Bootstrapping VIN Security

Jens Jensen, STFC
with Phil Kershaw, STFC

contrail is co-funded by the EC
7th Framework Programme
The Goal(s)

- Provide a network (tunnel) between VMs in IaaS
- Secure
- Private
- Elastic (obviously)
The Conundrum

- Build the network security in:
  - The OS?
  - The Hypervisor?
  - The VM?

- Consequences for bootstrapping
- Ended up selecting the VM...
  - Works on public clouds
  - But may support >1 model
Contrailese

- **VIN = Virtual Infrastructure Network**
  - A private virtual network
- **VEP = Virtual Execution Platform**
  - An interface (see Monday’s talk) to IaaS
The Security View

- Secure VMs with X.509 certificates

- Separate problem – needs CaaS, certificates as a service ;-)
High Level Architecture

Federation

VIN CA

Contrail

Cloud

Hosts

VEP

ONE ctrl

IaaS ctrl

Node

Node

Node
Technology View

- Secure VMs with X.509 certificates...
- Inside the VM, virtual host identity
- Use IPSec to link hosts
  ...federatedly!
1: startSession()

Create cert signing request for new VIN CA

2: csr, key pair = initCertRequest(vin ca cert dn)
3: getCert(vin ca csr)

3.1: policy decision = checkPolicy(vin ca csr)
3.2: vin ca cert = issueCert(vin ca csr)
3.3: vin ca cert = getCertResp

The VIN is now configured with its own CA with which to issue certificates to VMs in the VIN.

3.3.1: vin session id = startSession()
4: registerVM(vin session id)

Register VM with new VIN controller session

Start VIN Agent in order to register a VM

4.1: startVinAgent(agent 1 id, vin ca cert)
5: initTrustRoots(vin ca cert)

Take a copy of the VIN Controller CA cert so that it can verify calls from it.

6: vin agent id = startVinAgentResp
7: registerVinAgent(vin agent id)
8: registerVm(vm 1 id)

The VIN Controller acts as an online CA issuing certificates to VMs in its VIN

8.1: startVM(vm 1 id, vin ca cert)
8.1.1: initTrustRoots(vin ca cert)
8.1.2: csr, key pair = initCertRequest(vm 1 cert dn)
8.1.3: getCert(vm 1 csr)

8.1.3.1: policy decision = checkPolicy(vm 1 csr)
8.1.3.2: vm 1 cert = issueCert(vm 1 csr)
9: vm 1 cert = getCertResp

The VM needs a certificate issued from the VIN CA so that it can identify itself.

10: startVmResp

The VM should be restarted now that it has a new key and cert in place

11: registerVmResp

12: registerVmResp
Er, so far so good, but...

- The bootstrap problem...
  - The credential is to be put in the VM...
  - But the issuer (=VIN CA) doesn’t know where the VM will run, beforehand
  - And we don’t trust the IaaS controller 😏
- And VIN can span multiple VM controllers
  - And VEP supports multiple VINs (and multiple controllers), and doesn’t run the VIN CA
- The VIN CA is at the fed level (= VIN ctrlr)
Federation

VIN Ctrlr
VIN CA

IaaS Ctrlr

Node
VM
OAuth client

IaaS

VEP

req auz
grant
Federation

VIN Ctrlr
VIN CA

req auz
grant

VEP

auz
grant

IaaS Ctrlr

VM

Node

OAuth client

IaaS
VIN Ctrlr
VIN CA
Federation

IaaS Ctrlr
VM
OAuth client
Node

IaaS

VEP

auez
grant
Generate CSR/key, submit request, return cert
Conclusion

- Scalable and elastic private network for IaaS
- Non-trivial bootstrapping problem... solved(?)
contrail is co-funded by the EC 7th Framework Programme

Funded under: FP7 (Seventh Framework Programme)
Area: Internet of Services, Software & virtualization (ICT-2009.1.2)
Project reference: 257438
Total cost: 11.29 million euro
EU contribution: 8.3 million euro
Execution: From 2010-10-01 till 2013-09-30
Duration: 36 months
Contract type: Collaborative project (generic)