ROTEIRO 4

Alunos: Bernardo Cunha Capoferri e Lívia Sayuri Makuta.

QUESTÕES

1. Qual o conceito por trás de Edge Computing? (Obs: Não é a rede de celular 2G)

O *edge computing* é uma tecnologia que tem relação com IoT (Internet das coisas ou “Internet of things”) e que é baseada em uma rede de data centers menores e que processam e armazenam os dados localmente. Isso porque na internet das coisas, os dados são recolhidos por dispositivos, os quais são encarregados a enviar os dados armazenados a um centro, ou nuvem de processamento. Porém, ao invés de pegar todos esses dados e enviar para esses centros ou nuvem, esse conceito diz que os dados devem ser classificados antes para separar aqueles que podem ser processados ali mesmo, e os que de fato exigem um processamento em um centro mais equipado ou em nuvem. E é daí que vem o nome *edge computing* (computação de borda) pois os dados são processados nos extremos de uma rede, isto é, são processados mais perto de onde são gerados, e só uma parte deles que vai ser enviada para centros, o que diminui o tráfego de dados. Isso consequentemente aumenta os volumes de dados e a velocidade de resposta, sendo uma arquitetura que busca melhores resultados em tempo real.

Você é o CTO (Chief Technology Officer) de uma grande empresa com sede em várias capitais no Brasil e precisa implantar um sistema crítico, de baixo custo e com dados sigilosos para a área operacional. (CONTEXTO)

2. Você escolheria Public Cloud ou Private Cloud?

Nós escolheríamos uma nuvem pública, e isso porque a nuvem pública seria mais adequada ao contexto que exige uma rede grande e bem preparada para muitas requisições e que esteja presente em várias partes do Brasil, além de segurança e baixo custo.

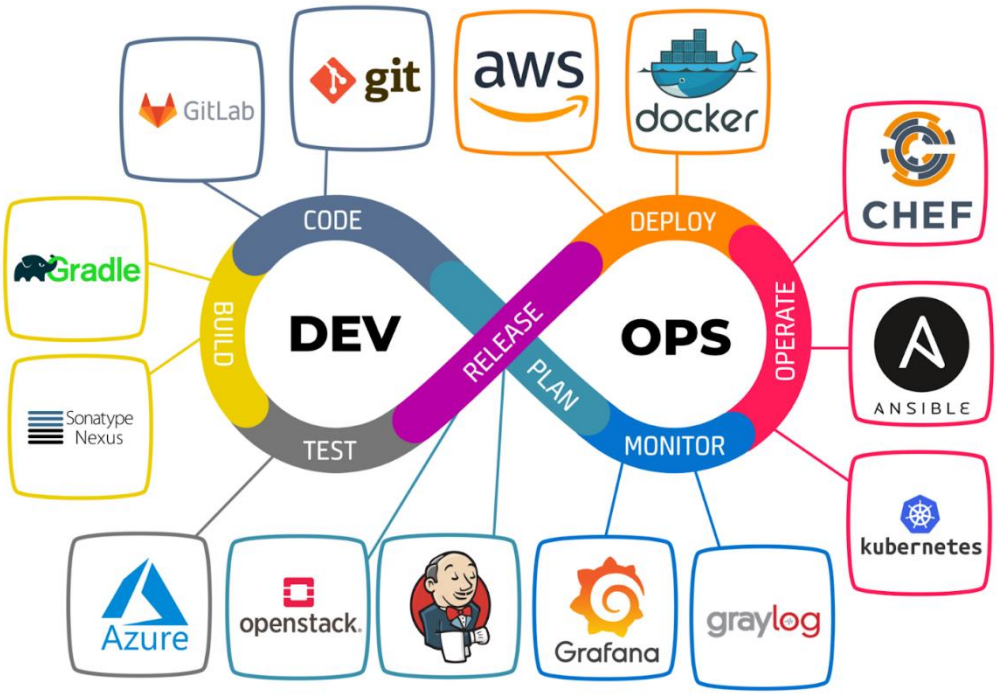
Em nuvens públicas a implantação é automatizada, pois o usuário não terá que investir em infraestrutura e em sua manutenção, sendo que essas tarefas são destinadas aos provedores de serviços, logo, o usuário não terá que gastar com energia, contratos de provedores de internet e com toda a organização e estrutura necessária de uma nuvem. Ademais, já que nossa empresa é grande, é essencial que a nuvem possua uma alta confiabilidade e escalabilidade - e isso em geral é garantido pelos provedores de nuvens públicas, que fornecem recursos e dimensionamento automático que garantem alta disponibilidade e distribuição de carga - o que evita inatividade e falhas na rede. Outrossim, por ser uma contratação de serviço, o custo é relativamente baixo e flexível, de tal forma que pagaremos apenas pelos recursos que usaremos. Por fim, em relação a segurança, sabemos que o dever de proteger a nuvem, o que inclui a segurança física do data center, é do provedor, mas tudo aquilo que colocamos na nuvem é de nossa responsabilidade, todavia esse último ponto não é um problema já que contamos com um time de especialistas em segurança que garantem que nenhuma informação importante será vazada. Ainda em relação a este tópico de segurança, tem-se que em nuvens públicas as aplicações podem suportar recursos de segurança avançados sem ter problemas com compatibilidade de infraestrutura - o que também mitiga vulnerabilidades.

3. Agora explique para ao RH por que você precisa de um time de DevOps.

Os engenheiros de DevOps são responsáveis por introduzir processos, ferramentas e metodologias que equilibrem as necessidades ao longo do ciclo de vida de um software (desde sua criação até a implantação e sua manutenção). De maneira geral, um DevOps busca executar processos que aceleram e automatizam aspectos dos processos de desenvolvimento, testes e lançamento de softwares, sites e aplicativos - o que garante continuamente atualizações de segurança.

Dessa forma, esses profissionais são essenciais na empresa para saber como construir a infraestrutura e a colocar em prática da melhor forma, seja usando, por exemplo, o Juju, o Ansible, o Openstack, entre outros, e também se serão utilizados provedores de infraestrutura, plataforma ou serviço. Além disso, tudo o que for construído precisa de manutenção, atualização e melhorias de segurança. E são os DevOps que fazem tudo isso, ou seja, eles são responsáveis pelo desenvolvimento do software, pelas operações e pela garantia de qualidade do que está sendo implementado.

Uma imagem interessante pode ser vista a seguir, ela mostra algumas possíveis ferramentas que são utilizadas pelos DevOps em alguns dos processos em que eles estão envolvidos.



Retirada do site: https://blog.4linux.com.br/qual-o-nivel-de-maturidade-devops-da-sua-empresa/ .

4. Considerando o mesmo sistema crítico, agora sua equipe deverá planejar e implementar um ambiente resiliente e capaz de mitigar possíveis interrupções/indisponibilidades. Para isso, identifiquem quais são as principais ameaças que podem colocar sua infraestrutura em risco, e descreva as principais ações que possibilitem o restabelecimento de todas as aplicações de forma rápida e organizada caso algum evento cause uma interrupção ou incidente de segurança. Para isso monte um plano de DR e HA que considere entre as ações:

- **Mapeamento das principais ameaças que podem colocar em riscos o seu ambiente.**
- **Elenque e priorize as ações para a recuperação de seu ambiente em uma possível interrupção/desastre.**
- **Como sua equipe irá tratar a política de backup?**
- **Considerando possíveis instabilidades e problemas, descreva como alta disponibilidade será implementada em sua infraestrutura.**

As principais ameaças que podem colocar em riscos os nossos ambientes são: queda de energia, queda de internet, o serviço que está sendo utilizado estar fora do ar, o sistema usado ser descontinuado, uma falha na segurança que vaza dados, um hacker que pode

invadir o sistema e os recursos que podem se tornar escassos com o tempo. Para cada um dos casos, existem algumas ações que podem ser tomadas para recuperar o ambiente em alguma possível interrupção ou desastre.

Caso aconteça uma queda de energia, a primeira coisa a se fazer é parar de alimentar todos os equipamentos da empresa, já que a energia pode voltar com picos momentâneos que podem causar danos ou até queimá-los. Além disso, depois todos os equipamentos precisam ser checados para garantir que não estão apresentando nenhum problema em seu hardware.

Agora, caso aconteça uma queda de internet, existem alguns passos a serem tomados. Um deles é reiniciar os equipamentos como o modem e o roteador, isso porque reiniciar zera o cache e outras funções que podem ter sido interrompidas em situações de sobrecarga. Além disso, caso o software esteja travado, após ser reiniciado ele poderá voltar a operar normalmente. Mas também existem outras etapas a serem consideradas, como: conectar algum aparelho diretamente ao roteador, verificar os cabos ou mudar o canal da rede wi-fi.

Se o serviço utilizado estiver fora do ar, o que precisa ser feito é utilizar algum outro serviço parecido temporariamente, ou se o serviço for descontinuado além de usar algum outro serviço temporariamente, será necessário encontrar um serviço compatível ou em que a migração de dados e funções seja relativamente simples.

Caso aconteça alguma falha de segurança e o sistema seja invadido por algum hacker, algumas medidas imediatas importantes são: desconectar o servidor e os computadores afetados do roteador, e no caso do wi-fi, também será necessário desabilitar as suas funcionalidades nos dispositivos conectados à rede. Ademais, se o site for o alvo do ataque, o serviço de hospedagem deve ser contatado para ajudar a normalizar os recursos do endereço. Por fim, a equipe de TI deve ser informada para conferir a integridade do banco de dados e do software e tentar mitigar e resolver os problemas ocasionados por isso - como por exemplo, restaurar e reinstalar tudo o que for preciso, ter um servidor como backup, mudar senhas, acrescentar etapas de autenticação, entre outros.

Ademais, se os recursos se tornarem escassos, deve-se contatar o serviço de nuvem e ampliar o serviço que está sendo contratado - sendo que essa é uma vantagem da nuvem pública: a possibilidade de escalar sem precisar arcar com o custo de novos produtos.

Mas tudo isso poderia ser evitado ou prevenido caso haja alta disponibilidade, que será implementada na empresa. Alguns exemplos de ações para garantir alta disponibilidade em cada uma das situações são:

- Estabilizadores, nobreaks e geradores de energia para evitar prejuízos por queda de energia.
- Ter mais de um gateway e contratar mais de uma empresa de internet.

- Mais servidores ou máquinas rodando o mesmo serviço.
- Adoção de serviços que permitam reprodução fácil - como o Terraform, para que o deploy de aplicações seja simplesmente rodar um script.
- Utilizar ferramentas e softwares que sejam orquestradoras para fazer o deploy de maneira automatizada, como o Ansible. Além de utilizar o Openstack para aproveitar bem todo o espaço disponível nos servidores.
- Sempre utilizar mais de um serviço para funções importantes ou ter implementações engatilhadas em outros softwares.
- Sempre exigir autenticação e senhas diferentes - mesmo que seja para o mesmo serviço.
- Ter um plano de backup muito bem estabelecido.

Em relação ao último tópico, pensamos que nossa empresa deve ter um sistema de backup de banco de dados diário e a cada hora, isso porque os dados estão sempre mudando, então o ideal é sempre garantir que esses dados estejam armazenados de alguma maneira. Vale ressaltar que conforme a empresa cresça, isso deve ser expandido para minutos, e não apenas contratar um único serviço de backup, mas vários.