Introduction to Content Centric Networking and the CCNx framework

Thibault Cholez, University of Luxembourg, Luxemburg

Based on the observation that today's Internet is more about content diffusion than point-to-point communication, Content Centric Networking (CCN) is a new routing paradigm that proposes a radical change on the Internet architecture while being incrementally deployable. CCN is one of the most promising research area for a future Internet, more scalable, secure, collaborative and efficient. It is currently raising the increasing interest of the network community. This workshop aims to give to the audience the key elements to better understand CCN and its possibilities.

- Presentation of CCN
  - The CCN paradigm
  - Challenges and research activities
- CCNx tools - how to use the framework to experiment CCN, hands-on exercises
  - Architecture of CCNx
  - Provided tools and libraries
  - Generation of CCN traffic
  - Writing of a CCN application
iSCSI. The nova-compute service, will be setup with the KVM hypervisor to instantiate virtual machines. OpenStack Glance will be used to maintain a registry of virtual machines available to Nova services. In the second part of the tutorial, participants will learn to work with the compute cloud by creating user credentials. They will then download, register and instantiate an image using the euca-tools package. They will also learn to create and attach persistent block storage to their virtual machine using euca-tools. Attaching floating and fixed IP addresses will also be covered.

Outline:

- An Introduction to Cloud Computing
- An Overview of the OpenStack Architecture
- Setting up an OpenStack Compute Cloud
  - Cloud controller service
  - Registry service for OpenStack
  - Persistent block storage with iSCSI
- Using the OpenStack Compute Cloud
  - Creating users
  - Using euca-tools
  - Instantiating VMs
  - Managing storage and IP addresses

16h30: Coffee-Break

Tutorial 3: Tuesday June 5, 2012 (Full Day  Room A14- 9h00-12h00/14h00-18h00)


Pavel Celeda, Masaryk University, Czech Republic

In the first part of tutorial participants will learn how to use NetFlow tools (NetFlow analysis tools NfSen/NFDUMP and the FlowMon probe) for network security monitoring. Participants will use the tools to identify and analyse network security threats in real network data. In the second part of tutorial, additional NfSen plugins will be presented and participants will use them to perform advanced analysis of network data. Possibilities of writing new plugins will be discussed together with further development.

Pavel Celeda, Ph.D., works as a researcher and a systems analyst at the Institute of Computer Science at the Masaryk University in Brno (http://www.muni.cz). He has an engineering degree in electrical engineering from the Military Academy Brno and Ph.D. in informatics from University of Defence. Pavel led in 2005-2010 the software group of Liberouter project (http://www.liberouter.org). His current research areas include security and monitoring of high-speed networks and development of network monitoring devices. His research results were successfully transferred to several university startup companies. You can reach him at celeda@ics.muni.cz.

Outline:

- NetFlow as an essential part of network security monitoring
- NetFlow tools - how to use NFDUMP and NfSen, hands-on exercises
  - Analysing NetFlow data
  - Creating NfSen profiles and alerts
  - Identifying network threats
- Overview of existing NfSen plug-ins and work with them
  - University of Twente: SurfMap, SSH plugin, Ethernet monitoring
  - Masaryk University: PortTracker, DelayWatch, CNDet, PeaKock
  - Cesnet: Hamster, InternetAlerts, BC Dimensions
- Further possibilities
  - Writing new plugins for NfSen and FlowMon
  - Further development

16h00: Coffee-Break