sVirt / KB – mai 2014

OBJECTIF DE SVIRT :

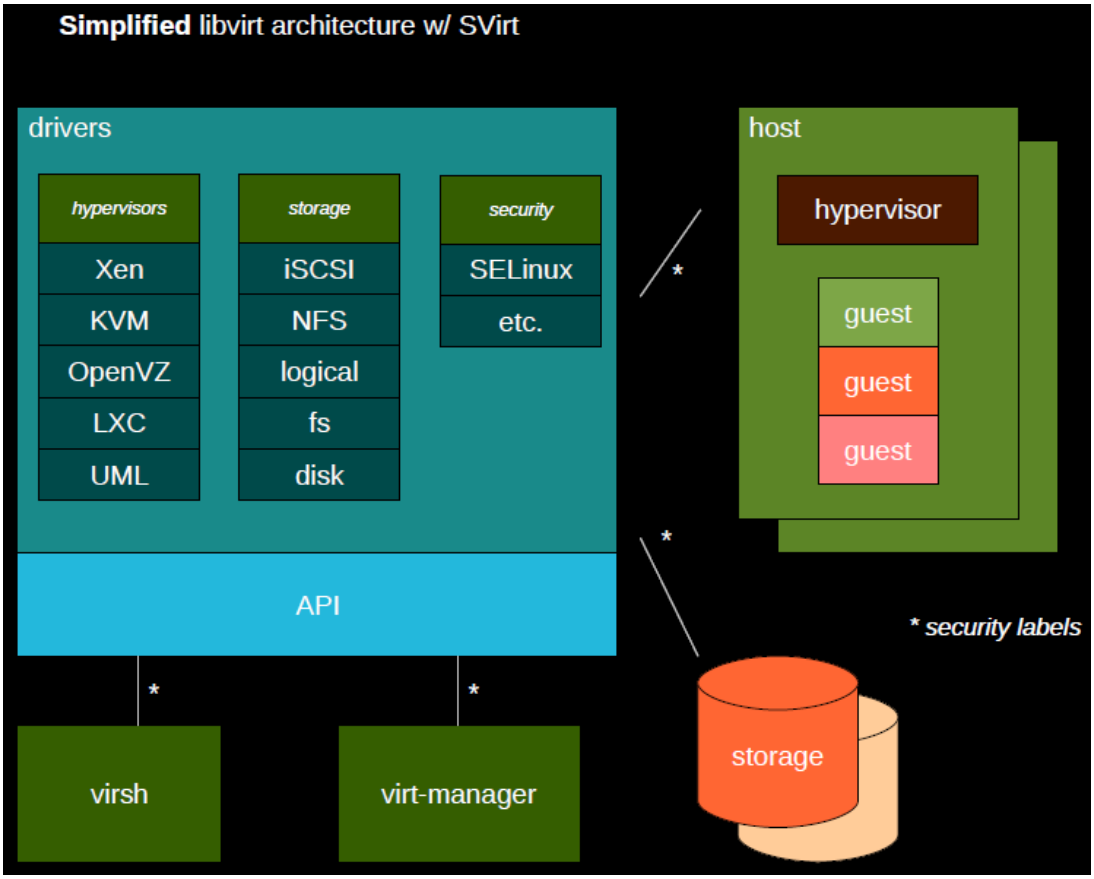
sVirt est en mesure d'appliquer des **labels** de sécurité **MCS** distincts à chaque VM.

La politique MAC veillera à empêcher toute tentative d'une VM_A à accéder à une VM_B si les labels de sécurité diffèrent.

sVirt entre en action dès que nous configurons et gérons les VM via **libvirt**.

Il est donc intégré dans libvirt en tant que drivers dans la catégorie « security », voir **figure** ci-dessous.

Une simple option lors de la création de la VM permettra de demander à ce que la VM soit « isolée », la chaîne d'outils s'occupera de faire l'étiquetage et la configuration des politiques en arrière-plan.



SITUATION ACTUELLE AVEC SELINUX ACTIVE SANS SVIRT

SELinux est déjà en mesure de fournir une protection MAC général a la virtualisation dans Linux, tels que la protection de l'intégrité et confidentialité des images disque et offrant une isolation solide du processus hyperviseur du reste du système.

GL – 17 avril 2013 : Remplacer les 3 lignes ci-dessus par une **analyse fine** aux niveaux lignes de commandes et attaques ?

Il n'y a aucun support explicite pour la virtualisation Linux dans SELinux, et toutes les VM sont actuellement dirigée dans le même contexte de sécurité. Ainsi, il n'y a pas d'isolation MAC appliquée entre VM.

SITUATION ACTUELLE AVEC SELINUX ACTIVE AVEC SVIRT :

Quand on active SELinux, le service sVirt, si présent, démarre automatiquement et créera dynamiquement et gérera les labels des VM.

Le service sVirt est inclus dans libvirt.

Le **labeling dynamique** est recommandé dans la plupart des cas. Mais nous avons la possibilité de désactiver le labeling dynamique et de créer nos propres **labels statiques**. Dans ce cas, c'est à nous de vérifier que les labels statiques sont uniques pour chaque VM.

Concrètement c'est le **contrôle d'accès Multi-Level Security (MLS)** qui est utilisé pour différencier le contexte de sécurité de chaque VM active.

Démonstration, affichage du domaine du processus d'une VM :

Activer SELinux. /etc/SELinux/config enforcing

Redémarrer ordinateur

Terminal : `getenforce`

Constater service libvirt actif :

Terminal root : `service --status-all`

Si pas de VM existante, créer une VM avec l'image UbuntuServer.raw du bureau :

```
virt-install --import --connect qemu:///system --name VM1 --ram 1024 --vcpus 1 --file /home/labotd/Desktop/UbuntuServer.raw
```

Si une VM est existante mais éteinte alors démarrer la VM :

```
virsh start NOM_VM
```

Terminal root : Récupérer le label défini dynamiquement à VM1 à l'aide de la commande ps qui affiche tous les processus qemu-kvm démarrés actuellement :

```
ps -C qemu-kvm -o label,command
```

```
LABEL                                        COMMAND
system_u:system_r:svirt_t:s0:c649,c851       /usr/bin/qemu-kvm -S -M pc-0.14 -enable-kvm -m 1024 -smp 2,sockets=2,cores=1,threads=1 -name VM1 -uuid 397b09bf-8bbb-8da9-f12f-2b8884649881 -nodefconfig -nodefaults -ch
```

Terminal root : Vérifier le label de l'image disk :

```
ls -Z /home/labotd/Desktop/UbuntuServer.raw
```

```
-rw-r--r--. qemu qemu system_u:object_r:svirt_image_t:s0:c649,c851 /home/labotd/Desktop/UbuntuServer.raw
```

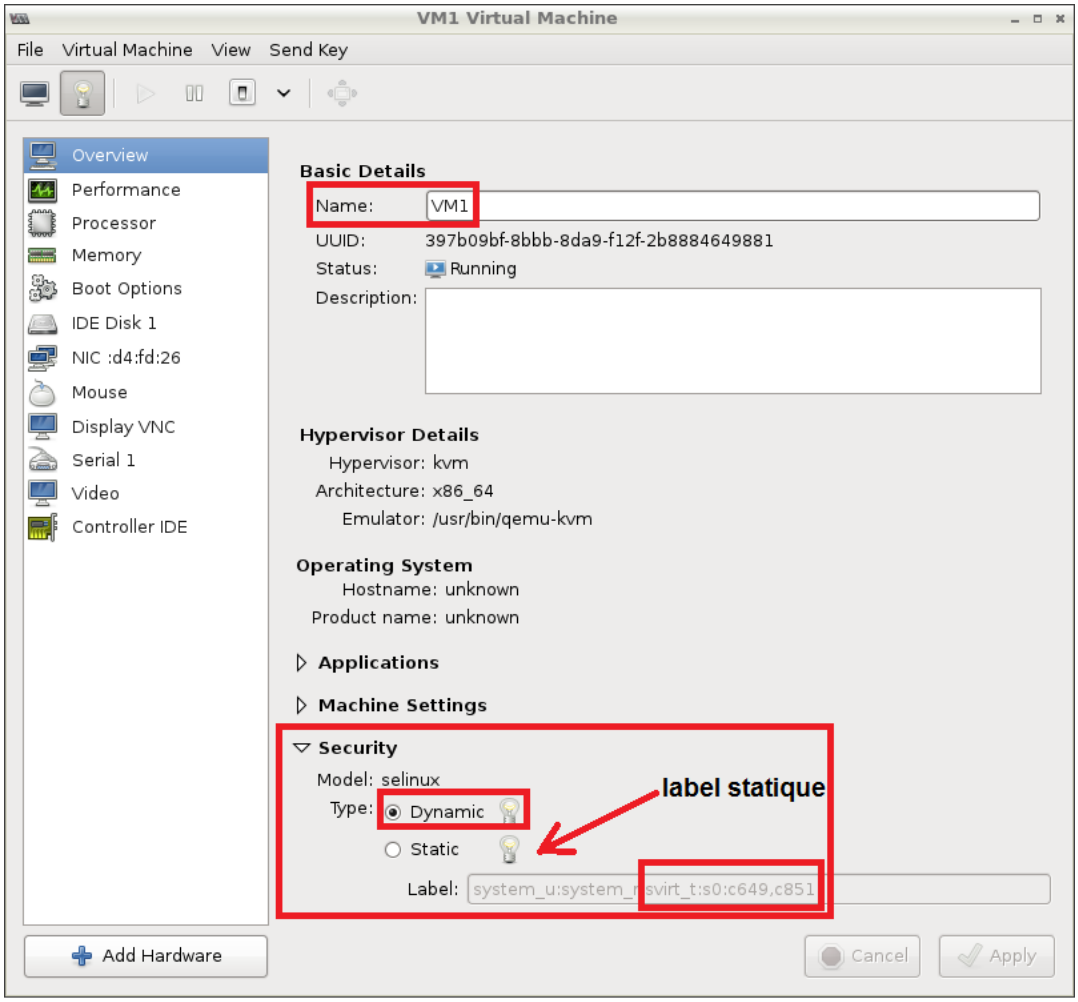
Terminal root : Vérifier dans le fichier xml qui décrit la configuration de la VM :

```
virsh dumpxml VM1 | grep label
```

```
<seclabel type='dynamic' model='selinux' relabel='yes'>
<label>system_u:system_r:svirt_t:s0:c649,c851</label>
<imagelabel>system_u:object_r:svirt_image_t:s0:c649,c851</imagelabel>
</seclabel>
```

Type/Description	SELinux Context
Virtualized guest processes. MCS1 is a random MCS field. Approximately 500,000 labels are supported.	system_u:system_r:svirt_t:MCS1
Virtualized guest images. Only *svirt_t* processes with the same MCS fields can read/write these images.	system_u:object_r:svirt_image_t:MCS1
Virtualized guest shared read/write content. All *svirt_t* processes can write to the svirt_image_t:s0 files.	system_u:object_r:svirt_image_t:s0
Virtualized guest shared read only content. All svirt_t processes can read these files/devices.	system_u:object_r:svirt_content_t:s0
Virtualized guest images. Default label for when an image exits. No *svirt_t* virtual processes can read files/devices with this label.	system_u:object_r:virt_content_t:s0

Configurer label dans virt-manager :



REFERENCE :

sVirt: Hardening Linux Virtualization with Mandatory Access Control

Présentation sur sVirt faite en 2009 par le créateur de sVirt (James Morris). James Morris est employé de Red Hat, collègue de Daniel Walsh :

http://namei.org/presentations/svirt-lca-2009.pdf

Cahier de charge de sVirt :

http://selinuxproject.org/page/Svirt_requirements_v1.0

Documentation RedHat qui présente la signification des labels

http://www.tdeig.ch/kvm/liens.pdf : Red Hat Enterprise Linux 6 - Virtualization Administration Guide

Site IBM avec information sur la virtualisation KVM et son fonctionnement :

http://www.tdeig.ch/kvm/liens.pdf : Virtualization for Linux on IBM x86 servers - KVM security