

# Proposta de análise e caracterização do tráfego de rede no domínio de controle do OpenStack com foco no ciclo de vida das máquinas virtuais

Adnei W. Donatti<sup>1</sup>, Guilherme P. Koslovski<sup>1</sup>, Charles C. Miers<sup>1</sup>

<sup>1</sup>Programa de Pós-Graduação em Computação Aplicada (PPGCA)  
Departamento de Ciência da Computação – Universidade do Estado de Santa Catarina  
Centro de Ciências Tecnológicas – Joinville, SC – Brasil

adnei.donatti@edu.udesc.br,

{guilherme.koslovski,charles.miers}@udesc.br

**Resumo.** *A infraestrutura de rede é um importante recurso para a implantação de uma nuvem computacional baseada em OpenStack. Neste sentido, o presente trabalho apresenta uma proposta para análise e caracterização do tráfego de rede no Domínio de Controle de nuvens OpenStack. A caracterização deste tráfego permitirá planejar e gerenciar melhor os recursos de rede para que não afete o desempenho da nuvem e das aplicações executadas na mesma.*

## 1. Introdução

O OpenStack é um software de código aberto que permite a criação e gerenciamento de nuvens computacionais *Infrastructure as a Service* (IaaS), que podem ser usadas tanto no modelo privado quanto público. As nuvens computacionais privadas operam sobre uma infraestrutura própria, mantida pela organização que a possui, *i.e.*, toda a manutenção da nuvem bem como aspectos de segurança e desempenho são de responsabilidade desta organização. Além disso, as nuvens privadas buscam atender os propósitos da organização, e são acessíveis somente aos indivíduos com permissão, o que garante à organização total controle sobre os recursos ali contidos [Jadeja and Modi 2012].

Neste contexto, a análise e caracterização do tráfego torna-se uma abordagem importante no levantamento de informações relativas tanto à segurança quanto ao desempenho da nuvem. Através da caracterização de tráfego, é possível identificar operações com base no tráfego de rede bem como o que está transitando e sua finalidade. Embora esta técnica ainda seja incipiente no contexto de nuvens, quando se trata de caracterização de tráfego de aplicações tradicionais (*e.g.*, servidores web) torna-se amplamente empregada [Williamson 2001, Braun and Claffy 1995, Gill et al. 2007].

O artigo está organizado de modo que a Seção 2 apresenta uma breve introdução ao OpenStack, bem como trata de aspectos essenciais ao entendimento do problema, como os serviços e organização de rede do OpenStack. A Seção 3 elucida os problemas em analisar e caracterizar o tráfego de rede no OpenStack. Por fim, a Seção 4 traz as considerações e próximos passos.

## 2. OpenStack

O OpenStack é um conjunto de *software* e ferramentas de código aberto para criar nuvens computacionais públicas e privadas. De acordo com [OpenStack 2018], trata-se de um sistema operacional para nuvens, que controla um amplo grupo de recursos de computação,

armazenamento e rede por todo o data center. Atualmente, o OpenStack está na sua 18ª versão (Rocky).

O OpenStack separa os seus serviços em módulos. Além disso, é possível que módulos opcionais sejam acoplados a uma instalação. Entre os módulos mais fundamentais do OpenStack estão:

- **Nova:** Responsável pela distribuição e gerenciamento das instâncias. Realiza tarefas como iniciação, escalonamento e desalocação de máquinas virtuais (MVs);
- **Neutron:** Fornece conectividade de rede entre os outros serviços, bem como disponibiliza uma API para que os consumidores configurem suas redes;
- **Glance:** Atua no processo de armazenamento e recuperação das imagens utilizadas nas MVs;
- **Swift:** Responsável pelo armazenamento e recuperação de objetos não estruturados. Usa técnicas de replicação de dados para tolerância de falhas;
- **Cinder:** Provê armazenamento persistente em bloco para instâncias em execução.

Nos serviços de alto nível, há relacionamento direto com múltiplos serviços, tanto para disponibilizar funcionalidades para outros serviços, como é o caso do Keystone, que fornece um serviço de autenticação e autorização dentro da nuvem, quanto para utilizar ou acessar recursos dos demais (*e.g.*, Horizon e Ceilometer). Em relação ao Ceilometer, trata-se de um serviço que permite monitorar o desempenho do OpenStack. Dessa forma, este é responsável por disponibilizar métricas relacionadas à rede (*e.g.*, bytes enviados por cada interface, erros de envio e recebimento por interface), armazenamento (*e.g.*, tamanho de imagem, latência do armazenamento de instância), processamento (*e.g.*, uso de memória de instância, quantia de instruções executadas), entre outros que podem ser levados em conta em *benchmarks* ou na própria cobrança pelo uso dos recursos, por exemplo.

## 2.1. Organização das redes no OpenStack

Para realizar a comunicação entre os *hosts* que hospedam diferentes serviços são utilizadas redes físicas. A Figura 1 ilustra a infraestrutura recomendada desta rede.

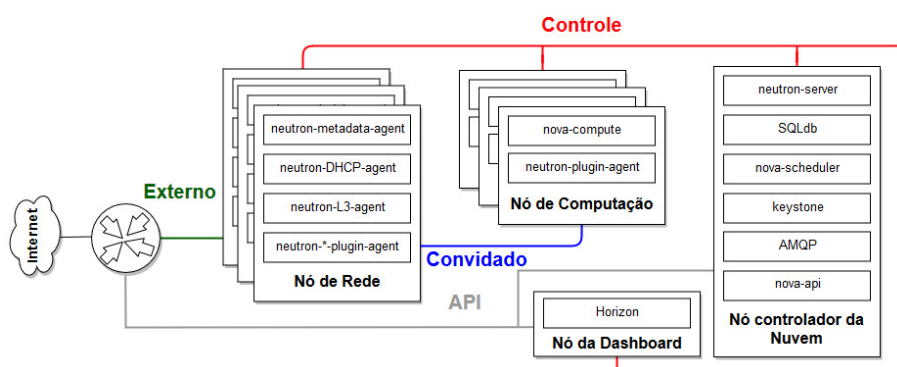


Figura 1. Organização da rede física recomendada pelo OpenStack.

Neste sentido (Figura 1), existem três domínios criados de acordo com políticas de segurança distintas: Domínio Público, de Controle e de Convidados [OpenStack 2018]. Cada domínio engloba grupos diferentes de redes de acordo com a política de segurança.

Em relação ao **Domínio Público**, são englobadas as redes Externa e de API, que são responsáveis pela visibilidade da API da nuvem criada na Internet e do acesso à Internet pelas MVs. Todos os endereços IPs das redes devem ser visíveis a partir da Internet para seu pleno funcionamento [OpenStack 2018].

O **Domínio de Convidados** é formado pela rede de comunicação entre as MVs. Os consumidores do serviço de oferta de MVs são referenciados como convidados por não possuírem vínculo direto com a administração da nuvem, logo, não há garantias sobre quem estes convidados são e quais os seus objetivos. Além disso, através do serviço Neutron, são utilizadas tecnologias de virtualização de rede tanto para isolar o tráfego entre as diversas MVs em um *host* quanto para criar redes virtuais entre elas e tornar possível a comunicação quando assim configurado pelo consumidor [OpenStack 2018].

O **Domínio de Controle** é formado principalmente pela rede responsável pelo tráfego de controle do OpenStack, que corresponde ao tráfego gerado pela comunicação entre os seus serviços. Esta é a rede mais interna da nuvem, sendo que somente os administradores devem acessá-la. Portanto, esta rede dispensa o uso de técnicas de virtualização da rede. Além disso, tanto os nós de controle quanto os nós de computação devem ter uma interface física de rede que conecta-se com a rede de controle. O uso de múltiplas interfaces de rede permite a conectividade a rede de controle e as outras redes conforme o caso, como a rede de convidados no caso dos nós de computação. Logo, em casos normais, uma MV em execução nunca poderá acessar a rede de controle [Krutz and Vines 2010].

### 3. Definição do Problema

O processo de caracterização de tráfego possui etapas genéricas aplicáveis em diferentes cenários, contudo, alguns detalhes do escopo devem ser levados em consideração, como aplicações e protocolos que operam na rede cujo tráfego será analisado. Tais detalhes são essenciais para guiar o modo como a caracterização irá ocorrer, como na escolha entre medição de tráfego passiva e ativa, por exemplo [Zhang and Moore 2007].

Pensando no cenário de nuvens baseadas em OpenStack, há dois locais com potencial para caracterização de tráfego: Domínio de Convidados e Domínio de Controle. Cada um exige diferentes formas de caracterização de acordo com suas particularidades. No Domínio de Convidados existem múltiplas redes virtualizadas, logo, ao medir o tráfego a partir de uma MV são coletados dados apenas da rede virtualizada na qual a instância está inserida, que também pode conter outras MVs que fazem parte do mesmo projeto [Denton 2015]. Dessa forma, para coletar este tráfego por inteiro, a medição deve ser feita em um nível mais baixo, no qual a virtualização não afete o processo, como em *switches* físicos ou no nível do hipervisor. Outra questão que é importante ao medir o tráfego gerado por MVs é a privacidade dos dados, ou seja, para manter a privacidade do tráfego, o conteúdo em si não pode ser coletado.

Já sobre o Domínio de Controle, a virtualização não é empregada com tanta frequência, o que de certa forma torna o seu funcionamento mais simples. A principal utilidade da virtualização neste domínio é isolar dos outros domínios que estejam operando na mesma rede física. Neste caso, empregam-se tecnologias como VLAN, que isola o tráfego da rede de controle, mas não acrescenta complexidade à rede. Além disso, o Domínio de Controle costuma receber atenção especial, já que o seu desempenho afeta diretamente o funcionamento de toda a nuvem. Portanto, para analisar o impacto resul-

tante na rede de controle, será elaborado um ambiente controlado no qual serão simuladas as ações de um consumidor sobre uma MV. O tráfego oriundo das interações do consumidor com a virtual machine (VM) será coletado de acordo com a variação de tráfego na rede de controle e requisições enviadas para a API. A fim de melhor limitar o escopo deste trabalho, serão analisadas interações que atuam diretamente na variação do ciclo de vida de uma instância, como a criação, desligamento ou suspensão.

#### 4. Considerações & Trabalhos futuros

Após apresentar algumas características fundamentais do OpenStack e explicar a necessidade de conhecer sobre aquilo que está trafegando e sua finalidade na rede de controle, percebe-se que a análise e caracterização do tráfego de rede neste contexto é de considerável importância, mesmo que ainda incipiente. É através desta análise que fica possível identificar tanto questões de desempenho quanto de segurança da nuvem. A fim de formular uma proposta de caracterização válida e coerente, deve-se analisar outros trabalhos já realizados com escopo similar. Dessa forma, será possível identificar técnicas de medição e análise do tráfego, bem como escolher aquela que mais se aplica ao cenário.

**Agradecimentos:** Os autores agradecem o apoio do LabP2D/UDESC e a FAPESC.

#### Referências

- Braun, H.-W. and Claffy, K. C. (1995). Web traffic characterization: an assessment of the impact of caching documents from ncsa's web server. *Computer Networks and ISDN Systems*, 28(1):37 – 51. Selected Papers from the Second World-Wide Web Conference.
- Denton, J. (2015). *Learning OpenStack Networking (Neutron)*. Packt Publishing.
- Gill, P., Arlitt, M., Li, Z., and Mahanti, A. (2007). Youtube traffic characterization: A view from the edge. In *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement, IMC '07*, pages 15–28, New York, NY, USA. ACM.
- Jadeja, Y. and Modi, K. (2012). Cloud computing - concepts, architecture and challenges. In *2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET)*, pages 877–880.
- Krutz, R. L. and Vines, R. D. (2010). *Cloud security: A comprehensive guide to secure cloud computing*. Wiley Publishing.
- OpenStack (2018). What is openstack? <https://www.openstack.org/software>. [Online; Acesso em: 08 Jan. 2019].
- Williamson, C. (2001). Internet traffic measurement. *IEEE Internet Computing*, 5(6):70–74.
- Zhang, J. and Moore, A. (2007). Traffic trace artifacts due to monitoring via port mirroring. In *2007 Workshop on End-to-End Monitoring Techniques and Services*, pages 1–8.