Fluxo de logs em ambiente de emulação CORE (Common Open Research Emulator)

Carlos de Moraes [1], Felipe Duarte[1], Luciano S da Silva[1]

[1]Centro de Processamento de Dados – Universidade Federal de Santa Maria (UFSM)
Caixa Postal 508 – 97105-900 – Santa Maria – RS – Brazil

{crgmoraes,luciano}@cpd.ufsm.br, felipe.dua@redes.ufsm.br

Abstract. *There are several tools that aid in the design and administration of computer networks. In this respect, the Common Open Research Emulator, also known as CORE, allows many tests of network operation before it is implemented as well as for network scalability tests or new services that are incorporated. However, because CORE uses a container for virtualization of applications running at the core of the system, this compromises the collection of activity logs of the node, since these are restricted to the host host and compromising the access of softwares That analyze the logs, since both use the same resource of the host.*

Resumo. *Existem diversas ferramentas que auxíliam tanto no projeto quanto na administração de redes de computadores. Neste aspecto o Common Open Research Emulator, também chamado de CORE, permite muitos testes de funcionamento de rede, antes mesmo desta ser implementada como também, para testes de escalabilidade da rede ou novos serviços que sejam incorporados. No entanto, pelo fato do CORE utilizar contêiner para virtualização de aplicações que executem no núcleo do sistema, isto compromete a coleta dos logs de atividades do nó, uma vez que estes ficam restritos ao host hospedeiro e comprometendo o acesso de softwares que analizam os logs, já que ambos utilizam o mesmo recurso do hospedeiro.*

1. Introdução

Para o projeto de uma rede que ainda está por ser implementada, é de considerável magnitude, que esta seja implementada em um simulador, bem como testada exaustivamente pois somente assim teremos que certeza que a rede estará longe de falhas por uma falha do projeto que foi descoberto após o seu projeto de execução. Para isto há diversas ferramentas de simulação de redes de computadores, entra elas o *CORE*, que é uma ferramenta que permite a implementação de uma rede virtual de computadores de maneira rápida através de uma interface customizável e de fácil utilização [CORE 2015]. O CORE fornece um ambiente para execução de aplicações e protocolos reais e pode ser conectado a roteadores e redes físicas existentes. Ele é usado para pesquisa de protocolos, demostrações, teste de plataformas, estudos de segurança, testes para aumento físico de rede, etc. Para a construção dos nós virtuais, o CORE utiliza o recurso de virtualização do Linux "network namespace" também conhecidos como nets ou Linux contêiners (LXC) junto com a construção de *Linux Ethernet bridging*.

2. Contêiner LXC

Contêiner é um recipiente que oferece um ambiente de execução o mais próximo possível de uma Máquina Virtual porém, sem a sobrecarga que acompanha a execução do núcleo separado e a simulação de todo o hardware do sistema computacional [LinuxContainers.org 2017]. Sistemas baseado em contêiners tem as aplicações que compartilham o mesmo sistema operacional resultando em aplicações que utilizam menos recursos. Cada conteiner deve fornecer aos seus processos a ilusão que não existem outros processos no sistema. Para isto o *namespace* deve fornecer uma visão isolada de um recurso global para o conjunto de processos participantes deste *namespace*. Porém tanto o núcleo do sistema operacional Linux quanto processos no espaço do usuário enviam seus registro de atividades para *rsyslogd* que classifica e grava em arquivos de registro "log" conforme a configuração utilizada [Kerrisk 2012].

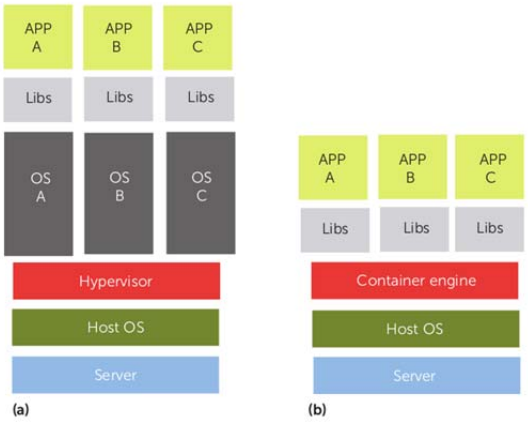

Figura 1. Comparação de sistemas: (a) *hipervisor* e (b) baseado em contêiner [Bernstein 2014].

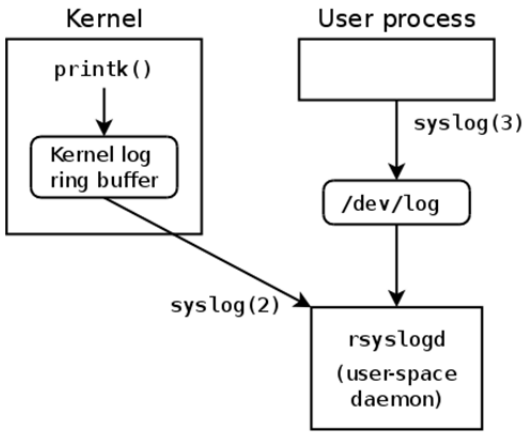

Figura 2. Fluxo de mensagens entre o núcleo e o *userspace* [Kerrisk 2012].

Análises realizadas em ambientes de redes dependem da visão dos arquivos de log gerados pelas aplicações. Em um acesso HTTP ao servidor web, normalmente é gerado

um log para esta atividade. O login ou a tentativa de login também deve ser registrado. Porém alguns registros partem do núcleo do Sistema operacional e não é disponibilizado ao nó cliente.

É possível a configuração de alguns serviços de modo que o registro ocorra dentro do espaço de usuário no emulador CORE como aplicação web mas não esta disponível para todos os serviços.

Netfilter é um framework de manipulação de pacotes de rede presente no Linux desde versões 2.4 do kernel do Linux ou posteriores. Normalmente é associado com o Iptables que é um interface de linha de comando que roda a partir do espaço do usuário permitindo a filtragem de pacotes, tradução de endereços/portas de rede, NA[P]T e outras modificações de pacotes [Netfilter 2017].

Aplicações de Firewall baseada no Netfilter executa apartir do núcleo no sistema operacional do hospedeiro enquanto que os comandos que são aplicados a partir do espaço do usuário como por exemplo o Iptables.

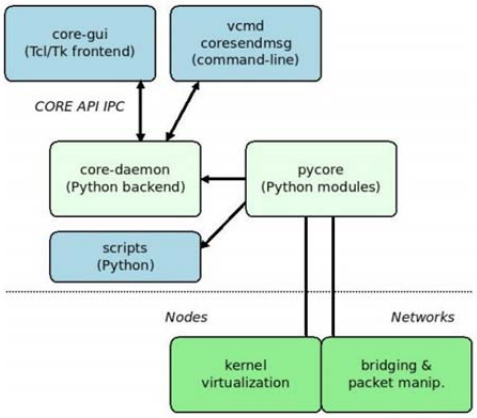

Figura 3. Arquitetura do CORE [CORE 2015].

De acordo com a figura 3, a linha tracejada representa a separação entre o espaço de usuário e o núcleo do sistema. A manipulação de pacotes é realizada abaixo desta linha pertencendo a área do núcleo.

3. Conclusão e Trabalhos Futuros

Este trabalho apresentou um ambiente de emulação de redes de computadores no qual se verificou que os registros de aplicações que são gerados pelo núcleo do sistema operacional não ficam disponibilizados para outras aplicações que estão dentro do *userspace* reservado para as aplicações de usuário, no caso o hosts emulados pelo CORE e suas aplicações locais sem acesso e não podem executar corretamente as suas funções. Uma proposta para o futuro pretende-se desenvolver uma aplicação que disponibilizasse estes registros para as aplicações que a requeressem.

Referências

Bernstein, D. (2014). Containers and cloud: From lxc to docker to kubernetes. In IEEE, editor, *IEEE Cloud Computing*, pages 81–84. IEEE.

CORE (2015). *CORE Documentation*. U.S. Naval Research Laboratory, 15th edition.

Kerrisk, M. (2012). *Stepping closer to practical containers: ”syslog”namespaces*. LWN.nety, 1th edition.

LinuxContainers.org (2017). Linuxcontainers.org infrastructure for container projects. Accesso em: Julho. 2017.

Netfilter (2017). The netfilter.org project. Accesso em: Julho. 2017.