Утвержден

РДЦП.10001-02-УД

ПРОГРАММНЫЙ КОМПЛЕКС «СРЕДСТВА ВИРТУАЛИЗАЦИИ «БРЕСТ»

Описание применения

РДЦП.10001-02 31 01

Листов 22

2018

Литера $О_1$

Инв.№ подл.	Подп. и дата	Взам. инв.№	Инв.№ дубл.	Подп. и дата

АННОТАЦИЯ

Настоящий документ является описанием применения программного комплекса «Средства виртуализации «Брест» (ПК СВ «Брест») РДЦП.10001-02 (далее по тексту — ПК).

В документе приведены назначение ПК, условия применения, описание задачи, а также приведено описание входных и выходных данных ПК.

СОДЕРЖАНИЕ

1. Назначение программы 4
1.1. Назначение 4
1.2. Область применения 4
1.3. Возможности 4
2. Условия применения 8
2.1. Требования к программным средствам 8
2.2. Требования к техническим средствам 8
2.3. Порядок эксплуатации 8
2.4. Порядок обновления 8
2.4.1. Очередное (плановое) обновление 8
2.4.2. Внеочередное (оперативное) обновление 9
2.4.3. Контроль целостности обновлений 10
3. Описание задачи 11
3.1. Сценарии использования 11
3.1.1. Локальная виртуализация 11
3.1.2. Серверная виртуализация 11
3.1.3. Облако ресурсов и виртуальных машин 11
3.2. Классы решаемых задач 12
3.2.1. Управление виртуальными машинами 12
3.2.2. Идентификация и аутентификация при доступе к серверу виртуализации libvirt 15
3.2.3. Идентификация и аутентификация при доступе к рабочему столу виртуальных машин 17
4. Входные и выходные данные 18
Перечень сокращений 21

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1. Назначение

ПК предназначен для создания виртуальной среды, обеспечивающей функционирование виртуальных машин и управление ими в операционной системе специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (далее по тексту — ОС СН). **??**

1.2. Область применения

Автоматизированные системы в защищенном исполнении, обрабатывающие информацию ограниченного доступа, в том числе содержащую сведения, составляющие государственную тайну, со степенью секретности до «совершенно секретно» включительно.

1.3. Возможности

Изделие функционирует под управлением ОС СН и совместно с ней предоставляет следующие возможности:

- создание виртуальных машин (ВМ), их образов и шаблонов с помощью графического и консольного интерфейсов с поддержкой 32 и 64-битных гостевых операционных систем (ОС);
- создание ВМ из настраиваемых шаблонов;
- управление конфигурацией ВМ с помощью графического и консольного интерфейсов;
- обеспечение возможности централизованного управления кластерами, серверной частью изделия на всех узлах кластера высокой доступности, хранилищами и виртуальными коммутаторами;
- обеспечение мониторинга работоспособности и использования ресурсов виртуальных машин и серверной частью изделия и генерации отчетов, в т.ч. за выбранный период с возможностью выдачи оповещения на интерфейс управления при превышении пороговых значений метрик использования ресурсов;
- поддержку виртуальных коммутаторов с технологией VLAN (Virtual Local Area Network);
- изменение без завершения функционирования ВМ количества выделенных им процессоров и размера оперативной памяти;
- подключение к ВМ устройств из состава аппаратных средств, на которых функционирует серверная часть изделия, включая устройства USB 3.0;
- подключение к ВМ по протоколу SPICE USB-устройств из состава аппаратных средств, на которых функционирует клиентская часть изделия;
- добавление виртуальных дисков в гостевую операционную систему и увеличение

их размеров без остановки ВМ;

- поддержку открытого стандарта для хранения и распространения виртуальных машин Open Virtualization Format (OVF);
- обеспечение возможности клонирования ВМ;
- управление приоритетом дисковых операций ввода-вывода для ВМ;
- выполнение миграции работающих ВМ между узлами кластера без прерывания работы в автоматическом и ручном режимах;
- обеспечение возможности переноса ВМ между виртуальными сетевыми устройствами без прерывания трафика;
- обеспечение возможности ограничения сетевого и дискового ввода-вывода виртуальных машин на основе их групповых или индивидуальных настроек;
- автоматическое распределение сервером виртуализации ресурсов между работающими ВМ;
- обеспечение возможности централизованного хранения конфигурационной информации о ВМ и среде виртуализации;
- обеспечение возможности создания копий трафика виртуальных машин внутри виртуального сетевого коммутатора на его сетевой порт;
- обеспечение возможности создания резервных копий виртуальных машин, а также последующего восстановления.

При этом средствами ОС СН обеспечиваются следующие возможности по созданию и защите среды виртуализации:

- эмуляция аппаратного обеспечения с использованием аппаратных возможностей архитектуры x86-64 по виртуализации процессоров на основе модуля KVM (Kernel-based Virtual Machine) из состава ОС СН;
- поддержка в ВМ до 240 виртуальных процессоров (физических ядер);
- поддержка в ВМ до 4000 GB оперативной памяти;
- поддержка IPMI 2.0;
- поддержка расширения количества управляемых ВМ до 10 000 (при наличии соответсвующей инфраструктуры серверов);
- возможность группового создания 500 и более ВМ из шаблонов;
- идентификация и аутентификация субъектов доступа (пользователей и администраторов) до предоставления доступа к функциям виртуализации и управления изделия, в том числе в режиме взаимодействия со средствами создания единого пространства пользователей (ALD) из состава ОС СН;
- функционирование в условиях мандатного и дискреционного управления доступом ОС СН при межпроцессном и сетевом взаимодействии, включая взаимодействие

между ВМ по протоколам стека IPv4 в условиях мандатного управления доступом и доступ субъектов к файлам-образам и экземплярам функционирующих ВМ;

- запуск ВМ в виде отдельного процесса ОС СН, функционирующего от имени учетной записи субъекта доступа (пользователя) с унаследованием его мандатных атрибутов;

- обеспечение создания тонких (терминальных) клиентов с использованием технологии VDI (Virtual Desktop Infrastructure) с предоставлением удаленного доступа к ВМ по протоколам VNC и SPICE, в т.ч. в условиях установленных в ОС СН правил дискреционного и мандатного управления доступом;

- поддержка серверной частью изделия следующих механизмов оптимизации оперативной памяти: дедупликация страниц, динамическое распределение, выгрузка в файл подкачки;

- создание динамически расширяющегося виртуального дискового пространства ВМ с обеспечением возможности выделения соответствующих аппаратных средств (физических дисков, блоков физических дисков) по мере заполнения виртуального дискового пространства ВМ;

- обеспечение возможности создания кластеров высокой доступности, обеспечивающих отказоустойчивое функционирование ВМ посредством репликации файлов ВМ между системами хранения и миграции ВМ между узлами кластера;

- обеспечение возможности ручной балансировки нагрузки на вычислительные ресурсы аппаратных средств за счет перераспределения ВМ между узлами кластера;

- обеспечение возможности миграции функционирующих ВМ между устройствами хранения без прерывания их работы;

- обеспечение маршрутизации сетевых пакетов ВМ;

- обеспечение возможности защиты файлов-образов ВМ от модификации в процессе функционирования ВМ;

- обеспечение возможности регистрации событий с использованием средств централизованного протоколирования из состава ОС СН;

- поддержка средств антивирусной защиты, реализованных на основе технологии обработки данных, собираемых устанавливаемыми в гостевые операционные системы агентами средств антивирусной защиты, в специально выделенной для этих целей ВМ;

- обеспечение возможности контроля сетевого трафика, передаваемого между ВМ с целью обнаружения (предупреждения) компьютерных атак;

- обеспечение возможности централизованного обновления изделия с использованием штатных средств ОС СН.

Защита информации в ПК обеспечивается средствами защиты информации ОС СН.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Требования к программным средствам

ПК функционирует только под управлением ОС СН версии не ниже 1.6.

2.2. Требования к техническим средствам

Серверное и клиентское программное обеспечение ПК должны функционировать на оборудовании, отвечающему требованиям к аппаратному обеспечению под управлением ОС СН.

Для функционирования сервера виртуализации ПК необходима следующая минимальная конфигурация оборудования:

- аппаратная платформа — процессор с архитектурой x86-64 с аппаратной поддержкой виртуализации (Intel VT, AMD-V);
- оперативная память — не менее 8 ГБ;
- объем свободного дискового пространства — не менее 30 ГБ;
- сетевая плата — не менее 100 Мбит/с;
- источник бесперебойного питания;
- устройство чтения/записи CD/DVD-дисков.

2.3. Порядок эксплуатации

Установка, настройка и эксплуатация ПК осуществляется в соответствии с эксплуатационной документацией согласно РДЦП.10001-02 20 01 «Программный комплекс «Средства виртуализации «Брест». Ведомость эксплуатационных документов».

Дополнительная информация о порядке эксплуатации, а также варианты реализации отдельных решений приведены на официальном сайте `wiki.astralinux.ru`.

2.4. Порядок обновления

Для ПК предусмотрен выпуск очередных (плановых) обновлений (новых версий) и выпуск внеочередных (оперативных) обновлений.

2.4.1. Очередное (плановое) обновление

Очередное (плановое) обновление ПК представляет собой новую версию ПК и решает следующий комплекс задач:

- реализация новых функциональных возможностей ПК;
- устранение уязвимостей;
- повышение удобства использования и управления средствами виртуализации.

Лицензиаты (потребители) оповещаются о возможности и порядке получения очередного обновления ПК как с использованием контактной информации, указанной в заклю-

ченных ранее лицензионных договорах (дополнениях к лицензионным договорам), так и путем размещения соответствующей информации на сайте разработчика astralinux.ru.

Получение очередного обновления ПК осуществляется установленным порядком при заключении соответствующего лицензионного договора (дополнения к имеющемуся лицензионному договору).

Контроль целостности потребителями очередного обновления ПК (входной контроль) осуществляется посредством подсчета контрольных сумм компакт-дисков. Значения контрольных сумм и порядок их вычисления определены в документе РДЦП.10001-02 30 01 «Программный комплекс «Средства виртуализации «Брест». Формуляр».

Дополнительный контроль целостности файлов, входящих в состав очередного обновления ПК, осуществляется:

- регламентно — средствами контроля целостности путем вычисления и сравнения контрольных сумм файлов ПК с эталонными значениями, указанными в файле gostsums.txt, размещенном на установочном диске ПК, в соответствии с описанием, приведенном в документе РУСБ.10015-01 97 01-1 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1»;
- автоматически — средствами ограничения программной среды в соответствии с описанием, приведенным в документе РУСБ.10015-01 97 01-1.

Доведение очередного обновления ПК до автоматизированных систем в защищенном исполнении Министерства обороны Российской Федерации осуществляется через Главный вычислительный центр Министерства обороны Российской Федерации.

2.4.2. Внеочередное (оперативное) обновление

При получении сведений о наличии в компоненте ПК уязвимости разработчик ПК выпускает внеочередное обновление ПК.

Внеочередное обновление ПК может быть доступно в виде:

1) отдельных инструкций, содержащих сведения об обязательных к проведению при эксплуатации ПК организационно-технических мероприятиях;

2) отдельных файлов программ, инструкций по их установке и настройке, а также информации, содержащей сведения о контрольных суммах всех файлов внеочередного обновления ПК;

3) пакетов программ, инструкций по их установке и настройке, а также информации, содержащей сведения о контрольных суммах всех файлов внеочередного обновления ПК;

4) методических указаний по настройке и особенностям эксплуатации ПК с установленным внеочередным обновлением ПК.

Лицензиаты (потребители) оповещаются о возможности и порядке получения вне-

очередного обновления ПК как с использованием контактной информации, указанной в заключенных ранее лицензионных договорах (дополнениях к лицензионным договорам), так и путем размещения соответствующей информации на сайте разработчика astralinux.ru.

Контроль целостности внеочередных обновлений ПК осуществляется с помощью контрольных сумм, рассчитанных с использованием программ подсчета контрольных сумм gostsum (для файлов) и gostsum_from_deb (для deb-пакетов) из состава ОС СН в соответствии с документом РУСБ.10015-01 97 01-1.

Дополнительный контроль целостности файлов, входящих в состав внеочередного обновления ПК, осуществляется:

- регламентно — средствами контроля целостности путем вычисления и сравнения контрольных сумм файлов ПК с эталонными значениями, указанными в файле gostsums.txt, входящем в состав внеочередного обновления ПК, в соответствии с описанием, приведенном в документе РУСБ.10015-01 97 01-1;
- автоматически — средствами ограничения программной среды в соответствии с описанием, приведенным в документе РУСБ.10015-01 97 01-1.

Источником внеочередного обновления ПК для информационных (автоматизированных) систем, находящихся в компетенции ФСТЭК России, является соответствующий раздел на официальном сайте разработчика ПК (astralinux.ru/update).

Доведение внеочередного обновления ПК до автоматизированных систем в защищенном исполнении Министерства обороны Российской Федерации осуществляется через Главный вычислительный центр Министерства обороны Российской Федерации.

2.4.3. Контроль целостности обновлений

Для обеспечения контроля целостности объектов ПК в состав дистрибутива входит файл gostsums.txt со списком контрольных сумм по ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит для всех файлов, входящих в пакеты программ дистрибутива. Используя утилиту integrity-check из состава ПК можно провести вычисление контрольных сумм файлов системы и проверку соответствия полученных контрольных сумм файлов системы эталонным контрольным суммам.

Для выполнения контроля целостности необходимо:

1) смонтировать установочный диск ПК и перейти в каталог монтирования, например:

```
mount /dev/cdrom /mnt
cd /mnt
```

2) выполнить команду:

```
sh ./integrity-check ./gostsums.txt
```

3. ОПИСАНИЕ ЗАДАЧИ

Основная задача, решаемая ПК в процессе своего функционирования, — создание и управление виртуальными машинами в защищенной среде виртуализации ОС СН.

3.1. Сценарии использования

Использование ПК основывается на трех сценариях:

- локальная виртуализация (см. 3.1.1);
- серверная виртуализация (см. 3.1.2);
- облако ресурсов и виртуальных машин (см. 3.1.3).

3.1.1. Локальная виртуализация

Локальная виртуализация подразумевает создание и использование на локальном компьютере нескольких виртуальных машин для одного или нескольких пользователей в однопользовательском режиме (посменная работа). В качестве инструментов работы с ВМ можно применять как графический интерфейс virt-manager, так и инструменты командной строки `virsh`, `virt-install`.

Данный сценарий использования ПК эффективен в случае применения одной или нескольких ВМ с разделением физических устройств компьютера между виртуальными и физическими средами или для организации изолированных сред (в основном, виртуализация приложений), которые могут быть скомпрометированы без последствий для ОС узла и ОС соседних виртуальных машин.

3.1.2. Серверная виртуализация

В отличие от локальной, серверная виртуализация преследует цель централизовано предоставить пользователям различное программное обеспечение как сервис. В этом случае администратор имеет единый инструмент управления пулом физических серверов и ВМ на них. Virt-manager позволяет подключать удаленные физические серверы по протоколам TCP (SASL+Kerberos), SSL/TLS и SSH. При этом администратор получает возможность производить миграцию ВМ между серверами, централизованно создавать и управлять снимками ВМ и др.

Данный сценарий эффективен при необходимости содержать большое число ВМ и управлять несколькими физическими серверами. При этом администратор может задействовать механизмы обеспечения отказоустойчивости, балансировки нагрузки (масштабируемость), высокой доступности.

3.1.3. Облако ресурсов и виртуальных машин

С помощью пакета OpenNebula, входящего в состав ПК, могут быть развернуты защищенные частные облака или гибридные облака, частично размещенные в Интернете

(за пределами доверенной зоны). Данная система объединяет вычислительные ресурсы и средства хранения данных. Данный сценарий позволяет создавать и управлять большим числом виртуальных машин вне зависимости от места их физического размещения. При этом применяются все преимущества облачного решения: масштабируемость, высокая доступность, безопасность. OpenNebula позволяет осуществлять управление виртуальными машинами, работающими в режиме дискретного и мандатного управления доступом с учетом требований по контролю целостности, через единый web-интерфейс.

3.2. Классы решаемых задач

Для решения основной задачи функционирования ПК она делится на следующие классы задач:

- управление виртуальными машинами (3.2.1);
- идентификация и аутентификация при доступе к серверу виртуализации libvirt (3.2.2);
- идентификация и аутентификация при доступе к рабочему столу виртуальных машин (3.2.3);
- дискреционное управление доступом к виртуальным машинам;
- мандатное управление доступом к виртуальным машинам;
- функционирование виртуальной машины в режиме запрета модификации ее файлов-образов.

ВНИМАНИЕ! Дискреционное и мандатное управление доступом, а также управление режимом запрета модификации файлов-образов виртуальных машин осуществляются СЗИ из состава ОС СН.

3.2.1. Управление виртуальными машинами

Управление виртуальными машинами в ПК осуществляется с помощью сервера виртуализации на основе libvirt из состава ОС СН, который предоставляет средства создания и учета виртуальных машин, настройки их конфигурации и непосредственно запуска. В эти задачи входит управление файлами-образов дисковых носителей виртуальных машин, виртуальными сетевыми адаптерами и сетями и формирование контекста функционирования виртуальной машины в виде процесса ОС СН.

Для хранения конфигурации и параметров виртуальных машин используются xml файлы описания конфигурации виртуальных машин. В файле конфигурации задается состав аппаратных средств, которые необходимо эмулировать для данной виртуальной машины, а также параметры использования ресурсов сервера виртуализации (процессора, оперативной памяти и других физических устройств).

При создании виртуальной машины задаются конфигурационные параметры и созда-

ется файл-образ загрузочного диска виртуальной машины. Формат файла-образа зависит от выбранного средства эмуляции аппаратного обеспечения. В ПК используются средства эмуляции аппаратного обеспечения на основе QEMU из состава ОС СН, которые поддерживают следующие форматы образов: `image` (raw-формат, является фактически представлением физического диска) и формат `qcow2` (родной формат QEMU, поддерживающий возможности сжатия, использования снимков и другие дополнительные возможности). Кроме того, существует возможность конвертирования форматов образов других средств эмуляции аппаратного обеспечения (например, VirtualBox).

При запуске виртуальной машины сервер виртуализации libvirt подготавливает необходимую для функционирования виртуальной машины инфраструктуру и формирует соответствующий набор параметров запуска средства эмуляции аппаратного обеспечения QEMU из состава ОС СН. После подготовительных действий производится порождения процесса ОС СН, в рамках которого будет функционировать виртуальная машина. Каждая запускаемая виртуальная машина функционирует от имени учетной записи запустившего ее пользователя и с его мандатными атрибутами безопасности.

Для обеспечения безопасности функционирования виртуальных машин сервер виртуализации libvirt использует концепцию драйверов безопасности sVirt . Данная концепция представляет собой специальный программный интерфейс для создания модулей безопасности, используемых для настройки окружения и инфраструктуры запуска и функционирования виртуальный машин в условиях их изоляции и мандатного управления доступом.

Выполнение требований по защите информации при функционировании виртуальных машин достигается совместным использованием программных компонентов ОС СН: sVirt, модуля дискреционного управления доступом `dac` и специально разработанного модуля мандатного управления доступом `parsec`, взаимодействующего с подсистемой безопасности ОС СН.

На рис. 1 приведен снимок вкладки «Безопасность» графической утилиты управления виртуальными машинами virt-manager.

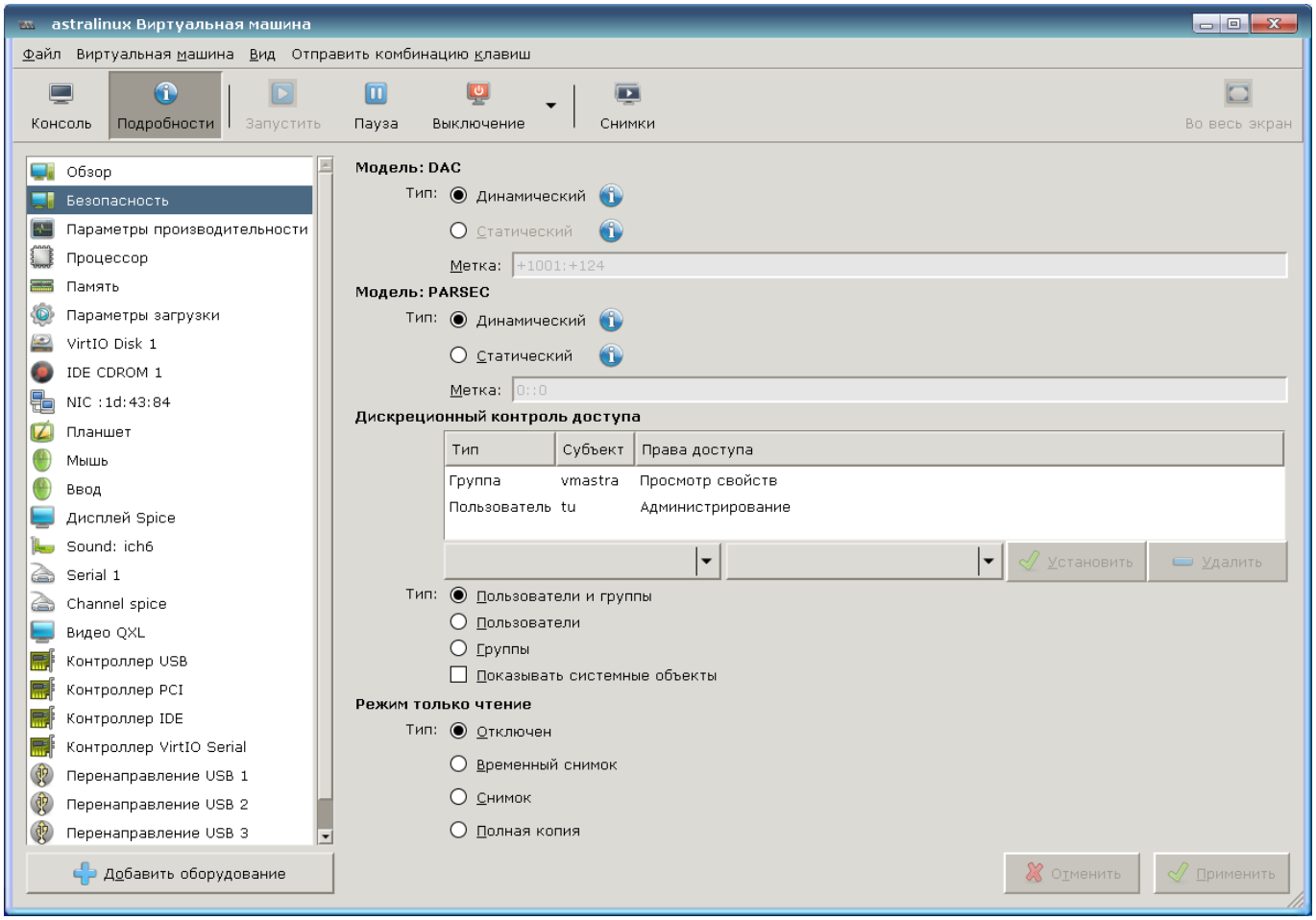

Рис. 1

Контекст безопасности виртуальной машины включает в себя метки безопасности используемых модулей sVirt, например:

- модуль поддержки дискреционного управления доступом `dac` использует метку безопасности, состоящую из уникального идентификатора владельца процесса виртуальной машины и уникального идентификатора группы;
- модуль поддержки мандатного управления доступом `parsec` использует мандатную метку подсистемы безопасности ОС СН.

Метки безопасности могут быть динамическими и статическими:

- динамическая метка безопасности генерируется динамически в момент запуска виртуальной машины на основе атрибутов безопасности запускающего пользователя: его уникального идентификатора и мандатного уровня доступа;
- статическая метка безопасности задается администратором в конфигурации виртуальной машины определяет контекст безопасности ее запуска.

Поддержка дискреционного и мандатного управление доступом к виртуальным машинам в сервере виртуализации реализуется средствами ОС СН с помощью драйвера доступа `parsec`, специально разработанного с использованием прикладного программного интерфейса драйверов доступа libvirt.

Поддержка функционирования виртуальной машины в режиме запрета модификации ее файлов-образов осуществляется специальными способами запуска виртуальной машины, реализованными в ОС СН, при которых основной файл-образ защищается от записи. В зависимости от выбранного режима используется создание физической копии или различные варианты создания снимков файл-образов с последующим их удалением после завершения работы виртуальной машины.

Рассматривая вопросы идентификации и аутентификации при доступе к виртуальным машинам следует различать доступ к серверу виртуализации libvirt для управления виртуальными машинами и доступ пользователя непосредственно к рабочему столу виртуальной машины.

3.2.2. Идентификация и аутентификация при доступе к серверу виртуализации libvirt

На рис. 2 приведено диалоговое окно задания параметров подключения к серверу виртуализации libvirt с использованием графической утилиты управления виртуальными машинами virt-manager.

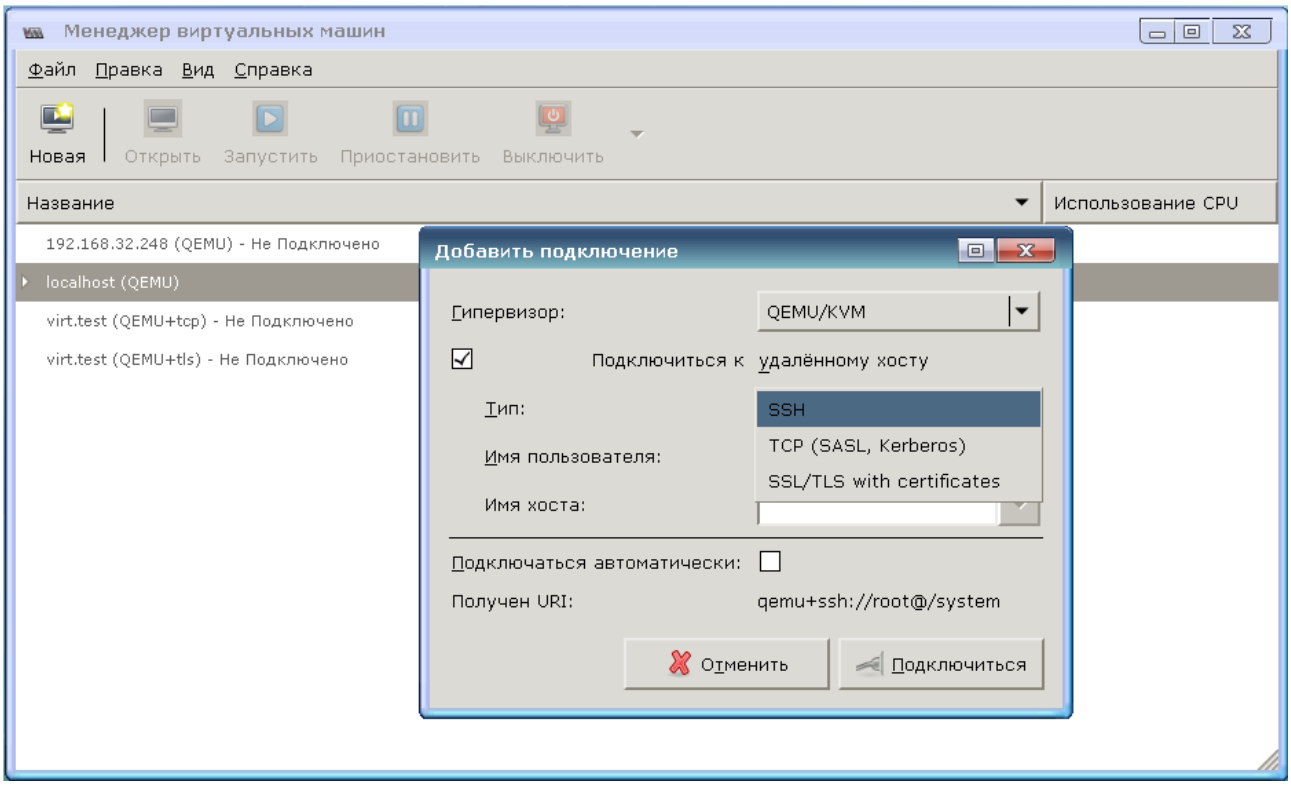

Рис. 2

Сервер виртуализации может использовать для идентификации и аутентификации клиентов следующие механизмы:

- локальная peer-cred аутентификация;
- удаленная SSH аутентификация (строка соединения `qemu+ssh://...`);

- удаленная SASL аутентификация в том числе с поддержкой Kerberos (строка соединения `qemu+tcp://...`);

- удаленная TLS аутентификация с использованием сертификатов (строка соединения `qemu+tls://...`).

Параметры аутентификации задаются в конфигурационном файле `/etc/libvirt/libvirtd.conf`. В конфигурационном файле отдельно задаются параметры для различных способов аутентификации: параметры локальных UNIX сокетов (секция «UNIX socket access control»), разрешение приема сетевых соединений (параметры `listen_tls` и `listen_tcp`) и порты для tcp и tls (параметры `tls_port` и `tcp_port`), расположение необходимых файлов при использовании сертификатов x509 (секция «TSL x509 certificate configuration») и варианты авторизации (параметры `auth_unix_ro`, `auth_unix_rw`, `auth_tcp`, `auth_tls`).

По умолчанию используется следующее расположение файлов сертификатов на сервере для аутентификации к серверу виртуализации libvirt:

- `/etc/pki/CA/cacert.pem` — корневой сертификат;

- `/etc/pki/CA/crl.pem` — файл отозванных сертификатов;

- `/etc/pki/libvirt/servercert.pem` — сертификат открытого ключа сервера виртуализации libvirt;

- `/etc/pki/libvirt/private/serverkey.pem` — закрытый ключ сервера виртуализации libvirt.

Примечание. Файлы ключей сервера виртуализации libvirt должны быть доступны на чтение группе `libvirt-qemu`.

По умолчанию используется следующее расположение файлов сертификатов на клиенте для аутентификации к серверу виртуализации libvirt (в домашнем каталоге пользователя ~):

- `/etc/pki/CA/cacert.pem` — корневой сертификат;

- `~/.pki/libvirt/clientcert.pem` — сертификат открытого ключа клиента;

- `~/.pki/libvirt/clientkey.pem` — закрытый ключ клиента.

В случае SASL аутентификации используется конфигурационный файл `/etc/sasl2/libvirt.conf`, в котором задаются параметры аутентификации SASL (например, применяемые механизмы). Имя сервиса сервера виртуализации libvirt при использовании SASL аутентификации регистрируется как `libvirt/<имя сервера>@<домен>`.

ВНИМАНИЕ! При указании механизма SASL `gssapi` следует в конфигурационном файле `/etc/default/libvirtd` указать с помощью соответствующей переменной окружения расположение файла ключей Kerberos сервера виртуализации, например:

```
export KRB5_KTNAME=/etc/libvirt/libvirt.keytab.
```

Примечание. Настройка сервера виртуализации для работы в ЕПП ОС СН производится в соответствием с документом РДЦП.10015-01 95 01-1 «Операционная система специального назначения «Astra Linux Special Edition Руководство администратора. Часть 1».

3.2.3. Идентификация и аутентификация при доступе к рабочему столу виртуальных машин

Параметры аутентификации при доступе к рабочему столу виртуальной машины задаются в конфигурационном файле `/etc/libvirt/qemu.conf` раздельно для протоколов VNC и SPICE. В данном конфигурационном файле указываются необходимые параметры аутентификации и пути к конфигурационным файлам SASL, например `/etc/sasl2/qemu.conf`. Имя сервисов VNC и SPICE при использовании SASL аутентификации регистрируется как `vnc/<имя сервера>@<домен>` и `spice/<имя сервера>@<домен>`, соответственно.

Примечание. Настройка сервисов VNC и SPICE для работы в ЕПП ОС СН производится в соответствии с документом РДЦП.10015-01 95 01-1.

По умолчанию используется следующее расположение файлов сертификатов на сервере для аутентификации к виртуальной машине для по протоколу VNC:

- `/etc/pki/libvirt-vnc/ca-cert.pem` — корневой сертификат;
- `/etc/pki/libvirt-vnc/server-cert.pem` — сертификат открытого ключа сервера VNC QEMU;
- `/etc/pki/libvirt-vnc/server-key.pem` — закрытый ключ сервера VNC QEMU.

Примечание. Файлы ключей сервера VNC QEMU должны быть доступны на чтение группе `libvirt-qemu`.

По умолчанию используется следующее расположение файлов сертификатов на клиенте для аутентификации к серверу VNC QEMU (в домашнем каталоге пользователя ~):

- `/etc/pki/CA/cacert.pem` — корневой сертификат;
- `~/.pki/libvirt-vnc/clientcert.pem` — сертификат открытого ключа клиента;
- `~/.pki/libvirt-vnc/private/clientkey.pem` — закрытый ключ клиента.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входными данными ПК являются:

- сведения о программно-аппаратной конфигурации оборудования сервера виртуализации и возможностях средства эмуляции аппаратного обеспечения на основе QEMU. Данные сведения собираются службой сервера виртуализации в процессе своего функционирования путем вызова внешних команд ОС и средства эмуляции. Собранные данные используются в дальнейшем при создании и запуске виртуальных машин;
- конфигурационные файлы службы сервера виртуализации и средства эмуляции аппаратного обеспечения на основе QEMU. Данные файлы расположены в каталоге `/etc/libvirt`. Конфигурационные параметры, содержащиеся в данных файлах, отвечают за различные аспекты функционирования виртуальных машин: интерфейсы взаимодействия и права доступа к ним, способы и параметры аутентификации, политику управления безопасностью и изоляцией виртуальных машин, значения по умолчанию некоторых параметров конфигурации виртуальных машин, состав выводимой в журнал информации и т.п.;
- загрузочные ISO-образы установочных дисков или оптические диски с дистрибутивами гостевых ОС. Установочные диски используются в процессе создания виртуальных машин для работы гостевых ОС и в процессе их функционирования для дополнения и обновления состава программных средств, установленных в гостевые ОС;
- запросы субъектов доступа к службе сервера виртуализации для управления виртуальными машинами. Служба сервера виртуализации `libvirtd` предоставляет возможность удаленного управления сервером виртуализации по сети с использованием различных протоколов и способов аутентификации. Доступ к службе сервера виртуализации возможен как с помощью локальных Unix-сокетов, так и по сети с помощью консольных или графических инструментов управления виртуальными машинами. В качестве способа аутентификации при использовании ПК в условиях ЕПП применяется аутентификация Kerberos с помощью механизма SASL `gssapi`, в иных случаях возможно применение других механизмов SASL или SSL/TLS аутентификации, основанной на сертификатах. Взаимодействие пользователей с сервером виртуализации состоит из обязательного прохождения процедуры аутентификации и работы в условиях применения дискреционных и мандатных правил разграничения доступа;
- запросы серверу виртуализации, передаваемые с помощью прикладного программ-

ного интерфейса (клиентской библиотеки). Для взаимодействия других программ с сервером виртуализации могут использоваться дополнительные программные интерфейсы из пакетов с префиксом `libvirt-`;

- запросы субъектов доступа к рабочим столам функционирующих виртуальных машин по протоколам VNC и SPICE. Средства эмуляции аппаратного обеспечения на основе QEMU предоставляют интерфейсы доступа к рабочим столам функционирующих виртуальных машин по протоколам VNC и SPICE, при этом применяются отдельные настройки аутентификации для каждого из протоколов. В качестве способа аутентификации при использовании ПК в условиях ЕПП применяется аутентификация Kerberos с помощью механизма SASL `gssapi`, в иных случаях возможно применение других механизмов SASL или SSL/TLS аутентификации, основанной на сертификатах.

Выходными данными ПК являются:

- XML-описания виртуальных машин, сохраняемые в каталоге `/etc/libvirt/qemu` при создании виртуальной машины. В файле конфигурации задается состав аппаратных средств, которые необходимо эмулировать для данной виртуальной машины, а также параметры использования ресурсов сервера виртуализации (процессора, оперативной памяти и других физических устройств);
- файлы-образов носителей, используемых виртуальными машинами. Формат файлаобраза зависит от выбранного средства эмуляции аппаратного обеспечения. В ПК используются средства эмуляции аппаратного обеспечения на основе QEMU, которые поддерживают следующие форматы образов: image (raw-формат, является фактически представлением физического диска) и формат `qcow2` (родной формат QEMU, поддерживающий возможности сжатия, использования снимков и другие дополнительные возможности). Кроме того, существует возможность конвертирования форматов образов других средств эмуляции аппаратного обеспечения (например, VirtualBox);
- файлы устройств хостовой ОС, создаваемые для отображения различных аппаратных устройств виртуальных машин, или файлы-устройств, используемые для взаимодействия с виртуальными машинами в том числе по протоколам VNC и SPICE;
- файлы процесса функционирования виртуальных машин: текущее состояние, сохраненные состояния виртуальных машин, снимки состояния виртуальных машин и служебная информация по блокировкам;
- результаты запросов субъектов доступа к серверу виртуализации, передаваемые консольным и графическим интерфейсам управления виртуальными машинами;

- информация, снимаемая с эмулируемых устройств вывода информации виртуальных машин и передаваемая пользователя по протоколам VNC и SPICE (например, изображения рабочих столов);
- журнал регистрации событий ПК, содержащий детальную информацию по всем действиям субъектов доступа по управлению виртуальными машинами.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

ВМ — виртуальная машина

ЕПП — единое пространство пользователей

ОС — операционная система

ОС СН — операционная система специального назначения «Astra Linux Special Edition»

ПК — программный комплекс «Средства виртуализации «Брест»

ALD — Astra Linux Directory (единое пространство пользователей)

KVM — Kernel-based Virtual Machine (программное решение, обеспечивающее виртуализацию в среде Linux на платформе, которая поддерживает аппаратную виртуализацию на базе Intel VT (Virtualization Technology) либо AMD SVM (Secure Virtual Machine))

QEMU — Quick Emulator (средства эмуляции аппаратного обеспечения)

SASL — Simple Authentication and Security Layer (простая аутентификация и слой безопасности)

SPICE — Simple Protocol for Independent Computing Environments (простой протокол для независимой вычислительной среды)

SSH — Secure Shell Protocol (протокол передачи информации в зашифрованном виде)

VDI — Virtual Desktop Infrastructure (инфраструктура виртуальных рабочих столов)

VLAN — Virtual Local Area Network

VNC — Virtual Network Computing (система удалённого доступа к рабочему столу компьютера)

Лист регистрации изменений

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					
1		Все			21	РДЦП.01-18			20.08.18
2		Все			21	РДЦП.02-18			21.08.18