Аккорд-KVM

Защита систем виртуализации на базе KVM

ОКБ САПР
2022

Назначение и состав

«Аккорд-KVM» – это ПО для защиты инфраструктур виртуализации на базе KVM с библиотекой для управления гипервизором libvirt.

«Аккорд-KVM» контролирует включение виртуальных машин (ВМ) и обеспечивает выполнение контрольных процедур до их запуска.

Поставляется в виде rpm-файла.

Назначение и состав

«Аккорд-KVM» состоит из двух модулей:

- ✓ модуль перехвата старта виртуальных машин, он называется qemu;
- ✓ модуль контроля целостности виртуальных машин и их компонентов, он называется accordkvm.

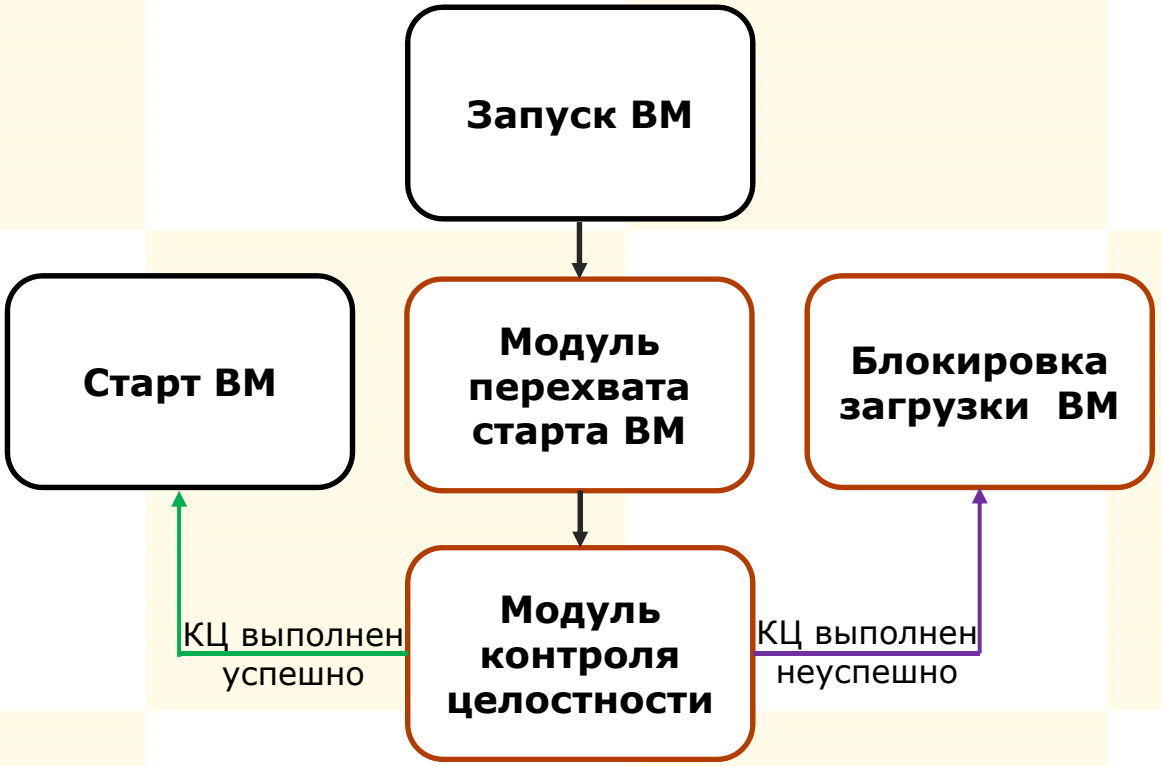
Эти модули устанавливаются в ОС каждого сервера виртуализации, при этом все экземпляры «Аккорд-KVM» могут использовать одну базу данных.

Защитные механизмы

«Аккорд-KVM»

- ✓ до запуска ВМ контролирует целостность конфигурации ВМ и целостность их программных компонентов (файлов общего, прикладного ПО и данных);
- ✓ управляет размещением и перемещением исполняемых ВМ между серверами виртуализации;
- ✓ регистрирует события безопасности в инфраструктуре виртуализации.

Принцип работы



ВМ – виртуальная машина;

КЦ – контроль целостности;

Линией темно-оранжевого цвета обозначена работа Аккорд-KVM;

Стрелка зеленого цвета обозначает, что контрольные процедуры Аккорд-KVM пройдены успешно;

Стрелка фиолетового цвета обозначает, что в ходе контроля целостности выявлены нарушения (при этом выполняется блокировка загрузки ВМ).

Выполнение требований регуляторов

«Аккорд-KVM» имеет сертификат ФСТЭК России.

Базовые меры Приказов 17-21 ФСТЭК России:
ИАФ: 1, 2, 3, 4, 5, 6;
УПД: 1, 2, 4, 5, 6, 9, 10, 11, 15, 17;
ОПС: 1;
ЗНИ: 2, 5, 8;
РСБ: 1, 2, 3, 4, 5, 7;
АНЗ: 1, 2, 3, 4, 5;
ОЦЛ: 1, 3, 6;
ЗСВ: 1, 2, 3, 6, 7;
ОДТ: 3, 4, 5;
ЗИС: 1, 5, 15, 21, 30;
ИНЦ: 2.

Выполнение требований регуляторов

Дополнительные (не включенные в базовый набор) меры Приказов 17-21 ФСТЭК России:

ИАФ: 7;
УПД: 12;
ОПС: 4;
ЗНИ: 6, 7;
РСБ: 8;
ОЦЛ: 2, 5, 8;
ЗСВ: 5;
ЗИС: 19, 29.

Выполнение требований регуляторов

Базовые меры 31 Приказа ФСТЭК России:

ИАФ: 1, 2, 3, 4, 5, 7;
УПД: 1, 2, 3, 4, 5, 6, 9, 10, 11;
ОПС: 1;
ЗНИ: 2, 5, 6, 7, 8;
АУД: 2, 4, 6, 7, 8, 9;
ОЦЛ: 1, 3, 4, 5;
ОДТ: 3, 4, 5;
ЗИС: 1, 13, 21, 33, 38, 39;
ИНЦ: 1, 2;
ОПО: 4;
ДНС: 4, 5

Выполнение требований регуляторов

Дополнительные (не включенные в базовый набор) меры 31 Приказа ФСТЭК России:

УПД: 12;

ОПС: 3;

ОЦЛ: 2;

ЗИС: 12, 37.

Спасибо за внимание!

Если у вас возникли вопросы, то **напишите нам**.

Наш сайт в интернете:
www.okbsapr.ru