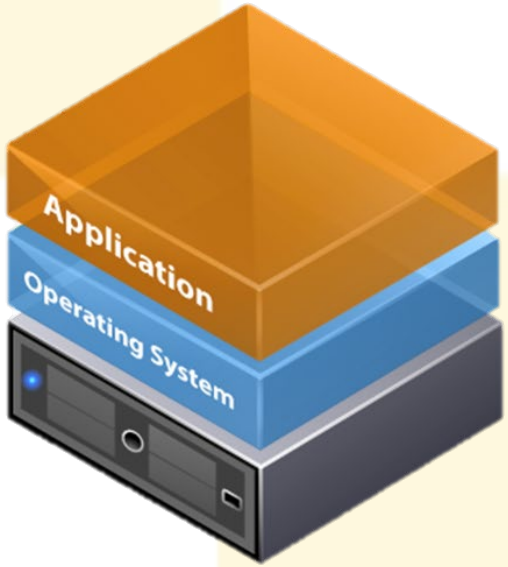
Контроль целостности файлов в образах виртуальных машин с применением Аккорд-KVM

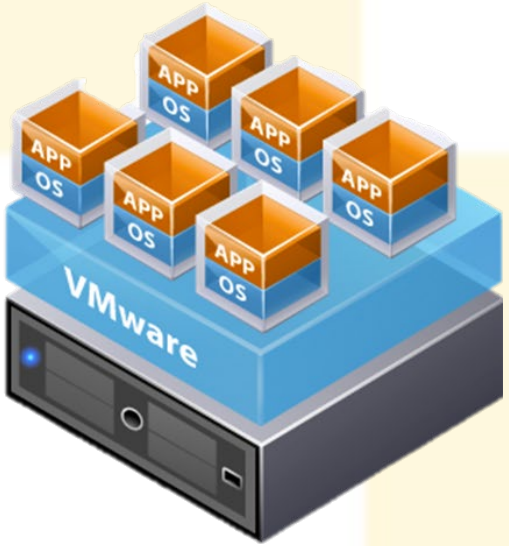
Татауров Степан Антонович
Каннер Татьяна Михайловна
okbsapr@okbsapr.ru

Виртуализация

Виртуализация — это технология, создающая на одном физическом сервере несколько логически изолированных вычислительных сред (виртуальных машин), каждая со своей собственной операционной системой и приложениями. Она абстрагирует аппаратные ресурсы от программного обеспечения, обеспечивая согласованное и предсказуемое окружение независимо от базового железа.



Традиционная архитектура



Виртуализованная архитектура

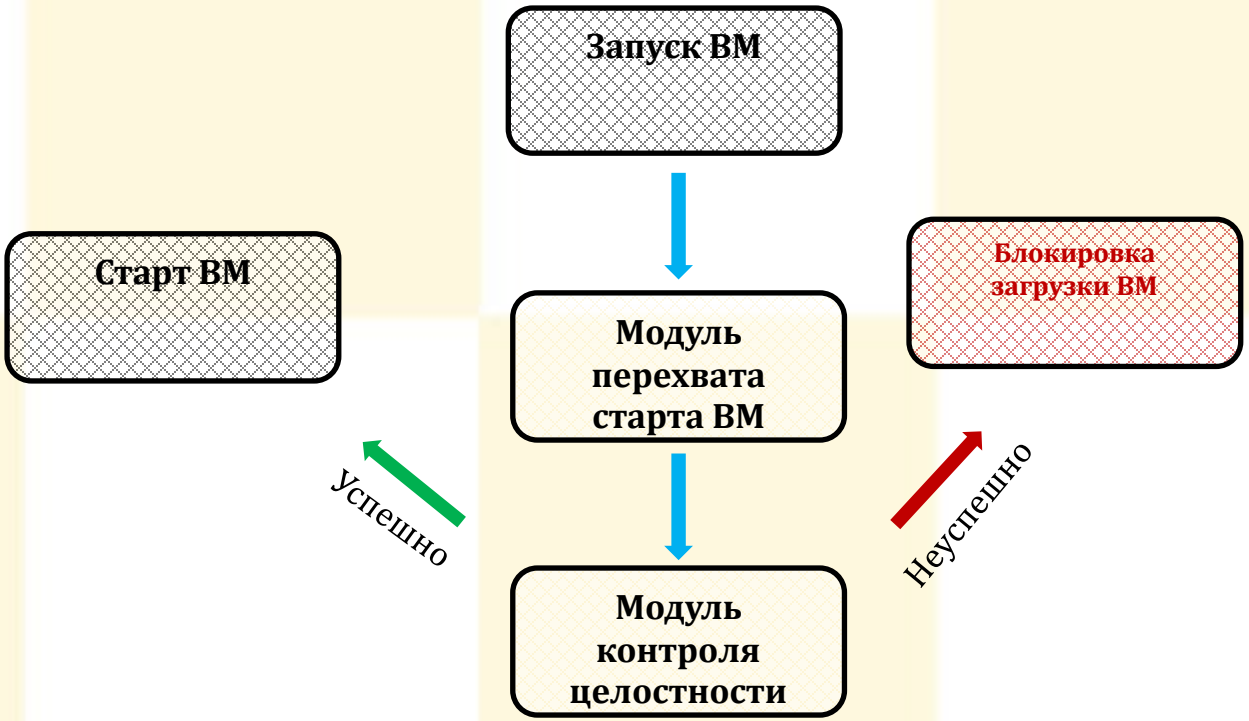
Типы гипервизоров

Гипервизоры бывают 1-го и 2-го типа. Гипервизор 1-го типа выполняет вычисления гостевой ОС напрямую на процессоре физической машины, а гипервизор 2-го типа работает как приложение, не взаимодействуя напрямую с физическим процессором.

Гипервизор 1 типа	Гипервизор 2 типа
KVM	Oracle VM VirtualBox
vmware vSphere	vmware Workstation

Принцип работы СПО «Аккорд-KVM»

Принцип работы СПО заключается в перехвате команды на старт виртуальной машины, после чего запускается проверка ВМ на целостность, на соответствие сохраненной конфигурации ВМ (количество ЦП, ОЗУ итд). Если все проверки проходят успешно, то отправляется команда на запуск ВМ. Если проверка завершается неуспешно, то загрузка ВМ блокируется



Файл-листы в СПО «Аккорд-KVM»

В СПО «Аккорд-KVM» контроль файлов внутри виртуальных дисков ВМ реализован путем создания списка файлов и последующем заполнении файл-листа на основе эталонной ВМ. В файл-листе содержатся абсолютные пути файлов и их контрольные суммы в виде хеша. При проверке модулем контроля целостности для каждого файла из сума, которая затем сравнивается файл-листа рассчитывается новая контрольная с эталонной. При их несовпадении старт ВМ блокируется.

Пример критических файлов

В Linux-подобных системах необходимо контролировать системные конфигурационное файлы: они являются основой учётных записей, сетевой конфигурации и системных настроек. Любые несанкционированные изменения этих файлов могут нарушить аутентификацию, вызвать сбои в сети или загрузке системы и предоставить злоумышленникам возможность повысить свои привилегии, поэтому их целостность важно проверять с помощью контрольных сумм.

Учетные данные, привилегии	Конфигурация сети	Системные конфигурации
/etc/passwd	/etc/hostname	/etc/fstab
/etc/shadow	/etc/resolv.conf	/etc/profile
/etc/group	/etc/nsswitch.conf	/etc/login.defs

File: **/etc/fstab**

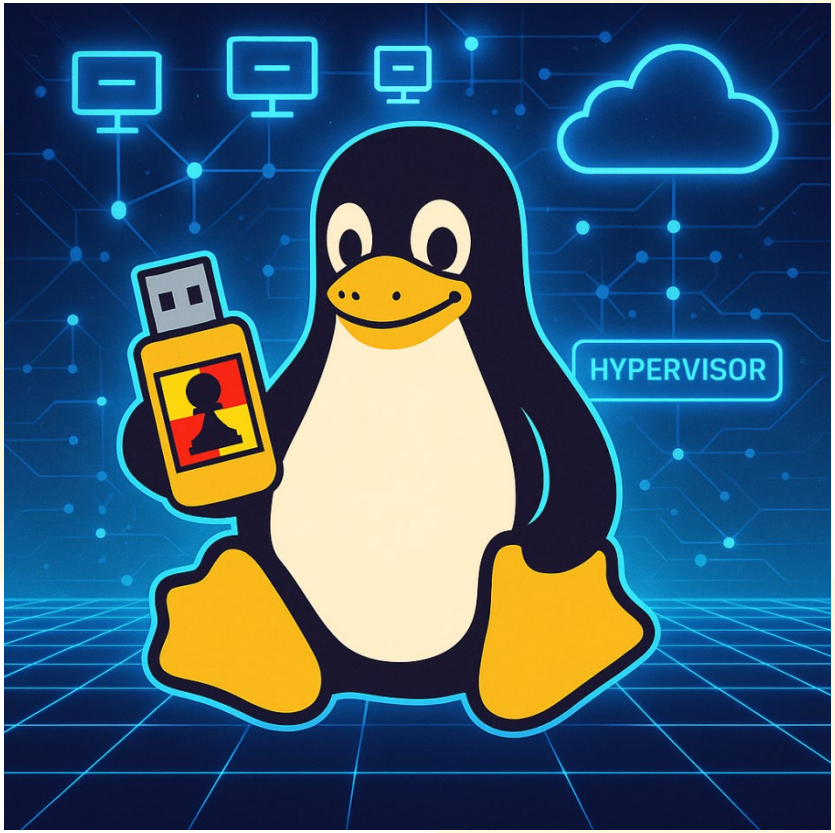
```
1  # Static information about the filesystems.
2  # See fstab(5) for details.
3
4  # <file system> <dir> <type> <options> <dump> <pass>
5  # /dev/sda2
6  UUID=5428f491-2e25-4504-b035-8faed473b3d6   /           ext4        rw,relatime 0 1
7
8  # /dev/sda1
9  UUID=99A3-3470          /boot       vfat        rw,relatime,fmask=0022,dmask=0022,codepage=4
   37,iocharset=ascii,shortname=mixed,utf8,errors=remount-ro   0 2
```

File: **/etc/resolv.conf**

```
1  # Generated by NetworkManager
2  search okbsapr.ru
3  nameserver 192.168.253.38
4  nameserver 192.168.253.40
```

Заключение

Использование виртуализации повышает гибкость ИТ-инфраструктуры, но и требует внимания с точки зрения обеспечения безопасности. Самое простое и эффективное решение это контроль целостности файлов и конфигурации ВМ. Под такую задачу идеально подойдет СПО «Аккорд-KVM» или его аналоги



Контроль целостности файлов в образах виртуальных машин с применением Аккорд-KVM

Татауров Степан Антонович
Каннер Татьяна Михайловна
okbsapr@okbsapr.ru