Virtual Appliance Applications

Yao-Min Chen

Outline

- ☐ Introduction to Virtual Appliances
- ☐ Case Study 1: License Server Virtual Appliance
- ☐ Case Study 2: Distributed Virtual Switch (DVS) Controller Virtual Appliance
- ☐ Intrusion Detection System VM

Introduction

- Virtual appliances to cloud computing
  - Is like Apps to iPhone or Android phones
- Ready to run (turnkey)
  - Can be deployed through the Internet
- Minimal initial setup
  - Networking and storage
- Web-based UI
  - For advanced configuration

What is a Virtual Appliance?

- ☐ It is self-contained *virtual machine* that includes a pre-installed *operating system*, *applications* and *services*.
- ☐ A virtual appliance allows you to quickly deploy POCs and full production deployments.
- ☐ Complex installations of SW solutions can be simplified and streamlined.
- ☐ Product installations can be performed in advance leaving little or no configuration left for the customer to perform.

Current State

- VMware claims 1000+ virtual appliances (www.vmware.com/appliances)
- Top categories
  - OS (Ubuntu, Fedora)
  - Networking (network mgmt, network monitoring)
  - IT (LAMP stack)
  - Enterprise Resource Planning (ERP) and CRM
  - Applications Infrastructure (ZEG Groupware, Zeus LB)
  - Storage (EMC, HP, FalconStor)
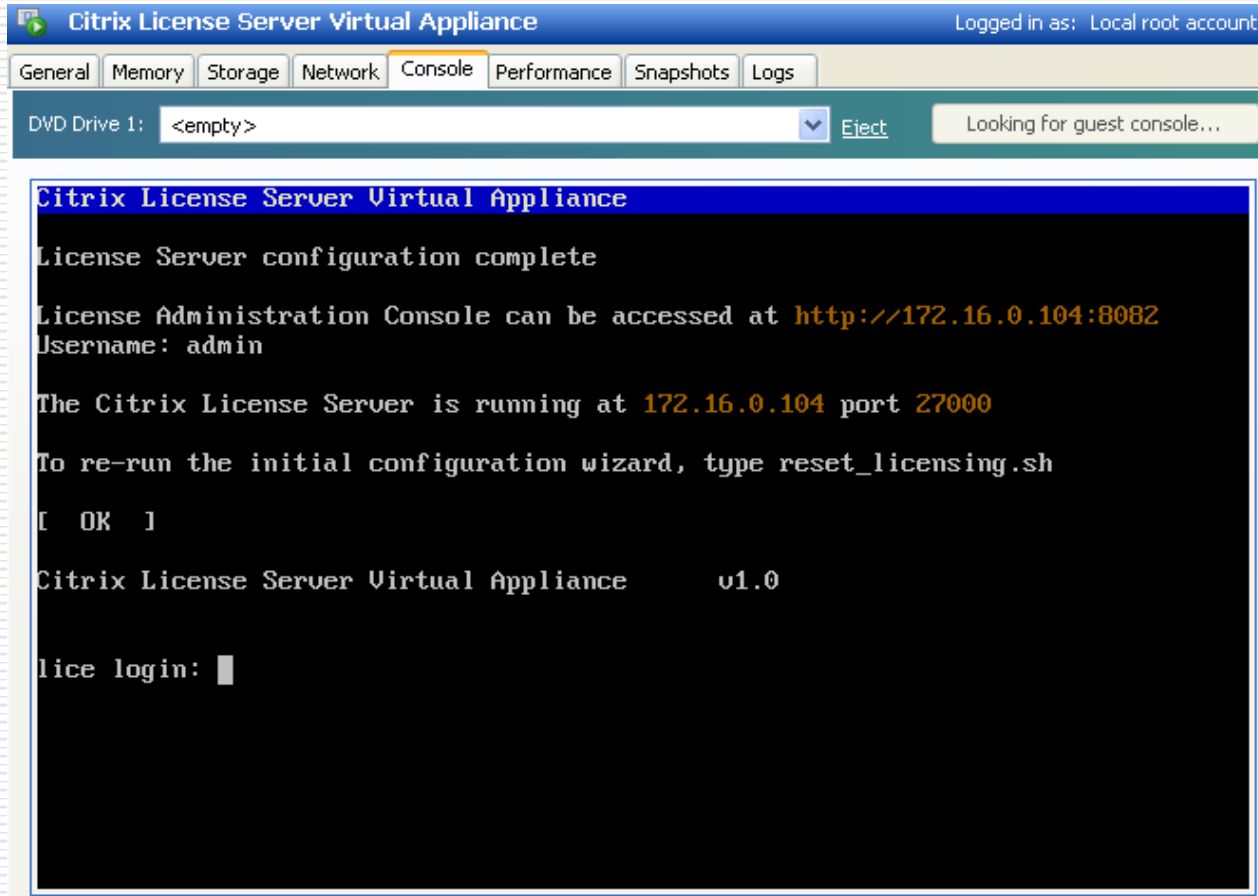 - Collaboration, Systems Infrastructure, Content Distributions

Current State (Cont'd)

- ☐ XenServer 5.6 Feature Pack 1 in Beta
  - ■ Distributed virtual switching is big step towards network virtualization
- ☐ Network (nodes and links) in a box
- ☐ Switching capabilities absorbed into servers
- ☐ New types of hardware accelerations may be needed
  - ■ TCP offloading, WAN optimization, Load Balancing
  - ■ QoS and Queue Management

License Server Virtual Appliance

How SW vendors collect revenue

License Server as a VM

License Server GUI

License Server VM GUI (Cont'd)

Import Licenses

Populated Licenses

Why Licensing Is Important

- ☐ Protect SW development return on investment (ROI)
- ☐ Foundation of a flourishing SW industry
- ☐ Help move from a consumer-based industry to enterprise and datacenter-centric industry
    - ■ Consumer industry – SW is add-on, usually free with HW purchase
    - ■ Enterprises/data center – HW platforms are relatively low cost ("commodity") compared with SW licensing cost

Case Study 2: DVS Controller Virtual Appliance

Networking in a box

DVS Controller Basics

- ☐ Each server has multiple virtual networks

- ☐ Servers are aggregated into a **"*resource pool*"**

  - ■ Each resource pool is identified a "pool master" server

- ☐ DVS Controller manages multiple resource pools

Adding Resource Pools

Adding Resource Pools (Cont'd)

Distributed Virtual Switch

- Consists of
  - a virtualization-aware switch (the *vSwitch*) running on each host
  - *DVS Controller*, a centralized server that manages and coordinates the behavior of each individual vSwitch to provide the appearance of a single distributed virtual switch.

DVS Features

□ The DVS Controller supports fine-grained security policies to control the flow of traffic sent to and from a VM.

□ It also provides detailed visibility into the behavior and performance of all traffic sent in the virtual network environment.

DVS Controller Features

- ☐ Dashboard
  - ◼ Server Statistics
  - ◼ Network Statistics
  - ◼ Network Event
  - ◼ Aggregate Throughput and Packet Rate
- ☐ Visibility and Control
  - ◼ Status
  - ◼ Flow Statistics
  - ◼ Access Control
  - ◼ Port Configuration

- ☐ Settings
  - ◼ IP Configuration
  - ◼ SW Version and Upgrade
  - ◼ Server Maintenance
  - ◼ Administrative Accounts
  - ◼ Configuration Snapshots
  - ◼ Time and NTP
  - ◼ Syslog

DVS Controller Dashboard
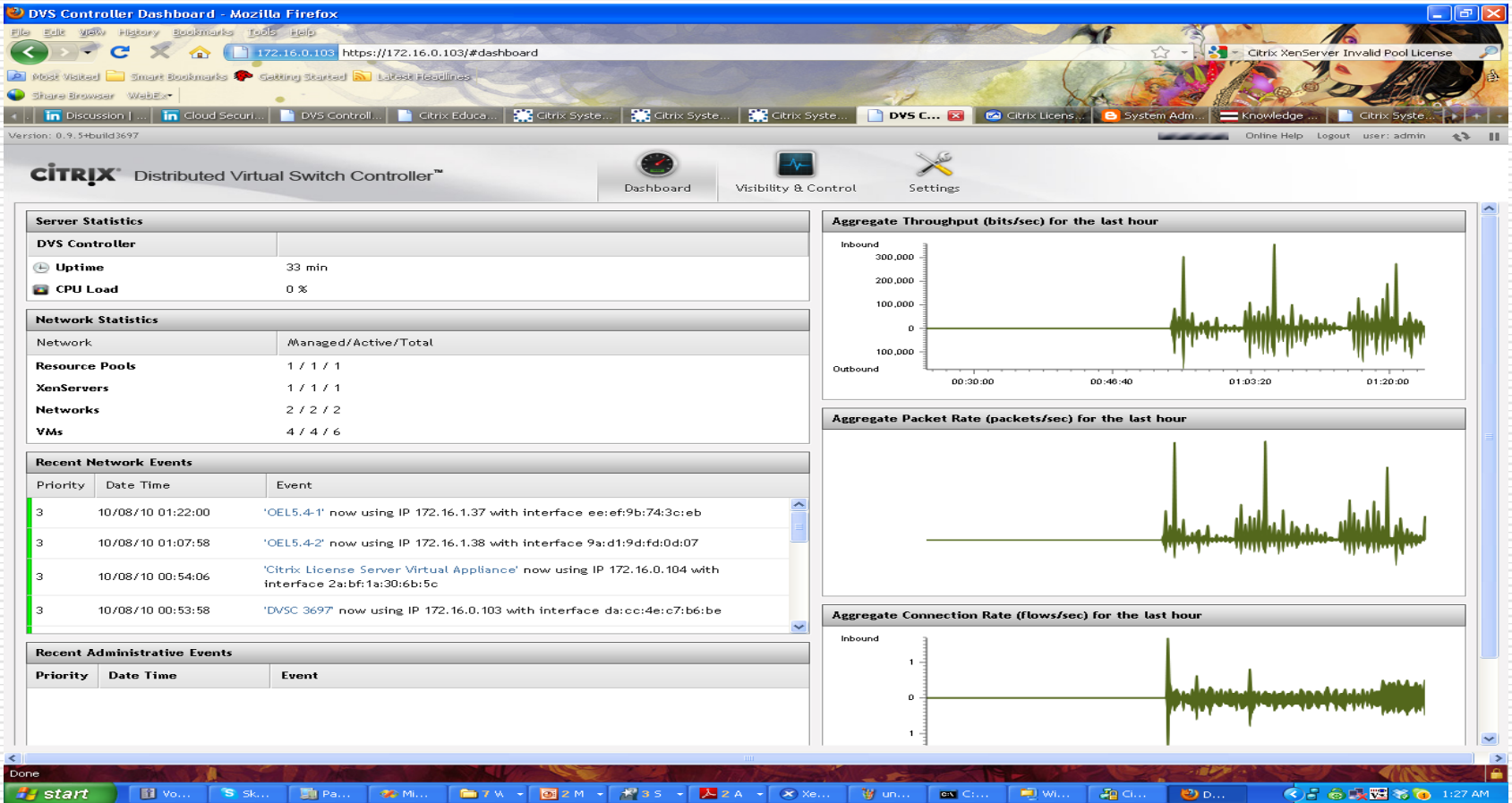
DVS Controller Flow Statistics

DVS Controller Security Policy

Status	Flow Statistics	**Access Control**	Port Configuration

Security Policy

Save Policy Changes   Undo Changes

▼ Global Policy

Action	Protocol	Direction	Remote Addresses	● Description ○ Rule Details	⚙
allow	ARP	to / from	Any	allow ARP to and from VMs	⚙
allow	DHCP	to	Any	allow VMs to acquire an IP via DHCP	⚙
allow	DNS	to	Any	allow VMs to perform DNS lookups	⚙
	Placeholder for more specific Pool, Network, VM, and Interface policies.				⚙
allow	Any	to / from	Any	Add New ACL Above Add New ACL Below	allow all traffic to and from VMs	⚙

DVS Controller Port Configuration

- QoS Policy
  - Rate limiting (Kb/s, Mb/s, or Gb/s) with burst size of Kbits, Mbits or Gbits
  - Applied at the VIF level
  - Policy hierarchy
    - Global: all VIFs in all resource pools
    - Resource pools: all VIFs in a particular resource pool
    - Port-wide networks: all VIFs attached to a particular network
    - VMs: all VIFs attached to a particular VM
   - VIFs: a single VIF

Why is QoS Important?

- ☐ Cloud providers charge tenants based on usage (Gbps, gigabytes etc).
- ☐ Elastic aspect of Clouds requires accurate measurement and monitoring of usage traffic for sizing, capacity planning, and migration.
  - ◼ Predictability is the key.

DVS Controller Port Configuration (Cont'd)

- ☐ Traffic Monitoring (RSPAN) Policy
  - ■ Mirroring traffic
    - ☐ Which is sent or received on a VIF to a VLAN
    - ☐ To support traffic monitoring applications
  - ■ Can be configured at the global, resource pool, network, VM and VIF levels
  - ■ Configurations at a given level override the configurations at the higher levels

Multi-layer Hierarchy for Policies
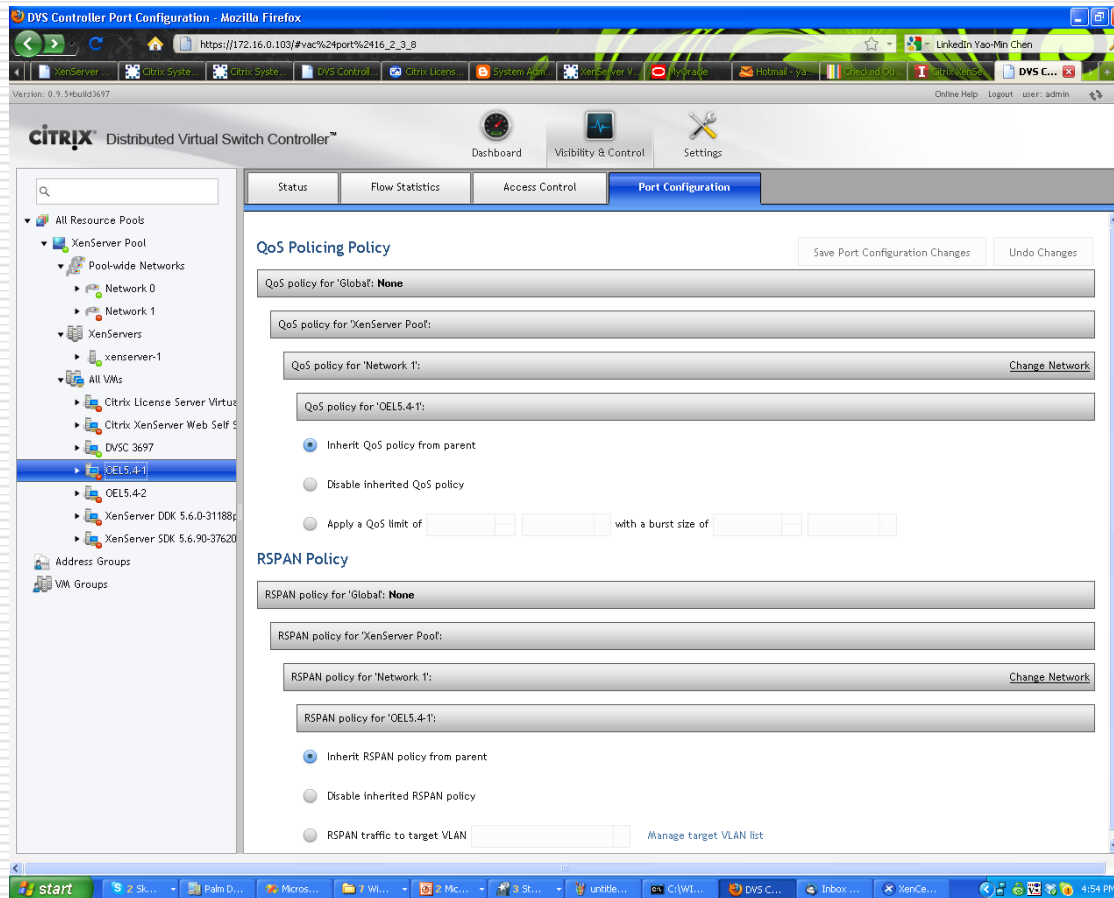
Why is RSPAN Important

- ☐ Security
  - ■ Intrusion detection
- ☐ Auditing
  - ■ Enabling 3rd-party "auditor appliances"
- ☐ Accounting and charging
  - ■ Usage-based charging
- ☐ Marketing
  - ■ Building usage profiles – "marketing research appliances"

Some Concluding Remarks

Where do we go from here?

To Do's for DVSC

- ☐ Good initial step, but it only manages the virtual switches inside Xen hosts but not physical switch

- ☐ Right now, cannot monitor and enforce policies from end to end

Two Views on Virtual Appliances

- ☐ LiveCD view
  - ■ Before installing full-fledged OS, try the LiveCD first
  - ■ Before installing production-ready product, try the virtual edition first
- ☐ C^2 View
  - ■ The product (with OS bundled) lives in the cloud, and is not tied down to particular hardware boxes
  - ■ Nomadic servers

Welcome Further Discussions

- ☐ Email: yaominchen@gmail.com
- ☐ Skype: yaominchen
- ☐ LinkedIn: Yao-Min Chen