Segurança de Infraestrutura Cloud

Bootcamp Analista de Defesa Cibernética

Macgayver Souza Marques

2021

Segurança de Infraestrutura Cloud

Bootcamp Analista de Defesa Cibernética

Macgayver Souza Marques

Sumário

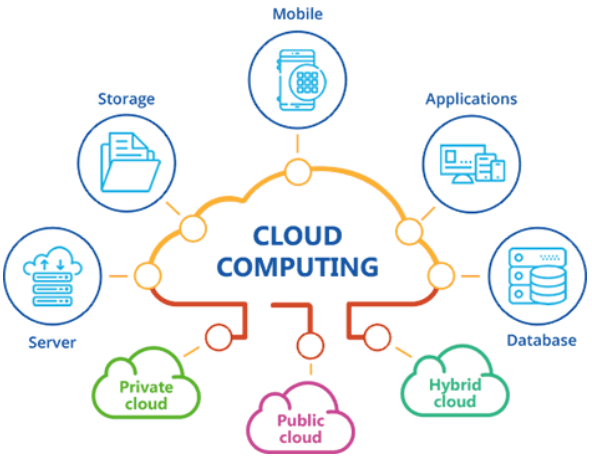
Capítulo 1. Fundamentos e Conceitos sobre Cloud Computing

Introdução

A computação em nuvem é a entrega de recursos de TI sob demanda por meio da Internet, com definição de preço de pagamento conforme o uso. Em vez de comprar, ter e manter datacenters e servidores físicos, você pode acessar serviços de tecnologia, como capacidade computacional, armazenamento e bancos de dados, conforme a necessidade, usando um provedor de nuvem como o Microsoft Azure e a Amazon Web Services (AWS). (AWS, 2021)

Organizações de todos os tipos, portes e setores usam a nuvem para uma grande variedade de casos de uso, como backup de dados, recuperação de desastres, e-mail, desktops virtuais, desenvolvimento e teste de software, análises de big data e aplicativos web voltados ao cliente. Por exemplo, as empresas do setor de saúde usam a nuvem para desenvolver tratamentos mais personalizados para os pacientes. Empresas de serviços financeiros usam a nuvem como base para detectar e prevenir fraudes em tempo real. E fabricantes de videogames usam a nuvem para entregar jogos on-line para milhões de jogadores em todo o mundo. (AWS, 2021)

Figura 1 – Cloud Computing



Fonte: http://ejrti.com.br/?p=127.

Benefícios da Cloud Computing

O NIST definiu algumas características que descrevem o modelo de cloud computing que serão abordadas nos próximos tópicos. Essas características representam algumas das vantagens deste paradigma e servem também para melhor identificar e distinguir a cloud computing de outros paradigmas.

Virtualização de Recursos

A virtualização de recursos já é muito difundida e utilizada por empresas há alguns anos. Essa tecnologia proporciona a virtualização de recursos computacionais como as máquinas virtuais, redes virtuais, memória e storage.

Por meio desta tecnologia, é possível a realização de uma separação dos serviços de infraestrutura dos recursos físicos como hardware ou redes, sendo então possível, por exemplo, tratar em uma camada inferior os aspectos relativos à localização de recursos, tornando, então, transparente este contexto para as demais camadas na estrutura da cloud. Com essa abstração, os recursos podem ser disponibilizados e utilizados como serviços utilitários, sem a necessidade de uma manipulação direta do hardware.

Serviços Sob Demanda

O cliente pode, conforme sua necessidade, requerer maior ou menor quantidade de recursos computacionais, tais como tempo de processamento, armazenamento ou largura de banda. Esses recursos devem ser disponibilizados de forma automática, sem a necessidade de interação humana com o provedor de cada serviço.

Um provedor de recursos cloud idealmente deve atender a vários consumidores através de um modelo multiclientes, utilizando diferentes recursos

físicos e virtuais, que podem ser atribuídos e reatribuídos dinamicamente, de acordo com a demanda dos consumidores.

Independência de Localização

Os recursos na cloud devem estar acessíveis através da internet por meio de dispositivos tecnológicos como smartphones, computadores, tablets, dentre outros.

A cloud é um ponto de acesso central para as necessidades computacionais dos usuários, estando disponível quase 100% do tempo e em qualquer localização geográfica.

Elasticidade e Escalabilidade

Elasticidade é um ponto chave para melhorar a qualidade dos serviços cloud. Essa propriedade permite que os provedores cloud adicionem ou removam recursos sem interrupção e em tempo de execução para lidar com uma variação de carga. (COUTINHO, 2014)

Um exemplo de elasticidade seria o site de uma empresa de varejo que possui um aumento nos acessos de seu site de e-commerce em um período de e os recursos são provisionados de forma automática durante o período de pico e são desprovisionados quando normaliza o número de acessos.

Em computação cloud, escalabilidade é a propriedade de se estar preparado para um ou mais recursos crescerem. (BONDI, 2000)

Um exemplo de escalabilidade vertical a inclusão de mais vCPU em um servidor web. Já um exemplo de escalabilidade horizontal seria a inclusão de mais um nó/servidor em uma aplicação, para que ela funcione clusterizada.

Medição de Serviços

A medição de serviços na cloud garante que o cliente pague somente pelos recursos que ele está utilizando e no tempo que estes recursos ficaram disponíveis para ele.

Cloud Privada

Uma cloud privada consiste na utilização de recursos computacionais por uma única empresa, podendo estar localizados em um datacenter da própria empresa ou hospedada por um provedor cloud terceiro. Esses recursos são dedicados para a própria empresa, portanto, sem divisão com terceiros. (MICROSOFT, 2021)

As clouds privadas geralmente são mais usadas por órgãos governamentais, instituições financeiras, manufaturas e outras organizações de grande porte com operações críticas para os negócios, que buscam manter um controle total sobre seu ambiente.

Cloud Híbrida

Uma cloud híbrida oferece às organizações vantagens como maior flexibilidade, mais opções de implantação, segurança, conformidade e obtenção de mais valor da infraestrutura existente que elas possuem. Quando há uma demanda maior de computação e processamento, as empresas podem realizar uma escala vertical de sua infraestrutura para a nuvem pública, para que possam operar sem que cause algum tipo de gargalo em seus recursos computacionais. (MICROSOFT, 2021)

Além disso, uma cloud híbrida possibilita que a empresa aproveite das tecnologias que os provedores cloud fornecem para modernizar seu ambiente local, sem a necessidade de comprar hardwares e gastar com desenvolvimento de software. Exemplos disso são:

- Utilização de sistemas de backup nativos na cloud.

- Atualização de patches de segurança no ambiente on premises por um software na cloud.
- Criação de políticas de gerenciamento de dispositivos móveis para dispositivos pessoais.

Cloud Pública

A cloud pública é a principal maneira de implantação de computação em nuvem. Através dela, os clientes conseguem realizar a implementação de recursos computacionais, sem ter que fazer a aquisição destes, pois eles pertencem a um provedor de serviços cloud e o cliente paga apenas pela hospedagem de suas aplicações e dados, pelo tempo que estes recursos foram utilizados no provedor cloud.

Exemplos de provedores de cloud pública são:

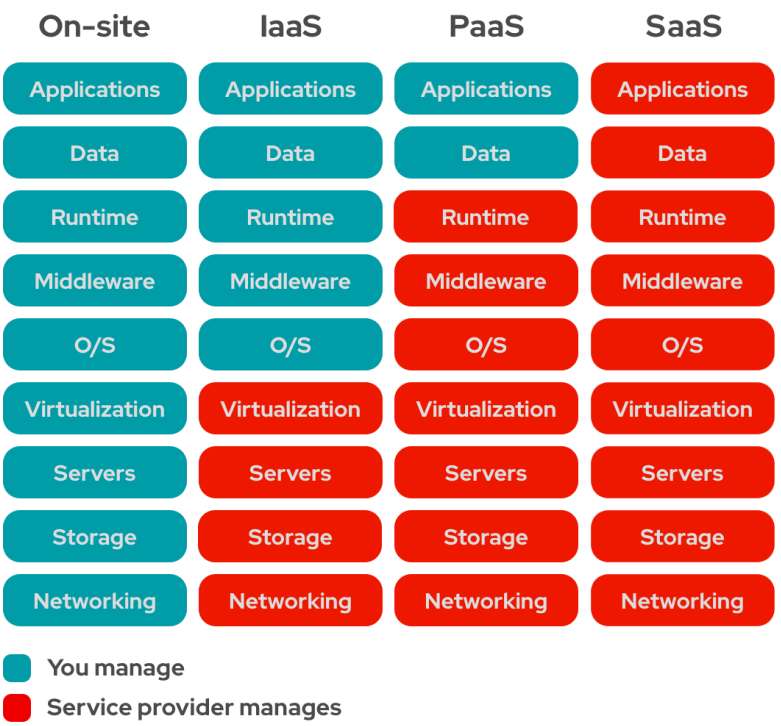
- Amazon Web Services (AWS).
- Microsoft Azure.
- Google Cloud Platform.
- Alibaba Cloud.
- Oracle Cloud.

Introdução aos tipos de Serviços Cloud

Quando falamos sobre tipos de serviços cloud, eles já se diferem de um ambiente on premises pelo fato de o cliente não ter mais preocupação com a gestão da camada física de data center, envolvendo desde a localização física até os hosts e dispositivos de rede e armazenamento físico, que passam a ser de responsabilidade do fornecedor cloud.

A figura abaixo detalha cada componente que é de gestão do cliente em azul e cada componente que é de gestão do provedor nos tipos de serviço que exploraremos neste capítulo:

Figura 2 – Tipos de Serviço.



Fonte: https://www.redhat.com/pt-br/topics/cloud-computing/iaas-vs-paas-vs-saas.

IaaS – Infraestrutura como Serviço

Neste tipo de serviço, os provedores cloud oferecem recursos de computação básicos, como máquinas virtuais, storage e demais componentes de infraestrutura para serem utilizados arbitrariamente pelos clientes. Ao adotar o IaaS, o cliente passa a ser responsável pela criação e atualização desta infraestrutura como um todo, deixando como responsabilidade do fornecedor apenas as camadas de virtualização, servidor físicos e storage físicos e redes.

Por ser o tipo de serviço mais parecido com um ambiente on premises tradicional, o IaaS é o tipo de serviço mais escolhido quando uma organização decide realizar a migração de sua infraestrutura para a cloud, pois não exige que os seus sistemas sejam redesenhados e otimizados para o ambiente em nuvem.

O IaaS é o tipo de serviço cloud que oferece maior flexibilidade e controle de gerenciamento sobre os recursos e que possui a maior semelhança com recursos existentes de TI on premises.

PaaS – Plataforma como Serviço

O tipo de serviço PaaS fornece ao cliente uma plataforma para o desenvolvimento de suas atividades. Essa plataforma pode ser, por exemplo, uma infraestrutura para que o cliente desenvolva, hospede, teste e execute uma aplicação web ou um banco de dados, sem ter que realizar a administração do sistema operacional e dos middlewares que estão sob responsabilidade do provedor cloud.

Esse tipo de serviço gera, além da maior praticidade na gestão dos recursos, uma economia em relação ao modelo de IaaS, pelo fato de o cliente não ter que preocupar com alguns fatores como licenciamento de sistemas operacionais e de bancos de dados. Portanto, o cliente paga apenas pelos recursos que são utilizados para o funcionamento da aplicação ou do banco de dados, como vCores, memória e storage.

SaaS – Software como Serviço

No tipo de serviço SaaS, aplicações são fornecidas para a utilização do cliente. O provedor cloud é responsável pelo desenvolvimento, configuração e manutenção, e o cliente fica com controles administrativos limitados.

Alguns exemplos de SaaS são:

- Salesforce.
- Dropbox.

- Slack.
- Google Apps.
- Netflix.
- Office 365.

Capítulo 2. On Premises vs. Cloud

Neste capítulo vamos discorrer sobre as principais características que diferem um ambiente on premises do ambiente cloud.

Modelo de Responsabilidade Compartilhada

Muitas organizações, de maneira equivocada, assumem que ao contratar um provedor de nuvem pública, ele se torna automaticamente responsável por tudo que for armazenado em seu datacenter. Mas, como podemos observar na Figura 2 – Tipos de Serviço, há uma grande diferença no que tange à responsabilidade pela criação, sustentação e gestão de recursos entre o ambiente on premises e o ambiente cloud.

Os provedores cloud comumente chamam essa matriz de responsabilidades de Modelo de Responsabilidade Compartilhada. Para cada tipo de serviço adotado na cloud, seja ele IaaS, PaaS ou SaaS, o cliente e o fornecedor terão responsabilidades distintas. Podemos observar nas figuras abaixo como os provedores de cloud AWS e Microsoft Azure consideram:

Figura 3 – Modelo de responsabilidade compartilhada AWS.

Fonte:

https://aws.amazon.com/pt/blogs/aws-brasil/por-onde-comecar-os-estudos-sobre-seguranca-na-aws/.

Figura 4 – Modelo de responsabilidade compartilhada Microsoft Azure.

Fonte:

https://docs.microsoft.com/pt-br/azure/security/fundamentals/shared-responsibility.

Principais Diferenças entre On Premises vs. Cloud

Neste módulo, serão abordadas as principais diferenças entre um ambiente on premises e um ambiente cloud no que se refere a desenvolvimento, controle, segurança, conformidade e custos.

Desenvolvimento

Um dos principais benefícios de se utilizar a cloud é o de poder se criar ambientes para hospedagem de aplicações de maneira muito dinâmica e rápida em relação a um ambiente on premises. Com apenas alguns cliques, já conseguimos realizar a criação de uma máquina virtual para hospedar uma aplicação replicada em mais de uma região geográfica e com diversos mecanismos de otimização.

Na cloud, não há mais a necessidade da verificação de disponibilidade de recursos computacionais disponíveis para o deploy de uma aplicação ou até mesmo para se criar um ambiente de homologação sem depender da disponibilidade de um profissional de Infraestrutura.

Controle

O controle de acesso físico em ambientes de datacenter on premises é uma das principais preocupações de uma organização.

Já quando falamos sobre um ambiente cloud, isso se torna uma responsabilidade do provedor cloud, e o cliente tem que se preocupar com quem tem acesso a qual recurso por meio de suas credenciais

Segurança

O tema segurança, quando estamos tratando de um ambiente on premises, é todo de responsabilidade do cliente ou da empresa dona do datacenter onde a

infraestrutura está hospedada. Desde a segurança física do datacenter até a camada lógica dos servidores, bancos de dados, redes e middlewares.

Já quando estamos tratando de um ambiente na cloud, a segurança é considerada uma responsabilidade compartilhada entre cliente e provedor. Essas responsabilidades se diferem dependendo do tipo de cloud que for adotado (IaaS, PaaS, SaaS). Podemos considerar que o cliente possui mais responsabilidades no modelo IaaS e o provedor cloud possui mais responsabilidades no modelo SaaS, pois os recursos são gerenciados como um todo pelo provedor e são fornecidos mecanismos de segurança para que o cliente implemente na aplicação que está consumindo do fornecedor.

Conformidade

Conformidade é um fator fundamental para uma organização decidir se deve ou não adotar alguma cloud para hospedar sua infraestrutura ou parte de seus workloads, pois devem ser respeitadas as regulamentações de mercado e auditorias que aquela empresa deve estar em conformidade.

Muitas instituições financeiras, por exemplo, precisam que os seus dados estejam hospedados no país que atuam. Portanto, não se pode contratar os serviços de um provedor cloud que não tenha datacenters no Brasil.

Custos

No conceito de custos, podemos entender que, quando tratamos de um ambiente on premises, estamos tratando de CapEx que pode ser definido como despesas realizadas com um custo inicial alto, para que a organização tenha benefícios a longo prazo no futuro. Tendo isso em mente, podemos considerar que os recursos de infraestrutura e tecnologia de uma empresa em ambiente on premises são sempre adquiridos antes de serem utilizados, através de um aporte financeiro que vai se justificar ao longo do tempo.

Já quando tratamos da contratação de serviços de cloud computing, os tipos de custos são relacionados com a operação, também denominados OpEx. Podemos definir OpEx como custos que são pagos de acordo com o uso em forma de subscrições.

Capítulo 3. Ambiente, Tecnologias e Recurso de Cloud (AWS e Azure)

Os provedores cloud escolhidos para esta disciplina foram a AWS e o Microsoft Azure, por serem líderes no quadrante mágico do Gartner para Infraestrutura e Serviços de Plataforma Cloud, isso indica que são os mais bem estruturados no tema.

Este capítulo busca dar uma visão geral dos recursos de ambos os provedores que possuem finalidades equivalentes, porém nomes distintos, para podermos explorar as maneiras de se realizar a segurança nestes recursos nos próximos capítulos.

Figura 5 – Quadrante Mágico do Gartnet para Infraestrutura e Serviços de Plataforma Cloud.

Fonte: https://cloud.google.com/gartner-cloud-infrastructure-as-a-service.

Computação

No quesito computação, podemos considerar os servidores virtuais que permitem ao contratante implementar, gerenciar e manter aplicações para servidores e o sistema operacional. Estes tipos de instância fornecem RAM e CPU que os clientes pagam de acordo com o uso e ainda possuem a flexibilidade de mudar o tamanho destas instâncias. Na AWS, esse serviço é chamado do Instâncias de cloud elástica (EC2) e, no Microsoft Azure, é chamado de Máquinas virtuais (VM).

Batch é um recurso que permite a execução de aplicativos paralelos em grande escala e aplicações de alto desempenho, a nomenclatura é a mesma tanto na AWS quanto no Azure.

Já um recurso que auxilia na propriedade da elasticidade na nuvem alterando automaticamente o número de instâncias de VM ativas de acordo com a demanda é o Dimensionamento automático na AWS e Conjunto de Escala de Máquina Virtual no Azure.

Para organizações que já estão adaptadas em utilizar o VMWare como hypervisor, recomenda-se o uso da VMWare Cloud na AWS ou Azure para integração dos ambientes on-premises e cloud, e o gerenciamento dos ambientes com as mesmas ferramentas VMWare.

Quando organizações planejam criar, gerenciar e otimizar grandes clusters, a AWS possui o serviço de Cluster Paralelo e o Azure o serviço CycleCloud.

Containers e orquestradores

O serviço para provisionar um serviço de container sem a necessidade de provisionar máquinas virtuais e nem adotar um serviço de orquestração, é

denominado Serviço de Container Elástico (ESC) na AWS e Instâncias de Container no Azure.

Para armazenamento de imagens formatadas do Docker temos o Registro de container elástico na AWS e o Registro de Container no Azure.

O serviço de gerenciamento de cluster e monitoramento por meio de atualizações automáticas em um console de operações internas, para a realização da implantação de aplicativos orquestrados em containers com Kubernetes, é denominado Serviço de kubernetes elástico (EKS) na AWS e Azure Kubernetes Services (AKS) no Azure.

Serverless

A integração de sistemas e execução de processos de back-end em resposta a eventos ou cronogramas sem provisionar ou gerenciar servidores é feita pelo servido Lambda na AWS e pelo serviço Functions no Azure.

Banco de Dados

O serviço de banco de dados relacionais gerenciados em que a escala, resiliência e manutenção são tratadas pela plataforma é denominado RDS na AWS e SQL Database, MySQL Database e PostgreSQL no Azure.

Já para o gerenciamento de bancos de dados não-SQL, onde existem vários modelos globalmente distribuídos que nativamente dá suporte a vários modelos de dados como documentos, colunas e gráficos, temos o DynamoDB, SimpleDB, Amazon DocumentDB na AWS e o Cosmos DB no Azure.

O serviço de gerenciamento de cache distribuído e baseado em memória, que fornece um repositório de alto desempenho tipicamente usado para descarregar

trabalho não tradicional de um banco de dados, é denominado ElastiCache na AWS e Cache for Redis no Microsoft Azure.

Para a migração de squema e bases de dados para o provedor cloud, temos o Serviço de migração de banco de dados tanto na AWS quanto no Azure.

DevOps e Monitoramento

No tema monitoramento, quando se trata da coleta, análise e ação na telemetria dos ambientes cloud, temos o AWS Cloud-Watch e o Azure Monitor.

Na colaboração de desenvolvimento de código na cloud, temos os serviços CodeDeploy, CodeCommit e CodePipeline na AWS e DevOps no Azure.

O CodeBuild na AWS e o DevOps no Azure são serviços de complicação totalmente gerenciados que oferecem suporte à implantação e integração contínuas.

A criação de soluções de maneiras mais simples via código baseada em API REST nativa em todos os serviços cloud é feita através da Interface de linha de comando na AWS e do CLI, ou PowerShell no Azure.

Na intenção de configurar e operar aplicativos de todas as formas e tamanhos, através de modelos para gerenciar uma coleção de recursos, temos o OpsWorks na AWS e o Automation no Azure.

Em relação ao tema automação, que é cada vez mais utilizado e necessário no nosso dia a dia, para que o time de TI foque em atividades mais estratégicas para o negócio, otimizando o seu tempo com a automação de tarefas manuais de longa duração e passíveis de erro se frequentemente repetidas, temos o CloudFormation na AWS e o Resourse Manager, VM Extensions e Azure Automation no Microsoft Azure.

Gerenciamento

O gerenciamento dos recursos de maneira unificada via console web é denominado Console de Gerenciamento na AWS e Portal no Azure.

Para a garantia que as melhores práticas estão sendo seguidas na implementação e configuração de recursos na cloud temos o serviço Trusted Advisor na AWS e o Advisor no Azure.

Os serviços que ajudam, geram e monitoram a previsão de cobranças referentes a uso de recursos, são o Relatório de uso e cobrança na AWS e API de cobrança no Azure.

Já o serviço para a realização de assessment, estimativas e migração dos workloads para o ambiente cloud é denominado Serviço de Descoberta de Aplicativos na AWS e Azure Migrate no Azure.

No intuito de identificarmos se os recursos estão íntegros e receber orientações de como aprimorar a integridade dos recursos na cloud, temos o Health Panel na AWS e o Resource Health no Azure.

Desenvolvedores e profissionais DevOps precisam de serviços para gerenciamento de desempenho de aplicativos (APM) e estes serviços são denominados CloudWatch na AWS e Application Insights no Azure.

Ações de otimização de custos e maximização de potencial na cloud são efetuados pelos serviços Cost Explorer na AWS e Cost Manager no Azure.

Mensagens e eventos

O Simple Queue Service (SQS) na AWS e o Queue Storage no Azure, fornecem serviço de enfileiramento de mensagens gerenciadas para a comunicação entre componente de aplicativos separados.

Já para o roteamento de eventos de maneira gerenciada, uniforme, usando um modelo de publicação por assinatura, temos o Amazon EventBridge na AWS e o EventGrid no Azure.

Networking

Nuvem Virtual Privada (VPC) na AWS e Rede Virtual no Azure são serviços para gerenciamento de redes virtuais e controles de seleção de intervalo de endereços IP, tabelas de rotas, criação de subredes e gateways de rede.

Na conexão entre locais, considerando conexão entre redes da cloud com redes on premises ou de outras cloud (site-to-site), temos o Gateway de VPN tanto na AWS quanto no Azure. Também temos o Direct Connect na AWS e o Express Route no Azure caso o cliente queira um link dedicado para o provedor cloud.

Para o gerenciamento de DNS ou serviço de tradução de endereços IP para nomes de domínio, temos o Route 53 na AWS e o Azure DNS no Azure.

O serviço de balanceamento de carga de tráfego na camada 4 (UDP ou TCP) é denominado Network Load Balancer na AWS e Load Balancer no Azure. Já quando estamos tratando de balanceador de carga de camada 7 (aplicação), temos o Application Load Balancer na AWS e o App Gateway no Azure.

Autenticação e Autorização

Com relação ao controle de acesso aos serviços e recursos na cloud, incluindo a criação e gerenciamento de usuários, grupos, funções, além de permissões para permitir ou negar acesso aos recursos temos o IAM na AWS e o Azure Active Directory no Azure. Ambos os provedores também possuem a funcionalidade de MFA para proteção de identidades.

Em ambientes de múltiplas assinaturas, é recomendável que se utilize o Organizations na AWS e o RBAC no Azure para gerenciar as políticas de segurança e acesso nas várias contas corporativas a nível de subscrição.

Criptografia

Para a criptografia na camada de armazenamento, temos o Gerenciamento de chaves S3 na AWS e o Serviço de criptografia de storage no Azure.

Já para o gerenciamento seguro de chaves de criptografia, podemos contar com os serviços KMS na AWS e o serviço Key Vault no Azure.

Firewall

Na proteção de entrada para protocolos não HTTP/S, proteção em nível de rede de saída para todos os protocolos e portas, temos o Web Application Firewall na AWS e o Firewall no Azure.

Quando estamos tratando de firewalls que protegem a camada 7 (aplicação), temos o Web Application Firewall em ambos os provedores.

Security

Serviços para avaliação de segurança do ambiente e na segurança de aplicativos de maneira automatizada, auxiliando na melhoria de quesitos como segurança, conformidade, descoberta de vulnerabilidades e desvios das práticas recomendadas, são o Inspector na AWS e o Security Center no Azure.

Para a criação e gerenciamento de certificados, temos o Certificate Manager na AWS e o App Service Certificates no Azure.

Já nas camadas de detecção e investigação de ataques avançados na cloud, temos o GuardDuty na AWS e o ATP no Azure.

As organizações precisam embasar sua segurança utilizando de relatórios de auditoria, guias de conformidade e documentos confiáveis dos serviços cloud, e, para tal finalidade, temos o Artifact na AWS e o Service Trust Portal no Azure.

Na proteção contra negação de serviço distribuída (DDoS), pode-se contar com os serviços Shield na AWS e o DDoS Protection Service no Azure.

Storage

Nos provedores cloud, existem diferentes tipos de storage para finalidades distintas. Iremos explorar estes tipos de storage nesta seção.

O Serviço de Armazenamento Simples (S3) na AWS e o Blob Storage no Azure são serviços de armazenamento de objeto para casos de uso por aplicativos na nuvem, backup, DR e análise de big data.

O armazenamento de máquinas virtuais é efetuado através do Elastic Block Storage (EBS) na AWS e através dos Managed Disks no Azure.

Para a criação e gerenciamento de arquivos compartilhados em rede, temos o Elastic File System na AWS e o Azure Files no Azure.

Na camada de arquivamento, temos o S3 Infrequent Access IA e S3 Glacier na AWS e o Storage cool tier e o Storage archive tier.

Já para a realização de backups de pastas e arquivos em cloud e proteção contra vazamento de dados, temos o Backup em ambos os provedores.

Aplicativos Web

Quando uma organização busca uma plataforma de hospedagem gerenciada que fornece a capacidade de implantar e dimensionar aplicativos web, temos o serviço Elastic Beanstalk na AWS e o serviço Application Service no Azure.

Na publicação de APIs para clientes externos e internos, existem os serviços API Gateway na AWS e API Management no Azure.

O CloudFront na AWS e o CDN no Azure são redes de distribuição de conteúdo (áudio, vídeo, app, imagens) globais.

Para obter a característica de balanceamento de carga HTTP e regras de roteamento de acordo com o caminho em aplicações de microsserviço, temos o Global Accelerator na AWS e o Front Door no Azure.

Capítulo 4. Segurança em Cloud

Existem frameworks e documentos para auxiliar na definição dos controles que devem ser realizados na cloud, como o Cloud Controls Matrix version 4.0 da Cloud Security Alliance, que foram a referência para a produção deste capítulo.

Modelo de Processo de Cloud Security

Para um correto gerenciamento de segurança na cloud, temos que nos guiar por um modelo de processo de segurança em cloud. Este modelo de processo deve conter as seguintes diretrizes:

- Identificação de requisitos de segurança e conformidade e tipos de controle existentes.
- Selecionar seu provedor cloud, serviços e modelos de desenvolvimento.
- Definir a arquitetura.
- Avaliar os controles de segurança, cujos exploraremos mais a fundo neste capítulo.
- Identificar os gaps de controle.
- Desenhar e implementar os controles para preencher os gaps.
- Gerenciar as mudanças ao longo do tempo.

Identity and Access Management (IAM)

Gerenciamento de Acesso e Identidade (IAM) é um fator fundamental para garantirmos a segurança de nossos usuários e os acessos aos recursos em um ambiente cloud. Para esta propriedade são recomendados os controles abaixo:

- Política de senhas fortes.
- Inventário de identidades.
- Least Privilege.
- Provisionamento, mudança, revisão e revogação de acesso de usuário.
- Segregação e aprovação de roles com acessos privilegiados.
- Manter integridade dos logs.
- Autenticação forte.
- Gestão de senhas.
- Mecanismos de autorização de acessos.

Controles de Segurança de Infraestrutura

No intuito de se realizar a segurança do ambiente cloud de maneira ampla, minimizando a superfície de ataque, devem ser respeitados os seguintes controles de segurança:

- Planejamento de capacidade e recursos.
- Segurança de redes.
- Hardening de Sistema Operacional e security baseline.
- Separação de ambientes de produção e não-produção.
- Definir, implementar e avaliar processos, procedimentos e técnicas de defesa em profundidade para proteção, detecção e resposta oportuna a ataques baseados em rede.
- Segmentação e segregação de acesso ao Tenant.
- Utilização de protocolos seguros para migração para Cloud.
- Documentação de arquitetura de redes para ambientes de alto-risco.

Controles de Segurança de Dados

A segurança de dados é fundamental para que uma organização mantenha sua imagem íntegra no mercado e não tenha prejuízo financeiro devido a técnicas como o sequestro de dados, por exemplo. Existem diversas regulamentações para a segurança de dados pessoais que devem ser seguidas em determinados países,

como a LGPD no Brasil. Para obter uma segurança de dados robusta na cloud, devem ser respeitados os seguintes controles:

- Classificação de dados.
- Inventário de dados.
- Documentação de fluxo de dados.
- Propriedade e administração de dados (quem é o dono dos dados e quem pode ter qual acesso naquele dado).
- Proteção de dados por design e padrão.
- Avaliação do impacto da proteção de dados.
- Proteger transferência da dados sensíveis.
- Acesso, reversão, retificação e exclusão de dados pessoais.

Controles de Log e Monitoramento

Log e monitoramento são ferramentas que auxiliam no rastreio das atividades e eventos que ocorrem no ambiente cloud, portanto, devem se ter uma atenção especial para que permaneçam íntegros. São recomendáveis os seguintes controles:

- Procedimento e políticas de log e monitoramento.

- Proteção e monitoramento de logs de auditoria.
- Monitoramento e alerta de segurança.
- Sincronização de relógio (NTS).
- Escopo, registro e proteção de logs.
- Monitorar e gerar relatórios de criptografia.
- Registro de transações/atividades.

Controles de Ameaças e Vulnerabilidades

A cada dia que se passa, surgem novas ameaças e são expostas novas vulnerabilidades de sistemas e tecnologias. Em resposta a isso, temos que manter nosso ambiente em cloud seguro seguindo os seguintes controles:

- Política e procedimentos de ameaças e vulnerabilidades.
- Política e procedimentos de proteção contra malwares.
- Agendar remediação de vulnerabilidades.
- Penetration Testing.
- Identificação, priorização e gerenciamento de vulnerabilidades.

Controles de Segurança de Aplicação e Interface

O desenvolvimento de aplicações vem sendo cada vez mais realizado pelas organizações utilizando das tecnologias cloud para hospedar e gerenciar estas aplicações. Percebe-se um aumento muito elevado no número de aplicações serverless e utilização de microsserviços para padronização no deploy dessas aplicações. São recomendados os seguintes controles para a segurança de aplicação:

- Política e procedimentos de segurança de aplicativos e interfaces.
- Estabilizar, documentar e manter requisitos de baseline para segurança de aplicações.
- Desenvolvimento e desenho de aplicações seguras.
- Desenvolvimento automatizado de aplicações seguras.
- Testes de segurança de aplicação automatizados.
- Remediação de vulnerabilidades de aplicações.

Controles de Criptografia e Key Management

Criptografia é um método de proteção de informações em repouso e em trânsito, através de algoritmos e protocolos seguros. Em um ambiente cloud, é de suma importância que se utilize de criptografia em todos os recursos que hospedem

ou trafeguem informações, além de uma tecnologia para gerenciamento dessas chaves. São recomendados os seguintes controles:

- Política e procedimentos de criptografia e Key Management.
- Definição e implementação roles e responsabilidades de criptografia e key management.
- Criptografia de dados.
- Gerenciamento de Mudanças de Criptografia.
- Auditoria de Criptografia e key management.
- Geração, rotação, revogação, suspensão, desativação, arquivamento, destruição e recuperação de chaves.
- Gerenciamento de Inventário de chaves.

Controles de Segurança de Gestão de Incidentes, E-discovery e Cloud Forensis

Nos processos de Gestão de Incidentes, E-Discovery e Cloud Forensis em um ambiente cloud, são recomendados os seguintes controles:

- Política e procedimentos de Gerenciamento de Incidentes de Segurança.
- Plano de resposta a incidentes.

- Testes de respostas a incidentes.

- Notificação de ameaça de segurança.

- Manter pontos de contato para autoridades regulatórias aplicáveis, autoridades locais e nacionais de aplicação da lei e outras autoridades jurisdicionais legais. (ANPD).

Controles de Segurança de Gerenciamento de Endpoints

Outro ponto fundamental para garantia de segurança em um ambiente cloud é o gerenciamento de segurança de endpoints. Podemos considerar endpoints como qualquer dispositivo (laptop, smartphone, tablet, dentre outros) que acesse de alguma forma as aplicações e serviços hospedados no provedor cloud, principalmente, se o usuário que estiver utilizando este endpoint tenha privilégios administrativos sobre algum desses recursos na cloud. São recomendados os seguintes controles para a proteção de endpoints:

- Política e procedimentos de Gerenciamento de endpoints.

- Aprovação de aplicações e serviços.

- Compatibilidade com sistemas e aplicações.

- Inventário de endpoints.

- Gerenciamento de endpoint.

- Bloqueio de tela automático.
- Criptografia de Storage.
- Prevenção e Detecção de Anti-malware.
- DLP.
- Wipe Remoto.
- Postura de segurança de endpoint de terceiros.

SIEM

As soluções de gerenciamento de eventos e informações de segurança (SIEM) oferecem às empresas a capacidade de coletar, armazenar e analisar informações de segurança de toda a organização e alertar administradores de TI / equipes de segurança sobre possíveis ataques.

Através de um sistema SIEM, podemos integrar os ativos de infraestrutura da organização para a centralização dos eventos de segurança e geração de incidentes de segurança com a correlação desses eventos, que é efetuada pelo SIEM.

Algumas das vantagens de um cloud-SIEM em relação a um SIEM on premises são:

- Não há a necessidade de compra de hardware.

- Elástico.
- Escalável.
- Rápido.
- Fácil de configurar.
- Pay as you go.
- Possibilidade de automação de respostas à incidentes.
- Utilização de inteligência artificial.

Web Application Firewall

Um Web Application Firewall (WAF) fornece segurança ao operar por meio de um aplicativo ou serviço, bloqueando chamadas de serviço, entradas e saídas que não atendem à política de um firewall, ou seja, conjunto de regras para uma conversa HTTP. WAFs atuam na camada 7 (aplicação) e não requerem modificação do código-fonte do aplicativo para sua implementação.

As proteções mais comuns de um Web Application Firewall nativo em nuvem são contra:

- Roubo de identidades.
- Acesso a informações confidenciais.

- SQL Injection.

- Cross site scripting (XSS).

- Ataques comuns, como injeção de comando, contrabando de solicitação HTTP, divisão de resposta HTTP e ataque de inclusão remota de arquivo.

- Violações de protocolo HTTP.

- Anomalias de protocolo HTTP.

- Bots, crawlers e scanners.

- Configurações incorretas de aplicativos comuns (por exemplo, Apache, IIS, dentre outros).

- Negação de serviço HTTP.

Capítulo 5. Contingência e Continuidade Cloud

Quando são implementados recursos na cloud, não podemos presumir que estes recursos sempre estarão lá, ou sempre estejam trabalhando da maneira esperada. Problemas e interrupções não são mais ou menos comuns na cloud do que em qualquer outra tecnologia, embora a nuvem no geral possa ser mais resiliente por conta de mecanismos que o provedor fornece para construção de aplicações e infraestruturas resilientes.

Plano de Continuidade de Negócios e Disaster Recovery na Cloud

A queda de um provedor cloud ou pelo menos parte de sua infraestrutura (em uma região geográfica específica) é sempre uma possibilidade iminente. Às vezes, em caso de quedas, podemos migrar parte do serviço para outra região ou para um ambiente de DR, caso a organização tenha estruturado um Plano de Continuidade de Negócios e Plano de Disaster Recovery.

Continuidade de negócios e Disaster Recovery (BCDR ou BC / DR) é um conjunto de processos e técnicas usados para ajudar uma organização a se recuperar de um desastre e continuar ou retomar as operações de negócios de rotina. É um termo amplo que combina as funções e funções de TI e negócios após um desastre.

Os principais aspectos de BCDR na cloud são:

- Garantir a continuidade e recuperação em um determinado provedor de cloud.
- Preparação e gerenciamento de interrupções no provedor de cloud.

- Considerar opções de portabilidade, caso precise migrar provedores ou plataformas.

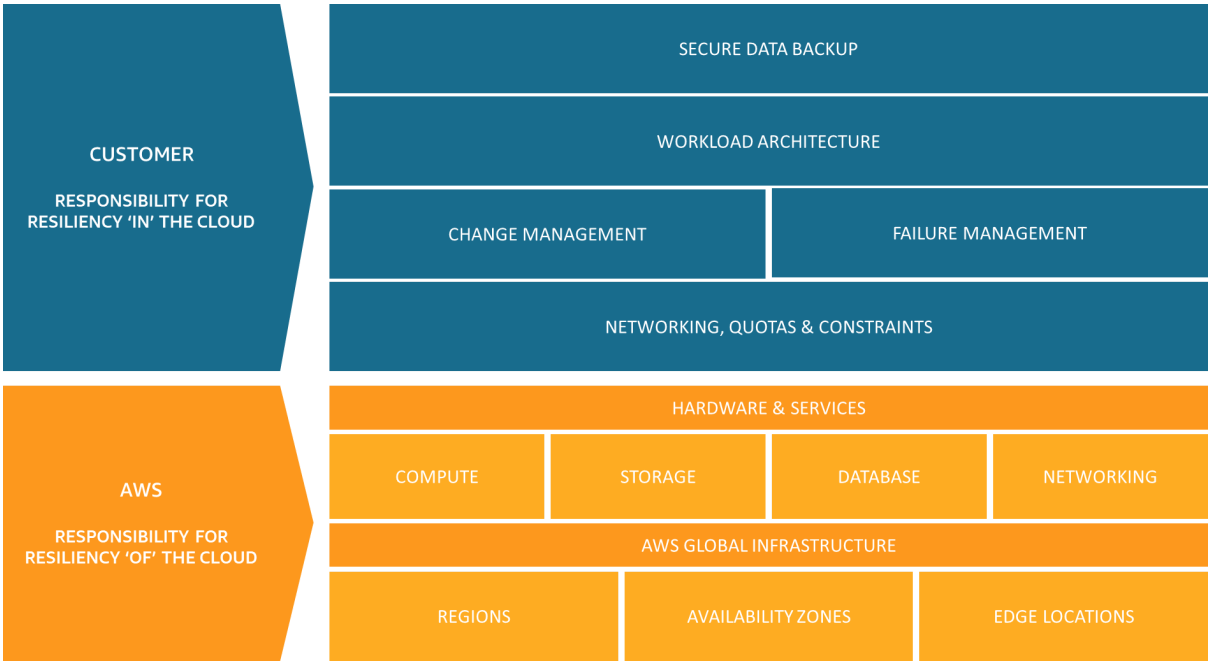
Modelo de Responsabilidade Compartilhada para Resiliência

Quando estamos tratando de um ambiente cloud, assim como existem as responsabilidades compartilhadas em termos de segurança, gerenciamento e infraestrutura, também temos um modelo de responsabilidade compartilhada no quesito resiliência.

Na Figura 6, podemos entender bem quais são as responsabilidades do provedor cloud que estão mais voltadas para critérios de hardware e serviços de computação, além de infraestrutura distribuída de datacenters.

Já a responsabilidade do cliente é mais focada na implementação de recursos para arquiteturas com alta disponibilidade, garantia de execução de backups e implementação de ambiente de disaster recovery.

Figura 6 – Modelo de Responsabilidade Compartilhada para Resiliência AWS.



Fonte:

https://docs.aws.amazon.com/pt_br/whitepapers/latest/disaster-recovery-workloads-on-aws/shared-responsibility-model-for-resiliency.html.

Cloud Backup

Podemos definir backup como uma cópia de segurança de dados, de um sistema ou de algum dispositivo de armazenamento, para que eles possam ser restaurados em caso de alguma perda de dados ou devido a algum acidente.

Existem duas métricas fundamentais quando estamos trabalhando no plano de backup de uma organização, essas métricas são o Recovery Point Objective (RPO) e o Recovery Time Objective (RTO).

O RPO trata da quantidade de dados que sua organização aceitaria perder em caso de falha de algum sistema ou servidor. Podemos citar, como exemplo, um backup em um servidor específico que ocorre uma vez por dia, portanto, a organização está aceitando um RPO de até 24 horas neste caso em específico. Isto é, aceitando perder até 1 dia de trabalho daquele workload em específico.

Já o RTO está relacionado com o tempo total de restauração de alguma inatividade a partir do início do incidente, até que normalize as operações. Por exemplo, se um servidor ficar indisponível às 13h de um dia e a restauração da cópia de segurança deste servidor ser finalizada às 15h, podemos considerar um RTO de duas horas.

O Backup efetuado na cloud pode nos trazer alguns benefícios, como economia de dinheiro e recursos, proteção de dados em caso de desastre, proteção contra ciberataques nativas da solução e claro, a propriedade de escalabilidade que temos na cloud.

Nas clouds AWS e Azure, podemos executar backup dos seguintes itens:

- Arquivos e máquinas virtuais on premises.
- Máquinas virtuais do Azure e AWS.
- Discos gerenciados.
- File shares.

- Bancos de dados SQL, Postgree, MySQL etc.
- SAP HANA Databases.
- Azure Blobs ou AWS Simple Storage Services (S3).

Capítulo 6. Segurança de Dados e Aplicações

Neste capítulo, iremos tratar sobre a segurança de dados e aplicações, mas, antes, é importante darmos uma breve definição sobre o conceito de dados.

Em geral, dados podem ser considerados como qualquer conjunto de caracteres que são coletados e traduzidos para algum propósito, em geral, para análise. Dados precisam ser colocados em algum contexto para que daí possam gerar uma informação. Alguns exemplos de dados são:

- Caractere simples.
- Boolean (verdadeiro ou falso).
- Texto.
- Número.
- Foto.
- Som.
- Vídeo.

Criptografia de Dados

A criptografia de dados na cloud é um fator fundamental para a proteção dos dados em seus determinados storages, que estão armazenados. Criptografia pode ser aplicada em storages de objetos, em discos gerenciados de máquinas

virtuais, em bancos de dados relacionais e não relacionais e nos dados que estão em repouso ou em trânsito através da utilização de protocolos de comunicação seguros como o SSL.

É de suma importância que se tenha implementada uma ferramenta de gerenciamento de chaves de criptografia, como o KMS na AWS e o Key Vault no Azure para o gerenciamento dessas chaves de criptografia para que se possa atualizar essas chaves com uma determinada frequência, executar rotinas de backup e garantir a comunicação de aplicações com esses storages de maneira segura.

Cloud Access Security Broker

As nuvens públicas vêm sendo cada vez mais utilizadas, e muitas organizações enfrentam grandes desafios para entender quais aplicações que não são homologadas para uso corporativo estão sendo utilizadas por seus usuários para esta finalidade; também denominadas de Shadow IT.

Um Cloud Access Security Broker serve justamente para a identificação dessas aplicações através da análise de tráfego e combater ameaças cibernéticas nas cloud SaaS públicas, descobrindo e controlando o uso de Shadow IT, protegendo informações confidenciais com DLP e realizando a avaliação de conformidade de aplicativos na cloud.

Data Loss Prevention

Ferramentas de Data Loss Prevention (DLP) cloud servem para identificação, rastreio e proteção de informação em clouds públicas SaaS, como Dropbox, Office 365, G-Suite, dentre outras.

Essas ferramentas possuem a capacidade de detectar tipos de informações confidenciais através de critérios que são definidos em suas políticas podendo ser

uma palavra em específico ou um dicionário com várias palavras ou expressões regulares que são expressões matemáticas que conseguem realizar a identificação de dígitos equivalentes a um CPF ou RG, por exemplo.

Essas ferramentas são essenciais para que a organização fique em conformidade com regulamentações de mercado como o LGPD, bloqueando e alertando o usuário em casos de compartilhamento de dados pessoais com entidades externas.

Fases de Desenho e Desenvolvimento de Aplicações Seguras

A Open Web Application Security Project (OWASP) é uma comunidade on-line que produz artigos, documentações, ferramentas e metodologias para a segurança de aplicações web.

Quanto ao desenvolvimento seguro, a OWASP define as seguintes fases para serem seguidas com suas determinadas atividades:

- Fase de Treinamento:
  - Práticas de Segurança de Código.
  - Escrita de testes de segurança.
  - Treinamento na plataforma/provedor.
- Fase de Definição:
  - Padronização de código.
  - Requisitos funcionais de segurança.
- Desenho
  - Modelagem de ameaças.
  - Desenho de segurança.
- Desenvolvimento:
  - Revisão de código.
  - Testes unitários.
  - Análise estática.

  - Análise dinâmica.

- Teste:
  - Vulnerability Assessment.
  - Análise Dinâmica.
  - Testes Funcionais.
  - QA.

Capítulo 7. Melhores Práticas de Segurança em Cloud

Para a produção deste capítulo, foram seguidas as recomendações de segurança dos provedores AWS e Azure. Ambos os provedores seguem as melhores práticas de frameworks e padrões de mercado como SOC 2, ISSO/IEC 27001, NIST SP800-53, FedRAMP e PCI DSS.

Melhores práticas para segurança de redes

Garantir um perímetro de acesso seguro é fundamental para que não sejam expostas backdoors desnecessariamente. A seguir, encontram-se as melhores práticas recomendadas por AWS e Azure para a segurança de redes:

- Segmentar logicamente as subredes:
  - Não atribuir regras de permissão com intervalos amplos (allow 0.0.0.0 – 255.255.255.255).
  - Segmentar o espaço de endereço maior em subredes.
  - Criar controle de acesso à rede entre subredes.
  - Evitar subredes virtuais pequenas para garantir simplicidade e flexibilidade.
- Adotar uma abordagem de Zero Trust:
  - Conceder acesso condicional a recursos com base em dispositivo, identidade, garantia, local de rede etc.
  - Habilitação de acesso a portas somente após aprovação.

  - Conceder permissões temporárias para executar tarefas privilegiadas, para impedir que usuários mal-intencionados ou não autorizados obtenham acesso após a expiração das permissões.

- Usar dispositivos de rede virtual:

  - Firewall.
  - Gerenciamento de vulnerabilidades.
  - Controle de aplicativo.
  - Filtragem web.
  - Antivírus.
  - Proteção contra botnet.

- Evitar a exposição à Internet por meio de links WAN dedicados:

  - VPN S2S.
  - Link dedicado.

Melhores práticas para segurança de bancos de dados

No quesito segurança de bancos de dados, AWS e Azure, recomendam as seguintes melhores práticas:

- Gerenciamento central de identidades:

  - Utilização de roles e grupos específicos para cada servidor ou instância de bancos de dados.

- Utilização de acesso condicional com habilitação de MFA.

- Minimizar o uso de autenticação com senha para usuários:
  - Utilização de SSO.

- Proteger senhas com segredos:
  - HSM, KeyVault.

- Gerenciamento de acesso:
  - Aplicar o princípio de privilégios mínimos.
  - Utilização de contas distintas em ambientes de testes e produção.

- Realizações de revisão de códigos constantes:
  - Padronização.
  - Vulnerability Assessment.
  - Testes.

- Proteção de dados
  - Criptografar dados em trânsito.
  - Criptografar dados em repouso.
  - Habilitar a função Always Encrypted para dados confidenciais.

  - Sempre armazenar as chaves de criptografia em um gerenciador de chaves.

- Minimizar a superfície de ataque:

  - Link dedicado, VPN.
  - Regras de firewall para garantir acesso para IPs autorizados.
  - Restrição de acesso à porta 3342.

- Proteção contra-ataques DDoS.

- Monitoramento, registro em log e auditoria.

- Auditar eventos de segurança críticos.

- Identificar e marcar dados confidenciais.

- Acompanhar o acesso aos dados confidenciais.

- Utilização de alta-disponibilidade.

Melhores práticas para segurança e criptografia de dados

Manter os dados seguros tanto em repouso quanto em trânsito é fundamental para a segurança desses dados. As melhores práticas para criptografia e segurança de dados recomendadas por Azure e AWS, são:

- Proteger dados:

  - Em repouso.
  - Criptografia de discos e BD.

- Em trânsito:
  - VPN S2S e VPN P2S.
  - HTTPS.

- Definir uma solução de gerenciamento de chaves criptográficas:
  - Conceder acesso a usuários, grupos e aplicativos em um escopo específico.
  - Controle o que os usuários têm acesso (RBAC).
  - Armazenar certificados no cofre de chaves.

- Garantir segurança de dispositivos que acessarem dados sensíveis.

- Proteger e-mails, documentos e dados confidenciais.

Melhores práticas para controle de acesso e IAM

Identidade deve ser tratada como perímetro de segurança primário, pois é de onde surgem grande parte dos ataques. As melhores práticas de segurança para IAM recomendadas por AWS e Azure são:

- Centralizar o gerenciamento de identidade.
- Login único de usuário (SSO).
- Ativar acesso condicional.
- Habilitar o gerenciamento de senhas.
- MFA.
- RBAC.
- Gestão de contas com acesso privilegiado.
- Monitoramento de identidades.

Melhores práticas de segurança operacional

A Operação de Segurança também possui papel fundamental na garantia de segurança em um ambiente cloud. As melhores práticas de AWS e Azure para este quesito são:

- Gerenciar e monitorar senhas de usuários.

- Utilização de Blueprints e Organizations para automatizar a governança de recursos.
- Monitoramento de serviços.
- Implantação de sistemas EDR e SIEM.
- Monitoramento de rede ponta a ponta.
- Proteção contra DDoS:
  - Aplicações escaláveis.
  - Alta disponibilidade.
  - NSG.
  - Anti DDoS.
- Habilitar Policy.

Melhores práticas para segurança PaaS

Plataforma como Serviço vem sendo cada vez mais utilizada pelas organizações, pelos seus benefícios em relação ao IaaS, porém existem critérios de segurança que devem ser respeitados para que não haja uma exposição desnecessária de informações confidenciais. AWS e Azure recomendam:

- Identidade como perímetro de segurança primário:

  - Proteger suas chaves e credenciais para proteger a implantação de PaaS.
  - Não armazenar as credenciais e outros segredos no código-fonte nem no GitHub.
  - Uso de MFA.
  - Utilizar protocolos de segurança padrão OAuth2 e Kerberos.

- Instalar um WAF.
- Monitorar o desempenho dos aplicativos.
- Executar Pentest.

Melhores práticas para segurança de bancos de dados PaaS

As melhores práticas para bancos de dados PaaS são bastante parecidas com as de bancos de dados IaaS, porém é importante destacarmos os seguintes pontos recomendados por AWS e Azure:

- Utilizar repositório de identidades centralizado.
- Restringir o acesso com base no IP.
- Criptografar dados em repouso e em trânsito:
  - Habilitação do Always Encrypted.
- Realização de backups.

Melhores práticas para segurança IaaS

As melhores práticas para a segurança de um ambiente de Infraestrutura como Serviço (IaaS), de acordo com os provedores AWS e Azure, são:

- Proteção de VMs:
  - Definir políticas para VMs em grupos de recursos.
  - Reduzir a variabilidade na configuração de VMs com templates.
  - Abordagem de privilégios mínimos.
  - Usar mais de uma VM para melhorar a disponibilidade.
  - Proteção contra Malware.
  - Gerenciar atualizações de VM.
  - Realização de backups.
  - Monitoramento de segurança e desempenho.
  - Criptografar discos.
  - Restringir conexão direta com a Internet.

Referências

AWS. What is cloud computing. **Site da Amazon Web Services**, 2021. Disponivel em: <https://aws.amazon.com/pt/what-is-cloud-computing/>. Acesso em: 16 Maio 2021.

AWS Security Best Practices. **Amazon Web Services**, 2021. Disponivel em: <https://docs.aws.amazon.com/pt_br/whitepapers/latest/aws-security-best-practices/welcome.html>. Acesso em: 15 Maio 2021.

BONDI, A. B. Characteristics of scalability and their impact on performance. **Proceedings of the 2nd international workshop on Software and performance**, Ottawa, Setembro 2000. 195-203.

CLOUD Security Alliance Releases (SecaaS) Implementation Guidance. **Cloud Security Alliance**, 2012. Disponivel em: <https://cloudsecurityalliance.org/press-releases/2012/10/09/csa-releases-secaas-implementation-guidance/>. Acesso em: 15 Maio 2021.

COUTINHO, E. F. . D. C. S. F. R. . R. P. A. L. Elasticity in cloud computing: a survey. **Elasticity in cloud computing: a survey**, Fortaleza, 23 Novembro 2014. 21.

DOCS Microsoft. **Azure Security Best Practices and Patterns**, 2019. Disponivel em: <https://docs.microsoft.com/en-us/azure/security/fundamentals/best-practices-and-patterns>. Acesso em: 15 Maio 2021.

MICROSOFT. O que são nuvens públicas, privadas e híbridas? **Azure**, 2021. Disponivel em: <https://azure.microsoft.com/>. Acesso em: 16 Maio 2021.

MOGULL, et al. Security Guidance v4.0. **Cloud Security Alliance**, 2019. Disponivel em: <https://cloudsecurityalliance.org/research/guidance/>. Acesso em: 15 Maio 2021.