

Os provedores de serviço do Rio estavam prontos?

Grandes eventos exigem etapas de preparação fundamentais para atender a demanda e evitar contratempos

06/09/2016 17:17:37

“Nós vamos congelar a rede”, começou o diálogo com uma grande operadora. “Não podemos testar, implantar provas de conceito ou tocar na nossa rede por nenhuma razão, exceto para manutenção essencial”, continuou. Essa foi a discussão interna relacionada a UEFA Euro 2016, recentemente sediada na França. A operadora respondeu: “Tudo está atrasado – tudo! ”

Com o pontapé inicial dos Jogos Olímpicos, o risco de surgir desafios semelhantes é muito grande, visto o medo das operadoras em perder o controle e a performance de sua rede durante grandes eventos. Quando olhamos para a realidade do Rio de Janeiro, o que preocupa não são os milhares de participantes ou o impacto operacional de centenas de visitantes demandando serviço de telefonia móvel, mas a incapacidade das empresas de telecomunicação em experimentar novas tecnologias ou responder a eventuais problemas, como uma queda ou interrupção maior de seus serviços.

Nesse sentido, o ponto crucial dos problemas dessas companhias surge da tendência de mercado em migrar do modelo de receita média por usuário para lucro médio por cliente. Corroborada pelas transformações das tecnologias de software, como soluções de rede orientadas por software (SDN) e a virtualização de funções de rede (NFV), essas mudanças visam enxugar até o último custo de rede. Entretanto, a já mencionada inflexibilidade – e a preocupação de que implantar um novo elemento na rede ou uma tentativa de empreender um novo serviço poderia abalar o negócio – adiciona um tópico extra para esse desafio. Um claro exemplo é a falta de visibilidade de rede dentro de novas tecnologias virtualizadas como NFV, onde há poucas formas de monitoramento e visibilidade ao nível de pacote para encontrar as causas de falhas de maneira emergencial, quando erros ocorrerem.

Apesar de prudente, optar por congelar a rede para um grande evento pode ser uma ideia exagerada. Um jeito melhor para superar esse tipo de ocorrência é implantar uma arquitetura de visibilidade, que não ajuda somente o operador a tomar o controle da rede durante imprevistos, mas também facilita provas de conceito e testes melhor gerenciados e mais rápidos. O leque de benefícios também inclui:

- Entender sobre as mudanças de rede quando um novo serviço ou elemento é adicionado.
- Ganhar visibilidade dentro de ambientes virtualizados, como SDN ou NFV.
- Aumentar de velocidade nos períodos de teste, visto que o operador pode agora ver e entender diretamente se o novo equipamento é aprovado ou não nos testes de aceitação (ao invés de procurar culpados).
- Viabilizar a localização os problemas de inoperabilidade dentro das funções na cadeia de serviços e no fluxo de tráfego correspondente.

Ambientes com visibilidade pervasiva constituída e um método para retirar rapidamente novos elementos recém-inseridos na rede não precisarão mais interromper suas operações. Há um argumento positivo e muito realista de que possivelmente você precise verificar o desempenho dessas tecnologias mais recentes quando inseridas num teste extremo. Enquanto exista formas de rapidamente remediar e voltar a utilizar os antigos e conhecidos elementos, a operadora pode ver as diferenças entre as soluções mais antigas e as novas para assim tomar decisões em tempo real.

O projeto Tap-as-a-service

Outra abordagem em ascensão para visibilidade a nível de pacote envolve o projeto Tap-as-a-Service (TaaS), desenvolvido com o objetivo de ajudar clientes e administradores de cloud a depurar redes virtuais complexas e ganhar visibilidade de tráfego das máquinas virtuais. A estratégia usa um método independente de fabricantes para acessar dados dentro do servidor por meio de espelhamento remoto. Além de garantir a integridade da rede do cliente, as sessões de espelhamento navegam através de múltiplos nós de rede e ficam acessíveis de modo tradicional, como se uma Test Anything Protocol (TAP) ou porta Switched Port Analyzer/Mirror (SPAN) estivesse abastecendo o tráfego a partir de uma rede física.

Ao fornecer dados para uma variedade de soluções de Analytics e aplicações de segurança, TaaS oferece uma visibilidade para as operadoras que agora podem assegurar a implantação de novas tecnologias sem risco, por meio do uso de ferramentas de depuração, Analytics e de performance já existentes.

O aumento de custos pela interrupção dos serviços

Os benefícios dos recursos de visualização – como aqueles do NFV – são amplamente aceitos e procurados. Da economia de despesas com a redução de custos em hardware e a dependência das funções de rede para o escalonamento de serviços visando endereçar rapidamente às mudanças de demanda, operadoras e prestadoras de serviço estão se tornando mais ágeis e resilientes, ao mesmo tempo que aumentam a satisfação do cliente.

Contudo, mesmo com diminuição de custos proveniente da adoção de NFV, há um fator normalmente negligenciado – despesas pela interrupção dos serviços. Seja o impacto na solidez ou

reputação da empresa, esse tipo de problema vem aumentando devido ao tempo extra gasto para corrigir um sistema falho. Um minuto de interrupção, por exemplo, poderá potencialmente se tornar cinco sem visibilidade direta a nível de pacotes.

A realidade que a operadora previamente mencionada pode nunca mais recuperar as seis semanas perdidas na UEFA Euro 2016. Esse tempo se foi, e a oportunidade de mudar para uma nova tecnologia, aprender ou testar novas possibilidades está significativamente atrasada. Embora seja fácil comentar de fora essas questões, o desafio e as oportunidades perdidas são muito reais. Mas ao adotar uma estratégia que permite uma grande visibilidade de rede, as respostas se tornam mais transparentes.

*Andy Huckridge é diretor de Service Providers Solutions da Gigamon