Security Considerations
Securely Setting up your Open Nebula Cloud
A top 10 Best Practise Guide

OpenNebula Conf, September 25, 2013 in Berlin, Germany

Nils Magnus
inovex GmbH
Senior System Engineer
I. **Security** is 90% architecture and 10% implementation. Apparently trivial suggestions form the base of your protection.

II. **Security** is intrinsically understaffed. Management wants „quick wins“, team is looking to „get the job done“. Somehow.

III. **Security** is not about checklists. If you are (or feel) responsible, you need to know your individual vulnerabilities. In this mode think like an attacker.

**Share my thoughts how to protect an Open Nebula cloud!**
Don't underestimate the necessity of security.

Assign proper ressources to adress this issue. Security is a costly investment in the future.

It is a bargain compared to the loss of your main business processes. The possible damage scales to the same extend as your cloud itself.
Admin Account

Protect access to the ONE admin account, the SunStone UI, and infrastructure.

Once attackers gain unlawful access to your command bridge, your systems might be doomed. All of them.
VLAN Hopping

Prevent VLAN hopping in the scope of your SDN and between physical hosts.

Network virtualization with VLAN tagging comes very handy, but keep in mind that the very frames of all virtual segments may travel on a shared medium.
Environments

Partition your cloud network segments into distinct security areas.

Protect the different security environments and border them from each other.

Actively separate maturity environments and different types of processed data.
Apply Classic Best Practises Anyway

Despite in the cloud, nonetheless apply network security best practises like

- firewalls,
- intrusion detection, or
- data leak prevention,

based on the very requirements of your environment.
Host Protection

Securing virtual machines is not enough.

Make sure you also protect the access to all of your hosts, even if they are not designed to have users on them.
Key and User Management

Set up a working SSH infrastructure and enforce it.

Open Nebula heavily relies on a working and secured way to communicate with your hosts and virtual machines.

Properly configured keys help both automating the system deployment process and restricting access on a need-to-know basis.
Sensible Distrust

Auto discovery and self registration to the inventory are powerful features that alleviate the system engineer's duties.

But make sure that only known bare metal systems register into your cloud store and virtual ressources.

Don't boot systems you don't have full control over.
Protect access to your shared storage. Several hosts have to access the images of all security environments. Rogue images injected in the right place might act as trojan horses in otherwise well-protected environments.
Availability

Keep resources in mind. One major advantage of virtualization is to share resources like CPU or IO bandwidth.

But some player in your cloud may or may not play fair.

Those situations, both intended and unintended, threaten your availability.

Enacting QoS measure could be helpful.
Wrap-up

1. assign proper resources
2. protect your admin account
3. secure the networks
4. partition into environments
5. apply classic network security measures
6. protect your hosts
7. install a key infrastructure
8. authenticate all repositories
9. protect the shared storage
10. keep an eye on availability
Sources and Acknowledgment

Freedom is the brother of security. The great photos of this presentation are licensed under the free Creative Commons license (CC-BY SA) that allows use and redistribution (share alike) as long as you give proper attribution. A big thank you goes to:

**UCL Engineering** for the chainmail:
http://flickr.com/photos/uclengineering/6946862623

**Jwalanta Shrestha** for the multi lanes in Kathmandu:
http://flickr.com/photos/jwalanta/4496289019/

**Drgriz52** and the bears at the tent:
http://flickr.com/photos/drbair_photography/3571049565/

**Steve Tannock** and his meadows of the Peak District:
http://flickr.com/photos/stv/2586761094/

**Chris McBrien** for his photo of the blue keys:
http://flickr.com/photos/cmcbrien/4715320000/

**Sergio Morchon** for the array of cannons:
http://flickr.com/photos/smorchon/2951615532/

**Simon Hooks** for his shot of the Trojan Horse:
http://flickr.com/photos/gogap/253649673/

**Sam Greenhalgh** took a photo of a rack in a data center:
http://flickr.com/photos/80476901

**Matt Peoples** for the kegs:
http://flickr.com/photos/leftymgp/7332282888/

**Justin Ennis** photographed the Swiss Guard in Rome:
http://flickr.com/photos/averain/5307438963/

**Schub@** took a photo a looking glass:
http://flickr.com/photos/schubi74/5793584347

**Maury Landsman** for the applause:
http://www.flickr.com/photos/mau3ry/3763640652
Thanks for listening! Questions?

Contact

Nils Magnus
Senior System Engineer

inovex GmbH
Office Munich
Valentin-Linhof-Str. 2
81829 Munich, Germany

+49-173-3181-057
nils.magnus@inovex.de

Agent L9 Oxycryocrypt