Best Practices for Securing your Openstack / Amazon VM instances / Containers

Ken Bigelow

UBC Advanced Research Computing (ARC)

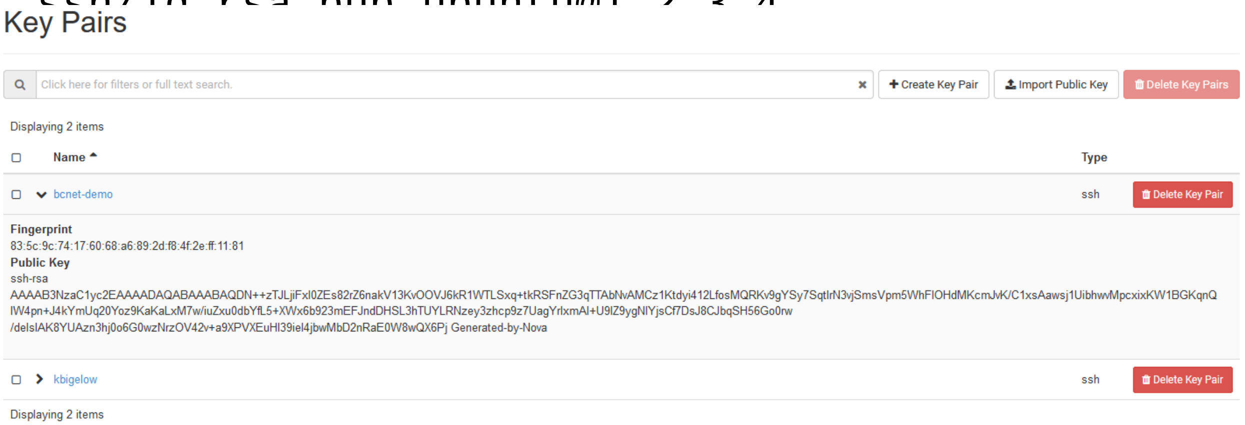
3/30/2022

Todays discussion

- SSH keys & virtual machine first time login
- The end of zombie virtual machines
- Never Trust, Always Verify – Zero trust model
- Vulnerabilities and attack vectors within containers
- Full lifecycle container security

Virtual machine first time login using SSH keys

```
ubuntu@westgrid-demo:~$ ls -l ~/.ssh/id_*.pub
ls: cannot access '/home/ubuntu/.ssh/id_*.pub': No such file or directory
ubuntu@westgrid-demo:~$ ssh-keygen -t rsa -b 4096 -C "your_email@domain.com"
ubuntu@westgrid-demo:~$ ssh-copy-id -o 'IdentityFile=bcnet-demo.pem' -i
 ssh/id_rsa.pub ubuntu@1.2.3.4
```



Key Pairs

Displaying 2 items

□	Name	Type	
□	bcnet-demo	ssh	Delete Key Pair
□	kbigelow	ssh	Delete Key Pair

Fingerprint
83:5c:9c:74:17:60:68:a6:89:2d:f8:4f:2e:ff:11:81
Public Key

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDN++zTJLjiFxl0ZEs82rZ6nakV13KvOOVJ6kR1WTLSxq+tkRSFnZG3qTTAbNvAMCz1Ktdyi412LfosMQRKv9gYSy7SqtIrN3vjSmsVpm5WhFIOHdMKcmJvK/C1xsAawsj1UibhwMpcxixKW1BGKqnQ
lW4pn+J4kYmUq20Yoz9KaKaLxM7w/iuZxu0dbYfL5+XWx6b923mEFJndDHSL3hTUYLRNzey3zhcp9z7UagYrlxmAI+U9lZ9ygNlYjsCf7DsJ8CJbqSH56Go0rw
/delslAK8YUAzn3hj0o6G0wzNrzOV42v+a9XPVXEuHl39iel4jbwMbD2nRaE0W8wQX6Pj Generated-by-Nova
```

Displaying 2 items

```
'bcnet-demo.pem.pub': No such file
```

```
ubuntu@westgrid-demo:~$ vi ~/.ssh/authorized_keys
```

Enter the created ~/.ssh/id_rsa.pub key from your remote workstation into ~/.ssh/authorized_keys on the host server / user that you want to log in with.

Let us test it out.

```
User@DESKTOP:~$ ssh ubuntu@1.2.3.4
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-105-generic x86_64)
ubuntu@westgrid-demo:~$
```

DID YOU SAVE YOUR PRIVATE KE

The end of zombie virtual machines

UBC

WEST GRID

Step 1: Install unattended-upgrades package

```
ubuntu@westgrid-demo:~$ sudo apt update
ubuntu@westgrid-demo:~$ sudo apt upgrade
Do you want to continue? [Y/n] Y
ubuntu@westgrid-demo:~$ sudo apt install unattended-upgrades
ubuntu@westgrid-demo:~$ sudo apt install update-notifier-common
ubuntu@westgrid-demo:~$ systemctl status unattended-upgrades
Active: active (running) since Mon 2022-03-28 22:28:51 UTC; 1 day 3h ago
```

Step 2: Configure unattended-upgrades service

```
ubuntu@westgrid-demo:~$ sudo vi /etc/apt/apt.conf.d/50unattended-upgrades
// Python regular expressions, matching packages to exclude from upgrading
Unattended-Upgrade::Package-Blacklist {
mariadb
nginx
};
```

```
// This option controls whether the development release of Ubuntu will be
// upgraded automatically. Valid values are "true", "false", and "auto".
Unattended-Upgrade::DevRelease "auto";
// Send email to this address for problems or packages upgrades
// If empty or unset then no email is sent, make sure that you
// have a working mail setup on your system. A package that provides
// 'mailx' must be installed. E.g. "user@example.com"
Unattended-Upgrade::Mail “user@your-domain.com";
// is used to chose between "only-on-error" and "on-change"
Unattended-Upgrade::MailReport "on-change";
// Automatically reboot *WITHOUT CONFIRMATION* if
//  the file /var/run/reboot-required is found after the upgrade
Unattended-Upgrade::Automatic-Reboot "true";
```

```
// Automatically reboot even if there are users currently logged in
// when Unattended-Upgrade::Automatic-Reboot is set to true
Unattended-Upgrade::Automatic-Reboot-WithUsers "true";
// If automatic reboot is enabled and needed, reboot at the specific
// time instead of immediately
//  Default: "now"
Unattended-Upgrade::Automatic-Reboot-Time "04:00";
ubuntu@westgrid-demo:~$ sudo vi /etc/apt/apt.conf.d/20auto-upgrades
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Unattended-Upgrade "1";
```

Note – If you do not have the following file /etc/apt/apt.conf.d/20auto-upgrade run the following.

```
ubuntu@westgrid-demo:~$ sudo dpkg-reconfigure --priority=low unattended-upgrades
```

Step 3: Configure mail service for update notifications

Test the server for mail out functions.

```
ubuntu@westgrid-demo:~$  echo "Testing the body of the email" | mail -s "Testing subject line" your-email@your-domain.com

mail: command not found

mail can be installed using the following command: apt-get install mailutils

ubuntu@westgrid-demo:~$ sudo apt install mailutils

ubuntu@westgrid-demo:~$  echo "Testing the body of the email" | mail -s "Testing subject line" your-email@your-domain.com
```

If all goes well you will rec[illegible]r inbox.

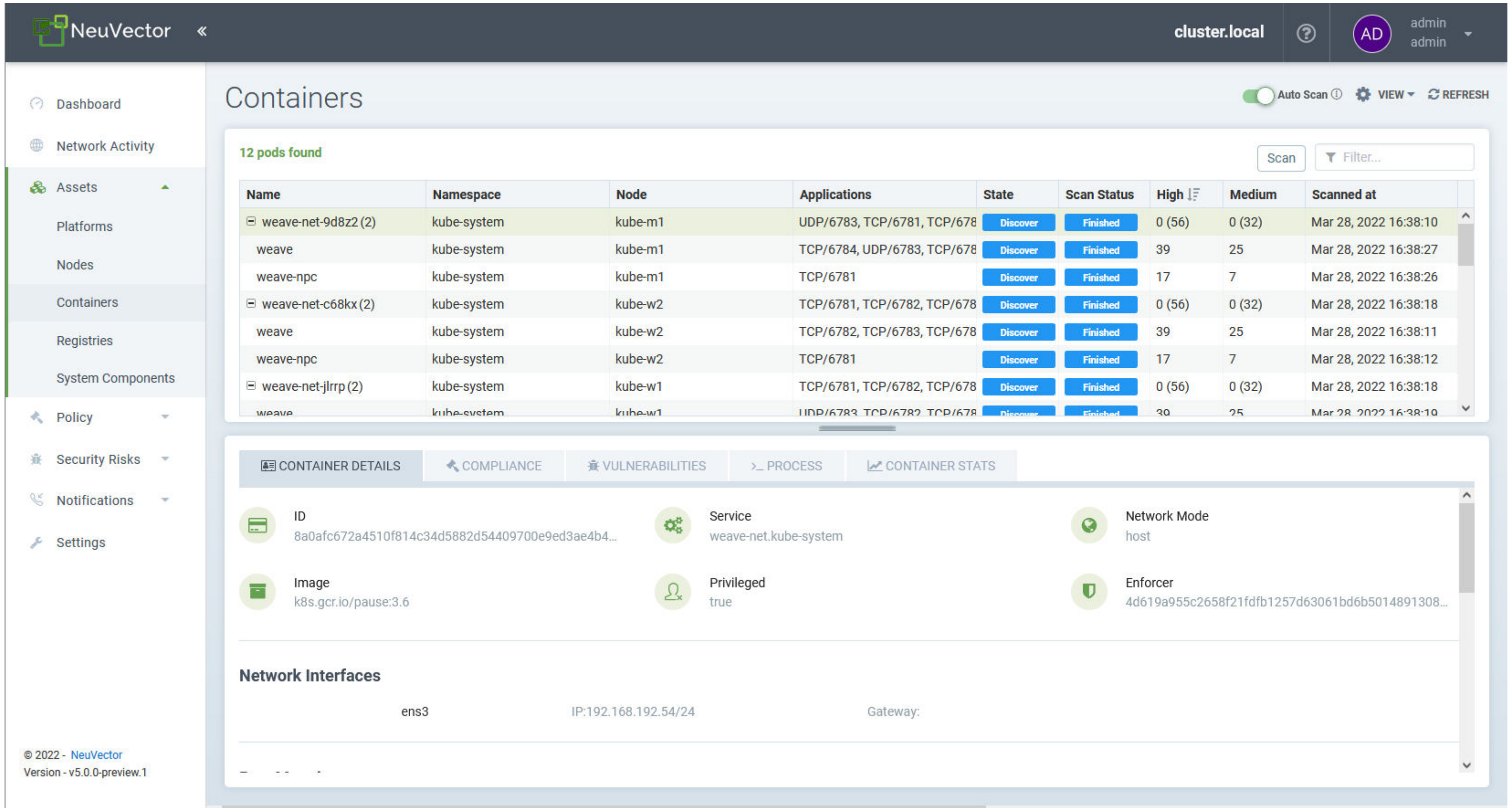
Never Trust, Always Verify – Zero trust model

- The zero trust model is NOT a new concept.
- Implicit Trust vs Explicit Trust
- Core zero trust principles

Vulnerabilities and attack vectors within containers

- Traditional tools have a hard time in container environments
- Overstuffed container images are difficult to secure
- Container sprawl introduces runtime complexity
- Gaps in controls make it hard to ensure image integrity and authenticity

Full lifecycle container security



Containers

12 pods found

Name	Namespace	Node	Applications	State	Scan Status	High	Medium	Scanned at
⊟ weave-net-9d8z2 (2)	kube-system	kube-m1	UDP/6783, TCP/6781, TCP/678	Discover	Finished	0 (56)	0 (32)	Mar 28, 2022 16:38:10
weave	kube-system	kube-m1	TCP/6784, UDP/6783, TCP/678	Discover	Finished	39	25	Mar 28, 2022 16:38:27
weave-npc	kube-system	kube-m1	TCP/6781	Discover	Finished	17	7	Mar 28, 2022 16:38:26
⊟ weave-net-c68kx (2)	kube-system	kube-w2	TCP/6781, TCP/6782, TCP/678	Discover	Finished	0 (56)	0 (32)	Mar 28, 2022 16:38:18
weave	kube-system	kube-w2	TCP/6782, TCP/6783, TCP/678	Discover	Finished	39	25	Mar 28, 2022 16:38:11
weave-npc	kube-system	kube-w2	TCP/6781	Discover	Finished	17	7	Mar 28, 2022 16:38:12
⊟ weave-net-jlrrp (2)	kube-system	kube-w1	TCP/6781, TCP/6782, TCP/678	Discover	Finished	0 (56)	0 (32)	Mar 28, 2022 16:38:18
weave	kube-system	kube-w1	UDP/6783, TCP/6782, TCP/678	Discover	Finished	39	25	Mar 28, 2022 16:38:19

ID
8a0afc672a4510f814c34d5882d54409700e9ed3ae4b4...

Service
weave-net.kube-system

Network Mode
host

Image
k8s.gcr.io/pause:3.6

Privileged
true

Enforcer
4d619a955c2658f21fdfb1257d63061bd6b5014891308...

Network Interfaces

ens3 IP:192.168.192.54/24 Gateway:

UBC

WESTGRID

Questions?