Computação em Nuvem

Arquitetura de Aplicações em Nuvem

Ma. Patrícia Valério Martinez

- Unidade de Ensino: 04.
- Competência da Unidade: Arquitetura de Aplicação em Nuvem e modelos; Qualidade de Serviço em Nuvem e Mecanismos; Ameaças das Aplicações em Nuvem e Mecanismos de Segurança em Nuvem.
- Resumo: o objetivo é aprender sobre os modelos de arquitetura para aplicações em nuvem.
- Palavras-chave: Arquitetura, modelos, qualidade, ameaças e segurança.
- Título da Teleaula: Arquitetura de Aplicações em Nuvem.
- Teleaula nº: 04.

Contextualizando

- Arquitetura de Aplicação em Nuvem e modelos;
- Qualidade de Serviço em Nuvem e Mecanismos;
- Ameaças das Aplicações em Nuvem;
- Mecanismos de Segurança em Nuvem.

Conceitos

Arquitetura de Aplicação em Nuvem

Arquitetura de Aplicação em Nuvem

- As aplicações em nuvem são sistemas de software complexos, na medida em que implementam diversas funcionalidades e fazem uso de variados serviços que são acessados por meio da Internet.
- Para lidar com essa complexidade as aplicações podem ser divididas em módulos ou componentes funcionais.

Arquitetura de Aplicação em Nuvem

- Por exemplo, uma aplicação web de comércio eletrônico pode incluir vários módulos, como um responsável pela autenticação de usuários ou outro responsável pela geração de relatórios de vendas.
- A definição da arquitetura de uma aplicação consiste em definir quais seriam os módulos funcionais e como eles devem interagir entre si.

Arquitetura de Aplicação em Nuvem

- O projeto da arquitetura de aplicações em nuvem é um grande desafio e as decisões nele envolvidas podem influenciar vários aspectos da aplicação, como desempenho, escalabilidade e segurança.
- Existem três modelos para a arquitetura de aplicações distribuídas: arquitetura centralizada, descentralizada e híbrida.

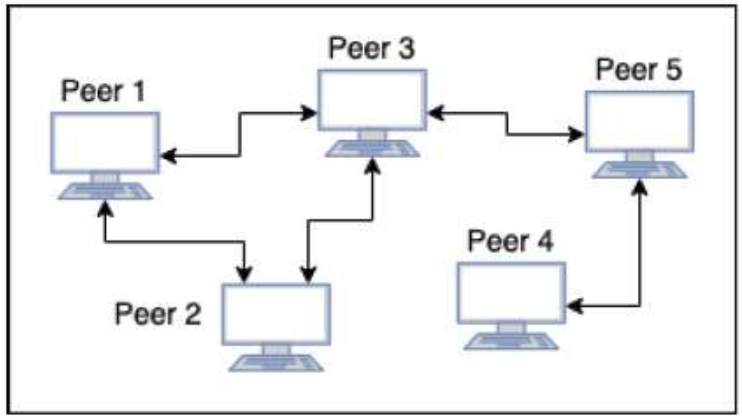
Arquitetura Centralizada

- A arquitetura centralizada é o modelo tradicional cliente-servidor.
- Quando um componente requisita um serviço de outro, o que faz a requisição é o cliente e o que responde é o servidor.
- As aplicações web representam um exemplo típico do modelo de arquitetura centralizada: o servidor web responde as requisições enviadas por navegadores web.

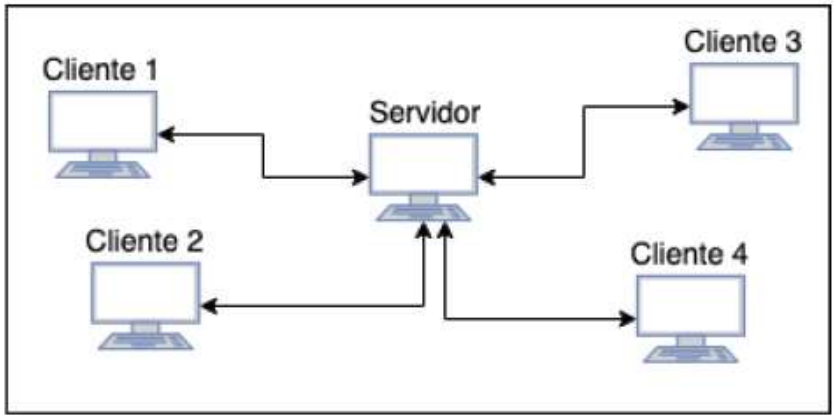
Arquitetura Descentralizada

- A arquitetura descentralizada é caracterizada pelo modelo Peer-to-Peer (P2P).
- Não há distinção entre clientes e servidores e os componentes de software podem fazer requisições entre si de forma arbitrária.

Arquitetura Centralizada e Descentralizada



P2P



Cliente-Servidor

Fonte: KLS, Malheiros Neumar (2019).

Arquitetura de Aplicação em Nuvem

- Uma alternativa interessante a escolher um modelo centralizado ou descentralizado é a arquitetura híbrida, na qual uma mesma aplicação utiliza os dois modelos, ou seja, algumas funcionalidades da aplicação são implementadas na forma cliente-servidor e outras são implementadas na forma P2P aproveitando o melhor de cada arquitetura.

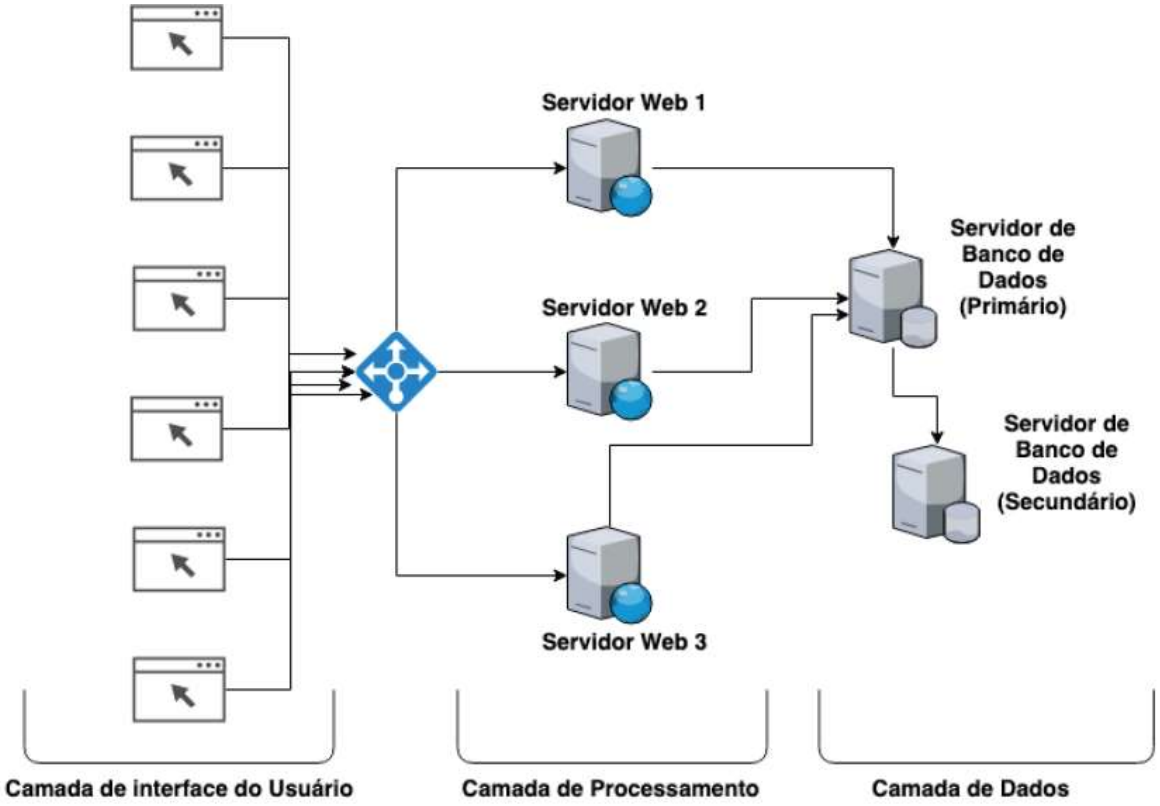
Arquitetura Múltiplas Camadas

- Devido as arquiteturas centralizada e descentralizada serem complexas ou problemas de desempenho e escabilidade surge novas abordagens.
- Uma delas é o modelo cliente-servidor com uma arquitetura em múltiplas camadas.
- Nesse modelo de arquitetura a aplicação é dividida em várias camadas sendo cada uma delas responsável por um conjunto específico de funcionalidades.

Arquitetura Múltiplas Camadas

- Os componentes de uma camada podem interagir com os componentes das camadas vizinhas, além de serem executados em servidores diferentes para melhorar o desempenho.
- Nesse caso temos uma separação física entre as camadas.

Arquitetura Múltiplas Camadas



Fonte: KLS, Malheiros Neumar (2019).

Modelos de Arquitetura – Monolítico

- As principais funcionalidades de uma aplicação são implementadas na camada de processamento, por exemplo, na forma de um Serviço Web (*Web Service*).
- Esse serviço é denominado monolítico quando todos os seus módulos funcionais estão implementados em um único componente de software.

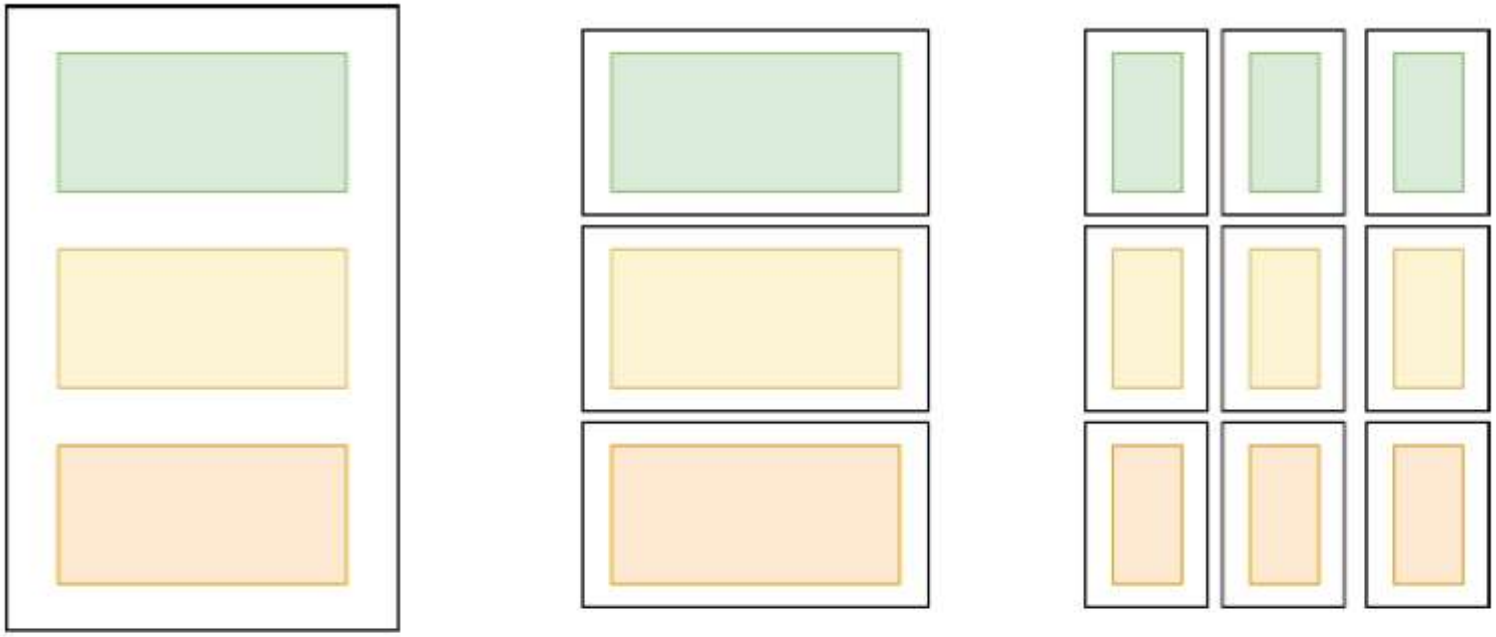
Modelos de Arquitetura – Monolítico

- Se a aplicação possui muitas funcionalidades, esse serviço pode apresentar alguns problemas como: ocupação de muito espaço de memória, dificuldade de implementar correções e de evolução do software, alto custo de replicação, etc.
- Com isso novas arquiteturas de serviços web foram propostas para melhorar o desempenho e a escalabilidade, assim como facilitar a replicação.

Modelos de Arquitetura

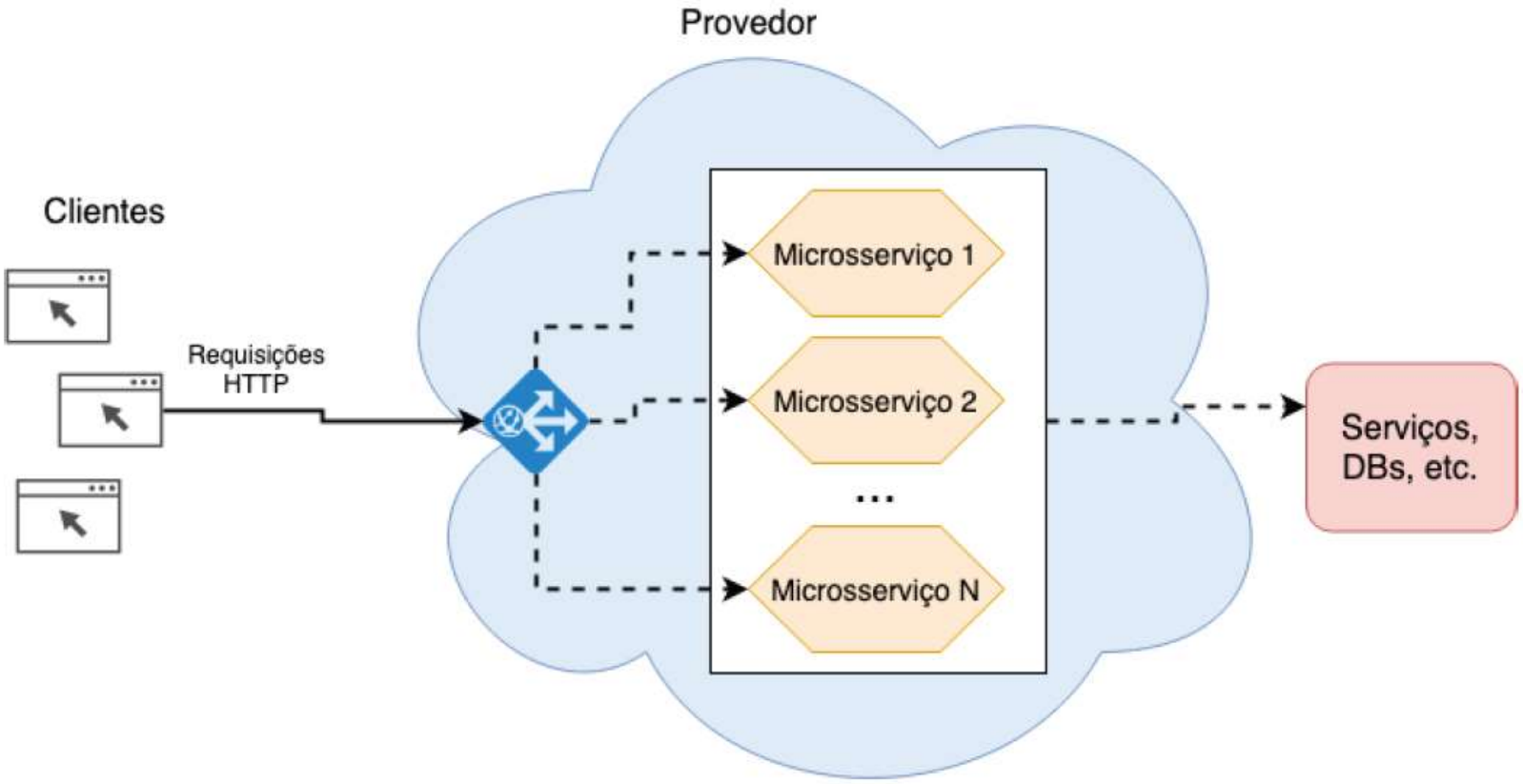
- A ideia é dividir o serviço web monolítico em diversos componentes de software independentes.
- Entre as principais abordagens podemos citar a arquitetura de microsserviços e a arquitetura *Serverless* (Computação sem Servidor), cujo principal exemplo é o modelo Função como Serviço (FaaS – Function as a Service).

Evolução – Modelos de Arquitetura



Fonte: KLS, Malheiros Neumar (2019).

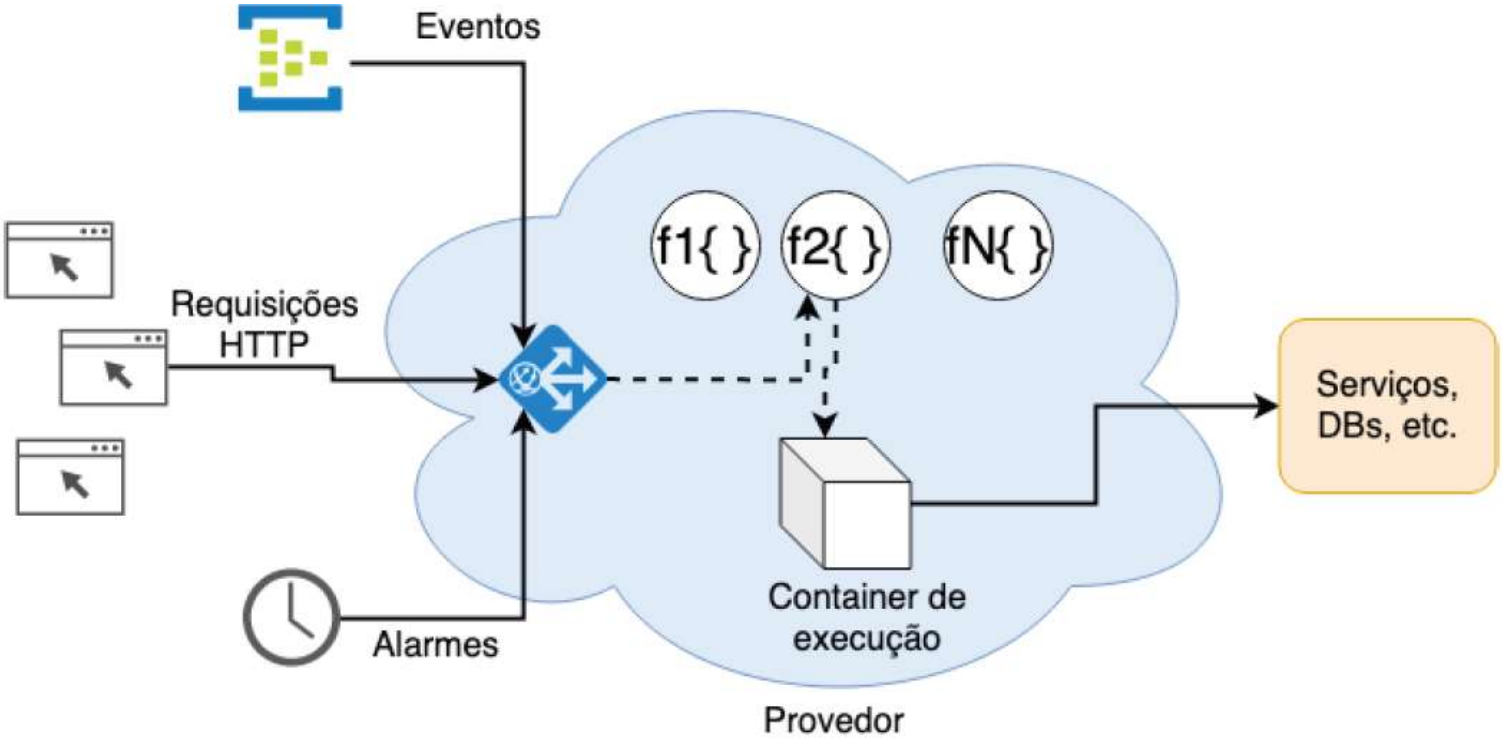
Modelos de Arquitetura – Microserviços



Modelos de Arquitetura – Serverless

- O próximo passo na evolução dos modelos de arquitetura foi o paradigma de Computação sem Servidor (*Serverless*).
- No modelo *Serverless* o nível de granularidade é ainda maior que na arquitetura de microsserviços.
- O objetivo é explorar o fato de que cada microsserviço pode ainda ser dividido em funções específicas e cada função pode ser invocada de forma independente por um software cliente.

Modelos de Arquitetura – Serverless



Modelos de Arquitetura – Serverless

- O nome "Computação sem Servidor" remete a ideia de que o cliente não precisa alocar servidores para a execução de uma aplicação é feito dinamicamente pelo provedor quando alguma função da aplicação é invocada.
- A arquitetura *Serverless* apresenta benefícios para aplicações em nuvem e o mais evidente é que os desenvolvedores não precisam se preocupar em alocar servidores o que facilita a implantação da aplicação.

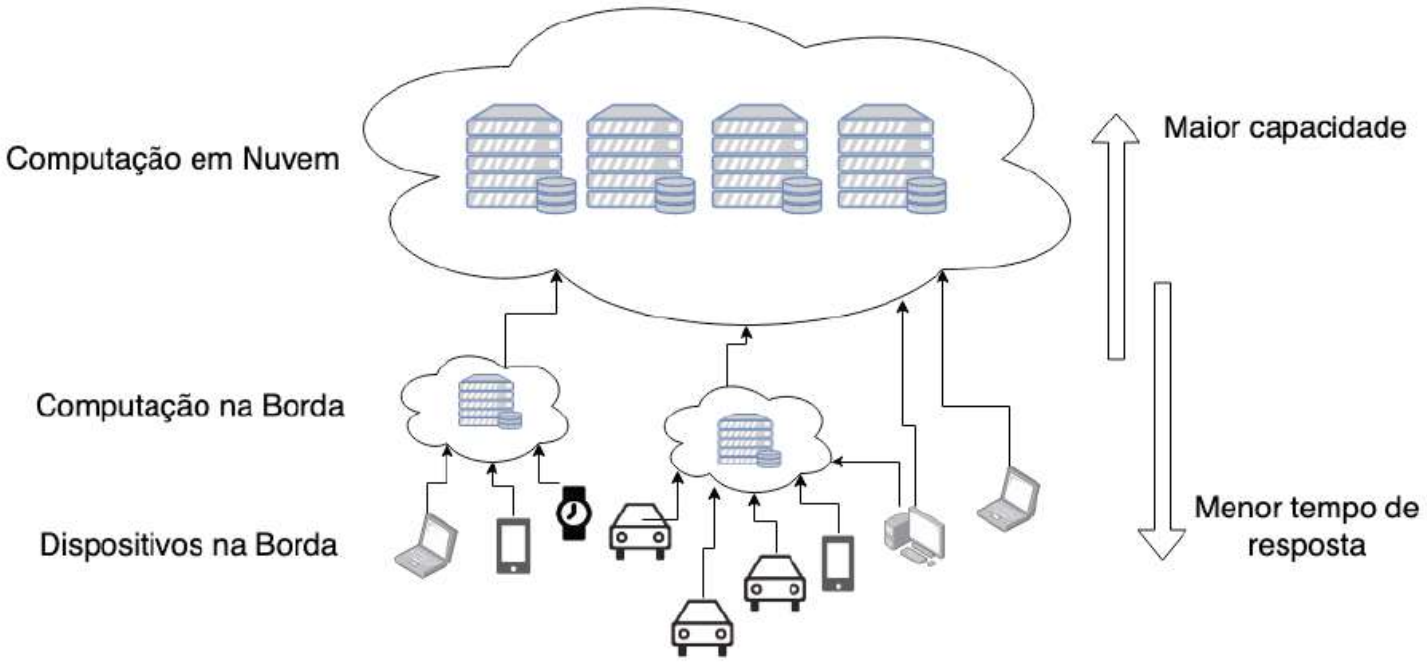
Modelos de Arquitetura – *Edge Computing*

- Mesmo com a evolução dos modelos de arquitetura ainda pode haver problemas de escalabilidade em soluções em nuvem.
- Essas questões motivaram a consolidação do paradigma de Computação nas Bordas (*Edge Computing*) cuja ideia principal é mover o processamento dos dados para a borda da rede.

Computação nas Bordas – *Edge Computing*

- *Edge Computing* apresentada a execução de serviços na borda da rede pode beneficiar algumas soluções, por exemplo, aplicações de mobilidade urbana que precisam de respostas rápidas para análise de dados do trânsito em uma determinada região.

Computação nas Bordas – *Edge Computing*



Fonte: KLS, Malheiros Neumar (2019).

Conceitos

Qualidade de Serviço em Nuvem

Qualidade de Serviço em Nuvem

- O desempenho das aplicações em nuvem pode ser um desafio se não houver disponibilidade de redes de comunicação de qualidade.
- Como o acesso aos serviços e dados no provedor é realizado por meio da Internet, pode haver problemas de desempenho ou até mesmo falhas na comunicação entre os componentes.

Qualidade de Serviço em Nuvem

- Vamos considerar o caso de sistemas com requisitos de tempo real, como jogos ou aplicações de chamada de voz.
- Esses tipos de aplicações não funcionam de forma adequada se a conexão for de baixa qualidade.
- Vamos caracterizar de forma objetiva a qualidade da comunicação.

Qualidade de Serviço em Nuvem

- Precisamos de métricas quantitativas para descrever os requisitos mínimos de desempenho.
- Vamos entender o conceito denominado Qualidade de Serviço (QoS – *Quality of Service*).

Qualidade de Serviço em Nuvem

- A QoS pode ser entendida como uma abordagem utilizada para especificar parâmetros de desempenho das aplicações, assim como os mecanismos necessários para garantir os requisitos de desempenho estabelecidos.

Qualidade de Serviço em Nuvem

- Os modelos de QoS podem ser utilizados para caracterizar objetivamente os requisitos de desempenho de uma aplicação e utilizam métricas de desempenho de rede:
  - Atraso: é o tempo total de transmissão de um pacote do nó remetente ao nó destinatário.
  - Aplicações de chamadas de voz na Internet, por exemplo, requerem um atraso máximo de 150ms.

Qualidade de Serviço em Nuvem

- Jitter: é uma medida da variação no atraso na transmissão dos pacotes.
- Quanto maior o jitter pior é o desempenho de aplicações multimídia como *streaming* de músicas na internet.
- Taxa de transmissão: é o volume de dados efetivamente transmitido entre o nó remetente e o nó destinatário.
- Em geral é medida em termos de megabits por segundo (Mbps).

Qualidade de Serviço em Nuvem

- Taxa de perda: porcentagem dos pacotes que não foram entregues com sucesso para o nó destinatário.
- Por exemplo, se foram transmitidos 50 pacotes e apenas 40 foram efetivamente entregues ao destinatário então a taxa de perda é de 20%, ou seja, 10 de 50 pacotes não foram entregues.

Qualidade de Serviço em Nuvem

- Utilizando estas e outras métricas mais específicas, os provedores especificam condições para provisão dos serviços de Computação em Nuvem em um documento chamado Acordo de Nível de Serviço (SLA – *Service Level Agreement*).
- O SLA descreve de forma objetiva as garantias de QoS a confiabilidade e o desempenho de cada serviço.

Qualidade de Serviço em Nuvem

- Os provedores de Computação em Nuvem podem considerar métricas de Qualidade de Serviço entre as principais:
  - Escalabilidade;
  - Performance;
  - Confiabilidade;
  - Resiliência.

Mecanismos para a Qualidade de Serviço

- Existem mecanismos que visam melhorar a Qualidade de Serviço no provedor de Computação em Nuvem.
- Podemos destacar os mecanismos: dimensionamento automático, balanceamento de carga e recuperação de desastres (falhas).

Mecanismos Dimensionamento Automático

- O mecanismo de dimensionamento automático (*automated scaling*) é responsável por ajustar a capacidade de um serviço em função das demandas.
- Se a carga de trabalho aumenta o mecanismo aloca mais recursos, para manter a performance do serviço.
- Por exemplo: esse mecanismo pode automaticamente criar uma réplica de um banco de dados, para lidar com um aumento no número de consultas ao banco.

Mecanismos Dimensionamento Automático

- Se a carga de trabalho diminui, o mecanismo libera recursos ociosos para reduzir custos.
- Esse mecanismo confere escalabilidade aos serviços em nuvem de forma automatizada, buscando otimizar a relação entre custo e performance.

Mecanismos Balanceamento de Carga

- É um mecanismo para distribuir a demanda de trabalho entre as réplicas de um serviço.
- Por exemplo: cada nova requisição que chega a rede do provedor pode ser encaminhada para a réplica menos sobrecarregada.
- Isso resulta em melhor performance, pois diminui o tempo de resposta das requisições.

Mecanismos Recuperação de Falhas

- O mecanismo de recuperação de falhas trabalha em conjunto com os demais mecanismos.
- O objetivo do mecanismo de recuperação a falhas é identificar a ocorrência de falhas para que as requisições sejam redirecionadas somente para as réplicas do serviço que estejam ativas e funcionando corretamente.

Mecanismos Recuperação de Falhas

- Quando uma instância falha o mecanismo de balanceamento de carga é avisado para não redirecionar requisições para essa instância.
- A implementação e recuperação a falhas contribui também para aumentar a confiabilidade e a disponibilidade do serviço.
- O mecanismo de recuperação a falhas depende da redundância (replicação) de recursos.

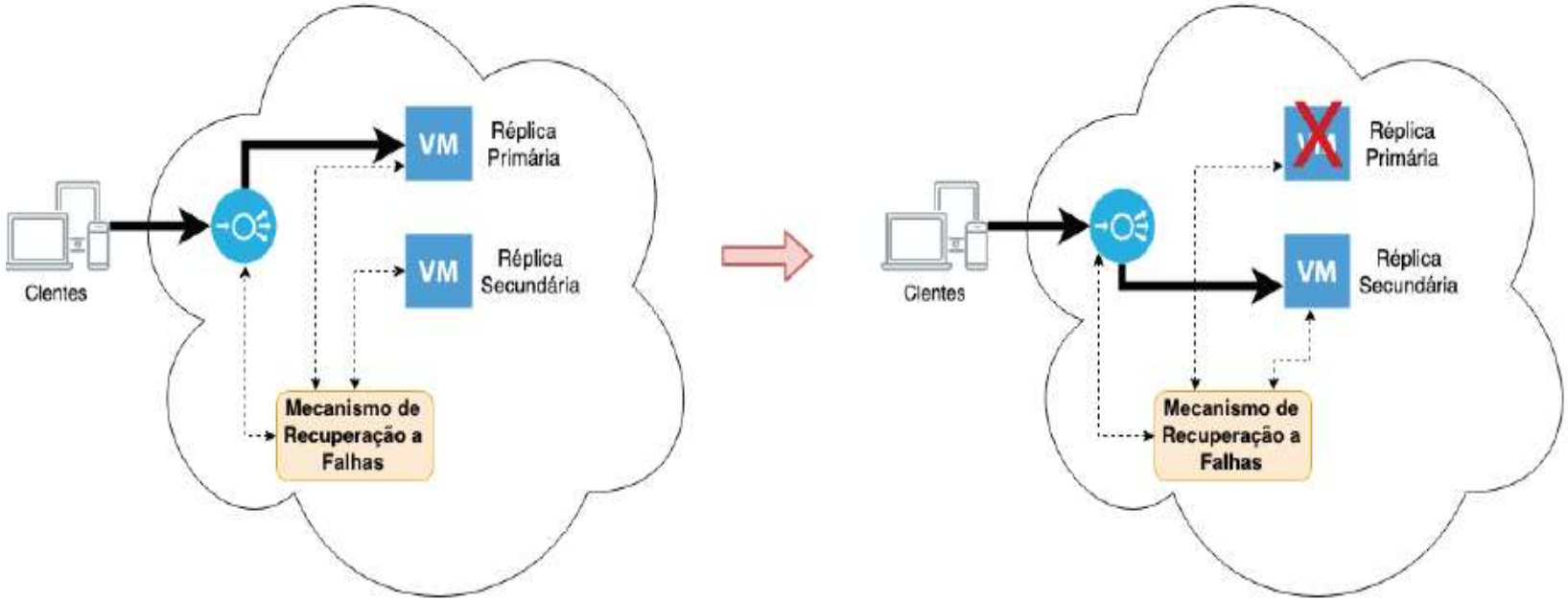
Mecanismos Recuperação de Falhas

- Por exemplo quando uma instância de um serviço falha deve haver uma réplica (secundária) desse serviço já preparada para receber as requisições.
- Existem dois modelos básicos de recuperação a falhas: modelo ativo-ativo e modelo ativo-passivo.

Mecanismos Ativo-passivo

- No modelo ativo-passivo, a réplica secundária não é utilizada para atender requisições regularmente.
- Ela só é acionada quando a réplica principal falha.
- Quando máquina virtual primária falha as requisições dos clientes são direcionadas para sua réplica.

Mecanismos Ativo-passivo

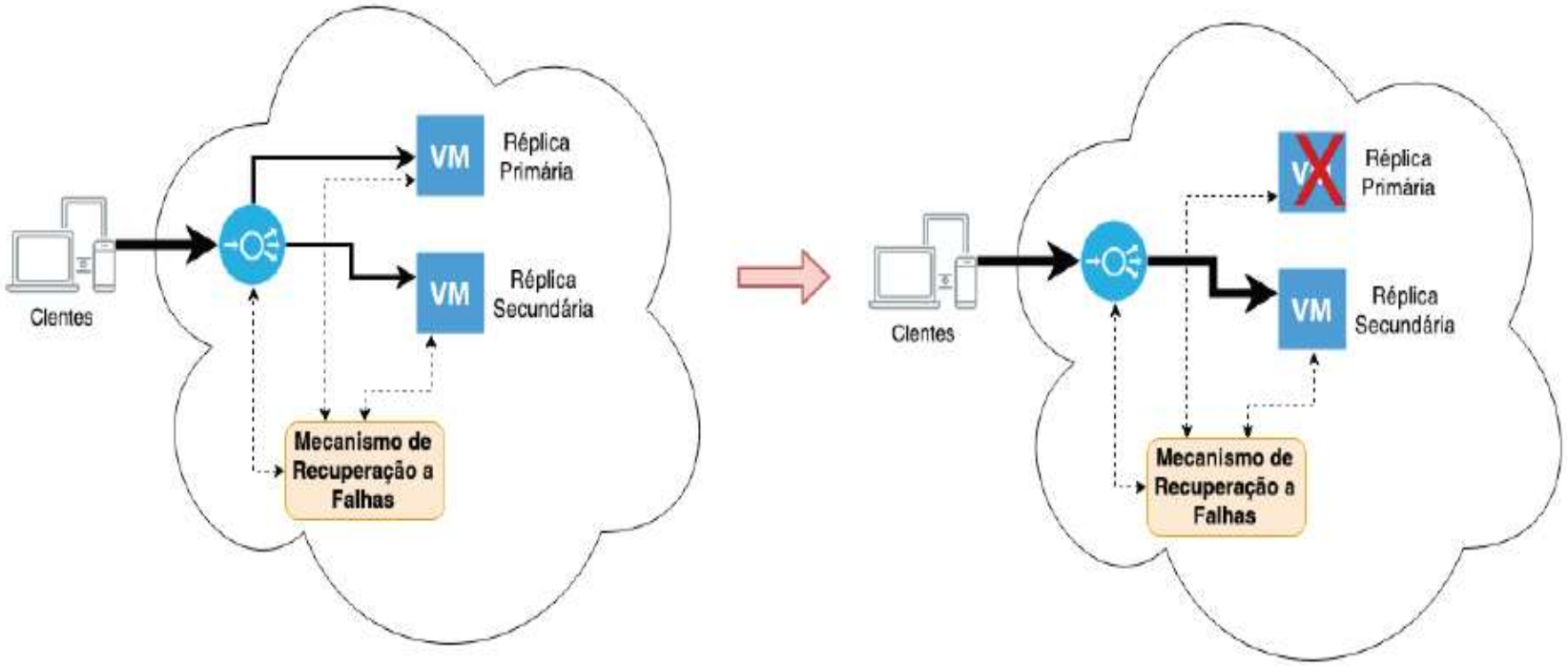


Fonte: KLS, Malheiros Neumar (2019).

Mecanismos Ativo-ativo

- No modelo ativo-ativo ambas as réplicas recebem requisições (sem distinção).
- Quando uma das réplicas falha então todas as requisições são redirecionadas para a outra até que a réplica que falhou seja corrigida ou uma nova réplica seja instanciada.

Mecanismos Ativo-ativo



Fonte: KLS, Malheiros Neumar (2019).

Conceitos

Ameaças das Aplicações em Nuvem

Ameaças das Aplicações em Nuvem

- Vamos compreender os princípios de segurança da informação e quais são as propriedades de um sistema seguro.
- As propriedades básicas de uma comunicação segura e confiável são:
  - Confidencialidade: sigilo do conteúdo dos pacotes transmitidos na rede.

Ameaças das Aplicações em Nuvem

- Integridade: garantia de que os dados transmitidos não podem ser alterados.
- Autenticidade: confirmação da identidade das partes envolvidas na transmissão dos dados.
- Disponibilidade: garantia de que um sistema estará apto para realizar as operações de transmissão ou processamento dos dados.

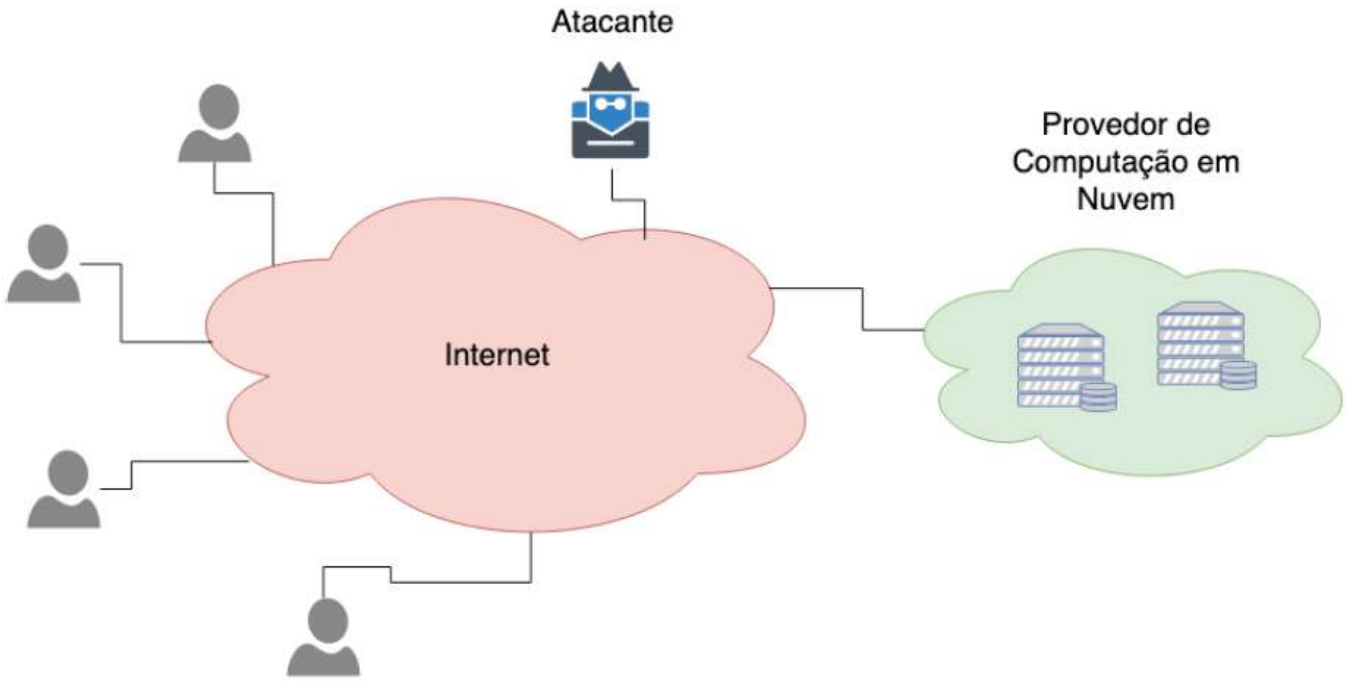
Ameaças das Aplicações em Nuvem

- Uma aplicação que utiliza a internet como rede de comunicação precisa ser protegida por meio de mecanismos de segurança como criptografia e controle de acesso.
- O projeto de aplicações em nuvem precisa contemplar estratégias e ferramentas de segurança para garantia de autenticidade, confidencialidade e integralidade dos dados transmitidos entre os clientes e o provedor.

Ameaças das Aplicações em Nuvem

- A comunicação de dados entre os usuários legítimos e os serviços disponíveis no provedor está sujeita as ações de agentes maliciosos que visam realizar ataques que exploram eventuais vulnerabilidades das aplicações.

Ameaças das Aplicações em Nuvem



Fonte: KLS, Malheiros Neumar (2019).

Ameaças das Aplicações em Nuvem

- As principais ameaças e vulnerabilidades que podem afetar as aplicações em nuvem.
- As principais ameaças de segurança para aplicações em Nuvem são: interceptação de tráfego, negação de serviço e ataques de virtualização.

Ameaças – Interceptação de Tráfego

- **Interceptação de tráfego:** ocorre quando uma entidade não autorizada é capaz de obter as informações transmitidas entre provedor em nuvem e clientes de forma que a confidencialidade dos dados é violada.
- Esse tipo de ataque é difícil de ser detectado, pois é passivo no sentido em que não há modificações nos dados ou sistemas.

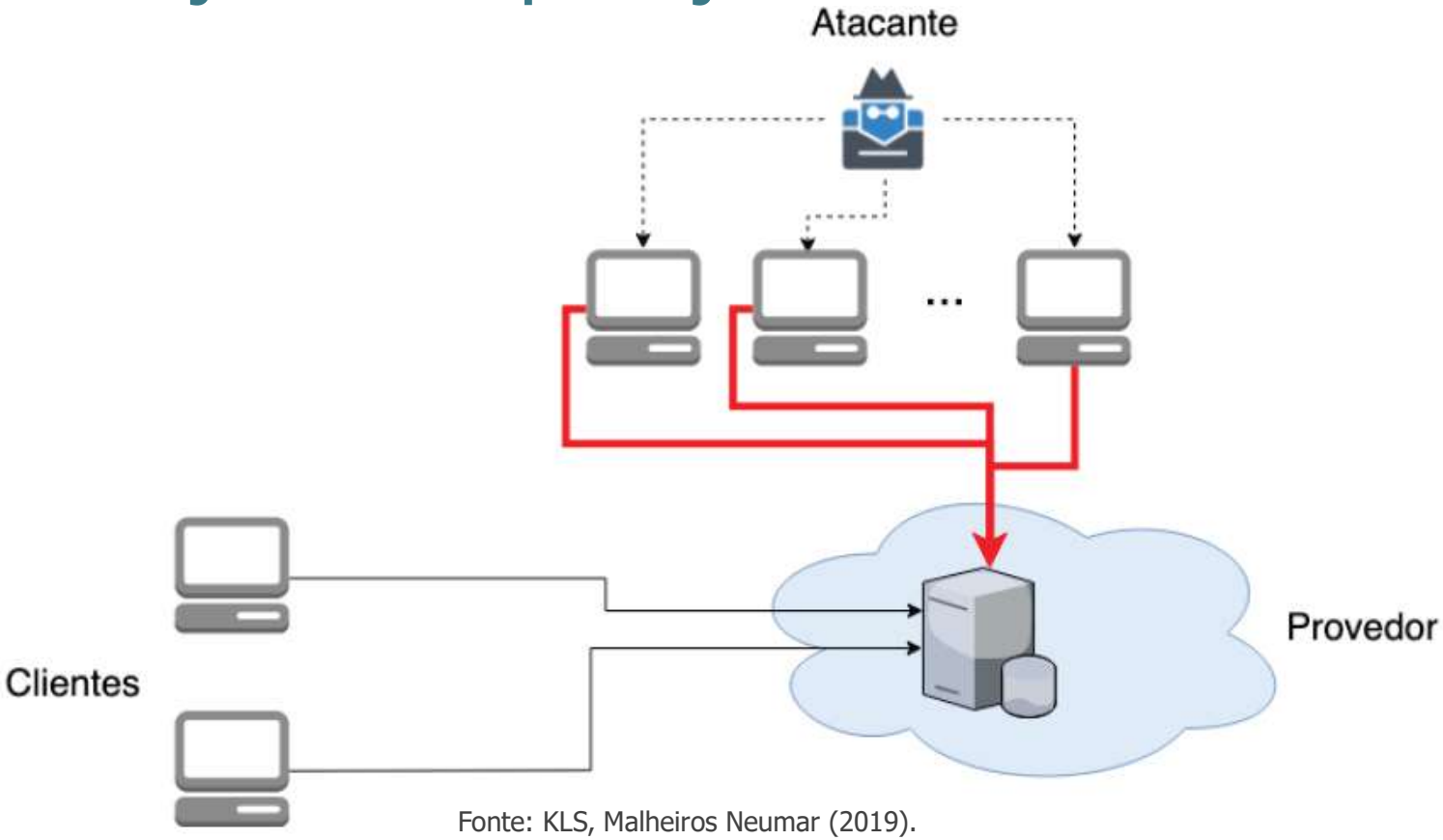
Ameaças – Interceptação de Tráfego

- O atacante apenas copia os dados transmitidos na rede para ter acesso a informações sigilosas dos provedores e seus clientes.
- Esse cenário caracteriza uma forma de espionagem.

Ameaças – Negação de Serviços

- **Negação de Serviço** (DoS – *Denial of Service*): tem o objetivo de afetar a disponibilidade dos serviços.
- Esse ataque consiste em sobrecarregar o serviço com um grande volume de requisições de forma que não consiga mais responder aos clientes legítimos com um desempenho satisfatório.

Ameaças das Aplicações em Nuvem



Fonte: KLS, Malheiros Neumar (2019).

Ataques DoS

- Para resistir aos ataques de DoS os provedores identificavam e bloqueavam os endereços dos nós da rede de onde os atacantes disparavam as requisições.
- Em vez de disparar um grande volume de requisições de alguns nós o que facilitava a identificação da fonte do ataque, os atacantes passaram a disparar poucas requisições de grande número de computadores dispersos pela internet.

Ataques DoS

- Essa estratégia é denominada ataque de DoS distribuído (DDoS – *Distributed DoS*).
- É muito difícil para o provedor distinguir as requisições envidas por clientes confiáveis das requisições geradas pelos atacantes em computadores que foram invadidos.

Ameaças – Ataques de Virtualização

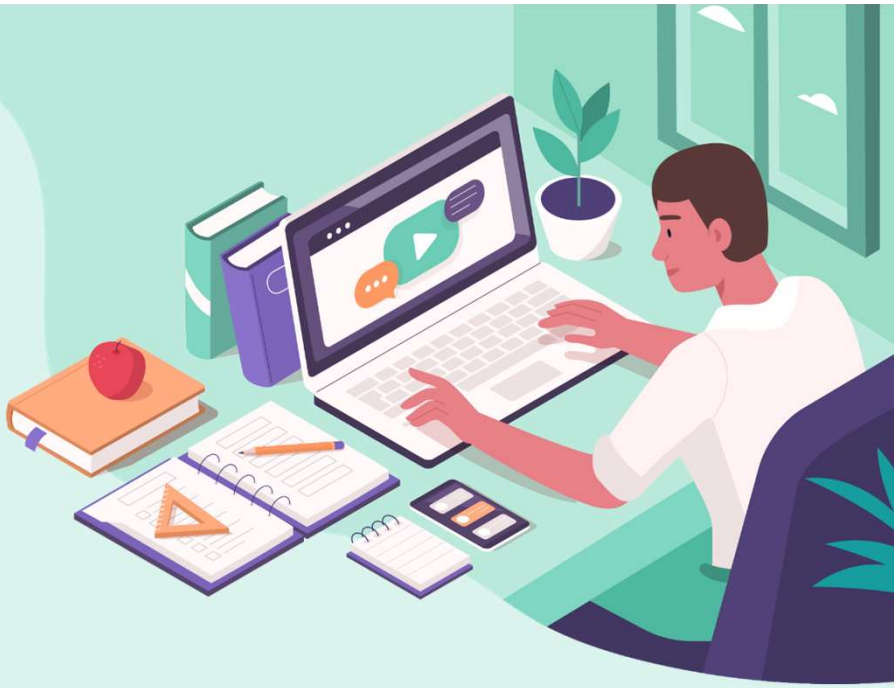
- **Ataques de virtualização**: buscam explorar eventuais falhas e vulnerabilidades nas ferramentas de virtualização utilizadas pelos provedores.
- O atacante pode conseguir algum nível de controle sobre a infraestrutura de TI do provedor.
- Outro problema é que pode haver violação da privacidade dos dados dos clientes do provedor.

Ameaças – Ataques de Virtualização

- Como a virtualização permite que diversos recursos compartilhem um mesmo recurso físico pode haver dados de diversos clientes em um mesmo equipamento.
- Os ataques as ferramentas de virtualização podem conseguir violar os mecanismos de proteção que existem para manter um isolamento entre os recursos e dados de diversos clientes que compartilham a infraestrutura do provedor.

Resolução da SP

Infográfico – Software de Controle para Veículos



Descrição da Situação Problema

- Você é analista de TI em uma empresa do setor automotivo que decidiu iniciar a fabricação de veículos autônomos, que não precisam de motoristas, pois eles possuem um sistema de controle sofisticado capaz de conduzir o veículo com segurança.
- Seu papel é liderar a equipe que vai implementar o software de controle para condução automática dos veículos.
- Você precisa escolher um modelo de arquitetura para a solução desses veículos.

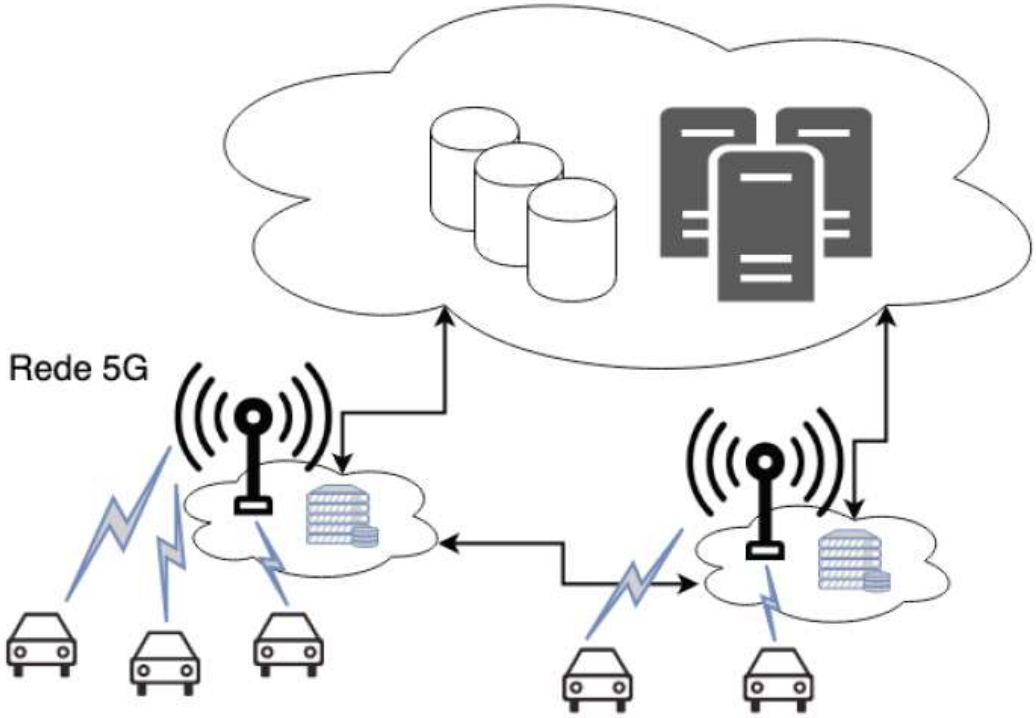
Solução da Situação Problema

- Existem muitos aplicativos de navegação para veículos baseados em soluções em nuvem.
- Um software de controle para condução de veículo precisa tomar decisões em tempo real.
- Além do uso de serviços de inteligência artificial esse tipo de aplicação requer baixa latência de comunicação e baixo tempo de resposta no processamento de dados.

Solução da Situação Problema

- Se os veículos tivessem que se comunicar com servidores na nuvem esses requisitos poderiam não ser atendidos.
- O modelo mais adequado nesse caso seria uma abordagem de *Edge Computing*.

Solução da Situação Problema



Fonte: KLS, Malheiros Neumar (2019).

Solução da Situação Problema

- Os carros poderiam se comunicar com altas taxas de transmissão por meio de uma rede sem fio 5G e aproveitar a capacidade de processamento e armazenamento de dados das estações de transmissão de dados para executar funcionalidades em tempo real.
- Serviços em nuvem poderiam ser utilizados para agregar informações, armazenar dados históricos para análise de estatísticas e para cálculos de rotas longas que exigem dados do trânsito em várias regiões.

Conceitos

Mecanismos de Segurança em Nuvem

Mecanismos de Segurança em Nuvem

- Os mecanismos de segurança devem ser usados em conjunto e aprimorados continuamente para lidarem com eventuais ações maliciosas contra as aplicações em ambientes de nuvem.
- Vamos estudar os principais mecanismos de segurança disponíveis.

Mecanismos de Segurança em Nuvem

- Podemos mencionar como mecanismos de segurança:
  - Criptografia;
  - Gerenciamento de acesso e identidade;
  - Autenticação unificada;
  - Imagens fortalecidas de máquinas virtuais.

Segurança – Criptografia

- A criptografia consiste em técnicas que permitem disfarçar os dados enviados de forma que um atacante não consiga obter nenhuma informação dos dados interceptados.
- Isso implica codificar os dados de modo que somente o destinatário legítimo poderá decifrá-los tornando-os assim ininteligíveis para terceiros.

Segurança – Criptografia

- A principal aplicação da criptografia é assegurar a confidencialidade dos dados armazenados nos provedores de nuvem pública e dos dados transmitidos entre um provedor e seus clientes.
- A criptografia pode ser usada em mecanismos para garantia de integridade e autenticidade.
- Os algoritmos utilizados para codificar os dados são de conhecimento público, mas para decodifica-los é necessário um código secreto denominado chave de criptografia.

Segurança – Criptografia

- Existem duas abordagens: a criptografia de chaves simétricas e a criptografia de chave pública.
- A criptografia de chaves simétricas: existe uma única chave que é utilizada pelo remetente para criptografar os dados que serão enviados ou armazenados em nuvem.
- O receptor precisa de uma cópia dessa chave para decodificar os dados.

Segurança – Criptografia

- A criptografia de chaves pública: o processo envolve um par de chaves.
- Para o destinatário receber os dados ele precisa gerar o seu par de chaves.
- Uma delas é denominada pública e não precisa ser mantida em segredo.
- A outra chave é denominada privada e deve ser mantida em segredo.
- O remetente usa a chave pública do destinatário para criptografar os dados.

Segurança – Criptografia

- Os dados só podem ser decifrados com a chave privada correspondente mantida em segredo pelo destinatário.
- Outra solução de segurança de nuvem pública é o Gerenciamento de Acesso e Identidade (IAM – *Identity and Access Management*).
- Esse recurso é utilizado pelos provedores, para implementação de políticas de controle acesso.
- O IAM permite o gerenciamento e a autenticação de usuários assim como o controle de privilégios para grupos de usuários e gerenciamento de credenciais.

Segurança – Gerenciamento de Acesso e Identidade

- Esse tipo de recurso é importante na implementação de soluções de segurança para lidar com ataques de negação de serviços, autenticação fraca e violação de privacidade no acesso a dados e serviços.

Segurança – Autenticação unificada

- Se um cliente utiliza serviços em vários provedores é importante também para questões de controle de acesso o uso de mecanismos de autenticação unificada (SSO – *Single Sign On*).
- Esses mecanismos oferecem uma solução segura para autenticação em vários provedores utilizando as mesmas credenciais.

Segurança – Imagens fortalecidas de Máquinas Virtuais

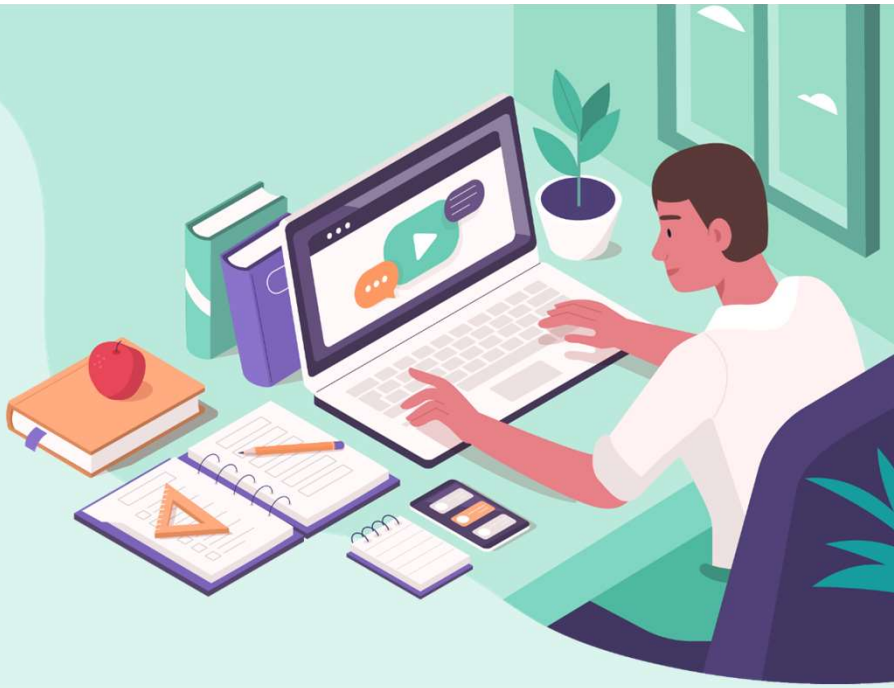
- Outro recurso para a segurança dos serviços é o uso de Imagens fortalecidas de Máquinas Virtuais (*Hardened VM Images*).
- As instâncias de máquinas virtuais são criadas a partir de imagens disponíveis no provedor.
- As imagens fortalecidas são aquelas que foram configuradas por especialistas considerando políticas de segurança rigorosas para eliminar possíveis vulnerabilidades.

Segurança – Imagens fortalecidas de Máquinas Virtuais

- Quando um cliente cria uma VM a partir de uma imagem fortalecida ele sabe que o sistema operacional dessa VM já foi configurado com as melhores práticas de segurança conhecidas.

Resolução da SP

Infográfico – Recuperação de Falhas



Descrição da Situação Problema

- Aplicações em algumas áreas, como no setor financeiro, saúde e governamental, apresentam requisitos bastante rigorosos em relação a confiabilidade e disponibilidade dos serviços.
- Nesses casos é importante o uso de mecanismos de recuperação a falhas.
- Existem dois modelos básicos para isso: ativo-ativo e ativo-passivo.
- Faça uma análise comparativa desses modelos a fim de destacar suas vantagens e desvantagens em termos de custo e desempenho.

Solução da Situação Problema

- A estratégia básica de recuperação a falhas é a redundância: recursos adicionais são usados em caso de falha dos recursos inicialmente alocados, assim o serviço continuará disponível.
- Vimos que existem dois modelos básicos para mecanismos de recuperação a falhas: ativo-ativo e ativo-passivo.

Solução da Situação Problema

- Para compreender melhor a diferença entre eles vamos considerar que para um dado serviço em nuvem existe a instância principal do serviço e uma instância secundária (uma réplica criada para viabilizar a implementação da recuperação de falhas).
- No modelo ativo-passivo a réplica secundária é utilizada apenas no caso de falha na instância principal.

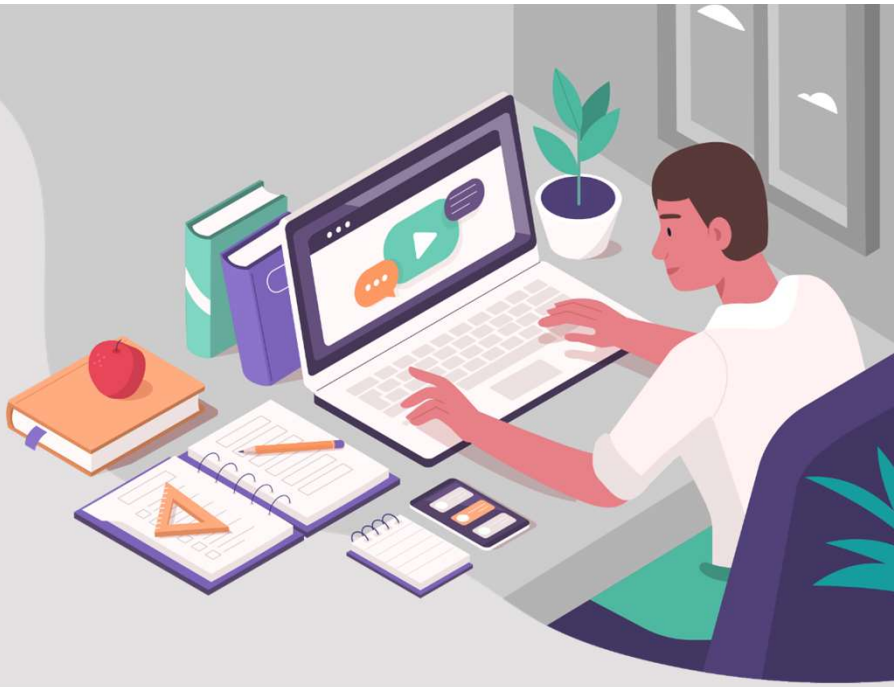
Solução da Situação Problema

- No modelo ativo-ativo a réplica secundária é utilizada no balanceamento de carga para ajudar no processamento das requisições ao serviço.
- A vantagem do modelo ativo-ativo é um custo menor, pois não há ociosidade de uma réplica secundária alocada somente para recuperação a falhas.

Solução da Situação Problema

- Por outro lado esse modelo implica em um risco.
- Se a réplica secundária é utilizada no balanceamento de carga regularmente, ela pode estar sobrecarregada no momento em que a instância principal falhar.
- Nesse caso a falta de recursos disponíveis na réplica secundária pode comprometer o desempenho.

Recapitulando



Recapitulando

- Arquitetura de Aplicação em Nuvem e modelos;
- Qualidade de Serviço em Nuvem e Mecanismos;
- Ameaças das Aplicações em Nuvem;
- Mecanismos de Segurança em Nuvem.

- Siga em frente e bons estudos! Obrigada!