Sine Nomine Associates

VM/Advanced Network Services

A New Reference Architecture for VM TCP Services

David Boyes
Sine Nomine Associates
MVMUA, January 24, 2005

Problem Overview

- Services dated in terms of function and capability
- Unable to quickly assimilate and deploy new services and functions
- VM TCP perceived to be complex to set up
- Linux hosting strategy complicated by host-orientation vs network-orientation

Sine Nomine Associates

Impact

- Perceived as additional barrier to Linux on zSeries adoption
- Perceived as insecure/antiquated
  - Most VM systems attached to the public Internet are in popular RBLs as risk to public infrastructure
- Complicates L2 adoption strategy
- Complicates HW assist implementation

Sine Nomine Associates

Proposal Overview

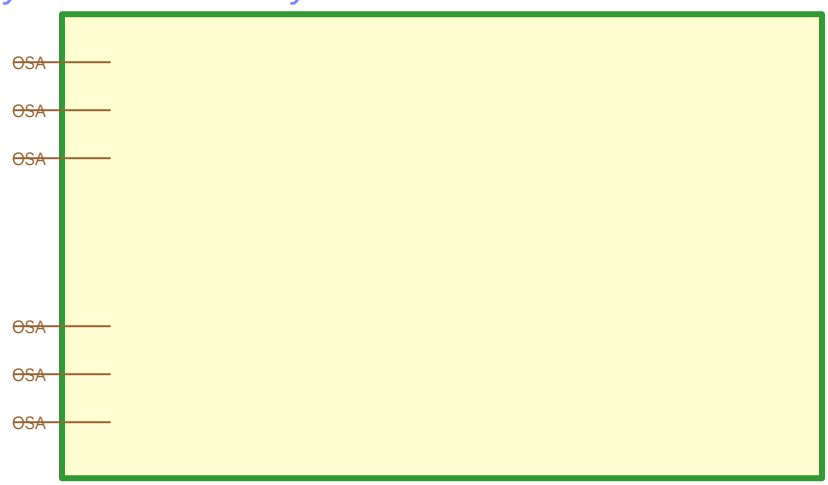
- Use Linux-based appliances to replace existing CMS services
  - Use existing code to support legacy services where public interfaces are not available
- Add new multi-platform functionality
- Ship a fully-configured system requiring only minimal setup

Sine Nomine Associates

Design Overview

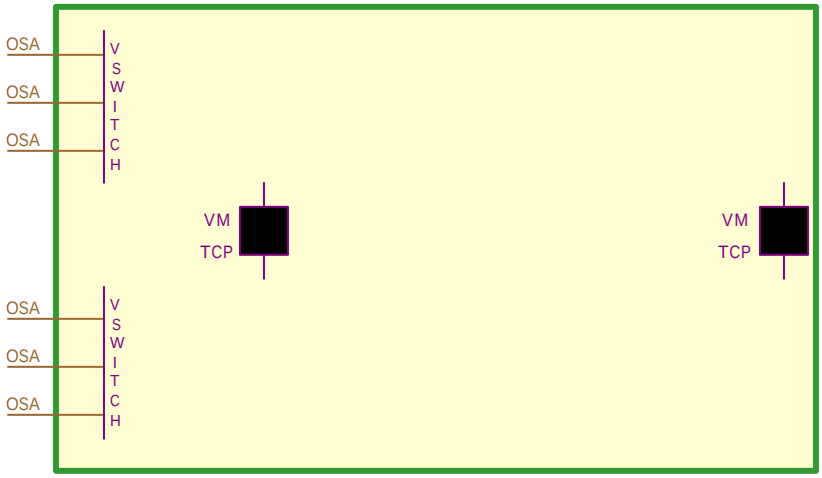
Sine Nomine Associates

Physical Connectivity



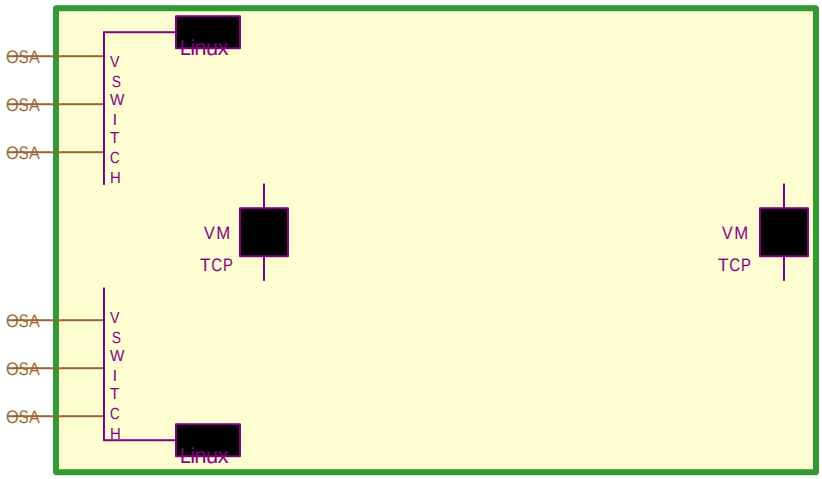
Sine Nomine Associates

VSWITCH Controllers



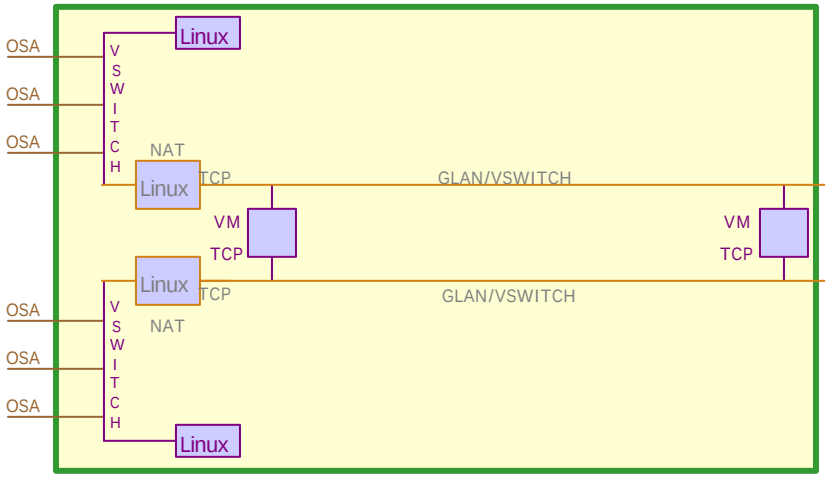
Sine Nomine Associates

Linux Guest Networking



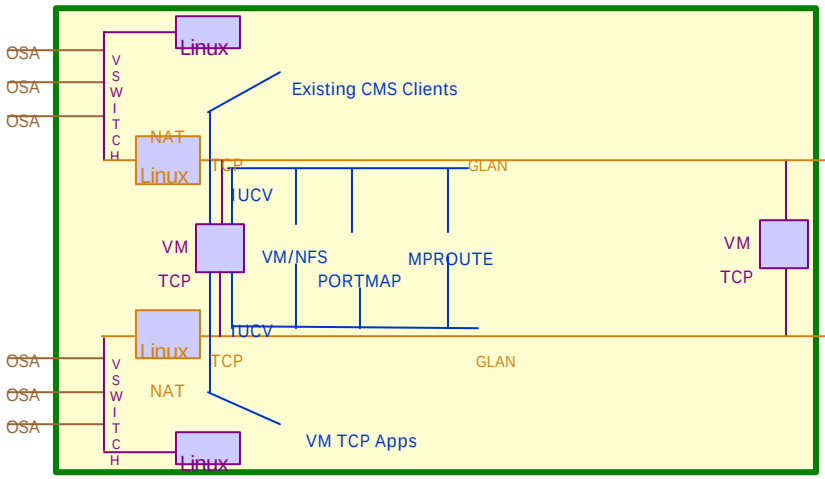
Sine Nomine Associates

VM TCP Connectivity



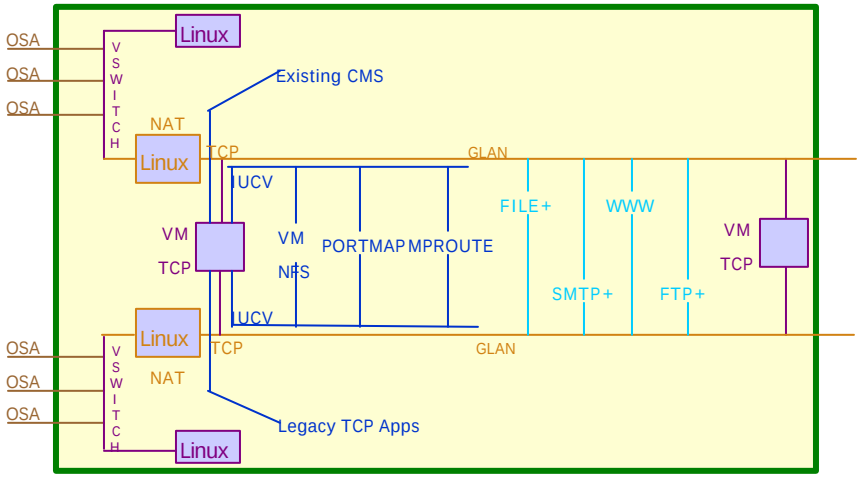
Sine Nomine Associates

Existing CMS TCP Applications



Sine Nomine Associates

Modern Applications



Sine Nomine Associates

New Function

- Packet Filtering
- Traffic Shaping
- Traffic Authentication
- SMB/NFSv4 Support
- FTP Checkpoint
- Grid Services Support
- Full redundancy in default implementation
- Robust Cisco-style routing implementation
- WWW Server
- "Couple and Go" Support for Guests
- Spam/virus scanning
- RBL support
- Full DNS implementation w/o DB2
- Easy implementation of new protocols
- Kerberos support in tools
- LDAP Server

Sine Nomine Associates

Backward Compatibility

- Completely backward compatible
  - CMS clients continue to communicate with VM TCP as interim step
  - Support for migration to complete Linux stack when AF_IUCV support completed and tested in Linux NAT appliance
  - Conversion tools to migrate existing configuration partially done
    - SMTP (100%)
    - FTP (100%)

Sine Nomine Associates

New Services/APIs

- IPP support (via CUPS/lpr and RSCS)
- Kerberos 5
- LDAP
- HTTP
- WWW based configurator
  - TCP services
  - VM management (later)
- User SNMP proxy/ integration
- TCPwrappers
- Outbound SSL (predefined ports)
- Crypto Engine exploitation (if present) in SSL

Sine Nomine Associates

Documentation

- Current weak point
  - Design: completed
  - Application manuals: completed
  - Messages & Codes: pending
  - Built to Unix standard

Sine Nomine Associates

Maintenance

- Total replacement service
- Kernel in NSS, /usr in DCSS
- User configuration data on individual disk attached to service machine
  - Editable from Linux or CMS
  - Working on WWW configurator

Sine Nomine Associates

Performance

- No additional impact to Linux guests attached to VSWITCH
- CMS users average 3-5% throughput impact due to NAT processing (prototype on MP3K)
- Approx 10% increase in disk footprint over existing TCP stack (in prototype)

Sine Nomine Associates

Completeness

GW+	100%
SMTP+	100%
FTP+	100%
FILE+	100%
LDAP+	90%
WWW+	90%
IPP+	100%
Configurator	80%
Documentation	70%

Sine Nomine Associates

Benefits

- Simplifies VM TCP configuration to supplying a minimum of 1 IP address, netmask, default gw and DNS server
- Allows shipping completely configured, fully redundant services behind GW servers
- Promotes "building blocks" support services for Linux farms
- Provides modern secure services for CMS users w/o significant development

Sine Nomine Associates

Summary

- The work done so far has endured almost 9 months of production use, and is mature and stable.
- Using the appliance approach, we can rapidly design and implement compatible function for both Linux and CMS users with a minimum of effort and time
- If desired, additional appliances can be quickly implemented. Requests are being taken…8-)

Sine Nomine Associates

Q&A

Sine Nomine Associates

Contact Info

David Boyes
Sine Nomine Associates
+1 703 723 6673
dboyes@sinenomine.net