Segurança em computação em nuvem

Fundamentos e conceitos de segurança da computação em nuvem e seus empregos nos diversos serviços relacionados, bem como as preocupações com os aspectos de segurança nas principais áreas críticas dos ambientes em nuvem.

Prof. Roberto Miranda Gomes

Propósito

Proporcionar ao estudante a compreensão da importância da segurança no provimento dos serviços em nuvem e suas principais formas de manutenção.

Objetivos

- Reconhecer os fundamentos e principais conceitos do paradigma da computação em nuvem.
- Identificar os aspectos gerais de segurança e responsabilidades de cada um dos polos nos contratos de prestação de serviços de nuvem.
- Identificar os aspectos de segurança dos principais serviços dos provedores de serviços de nuvem.
- Reconhecer os domínios descritos nas orientações de segurança da CSA em sua versão 4.0.

Introdução

O mundo da Tecnologia da Informação vem atravessando muitas mudanças desde o advento da internet. Durante décadas, as organizações estruturavam sua infraestrutura de computação a partir da aquisição de hardware, instalação de sistemas operacionais e implantação de software. Essa rotina exigia manutenção contínua, exaustiva e cara, principalmente nos aspectos de segurança, demandando implantação de patches de atualização, backup, monitoramento e diversas outras atividades.

A computação em nuvem introduziu um novo paradigma, ou seja, a capacidade de consumir serviços gerenciados para atingir o mesmo objetivo originalmente alcançado pela execução local de softwares, desde os mais simples, de prateleira, até servidores de arquivos e produtos tipo Enterprise Resource Planning (ERP) ou Customer Relationship Management (CRM), cada vez mais essenciais para os negócios.

Do ponto de vista da segurança, os serviços gerenciados na nuvem oferecem capacidades de automatizar tarefas de segurança, antes extremamente manuais, de forma que as empresas passaram a poder se concentrar na escalabilidade e na inovação de seu próprio negócio.

Introdução

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Fundamentos e conceitos da computação em nuvem

Fundamentos e conceitos da computação em nuvem

Neste vídeo, apresentaremos um panorama da computação em nuvem.

> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

Iniciamos com uma breve recapitulação sobre o que é um serviço de nuvem utilizando a definição atribuída pelo National Institute os Standards and Technology (NIST), órgão norte-americano responsável pela elaboração de padrões em Tecnologia da Informação. As recomendações da publicação 800-145 descrevem o serviço de nuvem com base em cinco características essenciais, como veremos a seguir.

On-demand self-service

Traduzindo, autoatendimento sob demanda. É uma alternativa moderna para o modelo original de se colocar um negócio no ar a partir da compra de computadores, espera pela logística de entrega e implantação dos softwares necessários ao negócio em si. Com o autoatendimento sob demanda, a empresa cliente pode provisionar o hardware e selecionar um sistema operacional a ser instalado nos equipamentos, além de outros sistemas, implantando tudo até mesmo com um único recurso humano atuando solitariamente, em questão de minutos e sem a interação física do humano com o provedor do serviço.

Broad network access

Traduzindo, "amplo acesso à rede". A consideração aqui está calcada na disponibilidade de acesso à rede suficiente para atender a milhões de usuários finais, clientes do negócio da empresa, independentemente de suas plataformas de acesso (celulares, tablets, laptops ou estações de trabalho). Estamos falando de acesso à rede nos moldes dos grandes provedores de serviços de internet (ISP).

Resource pooling

Algo como um conjunto de recursos diversos relacionados à computação.

> Exemplo
>
> Milhares de computadores, operando de forma coordenada em formato de compartilhamento de recursos.

Isto é, de forma a maximizar a utilização de CPU, memória e capacidade de armazenamento, em vez de ter um único servidor executando 10% de seus recursos na maior parte do tempo e podendo estourar 100% de sua capacidade em momentos específicos de pico.

Rapid elasticity

Traduzindo, "elasticidade rápida". Confere capacidade ao sistema de aumentar e diminuir a quantidade de recursos de computação, desde um único servidor para milhares de servidores, eventualmente, e depois retornar para o uso de um único servidor, tudo de acordo com suas necessidades do negócio.

Measured service

Traduzindo, "serviço medido". Baseia-se na possibilidade de a empresa pagar apenas pelos recursos consumidos, gerando um relatório de cobrança que mostre quais recursos foram utilizados e quanto deve ser pago por cada um desses recursos.

Modelos de Serviço

Modelos de implantação da computação em nuvem

Neste vídeo, vamos conhecer os principais modelos de implementação da computação em nuvem.

> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

A publicação do NIST destaca três modelos de serviço possíveis, como veremos a seguir.

Software as a service (SaaS)

Também chamado de software como serviço. Por esse modelo, o provedor do serviço oferece ao cliente a possibilidade de usar os aplicativos do provedor a partir de uma infraestrutura em nuvem. Toda a gestão da infraestrutura da nuvem, incluindo rede, servidores, sistemas operacionais, armazenadores e mesmo os recursos de aplicativos individuais, fica totalmente transparente para o cliente, salvo pela eventual e limitada configuração de alguns aplicativos específicos do usuário.

> Exemplo
>
> O acesso aos aplicativos pode ocorrer por um navegador web ou interface de um programa acessado remotamente.

Platform as a service (PaaS)

Também chamado de “plataforma como serviço”. Por intermédio desse modelo, o cliente do serviço recebe a capacidade de implantar na infraestrutura de nuvem seus próprios aplicativos, criados ou adquiridos, usando linguagens de programação, bibliotecas, serviços, bem como outras ferramentas suportadas pelo provedor do serviço de nuvem. Assim como no modelo SaaS, não são delegadas ao cliente as tarefas de gerenciamento e controle da infraestrutura de nuvem, incluindo rede, servidores, sistemas operacionais ou armazenadores, mas apenas o controle sobre os aplicativos criados, adquiridos ou implantados pelos próprios clientes e, possivelmente, sobre algumas definições de configuração do ambiente de hospedagem dos aplicativos.

Infrastructure as a service (IaaS)

Também chamado de “infraestrutura como serviço”. Com esse modelo, o provedor do serviço oferece processamento, armazenamento, rede e outros recursos computacionais fundamentais onde o cliente consegue implantar e executar softwares aplicativos e sistemas operacionais específicos. O cliente não tem responsabilidade sobre o gerenciamento e controle da infraestrutura de nuvem em si. Fica sob encargo do cliente apenas o controle sobre os sistemas operacionais, armazenamento e aplicativos implantados, além de algum possível controle limitado a componentes de rede específicos, como firewalls de host.

Modelos de Implantação

A publicação 800-145 do NIST relaciona ainda **quatro modelos de implantação** para os serviços em nuvem.

Private cloud

Traduzindo, “nuvem privada”. Representa a infraestrutura de nuvem que é provisionada para uso exclusivo por uma única organização. Pode-se pensar na organização como unidades de negócios compondo os diversos clientes diferentes, consumidores dos serviços. Uma nuvem privada pode ser de propriedade, gerenciada e operada pela própria organização, por terceiros ou por alguma combinação deles, podendo ser implantada fisicamente dentro ou fora das instalações da organização.

Community cloud

Traduzindo, “nuvem comunitária”. Representa a infraestrutura de nuvem que é provisionada para uso por uma comunidade específica de clientes consumidores dos serviços, composta por entes que compartilhem as mesmas preocupações, como a missão, os requisitos de segurança, a política e as regras de conformidade.

> Uma nuvem comunitária pode ser administrada e operada por uma ou mais organizações da comunidade dona da nuvem, um terceiro ou uma combinação de ambos.

Pode também existir localmente, dentro ou fora das instalações das organizações participantes da comunidade.

Public cloud

Traduzindo, “nuvem pública”. Representa a infraestrutura de nuvem que é provisionada para uso aberto ao público em geral. Uma nuvem pública pode ser gerenciada e operada por uma organização empresarial, acadêmica ou governamental proprietária, ou ainda por alguma combinação delas. É implantada sempre nas instalações de um provedor de nuvem, fisicamente fora das instalações do proprietário da nuvem em si.

Hybrid cloud

Traduzindo, “nuvem híbrida”. Representa a infraestrutura de nuvem composta por duas ou mais infraestruturas de nuvem de modelos distintos:

- Privadas
- Comunitárias
- Públicas

Em termos físicos, as diferentes infraestruturas são vistas como entidades únicas, mas são logicamente unidas por tecnologia proprietária ou alguma tecnologia padrão que permita a portabilidade de dados e aplicativos.

Mercado de Serviço de Nuvem

Modelos de serviço em nuvem

Neste vídeo, veremos os modelos de serviço em nuvem.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Existem, atualmente, três grandes empresas que se destacam no provimento de serviços na nuvem em grande escala: Amazon Web Service (AWS); Microsoft Azure; e Google Cloud Platform (GCP). Como grandes cases de cada um dos serviços, podemos citam as empresas a seguir.

Netflix

Um dos maiores provedores de serviço de streaming de vídeo do planeta utiliza a AWS para abrigar sua infraestrutura e rodar seus sistemas.

Mercedes-Benz

A famosa marca fabricante de automóveis utiliza os serviços Azure para abrigar tudo relacionado à sua área de pesquisa e desenvolvimento.

Home Depot

O maior revendedor de materiais de reforma de casas dos Estados Unidos abriga e roda os sistemas de suas lojas on-line na GCP.

Cabe destacar que os três exemplos de provedores de nuvem citados abrigam em seu portfólio uma gama de serviços, podendo operar em qualquer um dos três modelos de serviço.

1

IaaS

O mais fundamental dos modelos de serviço permite ao cliente pode selecionar o tamanho da máquina virtual (em termos de quantidade de processamento e de memória), escolher sistemas operacionais previamente configurados e implantar softwares aplicativos dentro da máquina virtual de acordo com as necessidades do negócio. É representado por:

- Amazon EC2
- Azure Virtual Machine
- Google Compute Engine

Existem diversos tamanhos para os serviços citados, incluindo os capazes de serem contratados por pessoas comuns que simplesmente necessitem provisionar uma infraestrutura em minutos para rodar alguma aplicação específica.

2

PaaS

Esse tipo de serviço varia dos serviços de base de dados gerenciadas até os serviços mais completos de aplicativos gerenciados. O cliente pode importar um código e rodá-lo dentro de um ambiente gerenciado. São exemplos práticos os serviços:

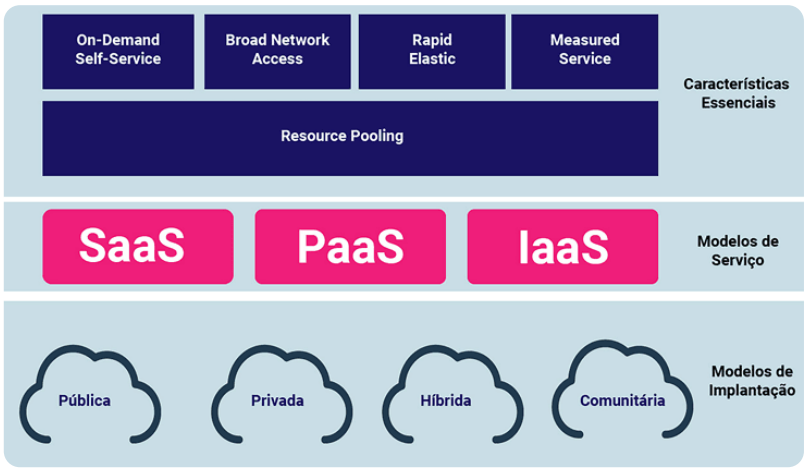
- AWS Elastic Beanstalk
- Azure Web Apps
- Google App Engine

3SaaS

O mais usado entre os modelos é um ambiente de software integralmente gerenciado onde o cliente normalmente abre um navegador web, ingressa em uma aplicação e consome serviços. Abrange uma gama de aplicações como serviço de mensageria, ERP, CRM, business analytics, entre outros. Podemos citar também outras empresas famosas nas suas respectivas áreas, com os seguintes serviços:

- Microsoft Office 365
- Google Workspaces
- Salesforce CRM
- SAP Success Factors
- Oracle Cloud HCM

A imagem a seguir apresenta uma consolidação sumarizada dos três aspectos trazidos neste conteúdo, com base em documentação do Cloud Security Alliance (CSA), um importante órgão mundial na área de serviços em nuvem que será tema de estudo adiante.



Consolidação dos aspectos introdutórios de serviços em nuvem

Verificando o aprendizado

Questão 1

De acordo com um novo paradigma de computação, uma empresa que oferece serviços de computação deve possuir cinco características essenciais para ser caracterizada como uma provedora de serviços em nuvem. Assinale a alternativa em que apresente alguns deles.

A

Software as a service; platform as a service; e infrastructure as a service.

B

Measured service; rapid elastic; e resource polling.

C

Private cloud; public cloud; hybrid cloud.

D

On-demand self-service; measured service; e software as a service.

E

On-demand self-service; platform as a service; e infrastructure as a service.

A alternativa B está correta.

O NIST categoriza o provimento de serviço em nuvem a partir de cinco característica essenciais: on-demand self-service; broad network access; measured service; rapid elastic; e resource polling.

Questão 2

Entre os modelos de serviço de nuvem, existe um para o qual grandes players de mercado oferecem máquinas virtuais cobradas apenas pelo uso específico dos recursos provisionados, sendo possível até mesmo para pessoas comuns a sua contratação. Esse modelo é conhecido como:

A

Private Cloud.

B

SaaS.

C

PaaS.

D

IaaS.

E

On-Demand Self-Service.

A alternativa D está correta.

Os três provedores de serviços mais famosos oferecem serviços de contratação de máquinas virtuais a preços acessíveis a pessoas comuns. Para cada uma das empresas podemos citar: Amazon EC2, Azure Virtual Machine e Google Compute Engine.

Necessidades de Segurança

Aspectos de segurança

Neste vídeo, apresentaremos as principais reflexões sobre os aspectos de segurança.

> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

Não deve ser difícil compreender a importância que a segurança tem no que diz respeito aos serviços na nuvem. Imagine, no exemplo citado da Mercedes-Benz, que guarda as informações de toda a sua área de pesquisa e desenvolvimento em servidores localizados em algum lugar do planeta onde ela não detém ingerência direta sobre a segurança. Qual o valor dos segredos envolvidos com essa área e, consequentemente o valor das informações ali mantidas? Ou as pesquisas de ponta de alguém laboratório farmacêutico? Ou imagine também quanto Netflix ou Home Depot, exemplos também citados, perderiam em valor se os seus serviços parassem de funcionar por algumas horas.

A nuvem mudou o paradigma com o qual as organizações controlam seus dados, que, em grande parte, migrou do que é conhecido como on-premises, ou seja, no local, para algo distribuído por vários cantos do globo, no caso de modelos de negócios baseados em operações também dispersas por muitas áreas geográficas do planeta.

Manter estruturas de data center, com servidores, storages (armazenadores), equipamentos de rede e outros de camada de aplicação demanda vultosos investimentos, e a terceirização dos serviços para empresas especializadas que cobram apenas pela parcela utilizada otimizou muito esses custos. O custo da área física para colocação dos equipamentos e o gasto de energia, infraestrutura para conectividade, também fazem parte dessa conta e servem como um reforço para a mudança de abordagem.

> A área de computação, observada de forma ampla, conta com uma subárea bastante importante que se preocupa com a manutenção de princípios associados à informação, como confidencialidade, integridade e disponibilidade.

No ramo geral da Tecnologia da Informação, essa área é conhecida como **segurança da informação**, e especificamente no ramo dos serviços de computação em nuvem existe uma subárea do conhecimento conhecida como **cloud security** (“segurança da nuvem”), encontrada também na literatura em português como **nuvem segura**.

Os mesmos princípios gerais que norteiam a segurança da informação precisam ser adotados pelos provedores de serviço em nuvem com as devidas adaptações associadas ao contexto e ao ambiente no qual as informações são guardadas e transmitidas não apenas da origem para o destino, mas também por todos os equipamentos incluídos no caminho entre eles e que estejam sob controle do provedor do serviço.

Atenção

Independentemente do modelo de serviço implantado, a nuvem pode ser de propriedade, gerenciada e operada pela organização cliente, por terceiros ou por alguma combinação deles, e pode existir dentro ou fora das instalações da organização do cliente. Além disso, o cliente consumidor do serviço pode ter um nível de controle sobre a configuração do serviço em si bastante baixa, dependendo do modelo de serviço contratado.

O tema segurança também sofreu adaptações em termos de emprego de mecanismos a partir do novo paradigma da computação em nuvem. Vejamos alguns **aspectos comparativos** entre o modelo tradicional de data centers on-premise e os ambientes em nuvem mais atuais.

Gestão de vulnerabilidades

Neste vídeo, serão apresentados os aspectos específicos da gestão de vulnerabilidades.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Segurança física

No modelo on-premise o responsável pela segurança física era a própria organização, mas, pelo novo paradigma, fica a cargo do provedor do serviço em nuvem. Uma vez que os equipamentos estejam hospedados nas dependências do provedor, o controle de acesso físico às respectivas áreas é de responsabilidade exclusiva do provedor do serviço.

Onde está localizado o dado

No modelo on-premise a organização tinha total controle sobre esse quesito, já que abrigava todos os equipamentos dentro de suas próprias instalações. No extremo oposto do novo paradigma, o dado pode estar em qualquer lugar do planeta onde o provedor de serviços em nuvem tenha equipamentos e mantenha suas operações. Dependendo do modelo de implantação, pode existir algum nível de decisão e controle sobre a localização dos dados que esteja sob responsabilidade da organização cliente.

Gestão das vulnerabilidades

O paradigma atual da computação em nuvem tirou a responsabilidade pelo gerenciamento de atualizações de patches dos sistemas envolvidos da mão da organização cliente. De maneira geral, essa gestão passou a ser um encargo do provedor de serviço em nuvem, podendo ser compartilhado com a organização dependendo do modelo de serviço adotado.

Resposta a incidentes

Mais uma responsabilidade que se modificou a partir do novo paradigma. Nos data centers on-premise, todo o encargo de ações referentes a uma resposta a incidente ficava delegado à própria organização que cuidava dos equipamentos e dados abrigados em local de sua inteira responsabilidade. Já pelo novo paradigma dos serviços em nuvem, essa responsabilidade passou a ser compartilhada entre provedor de serviço e organização cliente, cabendo a cada um atuar dentro de uma esfera de ações.

Cumprimento de regulações normativas e legais

A respeito desse aspecto, a abordagem segue a do item anterior, cabendo tanto ao provedor de serviço em nuvem como à organização cliente tomar medidas que suportem as questões legais e normativas vigentes, dependendo dos territórios e jurisdições as quais estejam submetidos.

Muitas organizações, devido à natureza sensível dos dados com os quais têm de lidar, não estão dispostas a migrar para um modelo de implantação tipo "nuvem pública". Por motivos gerais de segurança – porque os servidores físicos estão localizados fora do seu controle direto e, às vezes, até mesmo geograficamente fora de uma jurisdição para a qual tenham um nível adequado de compreensão –, aquelas organizações adotam modelos de implantação com níveis de controle mais enquadrados sob sua própria responsabilidade.

> O fato é que a responsabilidade pelos aspectos de segurança não é tratada de forma estritamente binária, estando totalmente a cargo do provedor de serviço ou sob a organização cliente, como era no caso de um data center on-premise.

O modelo de negócios trazido pelo aumento de escala do novo paradigma fez com que os grandes provedores de serviço de nuvem investissem muito dinheiro na proteção de seus data centers, construindo serviços cada vez mais seguros, especializando mais seus funcionários e identificando incidentes de segurança e corrigindo-os mais rapidamente.

Pela escala alcançada com o novo modelo de negócio dá para arriscar dizer que os provedores de serviço em nuvem despendem mais atenção e investimento em segurança que a grande maioria das organizações seria capaz de fazer em observância a seus data centers locais. A razão para os vultosos investimentos dos grandes provedores é simples: manutenção do nível de confiança no serviço em padrão elevado.

Reflexão

Imagine o estrago que uma violação de segurança poderia provocar à imagem de um provedor de serviços em nuvem. A confiança de seus clientes poderia ser abalada a ponto de tal provedor ficar sem negócios.

Contudo, o retorno dos investimentos empregados em segurança pelos provedores de serviço em nuvem faz sentido uma vez que eles empregam seus métodos de forma padronizada com ganho de escala, alcançando de maneira eficiente objetivos como diminuição da superfície de ataque e conformidade com as regulamentações em amplitude global, a partir da padronização de boas práticas com o uso de ferramentas automatizadas.

Modelo de Responsabilidade Compartilhada

Cumprimento de regulações normativas e legais

Neste vídeo, será explicada a importância do cumprimento de regulações normativas e legais.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

A responsabilidade pela segurança não é uma variável binária, estando sob cuidados exclusivos da organização cliente ou do provedor de serviço em nuvem. Dependendo do modelo de serviço contratado, parte dessa responsabilidade pode ser passada para uma ou outra ponta. Existe uma associação óbvia com o preço pago por cada tipo de serviço, mas podemos explicar, de forma mais ampla, o funcionamento dessa divisão de encargos por meio de algo que é conhecido como **modelo de responsabilidade compartilhada**.

A partir dos três modelos de serviço, **IaaS**, **PaaS** e **SaaS**, podemos traçar uma linha divisória no ponto focal da responsabilidade, delegando a cada polo do contrato de serviço maior ou menor responsabilidade sobre os segmentos em particular. Um modelo de responsabilidade compartilhada é uma estrutura de segurança em nuvem que determina as obrigações de segurança de um provedor de computação em nuvem e suas organizações clientes, para garantir a responsabilidade de cada um.

Atenção

Quando falamos em organização cliente, devemos pensar até mesmo em um usuário comum, pessoa física, cliente que contrate uma máquina virtual para rodar algum tipo de aplicação específica na nuvem. Porém, para efeito didático, chamaremos simplesmente de cliente o polo contratante do serviço e provedor o polo contratado.

Também para efeito didático, iremos calcar a explicação do conceito de responsabilidade compartilhada no modelo de implantação "nuvem pública", pois é o modelo mais extremo de delegação de responsabilidade ao provedor do serviço em nuvem. A ideia é explicar como as responsabilidades são distribuídas dependendo do provedor e do modelo de serviço específico com base na implantação tipo "nuvem pública". Alguns exemplos de provedores serão apresentados com foco mais intenso nos três principais já mencionados: AWS, Azure e GCP. De forma geral, o tipo de modelo de serviço em nuvem determina quem é responsável por quais atividades relacionadas à segurança.

> De acordo com o Cloud Standards Customer Council, um famoso grupo de advocacia dedicado a acelerar a adoção de computação em nuvem e defender usuários da nuvem em esfera judicial, as responsabilidades dos usuários geralmente aumentam à medida que passam de SaaS para PaaS e IaaS.

A Cloud Security Alliance (CSA) é uma organização sem fins lucrativos cuja missão é “promover o uso das melhores práticas para fornecer garantia de segurança na computação em nuvem e educação sobre os usos da computação em nuvem para ajudar a proteger todas as outras formas de computação”. A CSA também enxerga, de maneira geral, que responsabilidade sobre a segurança pende mais para o lado do cliente no modelo IaaS, como a situação oposta no modelo SaaS e o modelo PaaS ocupando o meio do caminho.

Grau de responsabilidade sobre a segurança de acordo com o modelo de serviço

De forma geral, e com base em exemplos práticos, a distribuição de responsabilidades ante o modelo de serviço pode ser explicada da seguinte maneira:

1

SaaS

O provedor é responsável por quase todos os aspectos da segurança, desde a infraestrutura subjacente ao sistema aplicativo que suporta o negócio do cliente – por exemplo, uma ferramenta de ERP ou CRM – até os dados que o aplicativo produz. Ficam delegadas ao cliente algumas responsabilidades de segurança, como proteger as credenciais de login contra os ataques de phishing ou engenharia social. Serviços como Dropbox, Zoom, Microsoft 365 e Google Workspace são exemplos do tipo software como serviço e facilitam a compreensão do papel extremo que o provedor dos serviços tem, inclusive com os dados produzidos pelos softwares e armazenados na infraestrutura associada ao serviço.

2

PaaS

O provedor, oferecendo a plataforma como serviço, assume, em geral, uma responsabilidade que se estende aos aplicativos e sistemas operacionais da plataforma. Mas cabe ao usuário a responsabilidade pela segurança de qualquer código, dado ou outro conteúdo produzido na plataforma. Como exemplos dessa modalidade podemos citar serviços como Microsoft Azure App Service, AWS Elastic Beanstalk, Google Kubernetes Engine e Red Hat OpenShift, que cuidam de todas as camadas abaixo da virtualização, porém não se preocupam com a segurança do que é executado nas máquinas virtuais.

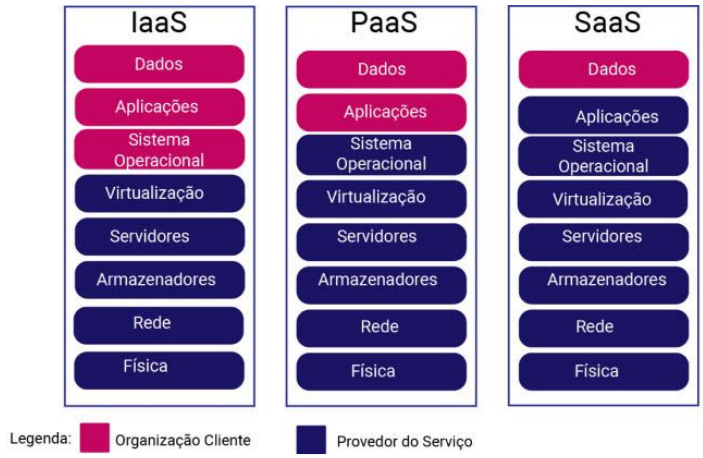
3

IaaS

O provedor de nuvem é responsável pelos serviços e armazenamento, que inclui os componentes básicos da infraestrutura de nuvem, como camada de virtualização, discos e redes. O provedor também é responsável pela segurança física dos data centers que abrigam sua infraestrutura. Os usuários de IaaS, no entanto, se responsabilizam geralmente pela segurança do sistema operacional e de toda a pilha de software necessária para executar seus aplicativos, bem como seus dados. Exemplos de serviços que podem ser citados são aqueles que servem como base para os de maior abstração: Microsoft Azure, Amazon Web Service e Google Compute Engine, ou seja, os equipamentos mais básicos, servidores e armazenadores, e os motores que garantem seu funcionamento correto.

Embora a computação em nuvem seja uma tecnologia bem-estabelecida, o conceito de responsabilidade compartilhada pode parecer confuso porque não existe um consenso de mercado para sua aplicação. De qualquer maneira, o conceito traz benefícios para modelar as linhas de demarcação de responsabilidade de segurança sob encargo de cada parte no contrato do serviço.

Para explicar o emprego geral, tomaremos como base uma pilha de elementos organizados em camadas. Considerando os três modelos de serviço e a visão sistêmica oferecida pela pilha de elementos constituintes de um serviço em nuvem, apresentamos, na imagem a seguir, a segmentação das responsabilidades com cortes em diferentes fronteiras entre camadas, caracterizando a segmentação de responsabilidades entre cliente e provedor de acordo com o modelo de serviço contratado.



Grau de responsabilidade sobre a segurança de acordo com o modelo de serviço

Exemplificando em termos práticos, ao trabalhar com IaaS, o cliente pode selecionar uma imagem pré-instalada de um sistema operacional (com ou sem software adicional instalado dentro da imagem), implantar seus aplicativos e gerenciar permissões para acesso seus dados, sendo responsável pela segurança de todas as camadas acima do sistema operacional.

Ao trabalhar com PaaS, os clientes podem ter a capacidade de controlar o código em um ambiente gerenciado (serviços como AWS Elastic Beanstalk, Azure Web Apps e Google App Engine) e gerenciar permissões para acessar nossos dados, assumindo responsabilidade pela segurança apenas das próprias aplicações e de seus dados.

Ao trabalhar com SaaS, o cliente recebe um serviço totalmente gerenciado, e tudo o que deve fazer é gerenciar permissões para acessar seus próprios dados.

Verificando o aprendizado

Questão 1

De forma ampla, o ramo do conhecimento chamado de segurança da nuvem deve se preocupar fundamentalmente em manter os mesmos princípios gerais da segurança da informação, que são:

A

clareza, integridade e intratabilidade.

B

retratabilidade, confiabilidade e disponibilidade.

C

confidencialidade, integridade e disponibilidade.

D

confidencialidade, transparência e clareza.

E

retratabilidade, integridade e transparência.

A alternativa C está correta.

Os três princípios fundamentais da segurança da informação são: confidencialidade, que garante que as informações serão acessadas apenas por quem detém direito para tal; integridade, que garante que as informações não sejam modificadas em alguma etapa da transmissão e do armazenamento; e disponibilidade, que garante que as informações estejam disponíveis sempre que necessário.

Questão 2

De forma geral, podemos ordenar os modelos de serviço em ordem crescente de aumento de responsabilidade sobre a segurança para o cliente da seguinte maneira:

A

PaaS < Iaas < SaaS.

B

IaaS < Paas < SaaS.

C

SaaS < Iaas < PaaS.

D

PaaS < Saas < IaaS.

E

SaaS < Paas < IaaS.

A alternativa E está correta.

Conforme descrito por vários organismos internacionais na área de serviços em nuvem, a responsabilidade do cliente pela segurança dos serviços aumenta na seguinte ordem para os modelos de serviço: SaaS, Paas e IaaS.

Serviço de Máquinas Virtuais

Serviços em nuvem

Neste vídeo, apresentaremos as principais reflexões sobre os serviços em nuvem.

> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

Já vimos, pela categorização atribuída pelo NIST para os tipos de serviços em nuvem, que infraestruturas, plataformas, softwares ou tecnologias acessadas pelos clientes a partir da internet, sem a necessidade de fazer download de nenhum outro software, podem ser considerados **serviços de computação em nuvem**. Veremos de forma mais específica alguns serviços associados às camadas de computação, armazenamento, rede, monitoramento e auditoria.

Falando sobre serviços em nuvem, especificamente para IaaS, o recurso mais comum e básico é a **computação**, que engloba desde as tradicionais máquinas virtuais (VMs), passando por bancos de dados gerenciados (executados nas VMs no back-end), até arquiteturas de computação mais modernas, conhecidas como **contêineres** e, eventualmente, arquiteturas que usam funções como serviço (abordagem conhecida como serverless).

Cada provedor na nuvem implementa as VMs de uma maneira diferente; porém, todas guardam a mesma ideia básica em comum com o cliente executando os passos abaixo:

1. Selecionar um tipo de máquina, normalmente caracterizada pelo tamanho, uma proporção entre a quantidade de CPU virtual (vCPU) e memória, de acordo com seus requisitos (uso geral, otimizado para computação, otimizado para memória e assim por diante).
2. Selecionar uma imagem pré-instalada de um sistema operacional (variando normalmente entre uma versão do Windows ou distribuições do Linux).
3. Configurar a parte de armazenamento (adicionando volumes adicionais, conectando-se a serviços de compartilhamento de arquivos e outros).
4. Definir as configurações de rede (desde controles de acesso à rede até microssegmentação de áreas dentro dela).
5. Configurar permissões para acessar cada um dos recursos da nuvem.
6. Implantar seus próprios aplicativos.
7. Ligar todos os serviços e começar a usar.
8. Fazer a manutenção contínua do sistema operacional, aplicando patches de atualização.

Serviço de Conteinerização

Vamos descrever brevemente o que é um contêiner. Podemos dizer que se trata de uma evolução da máquina virtual, devido às similaridades em termos de comportamento, porém, são extremamente mais enxutos e leves

em termos de uso de recursos de computação. É uma abordagem de virtualização que busca implantar e executar aplicativos distribuídos.

> Um contêiner contém tudo que é necessário para a execução da aplicação, como arquivos, variáveis de ambiente e bibliotecas próprias. Por meio dessa abordagem de virtualização, podem ser acionados vários contêineres (aplicativos distribuídos) em um único host, acessando um único kernel, ou seja, sem a necessidade de uma VM para cada aplicação. A leveza dessa abordagem propicia facilidades de escala, com os benefícios da computação em nuvem.

Em vez de precisar implantar um aplicativo rodando sobre um sistema operacional inteiro, você pode usar contêineres para implantar o aplicativo necessário, com apenas as bibliotecas e os binários mínimos do sistema operacional. Os contêineres têm os seguintes benefícios em relação às VMs:

Portabilidade

Um aplicativo pode ser desenvolvido dentro de um contêiner em uma máquina caseira e executado em grande escala em um ambiente de produção com centenas ou milhares de instâncias de contêiner.

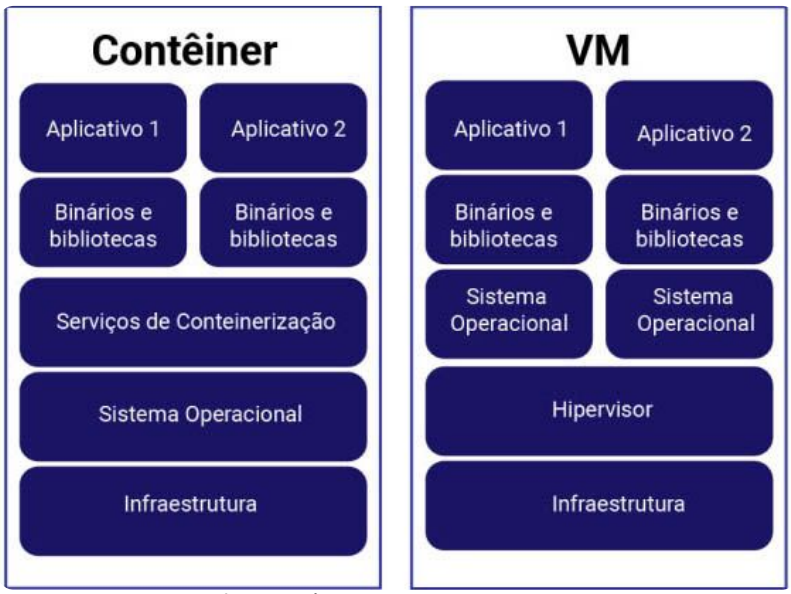
Espaço reduzido

Apenas as bibliotecas e os binários necessários são armazenados dentro de um contêiner.

Velocidade

As implementações e atualizações são mais rápidas se comparadas com as VMs.

A imagem a seguir apresenta as diferenças de arquitetura entre contêineres e VMs.



Comparação entre contêiner e máquina virtual

Ainda na fase de desenvolvimento, é possível instalar um serviço de contêiner em uma máquina caseira, criar um novo contêiner (ou baixar um existente) e concluir todo o desenvolvimento localmente. Passando para a produção, com um orquestrador (serviço de conteinerização) é possível executar centenas de instâncias do contêiner. O serviço é autogerenciado para implantação, monitoramento e verificação de integridade, reciclagem de contêineres e muito mais. Veja a seguir as características do Docker e do Kubernetes.

Docker

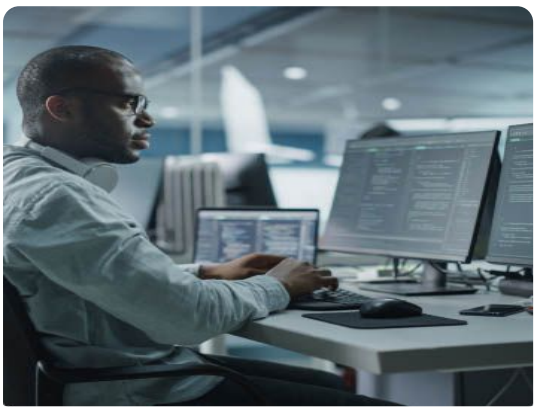
Foi adotado pela indústria como um padrão, de fato, para encapsular contêineres e, nos últimos anos, mais e mais fornecedores de nuvem começaram a oferecer suporte a uma nova iniciativa para encapsular contêineres, chamada Open Container Initiative (OCI).

Kubernetes

É um projeto de código aberto (desenvolvido originalmente pela Google) e agora está se popularizando no setor de computação em nuvem para orquestrar, implantar, dimensionar e gerenciar contêineres.

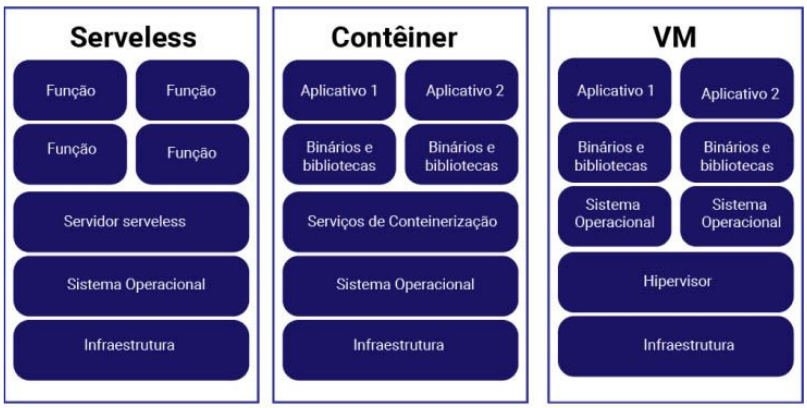
Funções como Serviço (abordagem serverless)

Embora o nome dê a entender que não há servidores, o termo serverless ou "função como serviço" significa que o cliente do serviço de nuvem não é responsável pela infraestrutura de computação subjacente, isto é, manutenção do sistema operacional, escala, gerenciamento de tempo de execução, e assim por diante.



Por intermédio dessa abordagem, basta importar um código com sintaxe de acordo com o provedor do serviço de nuvem, selecionar o interpretador, selecionar a quantidade de CPU e memória necessárias para rodar a função e definir o gatilho para invocar a função. Podemos dizer que o serverless é orientado a eventos, permitindo que os desenvolvedores criem, executem e gerenciem pacotes de aplicações como se fosse funções.

A imagem a seguir apresenta um diagrama esquemático que mostra as similaridades e diferenças da abordagem serverless para os já mencionados esquemas de implementação por contêiner e máquina virtual.



Comparação entre serverless, contêiner e máquina virtual

Alguns provedores classificam essa abordagem como um novo tipo de serviço, diferente da categorização estabelecida pelo NIST. Nesse caso, além dos tipos IaaS, PaaS e SaaS, haveria o FaaS, isto é, função como serviço.

Serviço de Base de Dados Gerenciadas

Mais uma vez, para sermos precisos, é preciso esclarecer que cada provedor tem sua própria forma de implementação de bases de dados gerenciadas.

> De forma geral, quando o cliente tem a necessidade de implantar uma compilação específica de um banco de dados, isso pode ser feito dentro de uma VM. Porém, de acordo com o modelo de responsabilidade compartilhada, se o cliente partiu para uma abordagem usando base de dados gerenciada, significa que o cliente “fugiu” do modelo IaaS. Nesse caso, o provedor do serviço de nuvem supervisiona a segurança de todo o sistema operacional e do banco de dados (incluindo hardening, backup, gerenciamento de patches, monitoramento e auditoria).

Então, uma solução gerenciada para executar um banco de dados – seja ele do tipo mais comum, como MySQL, PostgreSQL, Microsoft SQL Server, um servidor de banco de dados Oracle ou bancos de dados proprietários, como Amazon DynamoDB, Azure Cosmos DB ou Google Cloud Spanner – emprega basicamente o mesmo conjunto geral de passos a serem realizados pelo cliente.

1. Selecionar o tipo de banco de dados de acordo com sua finalidade ou caso de uso (banco de dados relacional, banco de dados NoSQL, banco de dados gráfico, banco de dados em memória, dentre outros).
2. Selecionar o banco de dados (por exemplo, MySQL, PostgreSQL, Microsoft SQL Server ou servidor de banco de dados Oracle).
3. No caso de bancos de dados relacionais, selecionar um tipo de máquina (ou tamanho) e uma proporção entre a quantidade de vCPU e memória, de acordo com seus requisitos (uso geral, otimização de memória e assim por diante).
4. Decidir, de acordo com suas necessidades, se há exigência de alta disponibilidade.
5. Implementar uma instância do banco de dados gerenciada (ou cluster).
6. Configurar o controle de acesso à rede do seu ambiente de nuvem para seu banco de dados gerenciado.
7. Ativar o registro (em logs) para qualquer tentativa de acesso ou alterações de configuração em seu banco de dados gerenciado.
8. Configurar backups em seu banco de dados gerenciado para fins de recuperação.
9. Conectar seu aplicativo ao banco de dados gerenciado e começar a usar o serviço.

Vários podem ser os motivos para se optar pelo uso de um serviço de banco de dados gerenciado em detrimento de simplesmente provisionar uma VM e instalar tudo lá dentro. Dentre essas vantagens, podemos destacar:

- A manutenção do banco de dados é de responsabilidade do provedor de nuvem.
- A atualização de patches de segurança é de responsabilidade do provedor de nuvem.
- A disponibilidade do banco de dados é de responsabilidade do provedor de nuvem.
- Os backups estão incluídos como parte do serviço (até certa quantidade de armazenamento e de histórico de backup) de acordo com planos oferecidos.
- A criptografia do tráfego e dos dados armazenados são incorporadas como parte da solução gerenciada.
- A auditoria também é incorporada como parte de uma solução gerenciada, como registro de logs e monitoramento oferecido pelo provedor.

Serviço de Armazenamento

Neste vídeo, detalharemos os serviços de armazenamento.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Outro serviço comumente oferecido nos serviços em nuvem é o **armazenamento (storage)**. Os serviços apresentados até então neste conteúdo guardam relação com recursos de computação. Storage diz respeito a um recurso de armazenamento e, normalmente, se divide em três categorias: file storage, object storage e block storage (que vamos traduzir aqui respectivamente como armazenamento de arquivo, armazenamento de objeto e armazenamento de bloco).

Todos se prestam a armazenar os dados do cliente em diferentes formatos e estão sujeitos, de maneira geral, às seguintes ameaças de segurança:

- Acesso não autorizado;
- Vazamento de dados;
- Exfiltração de dados;
- Perda de dados.

Existe outra categoria mais moderna de serviço de armazenamento, chamada de **Container Storage Interface**, conhecida pela sigla CSI.Para todos os serviços de armazenamento, considerando as principais ameaças apresentadas, existem contramedidas a serem empregadas, como veremos a seguir.

Lista de controle de acesso

Conhecidas nos provedores pela sigla ACL.

Gerenciamento de acesso e identidade

Conhecida em alguns provedores como IAM, sigla sugestiva que passa a ideia de identidade. Assim como a ACL, busca restringir o acesso ao serviço de armazenamento no ambiente da nuvem.

Criptografia

Conhecida tanto nos dados em trânsito como nos dados armazenados, busca assegurar confidencialidade.

Auditoria

Feita a partir de registro de logs de acesso sobre quem, quando e que ações foram executadas sobre os dados armazenados (por exemplo, uploads, downloads, modificações, apagamentos etc.).

Backups

Conhecidos por permitirem resgate de dados apagados, alterados ou, ao menos, retorno para uma versão anterior do dado.

Os armazenadores de objeto são um tipo especial de armazenamento destinado a armazenar dados. Os objetos (ou arquivos) são armazenados em buckets, que podem ser compreendidos como um conceito lógico similar ao conceito de algo de conhecimento mais amplo, diretórios. O acesso a arquivos nos armazenadores de objeto é feito por meio de Application Programming Interface (API) no protocolo HTTPS, com linha de comando ou interface específica, dependendo do provedor. Esses armazenadores não se destinam a armazenar sistemas operacionais ou bancos de dados.

Comentário

O armazenamento em bloco é um esquema de armazenamento como Storage Area Network (SAN) local. Oferece ao cliente funcionalidade para que ele monte um volume (disco), formate-o em um sistema de arquivos comum (como NTFS para Windows ou Ext4 para Linux, por exemplo) e armazene vários arquivos, bancos de dados ou sistemas operacionais inteiros.

O armazenamento de arquivos é um tipo de armazenamento similar ao **Network-attached Storage** (NAS) local. Oferece suporte para protocolos comuns de compartilhamento de arquivos (como NFS e SMB/CIFS). Tem a capacidade de montar um volume de um serviço de arquivo gerenciado em um sistema operacional para armazenar e recuperar arquivos paralelamente para várias VMs e de controlar as permissões de acesso ao sistema de arquivos remoto. Além disso, permite o crescimento automático do sistema de arquivos de forma transparente para o usuário.

Finalizando sobre o serviço de armazenamento, descrevemos o tipo CSI. De forma simples, podemos dizer que um CSI é um driver padrão para conectar sistemas de orquestração de contêineres, como Kubernetes, a fim de bloquear e armazenar arquivos de vários provedores de nuvem.Os provedores de serviço de nuvem mais citados, AWS, Azure e GCP, possuem serviços de armazenamento de arquivos, objetos, blocos e contêineres.

Serviço de Rede

Neste vídeo, detalharemos os serviços de armazenamento.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Outra classe de serviços em nuvem são os associados ao recurso rede, tais como:

- Domain Name System (DNS);
- Content Delivery Network (CDN);
- Virtual Private Network (VPN);
- Web Application Firewall (WAF);
- Proteção Distributed Denial of Service (DDoS protection).

Dentro de uma infraestrutura de nuvem, as redes são configuradas virtualmente, o que é conhecido como virtual networking. As redes virtuais dão poder para o cliente realizar configurações específicas. Porém, com essa abordagem, criam um desvio no modelo comum de responsabilidade compartilhada, uma vez que tornam a responsabilidade pela segurança da rede algo dividido entre cliente e provedor.

> A camada física da rede permanece sob encargo do provedor, mas a camada que possibilita o acesso entre servidores virtuais, serviços de armazenamento e bancos de dados gerenciados fica a cargo do cliente.

Os serviços gerenciados de DNS incluem funcionalidade para traduzir nomes de host para endereços IP, diferentes tipos de serviços de registros DNS (como Alias, CNAME etc.), balanceamento de carga, e outros.

Um serviço CDN é um serviço de entrega de conteúdo com base na abordagem de que quanto mais próximo do cliente estiver o conteúdo, mais eficiente o serviço será. Então, uma CDN armazena conteúdo em cache

(como imagens, vídeos ou páginas da web estáticas) em vários locais ao redor do mundo, permitindo que os clientes recebam o conteúdo rapidamente de um desses locais mais próximos. CDNs também servem como um mecanismo extra de defesa contra os ataques DDoS por servirem de camada prévia de resposta a requisições, ou seja, um dos primeiros serviços que atendem a solicitação de um cliente, antes mesmo que a solicitação chegue aos servidores ou aplicativos.

As VPNs oferecem acesso mais seguro a recursos privados em redes não confiáveis. Combinadas com um firewall, uma VPN permite que as organizações acessem e gerenciem seus recursos internos (por meio do que é conhecido como **túnel** VPN) de maneira segura. Uma VPN permite que usuários corporativos se conectem ao ambiente de nuvem de sua organização a partir da rede corporativa ou de casa por uma conexão criptografada. A conexão com o ambiente de nuvem é transparente para o cliente, isto é, tem a mesma aparência que trabalhar localmente de dentro da rede corporativa. É bastante comum nos principais provedores que a VPN imponha o uso de **autenticação multifator** (MFA) para usuários finais que se conectam ao ambiente.

Um serviço WAF é um firewall de camada de aplicação com capacidade de detectar e mitigar ataques comuns ao protocolo HTTP/HTTPS. Suas regras tomam por base a defesa aos ataques expostos publicamente sobre aplicações web.

Como têm largura de banda muito grande, os provedores de nuvem podem oferecer, adicionalmente, mecanismos para proteger os ambientes dos clientes contra os ataques DDoS, usualmente utilizando grupos de recurso autoescaláveis combinados com serviços de balanceamento de carga.

Amazon

Possui um serviço específico para esse fim, chamado AWS Shield, que no modo avançado opera conjuntamente com Route53 (DNS), CloudFront (CDN) e Elastic Load Balancing (ELB).

Microsoft

Oferece o Azure DDoS Protection, também com um modo de operação avançada que se combina com outras ferramentas como gateway e WAF.

Google

Emprega a mesma abordagem com o Google Cloud Armor Standard para configurações mais básicas e o Managed Protection Plus integrado a outros serviços.

Serviço de Monitoramento e Auditoria

O monitoramento é uma parte crucial da segurança na nuvem. O monitoramento refere-se às atividades de registro feitas nos serviços do ambiente de nuvem. Eventos de login do usuário (sucesso e falha) e ações tomadas (quem fez o quê e quando, e qual foi o resultado final com sucesso ou falha) são os exemplos principais.

> O registro documentado de todas as ações realizadas é conhecido como trilha de auditoria. É importante que esse registro de eventos seja armazenado em um repositório central de logs com acesso limitado, cumprindo o conceito da necessidade de conhecimento.

O sistema de geração de alertas de acordo com regras pré-configuradas, como só alertar quando a conta root ou o administrador conseguir fazer login com sucesso no console de gerenciamento, também faz parte do serviço de monitoramento e auditoria.

Atenção

Ao falarmos sobre monitoramento e auditoria, todos os serviços da nuvem vistos neste conteúdo podem e devem enviar seus logs para um serviço central que os organize e os mantenha em formato compatível para análise posterior. Recomenda-se realizar uma análise de risco nos respectivos serviços para habilitar o registro de eventos de dados de acordo com os objetivos de segurança estipulados porque o custo do armazenamento de eventos versus o valor pode não ser compensador, uma vez que o armazenamento de logs pode ser explosivo em termos de consumo de recursos.

Existe uma classe de produto conhecida como **Security Information and Event Management (SIEM)**, muito empregada atualmente em soluções complexas de monitoramento e auditoria que se responsabiliza por alertar condições associadas de logs em mais de um serviço conjuntamente.

Isto é, se um evento ocorre no serviço A e outro no serviço B, a correlação entre essa conjunção de fatores pode representar uma assinatura de risco muito mais alta do que cada um dos eventos separadamente. Apenas nessa condição específica seria disparado o alerta, economizando recursos para análise de um problema ou resultando numa ação inadequada de proteção devido a um falso positivo de ataque ao ambiente de nuvem.

Verificando o aprendizado

Questão 1

Com base nas afirmativas a seguir, assinale a alternativa correta sobre os serviços em nuvem mais associados à computação.

I. Os contêineres tendem a ser menores e mais rápidos que as máquinas virtuais.
II. Na abordagem serverless, o cliente do serviço de nuvem não possui encargo sobre a infraestrutura de computação.
III. Quando o cliente usa uma base de dados gerenciada, o provedor supervisiona não apenas o sistema operacional como também a manutenção do banco de dados (incluindo hardening, backup, gerenciamento de patches e monitoramento).
IV. O espaço ocupado por contêineres tende a ser maior do que o ocupado pelas máquinas virtuais, pois aqueles precisam guardar todos os binários e bibliotecas.

A

Apenas a IV está correta.

B

Apenas a I está correta.

C

Apenas a II está correta.

D

I e II estão corretas.

E

I, II e III estão corretas.

A alternativa E está correta.

Contêineres são estruturas similares às máquinas virtuais, porém muito mais enxutas. A abordagem serverless emprega funções como serviço, deixando a cargo do provedor do serviço cuidar da infraestrutura de computação. A opção do cliente pelo uso de base de dados gerenciada o libera dos cuidados com a segurança do sistema gerenciador do banco de dados em si.

Questão 2

São tipos de serviço de armazenamento:

A

arquivo, bloco e pastas.

B

arquivo, bloco e objetos.

C

contêineres, objetos e pastas.

D

blocos, binários e bibliotecas.

E

bibliotecas, objetos e pastas.

A alternativa B está correta.

O serviço de armazenamento em nuvem pode ser categorizado em: armazenamento de arquivos, de blocos, de objetos e de contêineres.

Apresentando a Cloud Security Alliance (CSA)

Orientações da Cloud Security Alliance

Neste vídeo, abordaremos as principais reflexões sobre as orientações da Cloud Security Alliance.

> **Conteúdo interativo**
>
> Acesse a versão digital para assistir ao vídeo.

A Cloud Security Alliance (CSA) é a organização líder em escala global dedicada a definir e fomentar conscientização sobre as melhores práticas de segurança em ambientes de computação em nuvem.

> **Dica**
>
> O site cloudsecurityalliance.org mantém um blog com diversos artigos interessantes para vários níveis de conhecimento na área, além de white papers instrutivos sobre resultados de pesquisas em segurança na nuvem. Também mantém cursos e certificações e um programa de associação para membros.

A CSA fornece orientações sobre segurança na nuvem como forma de suporte aos objetivos de negócio, gerenciando e mitigando riscos associados com a adoção de soluções abrigadas em ambiente de nuvem organizadas em quatorze domínios, veja a seguir.

- **DOMAIN 1**: Conceitos e arquiteturas de computação em nuvem.
- **DOMAIN 2**: Governança e gestão de risco corporativo.
- **DOMAIN 3**: Questões legais, contratos e descoberta eletrônica.
- **DOMAIN 4**: Gestão de conformidade e auditoria.
- **DOMAIN 5**: Governança da informação.
- **DOMAIN 6**: Plano de gestão e continuidade do negócio.
- **DOMAIN 7**: Segurança de infraestrutura.
- **DOMAIN 8**: Virtualização e contêineres.
- **DOMAIN 9**: Resposta a incidentes.
- **DOMAIN 10**: Segurança de aplicativos.
- **DOMAIN 11**: Segurança e criptografia de dados.
- **DOMAIN 12**: Gerenciamento de identidade, direitos e acesso.
- **DOMAIN 13**: Segurança como serviço.
- **DOMAIN 14**: Tecnologias relacionadas.

Conceitos e Arquiteturas de Computação em Nuvem

Esse domínio provê uma estrutura conceitual (**framework**) que descreve e define computação em nuvem, propõe uma terminologia base e detalha estruturas lógicas e arquiteturais para ambientes em nuvem.

A computação em nuvem pode ser vista como uma tecnologia ou coleção de tecnologias, um modelo de operações, modelo de negócios, um paradigma etc. A definição mais enxuta para computação em nuvem, na visão da CSA, é "um novo modelo operacional e conjunto de tecnologias para gerenciar conjuntos de recursos computacionais compartilhados". Sob uma perspectiva prática e simples, a nuvem pode ser descrita como um conjunto de recursos, tais como processadores e memórias, colocado para trabalhar conjuntamente (resource pooling) em uma operação que utiliza virtualização.

Comentário

O NIST define o usuário da nuvem, mencionado aqui como cliente ou organização cliente, como "a pessoa ou organização que requisita e usa recursos", e provedor de serviços de nuvem como "a pessoa ou organização que entrega os recursos".

As técnicas-chave para criar uma nuvem são **abstração** e **orquestração**. O provedor abstrai os recursos de infraestrutura física para criar o pool e utiliza orquestração para coordenar a montagem e entrega do pool de recursos para os clientes. Essa nova abordagem é uma evolução da virtualização tradicional, com a qual se fazia possível abstrair os recursos, mas não orquestrava a operação deles de forma conjunta. Outros importantes conceitos são:

Segregação

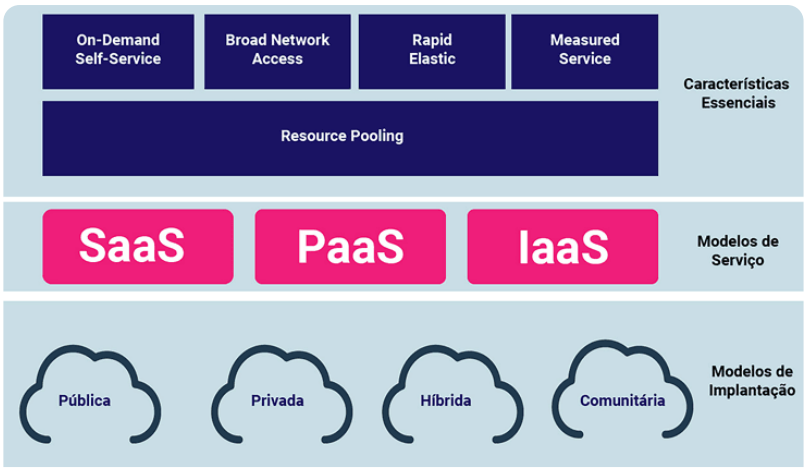
Que "permite que o provedor de nuvem divida os recursos para os diferentes grupos"

Isolamento

Que "garante que um grupo não possa ver ou modificar os ativos uns dos outros".

A junção da segregação com o isolamento é conhecida como **multilocação** e não se aplica apenas a diferentes organizações, podendo também ser usada para dividir recursos entre diferentes unidades em uma única empresa ou organização.

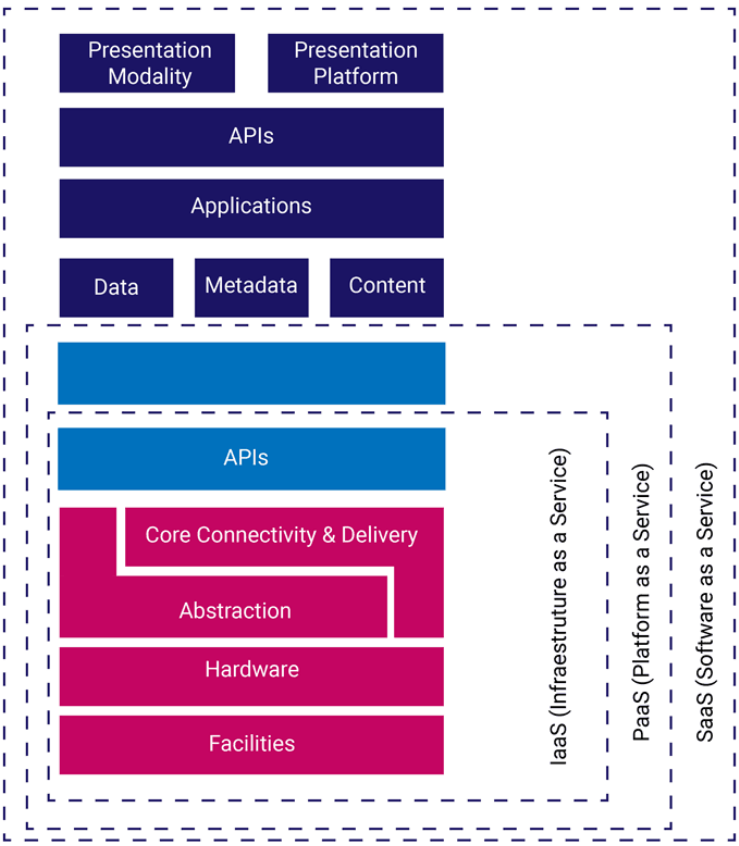
A CSA usa modelagem preconizada pelo NIST sintetizada na imagem: **Consolidação dos aspectos introdutórios de serviços em nuvem**. Endossa também o modelo preconizado pela **Norma ISO/IEC 17788:2014 – Information technology – Cloud computig – Overview and vocabulary**, um documento mais detalhado e exaustivo que apresenta um modelo de referência adicional.



Consolidação dos aspectos introdutórios de serviços em nuvem

> Sobre a modelagem arquitetural, a CSA provê fundamentos para ajudar os profissionais de segurança a tomarem decisões embasadas, bem como uma linha de base para a compreensão de modelos emergentes mais complexos.

Podemos dizer que o modelo de arquitetura preconizado pela CSA se presta a um metamodelo para os provedores montarem e oferecerem seus serviços da forma mais adequada a seus modelos de infraestrutura e negócios no mundo real. A arquitetura de referência da CSA é apresentada na imagem adiante.



Arquitetura de referência da CSA

Observando por um ponto de vista de mais alto nível, tanto a computação em nuvem quanto a tradicional aderem a um modelo lógico que ajuda a identificar diferentes camadas com base na sua funcionalidade. Isso é útil para ilustrar as diferenças entre os diferentes modelos de computação:

Infraestrutura

Os principais componentes de um sistema de computação, que são: computação, rede e armazenamento. São as partes móveis que funcionam como a base sobre a qual todo o resto é construído

Metaestrutura

Os protocolos e mecanismos que fornecem a interface entre a camada de infraestrutura e as demais camadas. É o amálgama que une as tecnologias e possibilita o gerenciamento e a configuração.

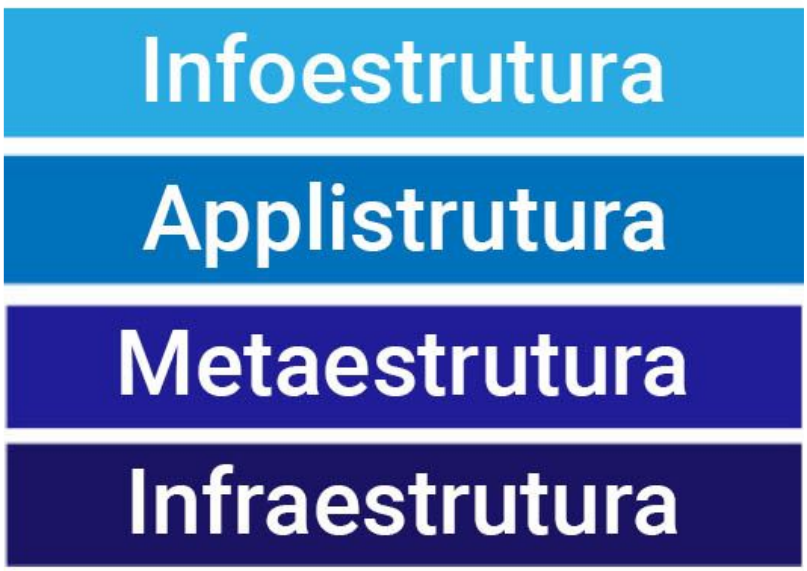
Appliestrutura

A palavra é uma contração que representa os aplicativos implantados na nuvem e os serviços de aplicativos subjacentes usado para construí-los. Por exemplo, recursos de plataforma como serviço, filas de mensagens, análise de inteligência artificial ou notificação, e todos de mais alto nível de abstração.

Infoestrutura

Os dados e informações que podem ser o conteúdo em um banco de dados, armazenamento de arquivos etc.

A imagem a seguir apresenta a pilha de camadas que representa essa arquitetura na visão funcional.



Arquitetura funcional de computação e nuvem

Os enfoques de segurança variam de acordo com a camada, mas guardam os mesmos princípios básicos de segurança da informação: confidencialidade, integridade e disponibilidade. Computação tradicional ou em nuvem se diferenciam sobretudo pela camada de metaestrutura. A nuvem inclui os componentes para

gerenciamento dos recursos das camadas superiores. A infraestrutura da nuvem também se diferencia pelo já explicado conceito da multilocação.

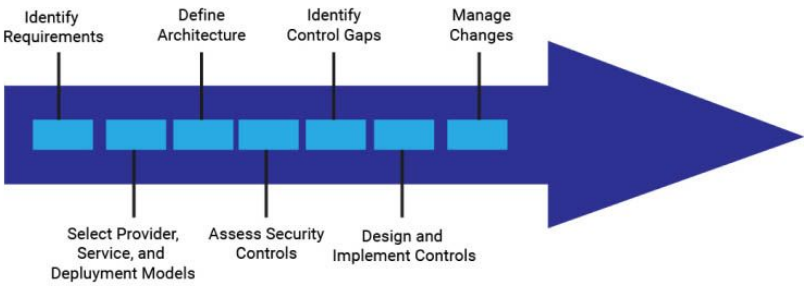
Os modelos de segurança na nuvem são ferramentas para ajudar a orientar as decisões de segurança. O CSA recomenda alguns modelos:

- CSA Enterprise Architecture;
- CSA Cloud Controls Matrix;
- NIST – Cloud Computing Security Reference Architecture (NIST Special Publication 500-299);
- ISO/IEC FDIS 27017 – Information technology – Security techniques – Code of pratice for information security controls based on ISO/IEC 270002 for cloud services.

A CSA estabelece um processo de alto nível, relativamente simples para gerenciar a segurança em nuvem, descrito textualmente pelos passos:

- Identificar os requisitos de segurança e conformidade necessários a quaisquer controles existentes;
- Selecionar o provedor de nuvem, serviço e modelos de implantação;
- Definir a arquitetura;
- Avaliar os controles de segurança;
- Identificar lacunas de controle;
- Projetar e implementar controles para preencher as lacunas;
- Gerenciar as mudanças ao longo do tempo.

Veja a seguir sintetizados na imagem a seguir:



Processo para gestão de segurança em nuvem

Uma vez estudado o domínio mais fundamental das orientações de segurança em nuvem do CSA, apresentaremos uma visão geral sintetizada dos outros treze domínios. Eles destacam áreas com as quais a computação em nuvem deve se preocupar. Os domínios restantes são divididos em duas grandes categorias: governança e operação.

Os **domínios de governança** são amplos e abordam questões estratégicas e políticas em um ambiente de computação em nuvem. Já os **domínios de operação** se concentram em questões de segurança mais táticas e implementação dentro da arquitetura.

Domínios de Governança

Governança e gestão de risco empresarial

É a capacidade de uma organização governar e gerir o risco corporativo introduzido a partir da adoção da computação em nuvem. Em termos práticos, tais preocupações encampam, por exemplo:

- A capacidade de as organizações clientes avaliarem adequadamente os riscos associados aos serviços do seu provedor de nuvem.
- Precedência legal para os casos de violações de acordos.
- Delegação de responsabilidades na proteção de dados confidenciais quando ambas as partes podem ser culpadas por vazamentos, perdas e outros danos associados aos dados.
- Como as questões jurisdicionais, limites internacionais etc. podem afetar esses problemas.

Aspectos legais

Possíveis problemas legais no uso da computação em nuvem. Incluem requisitos de proteção para informações e sistemas computacionais; leis de não divulgação e de violação de segurança; requisitos regulatórios; requisitos de privacidade; leis internacionais etc.

Compliance e gerenciamento de auditorias

Manter e comprovar a conformidade no uso da computação em nuvem. As questões relacionadas à avaliação de como a computação em nuvem afeta a conformidade com as políticas de segurança interna bem como vários requisitos de conformidade (regulamentares, legislativos e outros) estão incluídos nesse domínio, que engloba ainda algumas orientações sobre como provar a conformidade durante uma auditoria.

Governança da informação

Governança dos dados que são colocados na nuvem. Tais preocupações devem encampar a identificação e o controle de dados na nuvem, bem como controles de compensação que possam ser usados para lidar com a perda de controle físico ao mover dados para a nuvem. Além disso, também lida com questões como quem é responsável pela confidencialidade, integridade e disponibilidade dos dados.

Domínios de Operação

Plano de gestão e continuidade do negócio

Proteção do plano de gestão e de todas as interfaces administrativas usadas para acessar a nuvem, incluindo consoles da web e APIs. Além disso, observa as garantias para a continuidade dos negócios nas implantações em nuvem.

Segurança da infraestrutura

Fundamentos para se operar seguramente. Seus aspectos incluem a segurança dos níveis inferiores da pilha de serviços, como segurança física das instalações, hardware para processamento, memória e armazenamento, rede, e software para orquestração do pool de recursos.

Virtualização e conteinerização

Neste vídeo, será explicado os detalhes sobre o domínio de operação “Virtualização e Conteinerização”.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Aspectos de segurança que cobrem uma grande camada de tecnologia associada à abstração do pool de recursos, especificamente a computação, a rede, os armazenadores e os contêineres em sua relação com o serviço de virtualização. Em termos práticos refere-se à segurança dos hipervisores, contêineres e redes definidas por software.

> Compreender os impactos da virtualização na segurança é fundamental para arquitetar e implementar adequadamente a segurança na nuvem.

Em termos práticos, refere-se à segurança dos hipervisores, contêineres e redes definidas por software.

Resposta a incidentes

Detecção, resposta, notificação e remediação de incidentes de formas apropriadas. Estabelece os limites de responsabilidade por ações compartilhadas entre provedor e cliente para permitir o tratamento adequado de incidentes e a análise forense.

Segurança das aplicações

Neste vídeo, serão explicados os detalhes sobre o domínio de operação “Segurança das aplicações”.

> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

Proteção dos softwares aplicativos que estão sendo executados ou implantados na nuvem. Na prática, inclui questões como saber se é apropriado migrar ou projetar um aplicativo para ser executado na nuvem e, em caso afirmativo, que tipo de plataforma de nuvem é mais apropriada (SaaS, PaaS ou IaaS).

Criptografia e segurança de dados

Implementação dos mecanismos de segurança e criptografia de dados e toda a garantia de gerenciamento de chaves, considerando os aspectos de escalabilidade dos serviços e dos aplicativos que rodam no ambiente da nuvem.

Gerenciamento de acessos, privilégios e identidades

Gerenciamento de identidades apoiado nos serviços de diretório para fornecer controle de acesso. Identidades, privilégios e acessos (IAM) são profundamente impactados pela computação em nuvem. Tanto na nuvem pública quanto na particular, as duas pontas (provedor e cliente) são necessárias para gerenciar o IAM sem comprometer a segurança, e a divisão exata das responsabilidades é um aspecto extremamente crítico.

Tecnologias relacionadas

Tecnologias estabelecidas e emergentes que tenham estreito relacionamento com a computação em nuvem, incluindo Big Data, Internet das Coisas (IoT), computação móvel etc.

Verificando o aprendizado

Questão 1

De acordo com as orientações do CSA, quais os conceitos que, conjuntamente, compõem a multilocação?

A

Abstração e orquestração.

B

Abstração e segregação.

C

Segregação e isolamento.

D

Orquestração e isolamento.

E

Segregação e orquestração.

A alternativa C está correta.

A multilocação, funcionalidade utilizada para dividir recursos entre diferentes unidades em uma única empresa ou organização ou em diferentes organizações, é composta pelos conceitos de segregação e isolamento.

Questão 2

De acordo com as orientações do CSA, quais são os dois grupos de domínio, além do conceitual?

A

Tático e operacional.

B

Governança e operação.

C

Estratégico e governança.

D

Estratégico e operacional.

E

Governança e tático.

A alternativa B está correta.

Além do domínio conceitual, que se preocupa com os fundamentos, existem dois grupos de domínios de acordo com as orientações do CSA: governança e operações.

Considerações finais

Neste conteúdo, você foi apresentado a diversos conceitos que guardam íntimo relacionamento com a segurança de ambientes em nuvem. Muitos são herança dos fundamentos de Segurança da Informação, porém adaptados para o paradigma mais moderno de computação em nuvem.

O NIST, órgão norte-americano responsável pela elaboração de padrões em Tecnologia da Informação, definiu os conceitos fundamentais para compreensão da computação em nuvem. Descreveu modelos de serviço, de implantação e as características essenciais que todos os provedores de serviços em nuvem devem ter. Todo contrato de prestação de serviço em nuvem apresenta responsabilidades que devem ser compartilhadas entre os polos provedores do serviço e tomador do serviço. Para tratar esse problema concebeu-se um modelo geral de responsabilidades compartilhadas que serve como linha-base para guiar termos de serviço dos provedores de serviço em nuvem perante seus clientes.

São muitos os serviços providos, cada qual com suas próprias nuances de segurança, e as reponsabilidades dependem da implementação do provedor, bem como do modelo de serviço adotado. Entre esses serviços, organizando em grupos de camadas, destacamos os serviços de computação, de rede, de armazenamentos, e de monitoramento e auditoria, com seus respectivos serviços constituintes. Além dos aspectos de segurança organizados por tipo de serviço, apresentamos também as orientações de segurança do Cloud Security Alliance (CSA) organizadas em seus onze domínios agrupados em três grupos principais: conceitual, governança e operações. Os grupos cobrem aspectos de segurança relacionados com as principais áreas críticas que um ambiente de nuvem deve tratar.

Podcast

Ouça um resumo dos principais tópicos abordados no conteúdo.

Conteúdo interativo

Acesse a versão digital para ouvir o áudio.

Explore +

Pesquise na internet sobre os termos **Network-attached storage**, **Object Store**, **Web Application Firewall – WAF** e **Security information and event management – SIEM** para ampliar seus conhecimentos.

Veja também **Kubernetes Container Storage Interface (CSI) Documentation, Open Container Initiative, O que é um contêiner** e **OWASP Serverless Top 10**.

Referências

CLOUD SECURITY ALLIANCE. **Security Guidance**: For Critical Areas of Focus In Cloud Computing v4.0 – Cloud Security Alliance, 2021. Consultado na internet em: 30 nov. 2022.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**. The NIST Definition of Cloud Computing**. Special Publication 800-145, 2011.