Discente: Emily Almeida Abreu

Matrícula: 20220796436

Turma: C793TI

1. Defina o que é um sistema distribuído e explique por que ele difere de um sistema centralizado. Discuta as vantagens e desvantagens de usar sistemas distribuídos em comparação com sistemas centralizados, fornecendo exemplos relevantes.

Segundo Tanenbaum, é um conjunto de computadores independentes entre si, ligados através de uma rede de dados, que se apresentam ao usuário como um sistema único e coerente. Enquanto em um sistema distribuído os dados e o poder computacional estão espalhados por vários nós da rede, um sistema centralizado possui uma única autoridade que controla o sistema e que é o único responsável por todas as operações do sistema. Uma das vantagens de usar um sistema distribuído e a sua escalabilidade. Um sistema centralizado pode ter problemas de escalabilidade pelo fato das decisões serem tomadas por um único ponto de controle. Além disso, outra vantagem do sistema distribuído é poder, com computadores baratos e de baixo processamento, formar um supercomputador que normalmente sairia muito caro, o que não seria possível usando um sistema centralizado. Uma vantagem de usar um sistema distribuído e a simplicidade de implementação. O controle de concorrência é realizado em um único nó (no servidor) e não existem cópias dos recursos compartilhados, com isso as inconsistências são evitadas. Enquanto isso, sistemas distribuídos são mais complexos e difíceis de se compreender e testar.

2. Descreva os principais desafios de comunicação em sistemas distribuídos. Aborde tópicos como latência, consistência, concorrência e tolerância a falhas. Em seguida, explique como os sistemas distribuídos lidam com esses desafios.

Os sistemas distribuídos são mais resilientes a falhas por causa da sua natureza distribuída. Se um nó falhar, os outros nós ainda podem continuar operando, evitando interrupções no sistema. Manter a consistência dos dados em um ambiente distribuído é um desafio. Assim, garantir a coerência dos dados em diferentes réplicas e evitar conflitos e inconsistências exige protocolos de sincronização e gerenciamento de transações eficientes. Aproveitar o paralelismo e a capacidade de processamento distribuído em um sistema pode ser complexo. Coordenar e sincronizar tarefas concorrentes, gerenciar a concorrência de acesso aos recursos compartilhados e evitar condições de corrida são desafios comuns. Quanto mais amplamente o sistema for distribuído, mais latência pode ser experimentada com as comunicações. Isso pode levar a que as equipes façam trocas entre disponibilidade, consistência e latência.

3. Discuta os modelos de computação em grade, nuvem e edge computing em sistemas distribuídos. Compare e contraste esses modelos, destacando suas características distintas e os casos de uso comuns para cada um.

A computação em grade é um modelo de computação distribuída de alto desempenho. O modelo propõe a configuração de organizações virtuais (OV) ou federações. Em cada OV contém um grupo de servidores dedicados para executar tarefas da localidade em questão. Assim, o modelo permite a configuração em rede de longa distância e não tem restrições quanto ao hardware, sistema operacional e rede. Isto é, trata-se de um ambiente computacional heterogêneo. os meteorologistas usam a computação em grade para modelagem climática. A modelagem climática é um problema de computação intensiva que requer análise e gerenciamento de dados complexos. O processamento de grandes quantidades de dados meteorológicos em um único computador é lento e demorado. Por isso, os meteorologistas executam a análise em uma infraestrutura de computação em grade geograficamente dispersa e combinam os resultados.

A computação em nuvem é um modelo de arquitetura distribuída que oferece um ambiente de serviços de infraestrutura e de sistemas computacionais. A ideia inicial da nuvem veio para propor serviços limitados aos usuários que desejavam armazenar e acessar documentos e arquivos de áudio/vídeo através da Internet. Com a disseminação da nuvem, atualmente ela abrange também serviços de infraestrutura e desenvolvimento de sistemas que são cobrados mediante o uso destes recursos de tecnologia da informação. A estrutura de serviços é dividida em três camadas: Software as a Service (SaaS), Plataform as a Service (PaaS) e Infraestructure as a Service (IaaS). O Google é uma das principais plataformas que utilizam desse serviço, pois ele armazena seus dados enquanto você pesquisa por algo determinado na internet e consegue carregá-los através da nuvem. Além disso, o Google também possui o seu próprio serviço de computação na nuvem, que é bastante utilizado atualmente, de forma gratuita.

Edge computing ou computação de borda é um tipo de arquitetura de TI onde os dados do cliente são processados no limite da rede, ou o mais próximo possível da fonte de dados. Com o processamento mais próximo, os usuários se beneficiam de serviços mais rápidos e confiáveis, enquanto as empresas usufruem da flexibilidade da cloud computing híbrida. A edge computing é uma das formas como uma empresa pode usar e distribuir um pool de recursos por inúmeros locais. A edge computing pode ser usada para fortalecer a segurança no trabalho. Alguns ambientes de trabalho são altamente voláteis e, por isso, representam diferentes condições de segurança ao longo do expediente. Com auxílio da edge, é possível utilizar sensores que avaliam em tempo real as condições de temperatura, umidade, pressão, ventos, ruídos (entre outros) para fornecer insights sobre a possibilidade dos profissionais desempenharem suas funções. É algo que pode ser aplicado em diferentes indústrias, como em laboratórios ou mesmo em plataformas de petróleo em alto mar.

4. Analise o papel da escalabilidade e da redundância em sistemas distribuídos. Explique por que esses conceitos são cruciais em ambientes distribuídos e descreva estratégias e tecnologias comuns usadas para alcançar a escalabilidade e a redundância em sistemas distribuídos.

A escalabilidade é necessária quando há um aumento de usuários que precisam de mais recursos. Um bom exemplo é o aumento do público da Netflix a cada sexta-feira à noite. Isso significa adicionar dinamicamente mais recursos, como aumentar a capacidade da rede, permitindo maior transmissão de vídeo e reduzindo-a quando o consumo normalizar. Uma tecnologia comum usada para alcançar a escalabilidade é o Amazon EC2 Auto Scaling. Ele ajuda a garantir que haja o número correto de instâncias do Amazon EC2 disponíveis para processar a carga da aplicação.

A redundância de dados pode evitar a perda de dados. Nesse sentido, quando acontecem falhas no sistema, ou seja, quando existe uma redundância não controlada de dados, geralmente esses dados podem ser modificados ou apagados. Entretanto, se forem realizadas estratégias de backup, as informações podem ser protegidas e, assim, permanecer seguras. Um sistema pode ser redundante em diversos dos seus componentes. Para isso, basta que ele tenha pelo menos dois recursos diferentes integrados e capazes de se substituírem. As formas mais comuns de redundância são nas fontes de energia, nas redes, na memória RAM e nos dados.

5. Descreva as vantagens e desvantagens da migração de uma infraestrutura local para a nuvem. Forneça exemplos concretos de cenários em que a computação em nuvem pode ser benéfica e situações em que pode não ser a melhor opção.

Algumas das vantagens do sistema computação em nuvem são: O usuário não precisa se preocupar com o Sistema Operacional e Hardware que está sendo usado no computador pessoal, podendo acessar seus dados na “nuvem”; O usuário paga somente pelo tempo de utilização dos aplicativos e seus recursos, não sendo necessário pagar por uma licença integral de uso de software; A infraestrutura necessária para uma solução de uma “nuvem” consome menos energia, refrigeração e espaço físico, contribuindo consequentemente para preservação e uso racional dos recursos naturais; Escalabilidade: O usuário pode a qualquer momento aumentar ou diminuir os recursos alocados (memória, processamento e espaço de armazenamento) de acordo com suas necessidades; etc.

Sendo a computação em nuvem uma forma de centralizar aplicações e armazenar dados, há uma grande preocupação no que diz respeito à segurança e privacidade. Ao utilizar o sistema, o usuário entrega seus dados e informações importantes aos cuidados de outra empresa, o que para muitos é uma questão bastante complicada, causa uma sensação de vulnerabilidade; ao contrário de hoje que estes dados e informações são bem guardadas por seus proprietários.

A privacidade pode ser comprometida já que um cliente pode se logar de qualquer local e acessar aplicações, para este fim as empresas que fornecem os serviços da computação em nuvem estudam uma forma de proteção, como técnicas de autenticação (usuário e senha); outra forma é empregar um formato de autorização por níveis de permissões, onde cada usuário acessa somente o que lhe é permitido (Computação nas nuvens, 2011).

Outra coisa é caso a internet não esteja disponível em determinado local a computação em nuvem se torna inútil.

Um exemplo de caso em que pode ser benéfico a migração para a nuvem é lojas online. Em dias de promoção, por exemplo, o site será mais visitado do que o costume, então o poder de escalabilidade será essencial para que o sistema fique disponível para todos os usuários. Entretanto, se for preciso muitos recursos de computação e armazenamento, o custo pode ser muito elevado.

6. Explique os modelos de serviço na computação em nuvem, incluindo Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS). Dê exemplos de aplicativos ou serviços que se encaixam em cada um desses modelos e discuta as diferenças entre eles.

Infrastructure as a Service (IaaS): O provedor oferece infraestrutura de armazenamento e processamento, e tem como objetivo principal facilitar o fornecimento de recursos de computação necessários para criar um ambiente de aplicação. O usuário não tem controle dos servidores da nuvem como o controle do sistema operacional do servidor. Serviço no mercado: EC2 da AWS.

Platform as a Service (PaaS): O usuário não administra ou controla a infraestrutura subjacente, incluindo rede, servidores, sistemas operacionais ou armazenamento, mas tem controle sobre as aplicações implantadas e, possivelmente, as configurações das aplicações hospedadas nesta infraestrutura. Serviço no mercado: Amazon S3.

Software as a Service (SaaS): São os softwares disponibilizados aos usuários através da Internet, é direcionado ao usuário final. Serviço no mercado: Linkedin.

7. Analise os principais desafios de segurança relacionados à computação em nuvem e discuta como as organizações podem abordar esses desafios. Inclua considerações sobre autenticação, criptografia, gerenciamento de acesso e conformidade regulatória.

A autenticação multifator é um método de segurança que busca confirmar a identidade de alguém utilizando dois ou mais elementos de verificação. Por exemplo, além de digitar a senha, pode ser necessário fornecer um código temporário enviado para o celular, escanear uma impressão digital, tirar uma foto do rosto ou usar outro tipo de informação pessoal exclusiva.

Transferir dados através de uma rede em nuvem adiciona riscos de exposição e vazamentos. Para proteger os dados que são enviados, salvos ou carregados, deve-se aplicar uma das soluções de criptografia. Ao fazer isso, os dados não poderão ser lidos por usuários maliciosos ou não autorizados.

Os protocolos de criptografia utilizam uma chave para transformar dados legíveis em dados ilegíveis, ou um ciphertext (texto cifrado) para criptografar os dados. Apenas usuários que possuam as exatas chaves de decodificação podem descriptografar o ciphertext e tornar os dados criptografados em dados legíveis. Há dois tipos de chaves de criptografia: criptografia simétrica e assimétrica.

O gerenciamento de identidade e acesso (IAM) tornou-se fundamental para as estratégias de segurança cibernética. Embora as políticas, processos e tecnologias possam diferir entre organizações, o objetivo de qualquer iniciativa de IAM é garantir que apenas usuários e serviços autorizados acessem os recursos e dados na nuvem em um determinado período de tempo.

As regulamentações de privacidade de dados, como o General Data Protection Regulation (GDPR), os padrões do setor, como o Payment Card Industry Data Security Standard (PCI-DSS), e leis como a Health Insurance Portability and Accountability Act (HIPAA) e a LGPD no Brasil, têm implicações finais para organizações que capturam, processam e salvam dados, especialmente na nuvem. Os administradores devem equilibrar esses requisitos de compliance com os benefícios de agilidade da nuvem. Por meio das tecnologias de segurança, as empresas devem garantir que suas implantações sigam as melhores práticas de segurança; caso contrário, as multas que podem resultar de violações cometidas por desconhecimento, podem facilmente eliminar a economia de custos.

8. Explique os conceitos fundamentais da virtualização e como ela difere da emulação. Em seguida, descreva cenários em que a virtualização é uma solução valiosa, destacando suas vantagens em relação à execução direta de hardware.

Virtualização é a capacidade de criar um computador virtual no seu PC, permitindo instalar sistema operacional, rodar programas e realizar tarefas. Emulação é um processo em que um software ou dispositivo permite um a um sistema (chamado de "hospedeiro") imitar o funcionamento de outro sistema (o "convidado"), de modo que o primeiro possa rodar seus softwares e reconhecer periféricos para os quais não tem suporte.

Na virtualização, os programas de software chamados hipervisores separam os recursos físicos dos ambientes virtuais que precisam utilizar esses recursos. Os hipervisores podem ser executados em um sistema operacional (como em um laptop) ou instalados diretamente no hardware (como um servidor), este é o tipo de virtualização preferido da maioria das empresas. Os hipervisores dividem os recursos físicos para serem utilizados por diferentes ambientes virtuais.

Os recursos do ambiente físico são particionados, conforme a necessidade, entre os diversos ambientes virtuais. Os usuários interagem e executam as operações computacionais no ambiente virtual (normalmente chamado máquina guest ou máquina virtual). A máquina virtual funciona como um único arquivo de dados. E como qualquer outro arquivo digital, ela pode ser transferida de um computador a outro, aberta em qualquer um e funcionar da mesma forma.

Quando o ambiente virtual está em execução e um programa ou usuário emite uma instrução que requer recursos adicionais do ambiente físico, o hipervisor retransmite a solicitação ao sistema físico e armazena as mudanças em cache.

Em termos práticos, imagine que você tenha três servidores físicos, cada um com finalidades específicas. O primeiro é um servidor de email, o segundo é um servidor web e o terceiro executa aplicações legadas internas. Você utiliza cerca de 30% da capacidade de cada servidor (apenas uma pequena fração do potencial de execução). No entanto, como as aplicações legadas ainda são importantes para as suas operações internas, você é obrigado a mantê-las, assim como o servidor que as hospeda, certo? Tradicionalmente, sim. Muitas vezes, era mais fácil e confiável executar tarefas individuais em servidores individuais: um servidor, um sistema operacional e uma tarefa. Não era fácil dar vários "cérebros" a um único servidor. Porém, com a virtualização, você pode dividir o servidor de e-mail em dois servidores únicos, capazes de processar tarefas independentes. Assim, é possível migar os aplicativos legados. Trata-se do mesmo hardware, mas utilizado de maneira mais eficiente.

Pensando na segurança, você pode dividir o primeiro servidor novamente para processar outra tarefa, aumentando o aproveitamento de 30% para 60% e, por fim, para 90%. Depois disso, os servidores que agora estão desocupados podem ser reutilizados em outras tarefas ou ter o seu uso descontinuado de vez para reduzir os custos de refrigeração e manutenção.

9. Discuta os principais tipos de virtualização, incluindo virtualização de hardware, virtualização de sistema operacional e virtualização de aplicativos. Forneça exemplos de casos de uso para cada tipo e explique como eles funcionam.

Na virtualização de hardware, a máquina virtual criada tem acesso direto aos componentes nativos, ou seja, utiliza o processador, memória RAM, placa de vídeo e outros componentes de forma similar ao PC normal. Com ela, é possível ter mais performance na hora de criar ambientes, principalmente para testes mais específicos e que exigem mais da sua CPU.

A virtualização do sistema operacional é feita no kernel, o gerenciador de tarefas central dos sistemas operacionais. Ela permite a possibilidade de transferir uma máquina virtual entre servidores físicos diferentes sem se preocupar com o hardware (normalmente apenas copiando os arquivos da máquina virtual), e até a possibilidade de migrar servidores online entre hardware físicos diferentes, sem desligar a máquina virtual, técnica chamada de vMotion, XenMotion ou Live Migration, dependendo do fabricante.

A virtualização de aplicativos executa um software de aplicativo sem instalá-lo diretamente no SO do usuário. Existem três tipos de virtualização de aplicativos: virtualização de aplicativos locais, fluxo de aplicativos e virtualização de aplicativos com base em servidor. Ela permite a coexistência de múltiplas versões do mesmo aplicativo ao mesmo tempo no mesmo computador, por exemplo, por questões de compatibilidade de sites, algumas empresas precisam executar uma versão específica e antiga do Internet Explorer. Assim, é possível configurar para que a URL daquele site execute uma versão do Internet Explorer virtualizada, enquanto que as estações podem ser atualizadas para sempre rodar a última versão nos demais sites, garantindo a segurança.

10. Avalie os desafios de desempenho e segurança associados à virtualização. Descreva as técnicas e práticas recomendadas para otimizar o desempenho de máquinas virtuais e proteger ambientes virtualizados contra ameaças de segurança.

A virtualização introduz desafios de segurança contra os quais os sistemas de segurança física não conseguem proteger:

* O compartilhamento de arquivos entre hosts e convidados não é seguro.
* O isolamento entre componentes, tais como o sistema operacional convidado e aplicativos, hipervisores, hardware fica enfraquecido.
* Vários servidores são consolidados, o que aumenta o risco de que um risco de aplicativos no mesmo host possa se espalhar.
* Para sistemas de prevenção de intrusão (IPS), o malware direcionado para máquinas físicas e virtuais causa infecção por meio da rede virtual. Outras ameaças de segurança incluem o acesso não autorizado, serviços negados e explorações.

Em grandes ambientes de rede, a implementação ineficaz do VMware e o mau gerenciamento de virtualização podem sobrecarregar os recursos de rede. Isso pode causar consequências adversas no desempenho e na utilização das máquinas virtuais, como aplicações e serviços executados lentamente, ou a própria máquina virtual não responder.

A virtualização de segurança funciona como uma barreira para proteger o acesso ao perímetro em uma rede. Ela apresenta serviços de segurança dedicados e isolamento seguro de tráfego na nuvem, além de controles de firewall personalizáveis como um serviço gerenciado adicional. Empresas e provedores de serviços podem aproveitar o investimento de virtualização para criar um perímetro de segurança granular, oferecendo recursos de segurança dedicados em um conceito de nuvem para locatários e assinantes de serviços.

A eficácia da virtualização depende de suas redes físicas subjacentes. Os administradores de rede precisam estar totalmente cientes da integridade, do desempenho e de outros aspectos desses dispositivos por meio da visibilidade centralizada e do controle completo. Isso os ajuda a identificar, rastrear e sinalizar facilmente as causas dos problemas de rede na virtualização. No entanto, essa pode ser uma tarefa cansativa com grandes redes, que têm infraestruturas de TI complexas. O ManageEngine OpManager é uma solução de monitoramento de rede de nível empresarial, que permite obter informações detalhadas sobre os dispositivos de rede e ajuda a monitorar facilmente métricas cruciais.