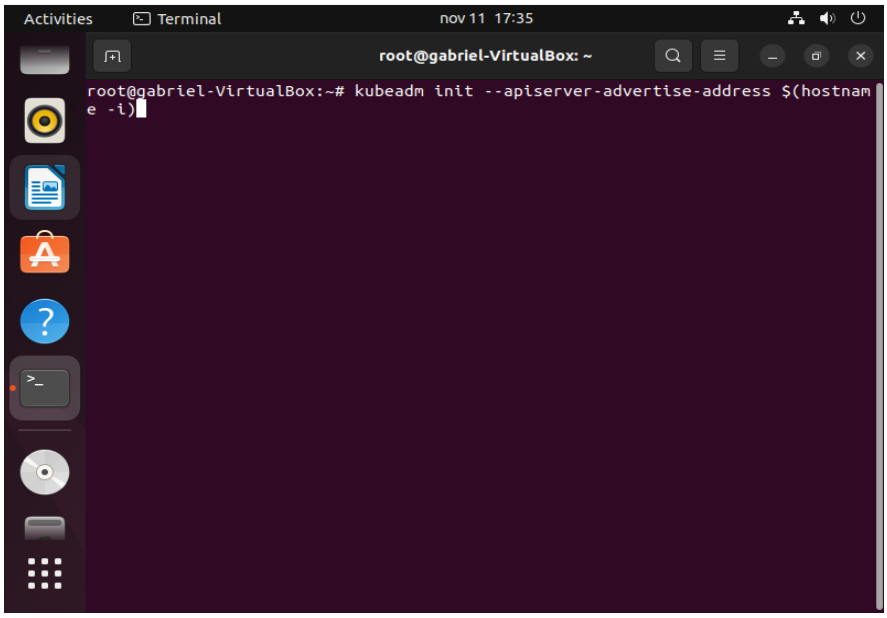


Fonte: Autores.

Possuímos o Docker instalado nas 3 máquinas assim como o Kubelet, Kubectl e Kubeadm, utilizaremos agora somente a máquina 1 (Ubuntu) pois essa foi eleita como a máquina master, onde o cluster será ativo através do Kubeadm.

Utilizaremos o seguinte comando para passarmos qual será o IP principal da master:

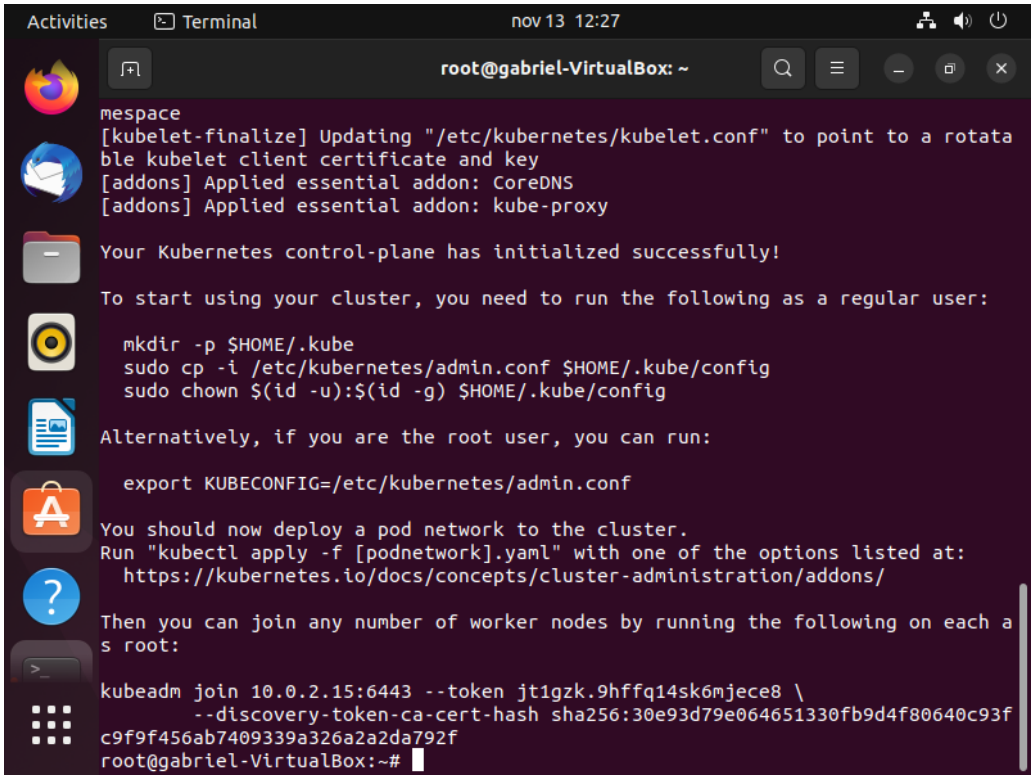
Figura 18 – Iniciando kubeadm



Fonte: Autores.

Após esse comando o cluster será iniciado, o kubeadm criará todo o ambiente necessário para o funcionamento do cluster. O resultado da saída é o mostrado na imagem a seguir.

Figura 19 – Kubeadm iniciado

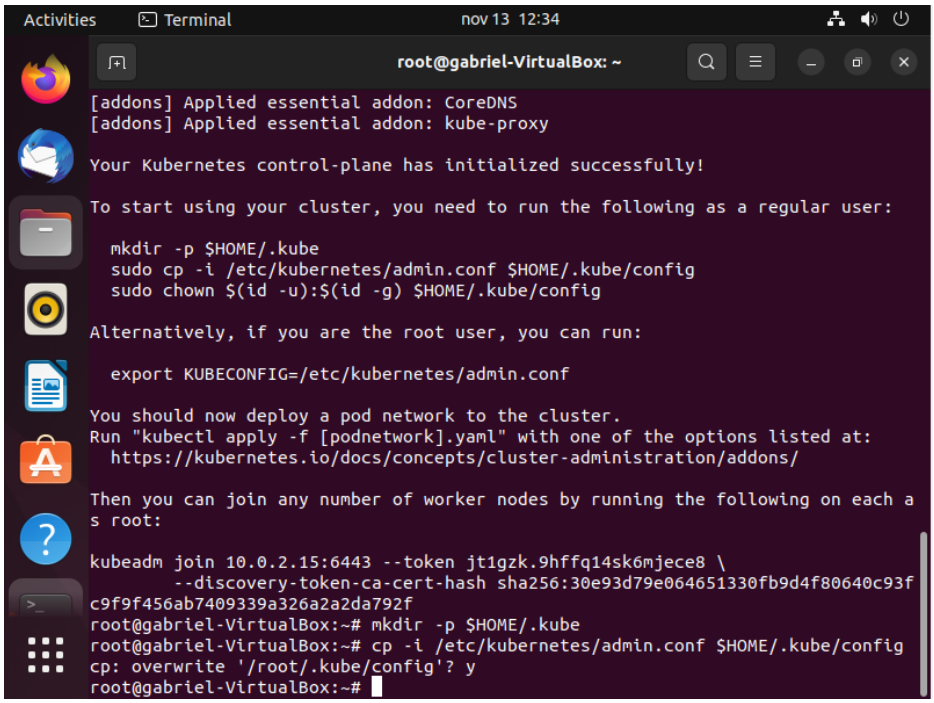


Fonte: Autores.

Precisamos criar uma estrutura de diretório no nosso diretório home, que guardará um arquivo de configuração que possuiu a chave para comunicação do kubectl com o cluster. Para isso utilizaremos o comando mkdir -p $HOME/ .kube.

Em seguida faremos a cópia do arquivo que foi criado em /etc/kubernetes, esse arquivo será jogado dentro do diretório. (.kube).

Figura 20 – Comando kubeadm join



Fonte: Autores.

Finalizadas as configurações podemos observar que o kubeadm retornou acima o comando kubeadm join e um IP com a sua chave de acesso, esse IP e chave é o utilizado para acessar o cluster através de outras máquinas.

Com esse acesso finalizado as máquinas secundárias entraram no cluster criado e hospedado na máquina master, finalizando assim o processo de criação e configuração de um cluster e seus *nodes*.

10. CONSIDERAÇÕES FINAIS

Pode-se concluir que o *Cloud Computing* entra para a TI e para o mercado de maneira definitiva, pois intensifica os três pilares da tecnologia da informação onde são aplicados, a disponibilidade, confidencialidade e a integridade. Com isso a disponibilidade recebe uma alta drástica em seu desempenho. Com o *cloud*, o acesso às informações passa a ser feito através de qualquer máquina conectada a uma rede de internet.

Foi analisado também as três formas principais de entrega do *Cloud Computing*, o SaaS, onde o software é entregue como serviço, o PaaS, onde a plataforma é entregue como o serviço, e o IaaS, onde a infraestrutura é entregue como o serviço, como cada um funciona, a forma que cada um é entregue, quais benefícios cada um proporciona para a infraestrutura de uma empresa, exemplos de como podem ser entregues para cada cliente, quando e por que optar por cada uma dessas formas de entrega do *Cloud* e que novos tipos de cada entrega podem ser desenvolvidos com um propósito especifico solicitado por um único cliente.

Junto com toda essa melhora e facilitação na entrega das formas de serviço em *Cloud*, surge também uma preocupação muito grande com a forma que os dados que são depositados nesses servidores na nuvem devem ser protegidos e quais são os meios legais para punição de crimes no ciberespaço. No Brasil, por exemplo, não existe uma lei que categorize os crimes cometidos no ciberespaço, apenas leis incompletas e fragmentadas sobre o tema.

Contudo, existem algumas formas encontradas com intenção de aumentar a segurança nesses servidores em nuvem, como por exemplo a implantação dos Kubernetes, que nada mais é que um sistema de código aberto para gerenciar aplicativos contidos nessas máquinas. O Kubernetes tem como função principal criar aplicativos fáceis de gerenciar e implantar em qualquer sistema baseados nos micros serviços nativos da nuvem e pode ser mais uma forma de entrega dos servidores *Cloud*.

Com foco em facilitar o aprendizado e familiarizarmos mais com a situação, fizemos um estudo e utilizamos um Minikube, um Kubernetes que contém apenas um *node* e implanta um cluster simples. Com esse exemplo, pudemos conhecer e entender um pouco mais uma das formas criadas para aumento da segurança e facilidade de atualização de arquivo dos servidores em nuvem.

REFERÊNCIAS

KASPERY. **O que é segurança na nuvem?** Kaspery. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-cloud-security>. Acesso em: 21 mai. 2022.

MALAR, João. **Risco para empresas com ataques cibernéticos supera o de pandemia, diz pesquisa.** CNN Brasil. Disponível em: <https://www.cnnbrasil.com.br/business/risco-para-empresas-com-ataques-ciberneticos-supera-o-de-pandemia-diz-pesquisa/>. Acesso em: 21 mai. 2022.

GRUSTNIY, Leonid. **Darknet, dark web, deep web e surface web – qual é a diferença?** Kaspery Daily. Disponível em: <https://www.kaspersky.com.br/blog/deep-web-dark-web-darknet-surface-web-difference/16921/>. Acesso em: 22 mai. 2022.

RODRIGUES, Renato. **Cibercrime reforça ataques contra a nuvem.** Kaspery Daily. Disponível em: <https://www.kaspersky.com.br/blog/hackers-ataques-cloud/18118/>. Acesso em: 11 mai. 2022.

VMWARE. **Segurança de nuvem.** VMWare. Disponível em: <https://www.vmware.com/br/topics/glossary/content/cloud-security.html>. Acesso em: 11 mai. 2022.

DEBECK, Charles. **X-Force Report:** No shortage of resources aimed at hacking cloud environments. Security Intelligence. Disponível em: <https://securityintelligence.com/posts/x-force-report-hacking-cloud-environments/>. Acesso em: 17 mai. 2022.

ZANNUTO, Bruno. **Segurança em Cloud Computing.** UFSCAR. São Paulo.

FERNANDES, Fristtram. **Riscos de Segurança em Cloud Computing.** Florianópolis. Disponível em: < https://www.researchgate.net/profile/Fristtram-Fernandes/publication/261878968_Riscos_de_segurancas_em_Cloud_Computing/links/0a85e535d88a45a1b6000000/Riscos-de-segurancas-em-Cloud-Computing.pdf>. Acesso em: 13 jun. 2022.

FERNANDO, Jeferson. **Série Descomplicando o Kubernetes.** YouTube, 19 jul. 2018. Disponível em: <https://www.youtube.com/watch?v=pV0nkr61XP8&list=PLf-O3X2-mxDmXQU-mJVgeaSL7Rtejvv0S&index=1>. Acesso em: 09 nov. de 2022.

ZANUTTO, Bruno Gonçalves. **Segurança em Cloud Computing.** Universidade Federal de São Carlos. Disponível em: <https://www.dcomp.ufscar.br/verdi/topicosCloud/Artigo-Seguranca-Cloud.pdf>. Acesso em: 12 ago. 2022.

STORM. **Cloud Security: o que é, benefícios e principais desafios.** Storm. Disponível em: < https://storm.kumulus.com.br/cloud-security/#:~:text=Assim%20como%20a%20computação%20em,atualizações%20de%20software%20e%20políticas. >. Acesso em: 13 nov. 2022.

GOOGLE, Learn. **O que é Kubernetes.** Google. Disponível em: <https://cloud.google.com/learn/what-is-kubernetes?hl=pt-br#:~:text=no%20Google%20Cloud.-,Kubernetes%20definido,em%20contêineres%20em%20qualquer%20lugar>. Acesso em: 04 nov. 2022.

VMWARE. **Cluster de Kubernetes.** VMWare. Disponível em: <https://www.vmware.com/br/topics/glossary/content/kubernetes-cluster.html>. Acesso em: 04 nov. 2022

NIST. **The NIST Definition of Cloud Computing.** NIST. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-145/final >. Acesso em: 10 set 2022