Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.31-47, 2023.
DOI: 10.18762/1982-4920.20230003

ANÁLISE E CRIAÇÃO DE UM AMBIENTE SEGURO COM ALTA DISPONIBILIDADE NA AWS

Danilo Nicoletti Amorim, Wdson de Oliveira

RESUMO

A computação em nuvem é a entrega sob demanda de recursos e aplicativos de TI sob via internet, cobrado na maioria das vezes de acordo com o uso, sem a necessidade de grandes investimentos em hardware. Isso possibilita que as empresas aumentem sua agilidade e flexibilidade, além de reduzir custos, permitindo que se concentrem em suas prioridades de negócios e projetos de inovação. A *Amazon Web Services* (AWS) é um provedor líder de serviços de computação em nuvem, oferecendo uma ampla gama de serviços altamente disponíveis e seguros que atendem às necessidades das organizações onde as empresas podem acessar novos recursos de TI em questão de minutos, permitindo que respondam rapidamente às demandas do mercado. Os serviços em nuvem também permitem que as empresas implantem facilmente seus aplicativos em vários locais do mundo, possibilitando redundância global e garantindo o menor tempo de acesso ou resposta possível, as empresas podem parar de gastar dinheiro com a execução e manutenção de data centers, Em resumo, a computação em nuvem oferece uma ampla gama de benefícios, incluindo maior agilidade, flexibilidade, redução de custos, enquanto a AWS oferece serviços altamente disponíveis e seguros para atender às necessidades de computação em nuvem das organizações.
Este estudo tem como intuito apresentar e analisar alguns dos principais serviços disponíveis na nuvem AWS bem como a possibilidade de atender as demandas das organizações, permitindo, assim, arquitetar e implementar serviços na nuvem, de modo a garantir segurança e alta disponibilidade.

Palavras-chave: Segurança da Informação; Computação em Nuvem; AWS

Abstract

Cloud computing is the on-demand delivery of IT resources and applications over the internet, typically billed based on usage, without the need for substantial investments in hardware. This enables organizations to increase their agility and flexibility, while also reducing costs, allowing them to focus on their business priorities and innovation projects. Amazon Web Services (AWS) is a leading provider of cloud computing services, offering a wide range of highly available and secure services that meet the needs of organizations, where companies can access new IT resources within minutes, enabling them to respond swiftly to market demands. Cloud services also allow organizations to easily deploy their applications across multiple global locations, ensuring global redundancy and minimizing access or response time. As a

result, companies can stop spending on the operation and maintenance of data centers. In summary, cloud computing provides a wide array of benefits, including enhanced agility, flexibility, and cost reduction, while AWS offers highly available and secure services to meet the cloud computing needs of organizations.
This study aims to present and analyze some of the key services available on the AWS cloud, as well as their ability to meet organizational demands, thereby enabling the design and implementation of cloud services that ensure security and high availability.

Keywords: Information Security; Cloud Computing; AWS

1 INTRODUÇÃO

Nos últimos anos, houve um aumento considerável sobre a utilização do termo *Cloud Computing*, por meio do qual é possível utilizar uma gama de serviços computacionais e pagá-los somente pela utilização, possibilitando que as empresas deixem de se preocupar por exemplo, com a administração, instalações e manutenções de seus data centers locais, bem como licenciamentos e futuras expansões, recursos ociosos, defasados, descartes, entre outros além de possibilitar um ambiente altamente seguro e disponível.

Os ambientes provisionados na nuvem podem estar acessíveis de qualquer localidade geográfica do mundo, além de possuir de forma dinâmica a capacidade de aumentar os recursos computacionais automaticamente em questões de minutos para atender desde um pico de uso da sua aplicação, e nos momentos de ociosidade flutuar para baixo, ou até mesmo subir uma cópia ou novo ambiente em outra localidade.

Entretanto, uma das maiores dificuldades encontradas para adoção e utilização da nuvem é devido às resistências de algumas empresas em utilizá-la, seja por serem empresas tradicionais que acreditam que o seu *data center* e instalações são melhores e mais seguros, ou por se considerarem pequenas e acreditar que nuvem é recomendada apenas para empresas de médio e grande porte. Além disso, nota-se que, em geral, as empresas têm receios por não ter tanto conhecimento sobre o funcionamento da nuvem.

Outro ponto que pode gerar receio nas pessoas e empresas de migrarem os seus serviços para a nuvens se dá pelo medo de compartilharem suas informações e não saberem ao certo onde os dados estarão alocados, o que gera insegurança.

Contudo, é justamente essa característica que proporciona maior segurança dos dados na nuvem.

Diante desta problemática, é importante explicar como a infraestrutura global da AWS é estruturada, além dos principais fatores e considerações que se deve levar em conta para poder criar um ambiente do zero, migrar totalmente um ambiente *on premisse* (ambiente interno de uma empresa onde os recursos e infraestrutura se encontram) para nuvem ou se trabalhar com uma solução hibrida, possibilitando aos empresários, CEO (*Chief Executive Office)* que seria a pessoa que possui a maior autoridade dentro de uma empresa e normalmente possuem o cargo de presidente ou diretor(a) geral) e qualquer pessoa interessada a conhecer um pouco mais sobre a *Cloud* e ter mais segurança e confiança para auxiliar na tomada de decisão se for–ou não pra nuvem e a partir disso responder a seguinte pergunta.

De acordo com o contexto exposta acima: Como podemos através de uma análise definir a criação de um ambiente seguro com alta disponibilidade na AWS?

No mundo globalizado em que vivemos hoje em dia, houve um aumento considerado no crescimento, utilização de serviços computacionais e aplicativos pelas pessoas e empresas, porém muitos serviços e aplicativos rodam atrás de sistemas desatualizados e/ou infraestrutura algumas vezes precária, devido ao fato de que nem todas as empresas conseguem acompanhar e prover infraestrutura, equipamentos decentes para atender esta demanda, isto acaba abrindo brechas na segurança física e lógica, se tornando alvo perfeito para pessoas mal intencionadas e que possuem um certo conhecimento em ataques cibernéticos, possibilitando que sua aplicação ou sistemas fiquem inoperantes ou inacessíveis por horas ou dias e ocasionado um grande transtorno e prejuízo para empresa provedora do serviço e para os clientes que utilizam o seus sistemas e aplicativos.

Com a computação em nuvem é permitido que se utilize sempre hardwares atualizados, com tecnologias mais robustas, softwares atualizados para atender a qualquer atividade do negócio.

A computação em nuvem permite que o contratante possa se precaver de alguns incidentes e obter um ambiente altamente escalável para atender algumas demandas específicas, como por exemplo, os tradicionais eventos Dia das Mães, Dias do País, Black Friday, Natal, etc., onde normalmente o número de requisições e

acessos aos sites de compras, por exemplo, acaba sendo muito maior se comparado aos outros dias do ano, podendo até mesmo fazer com que ele fique indisponível, lento, entre outras coisas, caso o número de requisições e acesso seja maior do que ele possa suportar.

Por se tratar de um ambiente resiliente e escalável, a nuvem possibilita que seu contratante modifique rapidamente os recursos utilizados que, em um primeiro momento, atendiam à demanda, mas que com o passar de algumas semanas ou meses, não consiga mais atendê-la em razão de diversos fatores, como por exemplo, um aumento massivo na utilização da nuvem, atualizações, entre outros.

Atualmente, existem vários provedores de nuvem públicas e privadas, enquanto a nuvem privada é oferecida pela Internet ou por uma rede interna privada exclusiva para usuários selecionados, a nuvem pública é o serviço gratuito ou pago sob demanda oferecido por provedores terceirizados, como por exemplo, AWS, Azure, Oracle Cloud, Google Cloud, entre outros, porém muitas pessoas e empresas possuem dúvidas e certos receios sobre armazenar ou migrar seus dados, aplicações e sistemas para a nuvem.

2 REFERENCIAL TEÓRICO

Este capítulo tem como objetivo descrever o contexto dos conceitos discutidos nesse artigo.

2.1 Segurança da informação

De acordo com Adil (2019), Segurança da Informação tem como finalidade realizar a proteção dos dados de uma pessoa física ou jurídica contra ataques digitais, falhas humanas, desastres ambientais e tecnológicos através de um conjunto de ações e recursos utilizados para deixar a informação livre de riscos e não está somente relacionado apenas a computadores, tablets, celulares, sistemas, mídias de armazenamento, arquivos digitais etc.., a segurança da informação pode incluir também pessoas, ambientes e documentos impressos, etc..

A informação é poder na mão de quem a detém e através dela é possível tomar decisões e resolver problemas.

Os pilares da segurança da Informação são a Confidencialidade, Integridade, Disponibilidade e Autenticidade.

De acordo com Alkmin (2021) a confidencialidade restringe o acesso da informação somente para as instituições autorizadas pelo proprietário da informação. Um dos grandes problemas e desafios que ocorre hoje em dia, principalmente nas empresas, é a falta de um controle de acesso eficaz seja ele físico, em redes, aplicações ou arquivos, é importante ter um controle de acesso bem definido para garantir que a confidencialidade possa estar em conformidade, um exemplo de confidencialidade é o salário de um funcionário, ele deve ser de conhecimento apenas do setor de recursos humanos e do próprio funcionário.

De acordo com Alkmin (2021) a integridade deve garantir que informação seja preservada e modificada apenas por pessoas ou sistemas autorizadas, não podendo haver perdas, modificações e nem acréscimos de informação, seja elas de forma intencional ou acidental, sendo necessário garantir o ciclo de vida da informação (nascimento, manutenção e destruição) um exemplo de integridade violada seria por exemplo o download de um arquivo que contabiliza 50Mb e hash L&Mbr@d0PS!, porém ao terminar de baixá-lo, é constado que o arquivo possui os mesmos 50Mb, mas com o hash EaP!ZZ4CaC40.

De acordo com Alkmin (2021) a disponibilidade é o fato de a informação estar sempre disponível quando solicitada por alguém autorizada. Um exemplo de disponibilidade é uma equipe da Polícia Federal que atua remotamente em conjunto com sistemas de monitoramento dos aeroportos do Brasil e acaba perdendo a conexão com sistema de reconhecimento facial dos procurados e foragidos da justiça, com isso impossibilita o recebimento da informação em tempo hábil as vezes, correndo-se o risco de deixar algum procurado ou foragido escapar, ferindo assim o princípio da disponibilidade.

De acordo com Alkmin (2021), a autenticidade deve garantir que determinada informação seja confiável e vinda do verdadeiro remetente que a enviou, além de não ter sido alvo mutações podendo torná-la maliciosa. Um exemplo de autenticidade são SPAMs que são enviados por golpistas através de *phishing* em e-mails, eles não são de fato autênticos, porque não são enviados oficialmente por quem digam que são.

É importante deixar claro que a Segurança da Informação não está somente relacionada aos pilares de segurança, ataques cibernéticos que infectam dispositivos numa rede corporativa, mas também a procedimentos, métodos e comportamentos adotados para evitar que as informações fiquem vulneráveis, portanto, além dos pilares, outros pontos são fundamentais para enfrentar as ciberameaças.

2.2 Computação em Nuvem

Segundo Wittig (2016, p. 27) a computação em nuvem foi definida pela NIST (National Institute of Standards and Techonology) como:

> A computação em nuvem é um modelo para permitir acesso de rede onipresente, conveniente e sob demanda a um pool compartilhado de recursos de computação configuráveis (por exemplo, redes, servidores, armazenamento, aplicações e serviços) que podem ser fornecidos e liberados rapidamente com pouco esforço de gerenciamento ou interação do provedor de serviços.

Em geral, as nuvens são divididas da seguinte forma:

- Pública – Nuvem gerenciada por uma empresa e aberta para uso pelo público geral.
- Privada – Nuvem que virtualiza e compartilha a infraestrutura de TI dentro de uma única empresa.
- Híbrida – Combinação de nuvem pública e privada.

Os serviços de computação em nuvem possuem 3 classificações de serviços conhecidas como IasS (Infraestrutura como serviço), PaaS (Plataforma como serviço) e SaaS (Software como serviço).

De acordo com Tabelini (2022), a Infraestrutura como serviço são os recursos de um data center onde toda a responsabilidade física do local e dos equipamentos é de responsabilidade do provedor *cloud* que através da virtualização oferecem aos clientes servidores, redes, sistemas operacionais, armazenamentos que podem ser utilizados conforme a necessidade sendo altamente escalável e o mais flexível dentre as 3 categorias, porém a responsabilidade do backup, acessos, atualização dos patchs de segurança do sistema operacional, softwares e aplicações que vierem a ser instalados bem como o suporte deles são do cliente.

De acordo com Microsoft (2022), a Plataforma como serviço é ideal para que desenvolvedores possam criar, gerenciar aplicativos para web, ela oferece suporte ao ciclo de vida do aplicativo web completo desde a fase de compilação, testes, implantação, gerenciamento e atualização, permitindo reduzir o tempo de programação, desenvolver para várias plataformas, também permite realizar a análise de dados e BI, faz com que o contratante deixe se preocupar com a compra e gerenciamento de licenças dos programas, infraestrutura, orquestradores de contêineres, preocupando-se exclusivamente com os aplicativos e serviços que desenvolve e deixando com o que o provedor cloud gerencie e administre o resto

De acordo com Tabelini (2022), o Software como Serviço permite que a maioria dos aplicativos e softwares sejam executados diretamente pelo navegador web do cliente, eliminado a necessidade de se realizar download e instalação em computadores, o cliente não tem necessidade de se preocupar com atualizações do sistema operacional onde a aplicação ou software se encontram instalados, patches de segurança, problemas com servidores, armazenamento, sendo de responsabilidade do cliente os acessos e configurações.

2.3 Principais Serviços AWS

De acordo com a AWS (2023), atualmente existem mais de 200 serviços disponíveis que estão distribuídos em diversas categorias como por exemplo Computação, Contêineres, Armazenamento, Banco de Dados, Migração e Transferência, Redes e entrega de conteúdo, Segurança Identidade e Conformidade, Gerenciamento de Custos da AWS, IoT, Machine Learning etc., dentre todos os serviços disponíveis atualmente, foram escolhidos alguns dos que são mais utilizados atualmente e que poderão ser disponibilizados durante a implantação que será realizada. Todos os serviços abaixo estão disponíveis para consulta e maiores informações no site da AWS.

* AWS Auto Scalling é um serviço no qual permite a tomada de decisões de escalabilidade mais inteligente de forma automática em minutos de alguns serviços provisionados como as instancias EC2, ECS, EKS, FARGATE, RDS, Dynamo e Aurora através de uma definição das *triggers de escala* (“gatilhos”), quais os limites e quantidades de instâncias, entre outros, que ele irá acompanhar a flutuação dessa métricas de *threshold* (limite) e poderá aumentar ou diminuir a quantidade de recur-

sos, para atender as flutuações das demandas esporádicas e especificas de acordo com as métricas definidas, o serviço em si é gratuito e o contratante pagará somente pelos serviços utilizados em conjunto para o monitoramento que podem ser utilizados e os serviços provisionados.

* AWS Cloud Front é serviço de cache no qual se permite melhorar a experiência do usuário com o tempo de resposta de uma solicitação de conteúdos estáticos e dinâmicos da web através da distribuição dos conteúdos pela rede global dos data centers denominados como ponto de presença que estão espalhados pelo mundo através dos cinco continentes.

* AWS Backup é um serviço gerenciado de backup e recuperação podendo-se definir políticas de backup e retenção em um único lugar, automatizar o processo de backup, monitorar e gerenciar backups e restaurações de forma eficiente, além de simplificar a conformidade e auditoria de backup. Ele também permite restaurar os dados de forma granular ou completa em minutos, independentemente da escala do ambiente, sendo uma solução segura e escalável que ajuda a proteger os dados contra falhas de hardware, erros humanos, ameaças cibernéticas, desastres naturais e outras situações que possam causar a perda de dados críticos. Com ele, é possível minimizar o tempo de inatividade e os custos associados à recuperação de dados e garantir a continuidade dos negócios.

* AWS Cloud Trail é um serviço que já vem ativo por padrão em todas as contas da AWS, ele é responsável por registrar todas as chamadas de API na AWS, sejam elas através da console de gerenciamento web da conta, CLI (“Command Line Interface” ou Interface de Linha de Comando) ou SDK (“*Software Development Kit*”ou Kit de Desenvolvimento de Software) com suas respectivas datas, horários, endereço de IP de origem do chamador da API, os parâmetros de solicitação bem e os elementos de respostas retornados pelo serviço e entrega tudo arquivos de log para auditoria e revisão no qual são armazenados atividades referente aos últimos 90 dias, caso seja necessário reter esses logs por um período superior a 90 dias, acabará sendo necessário realizar algumas configurações para armazenar os logs em um *bucket* do s3 onde será realizado a cobrança de armazenamento dos objetos cobrado de acordo com os as regras de cobrança do S3.

* AWS IAM é um serviço de gerenciamento de identidade de acesso totalmente gratuito, ele possibilita que as organizações possam controlar com segurança o

acesso aos serviços e recursos da AWS para seus respectivos usuários. É através dele que é realizado a criação e gerenciamento de usuários e grupos da AWS, bem como as permissões e negações de acessos para os recursos da AWS, por questões de boas práticas e segurança todos os usuários e grupos criados através do IAM vem com acesso negado a todos os serviços na AWS cabendo ao administrador da conta conceder as permissões de acessos para estes usuários e grupos.

* AWS EBS ("*Elastic Block Store"*) é um serviço de armazenamento em nível de bloco para uso com instancias do Amazon EC2 e do RDS (*"Relational Database Service"*), em outras palavras é o que conhecemos como HD do computador, servidor etc., porém cada EBS é replicado automaticamente dentro da sua Zona de Disponibilidade para protegê-lo contra falhas de componentes, oferecendo alta disponibilidade e durabilidade, existem vários tipos de EBS que diferem nas suas características de desempenho e preço, os tipos de volumes do EBS são Volumes Magnéticos, SSD de uso geral, SSD IOPS, HDD com taxa de transferência otimizada e HDD frio que serão mais detalhados na próxima etapa deste projeto de graduação.

* AWS EC2 (*Elalist Compute Cloud*) é um serviço que fornece a capacidade de computação redimensionável na nuvem, em outras palavras são os servidores que serão utilizadas na nuvem, ele permite que as organizações obtenham e configurem servidores virtuais nos datacenters da AWS e aproveitem esses recursos para criar e hospedar sistemas. Existe uma gama de variedades de instâncias, sistemas operacionais e configurações de recursos (memória, CPU, Armazenamento, etc.) permitindo que as organizações iniciem recursos de computação com uma variedade de sistemas operacionais, carreguem-nos com aplicativos personalizados e gerenciem permissões de acesso à rede, mantendo controle completo, permitindo também que vários volumes do Amazon EBS possam ser anexados a uma única instância do Amazon EC2, embora um volume do EBS possa ser anexado apenas a uma única instância de cada vez.

* AWS ELB (*Elastic Load Balancer*) é um serviço que pode ser público ou privado, é disponibilizado por região para balanceamento de carga permitindo distribuir automaticamente o tráfego entre várias instâncias do Amazon EC2, ECS, EKS, FARGATE e do RDS em uma ou mais zonas de disponibilidade garantindo a consistência em equilibrar a carga da solicitação em mais de um serviço permitindo assim

obter alta disponibilidade em seus aplicativos. O ELB é dividido em quatro tipos, sendo eles o ALB, NLB, Classic Load Balancer e o Gateway Load Balancer.

- AWS ELB - ALB (*Applications Load Balancer*) é um balanceador de carga em camada de rede que opera na camada 7 do modelo OSI praticamente (HTTP/HTTPS), na prática, ele é um balanceador de carga que consegue fazer a inspeção do *payload* das requisições, permitindo criar regras de roteamento baseado em URL baseada em *path* (caminhos) distintos (exemplo professorwdson.com.br, peritaisadmagnani.com.br), também pode ser feito de acordo com o *header* (cabeçalho) ou *cookie web* (arquivo de texto simples armazenado pelo navegador).
- AWS ELB- NBL (Network Load Balancer) é um balanceador de carga em camada de rede com suporte a protocolos TCP e UDP, ele trata IP e Porta da Camada 4 do modelo OSI, podendo processar milhões de requisições por segundo.
- AWS Classic Load Balancer é um balanceador de carga antigo da AWS no qual já está em desuso, mas ainda é mantido pois tem aplicações e sistemas que o utilizam e possui uma mescla de tratativas entre as camadas 4 e 7 do ALB e NLB.
- AWS Gateway Load Balancer é um balanceador de carga que opera na camada 3 do modelo OSI, ele só trata IP e é utilizado único e exclusivamente quando se tem uma implementação de Firewall Virtual na AWS, porém acaba se tornando um desafio enorme fazer a gestão do balanceamento de carga quando se tem ali alta disponibilidade, e de como será tratado o encaminhamento das conexões, as regras de entrada e saída.

* AWS RDS (*Relational Database Services)* é um serviço que fornece suporte para seis mecanismos populares de banco de dados relacional como MySQL, Oracle,PostgreeSQL, Microsoft SQL Server, Maria DB e Amazon Aurora, você também optar por executar qualquer mecanismo de banco de dados usando instâncias do Amazon EC2 para Windows ou Windows e gerenciar você mesmo a instalação e administração, mas com o RDS o contratante não precisa se preocupar com as instalações de patch de segurança, atualizações etc. É importante ressaltar que no por-

tifólio da AWS existem muitos outros tipos de serviços voltados para banco de dados, abaixo estará um breve resumo sobre alguns deles para conhecê-los.

- Amazon Aurora é uma implementação gerenciada do MySQL e/ou Postgree no modelo que a AWS realizou uma junção do melhor de ambos em um projeto open source, no qual ela oferece suporte comercial dele.
- Amazon Redshift é um serviço de banco de dados colunar otimizado por exemplo para execução de querys em parelho, opera numa arquitetura distribuída num padrão MPP e acaba sendo muito utilizado por analitcs.
- Amazon Dynamo DB é um serviço considerado como carro chefe dos bancos de dados não relacionais que opera no modelo *key-value* (chave valor)
- Amazon Document DB é um banco de dados orientado a documento que oferece compatibilidade com o MongoDB

* AWS Route53 é um serviço DNS (*"Domain Name Server"* ou Servidor de Resoluções de Nomes de Domínio) que é responsável por rotear o tráfego da internet para o seu site, convertendo nomes de domínio amigáveis em endereços IP, quando alguém digita seu nome de domínio em um navegador, aplicativo ou envia um e-mail, uma solicitação de DNS do Route53 mais próximo em uma rede global de servidores DNS autorizados será responsável por fazer essa conversão e direcionar o encaminhamento.

* AWS S3 (Serviço de Armazenamento Simples) é um serviço que fornece armazenamento de objetos altamente durável e escalável e que lida com quantidades praticamente ilimitadas de dados e grandes número de usuários simultâneos. As organizações podem armazenar qualquer número de objetos de qualquer tipo, como páginas HTML, arquivos de código-fonte, arquivos de imagem e dados criptografados e acessá-los usando protocolos baseados em HTTP. A única ressalva é que esses dados não excedam a 5TB. O S3 acaba fornecendo armazenamento econômico de objetos para uma ampla variedade de casos de uso, incluindo backup e recuperação, análise de big data, recuperação de desastres, aplicativos em nuvem e distribuição de conteúdo. A cobrança é realizada por cada GB que armazenar no S3 e ocorrerá pequenas cobranças por cada solicitação e dados transferidos.

Para transferências de dados em alta escala, a AWS disponibiliza também o *Snowball*, que é um serviço que acelera a transferência de grandes quantidades de dados para dentro e fora da AWS usando dispositivos de armazenamento físico, ignorando a internet, os dados são copiados para um dispositivo na origem, seja ele um datacenter *on premisse* ou uma região da AWS, enviados por mecanismo de envio padrão e em seguida, copiados para o destino no qual pode ser um datacenter *on premisse* ou uma região da AWS, mas este serviço não será tratado no projeto.

* AWS VPC é a camada de rede da AWS a qual permite a criação da sua própria rede virtual, é possível controlar vários aspectos como a escolha do próprio intervalo de endereços IP, criar sub-redes, configurar tabelas de rotas, gateways de rede e configurações de segurança. Em uma região da AWS, pode-se criar várias VPCs onde cada VPC é logicamente isolada uma da outra, mesmo que compartilhe o mesmo espaço de endereço IP. Ao se criar uma VPC deve-se especificar o intervalo de endereços IPv4, este intervalo pode ser tão grande quanto um /16, no qual possui 65.536 endereços IP disponíveis ou tão pequeno quanto um /28, no qual possui 16 endereços IP disponíveis, estes endereços não podem se sobrepor a nenhuma outra rede a qual eles devem ser conectados, além de que o intervalo não pode ser alterado após a criação, se necessário a VPC deverá ser excluída e criada novamente.

Uma VPC consiste nos seguintes componentes:

- Sub-redes
- Tabelas de rotas
- Conjunto de opções protocolo DHCP (Dynamic, Host Configuration Protocol)
- Listas de controle de acesso à rede (ACLs)

Uma VPC pode possuir os seguintes componentes opcionais:

- Gateways da internet (IGWs)
- Endereços de IP elástico “fixo” (EIP)
- Endpoints,
- Peering,
- Instâncias de conversão de endereço de rede (NATs) e gateways NAT
- Gateway Privado Virtual (VPG), Gateways de Clientes (CGWs) e Redes Privadas Virtuais (VPNs)

3 METODOLOGIA

A fim de atingir os objetivos delineados para o trabalho, se fez necessário efetuar uma pesquisa para o levantamento das informações através das documentações oficiais disponibilizadas na página oficial da AWS a respeito da segurança na nuvem, dos seus serviços, indicações, casos de uso, preços, regiões que possuem determinados serviços ou não. Além disso, foi consultado alguns profissionais com amplo conhecimento de arquitetura de soluções AWS que são referências no assunto e certificados pela própria AWS como Marlon Caeton Mitidieri (Co Founder na BeOnUp - Soluções de TI na nuvem), Lucas Barbosa da Silva e Ozeias Oliveira da Silva todos profissionais certificados como Arquitetos de Soluções Professional AWS e Coordenadores dos times Cloud, Segurança, Infraestrutura e Monitoramento da Beonup onde foi possível realizar um levantamento das melhores práticas utilizadas no dia a dia para as combinações de serviços, análise de requisitos, bem como as principais dificuldades e desafios encontrados antes, durante e após a criação ou migração de um ambiente para nuvem pois muitas coisas na teoria são mil maravilhas, mas na prática não.

O levantamento bibliográfico também contou com a pesquisa em livros, sites, vídeos.

A fim de demonstrar na prática o funcionamento de alguns serviços da AWS, foi realizado a implementação de um simples ambiente na nuvem AWS com alta disponibilidade e seguro, onde será demonstrado em sala a simulação de tentativas de acessos ao ambiente de locais não autorizados, e também será realizada a queda forçada de um dos serviços do ambiente para que seja acionado automaticamente a redundância que se encontra em outra zona de disponibilidade no qual está localizado fisicamente a mais de 80 km de distância mantendo o serviço no ar.

4 RESULTADOS E DISCUSSÃO

A AWS possui um modelo de responsabilidade compartilhada que é projetado para garantir a segurança e a conformidade dos serviços oferecidos. Neste modelo, a AWS é responsável pela segurança da infraestrutura física da nuvem, enquanto os

usuários da nuvem são responsáveis pela segurança dos aplicativos, dados e sistemas que são executados na nuvem.

Este modelo de responsabilidade compartilhada é detalhado em uma documentação disponibilizada pela AWS, que define as responsabilidades específicas da AWS e dos clientes em relação à segurança. O modelo de responsabilidade compartilhada da AWS é uma abordagem que permite que a AWS e seus clientes trabalhem juntos para garantir a segurança dos dados na nuvem. A AWS é responsável por proteger a infraestrutura da nuvem, incluindo a rede, servidores, armazenamento e instalações físicas. A AWS também fornece uma variedade de recursos de segurança e conformidade, como controles de acesso, criptografia e monitoramento de segurança.

Por outro lado, os clientes da AWS são responsáveis pela segurança de seus aplicativos e dados que são executados na nuvem. Isso inclui a configuração adequada de seus recursos na nuvem, gerenciamento de identidades e acessos, configuração de redes e firewall, criptografia de dados, gerenciamento de patches e atualizações, e assim por diante. Ao definir claramente as responsabilidades de cada parte, a AWS ajuda a garantir que os clientes entendam o que precisam fazer para manter seus dados seguros, enquanto a AWS cuida da segurança física da infraestrutura da nuvem.

Ao provisionar um ambiente em nuvem é necessário escolher a região e a zona de disponibilidade corretas é fundamental para garantir a disponibilidade, desempenho e segurança dos seus recursos em nuvem na AWS.

Existem vários aspectos a serem considerados na escolha da região e zona de disponibilidade (AZ) corretas para provisionar recursos em nuvem na AWS, no qual podemos destacar alguns dos principais:

- Localização geográfica: A região escolhida deve estar próxima dos seus usuários finais, para reduzir a latência e melhorar a experiência do usuário.
- Disponibilidade de serviços: Nem todos os serviços da AWS estão disponíveis em todas as regiões e AZs. Certifique-se de que os serviços necessários estejam disponíveis na região escolhida.
- Conformidade regulatória: Se você estiver lidando com dados confidenciais, pode ser necessário escolher uma região que atenda a

requisitos específicos de conformidade, como por exemplo LGPD, GDPR ou HIPAA.

- Custos: Os custos de infraestrutura na AWS podem variar de acordo com a região e a AZ escolhidas. Verifique os preços e compare antes de decidir.
- Redundância e resiliência: As AZs são projetadas para fornecer redundância e resiliência para seus recursos em nuvem. Certifique-se de escolher várias AZs na mesma região para garantir a disponibilidade dos seus recursos em caso de falha em uma AZ.
- Capacidade de escalabilidade: Algumas regiões podem ter capacidade limitada em termos de recursos disponíveis. Verifique se a região escolhida pode atender às suas necessidades de escalabilidade.
- Desempenho: Algumas regiões podem ter desempenho melhor do que outras. Verifique as métricas de desempenho para garantir que a região escolhida possa atender às suas necessidades de desempenho.

Em relação ao projeto de implantação ele será provisionado em duas AZ (zonas de disponibilidade) na região do Norte da Virginia que é a principal região da AWS onde praticamente a maioria dos serviços da AWS estão disponíveis além do custo ser mais barato se comparado a outras regiões, o tempo de resposta do sistema na casa 150 a 200 milissegundos é aceitável por se tratar de um ambiente de teste.

5 CONSIDERAÇÕES FINAIS

A computação em nuvem tem crescido exponencialmente no decorrer dos últimos anos, tornando-se presente na vida das pessoas e organizações com vários serviços disponíveis em diversas regiões e localidades ao redor mundo, porém a sua adoção ainda é motivo de receio e preocupação para uma certa parte da população e organizações por terem medo de compartilharem suas informações e não saberem ao certo onde os dados estarão alocados, o que gera insegurança. Contudo, é justamente essa característica que proporciona maior segurança dos dados na nuvem.

A AWS é um provedor líder de serviços de computação em nuvem, oferecendo uma ampla gama de serviços altamente disponíveis e seguros onde através de uma análise e criação de um ambiente seguro e altamente disponível na AWS requer uma abordagem holística, que envolve aspectos de segurança, arquiteturas resilientes, elasticidade, backups, recuperação de desastres, monitoramento e gerenciamento de identidade etc. Ao seguir as melhores práticas e utilizar os recursos e serviços adequados da AWS, é possível construir um ambiente robusto que proteja dados, minimize tempo de inatividade e garanta a continuidade dos serviços, além disso o modelo de responsabilidade compartilhada ajuda a estabelecer essa divisão clara de responsabilidades entre AWS e clientes, fornecendo diretrizes para garantir a segurança e o bom funcionamento dos ambientes implantados na AWS que oferece uma plataforma segura e confiável, mas cabe aos clientes implementar as práticas adequadas de segurança e conformidade em suas próprias aplicações e dados.

REFERÊNCIAS

ADIL, Josué. Segurança da informação: o que é e qual sua importância. [S. l.], 2022. Disponível em: https://acaditi.com.br/seguranca-da-informacao-o-que-e-e-qual-sua-importancia/. Acesso em: 10 nov. 2022.

ALKMIN, J.E D. Princípios de Segurança da Informação. 2021. Texto. PowerPoint (17p).

AMAZON (USA) (org.). Produtos da Nuvem AWS: A Amazon Web Services oferece um amplo conjunto de produtos baseados na nuvem que ajudam as organizações a se mover mais rapidamente, reduzir custos de TI e escalar. [S. l.], 2023. Disponível em: https://aws.amazon.com/pt/products/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc&awsf.re%3AInvent=*all&awsf.Free%20Tier%20Type=*all&awsf.tech-category=tech-category%23compute. Acesso em: 11 abr. 2023.

AMAZON Web Services Latin America. [S. l.: s. n.], [Entre 2020 e 2023]. Disponível em: https://www.youtube.com/@AmazonWebServicesLatinAmerica. Acesso em: 10 mar. 2023.

BARON, Joe et al. AWS certified solutions architect official study guide: associate exam. John Wiley & Sons, 2016.

MICROSOFT. O que e Pass: Plataforma como serviço. [S. l.], "s.d.". Disponível em: https://azure.microsoft.com/pt-br/resources/cloud-computing-dictionary/what-is-paas. Acesso em: 19 out. 2022

TABELINI, Jeferson. Descomplicando: IaaS, SaaS, PaaS. [S. l.], 9 maio 2022. Disponível em: https://www.linuxplace.com.br/o-que-e-iaas-saas-paas-caas/. Acesso em: 12 nov. 2022.

WITTIG, Andreas; WITTIG, Michael. Amazon Web Services: Em Ação. 1. ed. São Paulo: Novatec, 2016. 510 p. v. 1.