

Stavíme VM... aneb šlapeme na hrábě

Pavel Valach

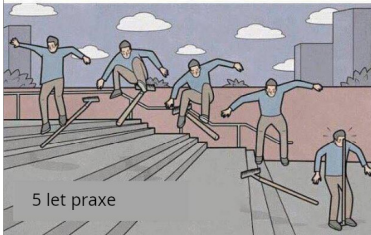
4. 10. 2026

LinuxDays 2026, Praha

Jak se člověk cítí?



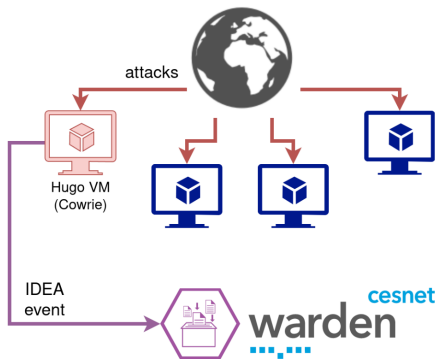
Virtualizace v mládí



5 let praxe

VM a honeypoty?

VM a honeypoty



- Samočinný sběr dat o útocích ze zapojených organizací
 - Datový zdroj pro Warden
 - Každá událost je platná
- Předpřipravené VM s honeypoty
 - Nyní Cowrie a Dionaea
- Cíl: co nejjednodušší start
 - Import VM & nastavit & spustit
 - Integrovaný monitoring a reporting stavu
- <https://hugo.cesnet.cz>

Nejsme ani zdaleka jediní...

stačí zmínit T-Pot

`https://github.com/telekom-security/tpotce`

Proces buildu VM



Obrázek: Zjednodušený proces buildu VM tak, jak jsme ho dělali.

Vývoj VM

- Začali jsme s VirtualBoxem.
- Postupný rozvoj.
- Úvodní instalace Debianu z ISO přes unattended install
 - `https://docs.oracle.com/en/virtualization/virtualbox/6.0/user/basic-unattended.html`
- Nejprve VMDK, poté VDI.
- Více stages buildu - použity snapshoty ke zrychlení.

VirtualBox a první sada trápení

VirtualBox a provozní drobnosti

- Vboxdrv module triggers IBT protection. VM's fail to start
 - <https://www.virtualbox.org/ticket/21435>
- Kernel moduly a Secure Boot
 - vboxdrv, vboxnetadp, vboxnetflt
 - Moduly je nutné zkompilovat (a pro Secure Boot podepsat).
 - Pomocník: <https://forja.gvisoc.com/gabriel/signmodules>

Práce s VM a disky

- VirtualBox má registr VM a disků, kde si drží stav.
- Disk i VM musí být zaregistrován.
- Spousta kontrol integrity: např. nelze odregistrovat disk, na který je navázaná VM.
- Pouze jedna operace zároveň.
- Umí snapshoty (VDI).
 - Použity ke zrychlení buildu - různé stages.

Práce s disky

Problém

Virtuální stroj nabírá na velikosti.

Práce s disky

Problém

Virtuální stroj nabírá na velikosti.

Řešení

Compacting!

- **TRIM, DISCARD, UNMAP** a jim podobní.
- Ve virtuálních strojích funkce emulovány.
- Použitím se diskovému řadiči nahlásí bloky jako volné, dochází k reclaimu místa.

Práce s disky

Problém

Virtuální stroj nabírá na velikosti.

Řešení

Compacting!

Příklad použití:

```
1 VBoxManage storageattach "GuestOsMachineName" \  
   --storagectl "SATA" --port 0 --device 0 \  
3   --nonrotational on --discard on
```

a poté `fstrim -va` ve virtuálním stroji.

Práce s disky – VirtualBox

Problém č. 2

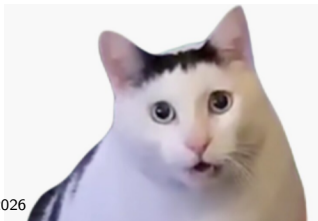
Virtuální stroj se občas zasekává.

<https://www.virtualbox.org/ticket/16450>

Vysvětlení

Funkcionalita TRIMu je experimentální a obsahuje známé chyby.

Řešení: Zmenšit `discard_max_bytes...` nebo použít řadič IDE...



Vzdálená plocha (RDP? VNC?!)

Vzdálená plocha (RDP? VNC?!)

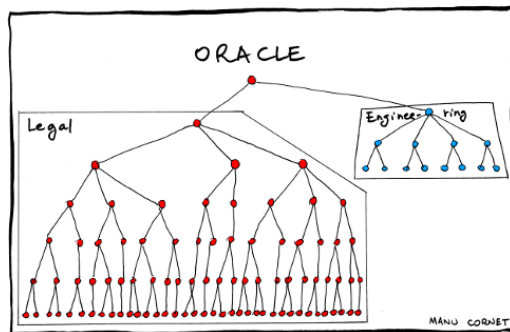
- Debian má v repozitářích VirtualBox. Kdysi jej měl i ve `stable` větvích.
 - Nyní jen pro `sid` [1].
- Verze Debianu neumí RDP. Ale má rozšíření VNC.
Oracle jej distribuuje pouze ve formě zdrojového kódu.
- RDP má pouze Extension Pack, který není OSS – striktně nekomerční použití.
- Extension VNC je zmíněna na jedné stránce [4], bez pořádných odkazů.
 - VNC extension je z roku 2012, kód není aktivně udržován [5].
 - Experimentální kód, musíte si ho zkompileovat, a prý má zásadní problémy s podporou jiných rozložení klávesnice než US [4].
 - Arch a Debian ho mají...

Reference k předchozímu slide

- 1 <https://tracker.debian.org/news/1038163/virtualbox-removed-from-testing/>
- 2 https://wiki.debian.org/VirtualBox#RDP_not_working_out_of_the_box.3F
- 3 <https://docs.oracle.com/en/virtualization/virtualbox/6.0/admin/vrde.html>
- 4 <https://docs.oracle.com/en/virtualization/virtualbox/6.0/admin/otherextpacks.html>
- 5 <https://github.com/VirtualBox/virtualbox/commit/71b30f21329c620b656e53cc5591d8f5b78b914e>

Vzdálená plocha (RDP? VNC?!)

- RDP je obsažen pouze v Extension Packu, který není OSS – striktně nekomerční použití.
- S právníky jsem se hádat nechtěl.



Obrázek: Zdroj: Manu Cornet,
<https://bonkersworld.net/organizational-charts>

Spolupráce VirtualBoxu a VMware

Import a export virtuálního stroje

- Standardizovaný Open Virtualization Format (OVF) a Open Virtual Appliance (OVA).
 - .ova = .tar se soubory OVF, VMDK a možná manifestem.
- Formát je standardní, interoperabilita zaručena není...

Import a export virtuálního stroje

- Co vytvoří VirtualBox:
 - Platný stream-optimized VMDK obraz.
 - Definiční soubor (.ovf) s HW specifickým pro VirtualBox.
- Co očekává VMware Workstation:
 - Provádí relaxovanou validaci.
 - Zahlásí potenciální problém, ale umožní import a běh.
- A co VMware ESXi / vSphere:
 - Provádí nejstriktnější validaci.
 - Přímý export z VirtualBoxu nelze importovat kvůli **nekompatibilnímu HW** v .ovf souboru.
 - I soubor, který VMware OVF Tool zvaliduje, nemusí být ESXi importovatelný.

Import a export virtuálního stroje

Problém

ESXi nepřijímá můj OVF soubor.

Import a export virtuálního stroje

Problém

ESXi nepřijímá můj OVF soubor.

```
1 <VirtualHardwareSection ovf:transport="">
  <Info>Virtual Hardware</Info>
3  <System>
    . . .
5    <vssd:VirtualSystemType>
      **virtualbox-2.2**
7    </vssd:VirtualSystemType>
  </System>
9 </VirtualHardwareSection>
```

Import a export virtuálního stroje

Problém

ESXi nepřijímá můj OVF soubor.

```
1 Issues detected with selected template. Details: - -1:-1:  
  VALUE_ILLEGAL: No supported hardware versions among [virtualbox  
  -2.2]; supported: [vmx-04, vmx-07, vmx-08, vmx-09, vmx-10, vmx-  
  -11, vmx-12, vmx-13, vmx-14, vmx-15, vmx-16, vmx-17, vmx-18,  
  vmx-19].
```

Import a export virtuálního stroje

Problém

ESXi nepřijímá můj OVF soubor.

Řešení č. 1

Napsat do VMware / Broadcomu naštvaný dopis!

Import a export virtuálního stroje

Problém

ESXi nepřijímá můj OVF soubor.

Řešení č. 2

Úprava OVF!

<https://knowledge.broadcom.com/external/article/315994/deploying-ovaovf-fails-with-error-no-sup.html>

Import a export virtuálního stroje

Problém

ESXi nepřijímá můj OVF soubor.

Řešení č. 3

Tvořit OVF v něčem od VMware.

- open-vmdk – obsahuje ova-compose, vmdk-convert
- <https://github.com/vmware/open-vmdk>
- Případně rovnou qemu-img místo vmdk-convert - je o trochu rychlejší.

Import a export virtuálního stroje

Řešení č. 3

Tvořit OVF v něčem od VMware.

Zvolil jsem `ova-compose`.

VM nešla v ESXi/vSphere spustit.

```
1 No host is compatible with the virtual machine.
```

Import a export virtuálního stroje

Řešení č. 3

Tvořit OVF v něčem od VMware.

Zvolil jsem `ova-compose`.

VM nešla v ESXi/vSphere spustit.

```
1 No host is compatible with the virtual machine.
```

Řešení č. 4

Odebrat definici grafické karty.

Stavíme si obraz s Podmanem

Pokus o zmenšení obrazu disku

- Jen základní, minimální instalace Debianu se extrahuje na cca 800 MB.

Pokus o zmenšení obrazu disku

- Jen základní, minimální instalace Debianu se extrahuje na cca 800 MB.

Vypravěč: Co si Pavel neuvědomil, je, že velká část je kvůli kernel modulům. (Toto je Debian 12 (bookworm).)

```
2 395M    /lib/modules/6.1.0-53-amd64
   30M    initrd.img-6.1.0-53-amd64
```

Pokus o zmenšení obrazu disku

- Jen základní, minimální instalace Debianu se extrahuje na cca 800 MB.

Vypravěč: Co si Pavel neuvědomil, je, že velká část je kvůli kernel modulům. (Toto je Debian 12 (bookworm).)

```
2 395M    /lib/modules/6.1.0-53-amd64
   30M    initrd.img-6.1.0-53-amd64
```

Vypravěč: Ale poté měl skvělý nápad....

```
2 92M     /lib/modules/6.1.0-53-cloud-amd64
   14M    initrd.img-6.1.0-53-cloud-amd64
```

Ne vše je vina jen VirtualBoxu – Boot cloud image

Problém č. 3

Chtěl jsem ušetřit místo. Vyměnil jsem Debianí kernel za variantu Cloud. Ted' virtuální stroj nejde nabootovat ve VirtualBoxu.

Ne vše je vina jen VirtualBoxu – Boot cloud image

Problém č. 3

Chtěl jsem ušetřit místo. Vyměnil jsem Debianí kernel za variantu Cloud. Ted' virtuální stroj nejde nabootovat ve VirtualBoxu.

Vysvětlení

Chybí ovladač pro řadič.

- `linux-image-amd64` obsahuje všechny ovladače.
- `linux-image-cloud-amd64` je **výrazně menší**, pro virtualizaci v cloudu.
 - VirtIO, Hyper-V, AWS, etc.
 - Ale ne LSI Logic nebo BusLogic SCSI (což používá ve výchozím VirtualBox)
- VirtIO ve VirtualBoxu nepodporuje TRIM.

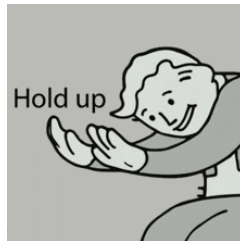
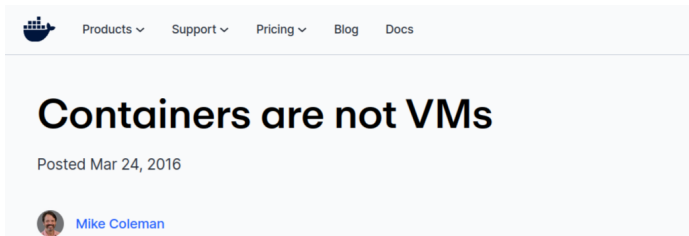
OCI obraz = malý OS bez kernelu

- OCI Image Format – archiv s `rootfs` a obsahující vše, co je třeba k běhu aplikace.
- Kontejner `debian` = malý OS s balíčkovacím systémem.
- Proč by nešlo **použít kontejnerový obraz jako základ** pro instalaci OS?

OCI obraz = malý OS bez kernelu

- OCI Image Format – archiv s `rootfs` a obsahující vše, co je třeba k běhu aplikace.
- Kontejner `debian` = malý OS s balíčkovacím systémem.
- Proč by nešlo **použít kontejnerový obraz jako základ** pro instalaci OS?

Obrázek: Zdroj: <https://www.docker.com/blog/containers-are-not-vms/>



OCI obraz = malý OS bez kernelu

K imagi `debian` v Docker Hubu:

“... More specifically, they’re built from the ‘minbase’ variant, which only installs ‘required’ packages, and thus creates the smallest possible footprint that is still ‘Debian’ (as defined/managed by the Release and FTP teams within the project). ...”

OCI obraz = malý OS bez kernelu

K imagi `debian` v Docker Hubu:

“... More specifically, they’re built from the ‘minbase’ variant, which only installs ‘required’ packages, and thus creates the smallest possible footprint that is still ‘Debian’ (as defined/managed by the Release and FTP teams within the project). ...”

*“The rootfs tarballs for this image are built using the reproducible-Debian-rootfs tool, **debuerreotype**, with an explicit goal being that they are transparent and reproducible. Using the same toolchain, it should be possible to regenerate (clean-room!) the same tarballs used for building the official Debian images. ...”*

`https://hub.docker.com/\_/debian`

I tak je to docela macek

```
paulos-fw :: ~ » podman images | grep -E 'alpine|debian'
```

docker.io/library/ debian	trixie-20260918	124 MB
docker.io/library/ debian	trixie-20260918-slim	81.3 MB
docker.io/library/ alpine	latest	8.72 MB



Bootovatelný Debian build – 1. Dockerfile

```
FROM debian:trixie-20260918
2
RUN apt-get -y update
4 RUN apt-get -y install --no-install-recommends zstd linux-image-
    amd64
RUN apt-get -y install --no-install-recommends systemd-sysv chrony
    systemd-resolved libnss-resolve libnss-myhostname
6 RUN apt-get -y install --no-install-recommends extlinux
RUN apt-get -y install --no-install-recommends iproute2 nano vim
    coreutils iputils-ping iputils-tracepath ifupdown dhcpd isc-
    dhcp-client
8 RUN systemctl enable systemd-journald systemd-resolved networking
RUN systemctl disable dhcpd
10 RUN echo "root:debian" | chpasswd
```

Bootovatelný Debian build – 2. Tvorba disku

Nutné balíčky:

util-linux, extlinux, guestfs-tools (guestfish), qemu-img

Postup

- 1 Spustíme `podman build` a poté exportujeme `.tar` (`podman export`),
- 2 vytvoříme soubor s diskovým obrazem (`fallocate`),
- 3 poté na něm oddíly (`sfdisk`, `mkfs.ext4`, `partx`),
- 4 extrahujeme souborový systém a nainstalujeme `extlinux` (`guestfish`)
+ boot sektor (`dd :-`),

a to vše, aniž bychom potřebovali práva roota.

Bootovatelný Debian build – 3. Problémy

Co zbývá dořešit:

- Přestal fungovat `virt-v2v` pro zavedení výsledného OVA do `libvirtu`.
 - Nedokáže zjistit, co je to za distribuci :-).
- Zatím neumím UEFI.
 - Řešení: Přidat systémový EFI oddíl a na něm `\EFI\Boot\BOOTX64.EFI`.

libvirt

Jak to funguje s libvirtem?

- Stavíme na QEMU, KVM, user-mode networking (passst).
- Základní diskový obraz je formátu QCOW2, postavený postupem dříve, převedený přes qemu-img z RAW do QCOW2.
- Použití backing images jako snapshotů.

Snapshoty

- V QCOW2 dělané pomocí tzv. **backing images**.
- Vytvořený obraz je rozdílový.
- Lze také zvětšit obraz (výše 64 GB).

```
qemu-img create -b deb13-test.img -B raw -f qcow2 deb13-test.v1.  
qcow2 64G
```

Další čtení:

https://www.libvirt.org/kbase/backing_chains.html

Funguje i ARM64

- Funkční virtualizace na Raspberry Pi 5 (8GB RAM).

- <https://cloud.debian.org/images/cloud/trixie/latest/debian-13-generic-arm64.qcow2>

```
1 virt-install --name "$VM_ID" --os-variant debian13 --disk "$VM_IMAGE" --import --vcpus=2 --ram=2048 --network network=builders --graphics none --noautoconsole --boot=uefi
```

- Funkční build systému pomocí kombinace libvirt + rpi-gen

Dotazy, podněty, připomínky?

paulos@paulos.cz

pavel.valach@cesnet.cz

nebo později v anketě :-)