М. В. Тогачев, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732, 004.722

ОРГАНИЗАЦИЯ БЕЗОПАСНОЙ И НАДЕЖНОЙ ВИРТУАЛЬНОЙ ОБЛАЧНОЙ ИНФРАСТРУКТУРЫ СРЕДСТВАМИ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация. В данной статье рассмотрены отечественные системы виртуализации, проведен их сравнительно-сопоставительный анализ, а также изучены методы по обеспечению отказоустойчивости и безопасности в выбранном программном решении. Результатом стал рабочий отказоустойчивый стенд, безопасность которого обеспечена встроенными средствами защиты.

Ключевые слова: облачная инфраструктура, виртуализация, отказоустойчивость, гипервизор, Astra Linux, Брест, Ceph.

Введение. Сегодня в мире каждый третий сервер — виртуальный, системы виртуализации повсеместно используются в крупном и среднем бизнесе, государственных организациях. По оценке компании ISPsystem, больше 90% российских компаний используют данную технологию в своих информационных системах [1]. Эти средства позволяют им эффективно управлять своими данными, обеспечивая высокую масштабируемость, доступность и непрерывность бизнес-процессов в критических ситуациях [2]. С таким широким применением технологий виртуализации становится актуальным вопрос о защите гипервизора, виртуальных машин и информации, обрабатываемой в подобных системах [3].

В связи с введением санкционных политик зарубежных компаний большинство иностранных вендоров прекратили поддерживать и поставлять свои решения на территорию Российской Федерации, — в ответ на это Правительство нашей страны взяло курс на импортозамещение недружественных программных продуктов, что сформировало отечественный рынок систем виртуализации [4]. В сложившейся ситуации российским компаниям потребовалось срочно искать отечественные альтернативы зарубежному программному обеспечению (далее — ПО), не уступающему зарубежному в производительности и по функционалу, так как регуляторы с каждым годом ужесточают требования, связанные с информационной безопасностью.

Проблема исследования. В данной статье предлагаются пути решения проблемы импортозамещения иностранных систем виртуализации отечественным ПО. В ходе работы решался ряд задач:

1. Изучить теоретические основы принципов работы виртуализации и методов обеспечения безопасности и отказоустойчивости;
2. Произвести сравнительный анализ функциональных возможностей гипервизоров и выбрать наиболее подходящий отечественный продукт;
3. Апробировать выбранное решение на инфраструктуре с применением встроенных средств защиты;
4. Автоматизировать процесс развертывания при помощи скриптов.

Материалы и методы. Методами исследования являются анализ, изучение, моделирование. Опыты проводились при помощи виртуального стенда на ресурсах собственного сервера. Применялось оборудование Intel Xeon E5-2660 v3 2.60GHz, 32ГБ оперативной памяти, HDD на 1 ТБ, гигабитный коммутатор, гигабитный маршрутизатор RT-GM-2 с выходом в интернет по оптическому кабелю Fiber-to-the-home. Серверы «Брест»: оперативная память на 6 ГБ, HDD на 50 ГБ, 8 vCPU; FreeIPA: оперативная память на 4 ГБ, HDD на 50 ГБ, 2 vCPU.

Результаты. Облачные технологии — это модель предоставления различных услуг через Интернет по требованию клиента. Виртуализация играет ключевую роль в облачных технологиях, поскольку она позволяет эффективно использовать вычислительные ресурсы и обеспечивает гибкость в управлении инфраструктурой [5]. Облачные ресурсы разделяются на публичные, частные и гибридные. В публичных облаках виртуальная инфраструктура предоставляется множеству клиентов, при этом программно разделяет их между собой; в случае с частным облаком — вся инфраструктура принадлежит одной компании, а гибридный вариант использует комбинацию публичного и частного облаков.

Главным компонентом любой технологии виртуализации является гипервизор — программное или аппаратное обеспечение, позволяющее создавать изолированные друг от друга виртуальные машины с определенным количеством вычислительных ресурсов на одном физическом компьютере.

Существует 3 типа гипервизоров: первый, второй и гибридный. Первый тип считается самым производительным, так как устанавливается непосредственно на само оборудование; в отличие от второго, работающего поверх установленной операционной системы (далее — ОС), из-за чего возрастают накладные расходы, что приводит к снижению скорости виртуализации. Гибридный гипервизор совмещает в себе преимущества быстродействия первого типа и удобства использования второго типа, так как гипервизор взаимодействует с аппаратными ресурсами напрямую, обособленно от ОС.

Российские системы виртуализации еще отстают по функциональным возможностям в сравнении с зарубежными аналогами, но это не делает их непригодными для использования в продуктовых средах: разработчики достаточно часто выпускают обновления, в которых улучшают существующие функции и добавляют новые.

На рынке отечественных систем виртуализации представлен их широкий выбор (более 30 продуктов). Нами был рассмотрен программный комплекс средства виртуализации Брест (далее — ПК СВ Брест), РЕД Виртуализация и Альт Сервер Виртуализации, так как, в отличие от конкурентов, все они основаны на собственных ОС: Astra Linux, РЕД ОС и Alt Linux соответственно, что сразу снимает вопросы о совместимости ПО и перспективности дальнейшего развития в силу всесторонней поддержки от государства. Сравнение технических характеристик каждого из решений представлено в табл. 1.

У каждого решения есть свои преимущества и недостатки, однако основными критериями выбора послужили используемая платформа виртуализации и наличие сертификата ФСТЭК. Сравнивая сертификаты операционных систем нами было принято решение выбрать в качестве системы виртуализации ПК СВ Брест, так как классы защиты, уровни доверия, требования по виртуализации и контейнеризации у Astra Linux выше, чем у Alt Linux и РЕД ОС, что обеспечивает высокий уровень безопасности, в частности в функциях идентификации и

аутентификации, управления доступом, доверенной загрузки ВМ. В системе ПК СВ Брест поддерживается режим запуска машин в режиме "read only", который не позволяет пользователям вносить изменения в образы их дисков, а также мандатное разграничение доступа (далее — МРД) и мандатный контроль целостности (далее — МКЦ) для запускаемых ВМ, разрешая разграничить доступ по уровням секретности. МРД и МКЦ реализуются в разработанном модуле ядра PARSEC в качестве аналога зарубежным AppArmor и Security-Enhanced Linux.

Таблица 1

Сравнение средств виртуализации

Критерии сравнения	*РЕД Виртуализация*	*ПК СВ БРЕСТ*	*Альт Сервер Виртуализации*
Платформа виртуализации	oVirt	Opennebula	Proxmox
Максимальное количество ВМ в кластере	4 000	10 000	Без ограничений
Максимальное количество хостов в кластере	250	2 500	Без ограничений
Максимальное количество виртуальных процессоров в одной ВМ	710	512	1024
Максимальный объем ОЗУ одной ВМ, Тб	16	2	1
Поддержка Hight-Availability	+	+	+
Сертификат ФСТЭК	Сертификат № 4060 для РЕД ОС	Сертификат № 2557 для ОС Astra Linux	Сертификат № 3866 для ОС Alt Linux

Система имеет две основные серверные роли: узел виртуализации, на котором запускаются ВМ, и Front-End, управляющий всеми узлами виртуализации и предоставляющий веб-интерфейс. Один сервер может совмещать в себе сразу обе роли. Предусматриваются режимы развертывания в сервисном и дискреционном режиме; для применения МРД и МКЦ необходимо применить дискреционный режим, в котором, помимо серверов системы виртуализации, дополнительно вводится контроллер домена FreeIPA — открытое ПО, предназначенное для централизованного управления аутентификацией, политикой доступа и аудита (функционал подобен Active Directory от компании Microsoft) [6].

Встроенным механизмом обеспечения отказоустойчивости является RAFT— консенсусный алгоритм, который предназначен для сохранения согласованности состояния системы между серверами управления (Front-End) (см. рис. 1). Участники алгоритма выбирают единственного лидера (Leader), обслуживающего входящие запросы от клиентов; все остальные серверы становятся последователями (Follower). При изменении состояния системы (добавления пользователя, создания ВМ) лидер обновляет журнал и реплицирует запись у последователей. Для работы алгоритма необходимы 2N+1 серверов (рекомендуется 3 или 5), то есть нечетное их количество, где N — максимальное количество серверов, способных выйти из строя. Таким образом увеличиваются задержки записи, но достигается отказоустойчивость кластера.

При реализации данной облачной инфраструктуры нужно использовать общее хранилище, которое будет доступно при отказе любого из Front-End узлов, например NFS, CEPH, CIFS, OCFS2. Хорошим выбором будет CEPH — распределенное программно-определяемое

объектное хранилище с открытым исходным кодом, упор на использование которого сделан исходя из масштабируемости, надежности и отказоустойчивости. Он способен продолжать работу при отказе нескольких узлов, реплицировать объекты на несколько дисков сразу (степень репликации определяется администратором при настройке кластера) и предоставлять пользователям доступ в виде блочных устройств (RBD — Rados Block Device) или файловой системы (CEPH FS — CEPH File System). В ПК СВ Брест подключается в виде блочного устройства RBD (рис. 2).

```
HA & FEDERATION SYNC STATUS
ID NAME              STATE     TERM   INDEX   COMMIT   VOTE  FED_INDEX
 0 astra-brest01.m   follower  854    86229   86229    -1    -1
 1 astra-brest02.m   follower  854    86229   86229    2     -1
 2 astra-brest03.m   leader    854    86229   86229    2     -1
```

Рис. 1. Пример вывода статуса RAFT-кластера

```
cluster:
  id:     c600b4b9-c320-4d94-b0fc-70485cf3bc03
  health: HEALTH_WARN
          mons are allowing insecure global_id reclaim

services:
  mon: 3 daemons, quorum astra-brest01,astra-brest02,astra-brest03 (age 39h)
  mgr: astra-brest03(active, since 39h), standbys: astra-brest01, astra-brest02
  osd: 3 osds: 3 up (since 39h), 3 in (since 4d)

data:
  pools:   2 pools, 33 pgs
  objects: 3.02k objects, 12 GiB
  usage:   35 GiB used, 115 GiB / 150 GiB avail
  pgs:     33 active+clean
```

Рис. 2. Пример вывода статуса CEPH-кластера

Для разворачивания стенда была выбрана модель частного облака с типом услуги «Инфраструктура как сервис». Было создано 5 виртуальных машин: 2 контроллера домена FreeIPA и 3 сервера ПК СВ Брест. Второй сервер FreeIPA используется как реплика основного контроллера домена для большей безопасности. Все 3 сервера совмещают в себе роли Front-End и узла виртуализации, а также объединены в кластер высокой доступности RAFT и кластер хранилища CEPH. Впоследствии были настроены и протестированы пользователи с МРД и МКЦ как внутри операционной системы, так и в системе виртуализации Брест. Виртуальные машины в дискреционном режиме, при настройке динамической модели PARSEC в параметрах безопасности, запускаются от имени пользователя, вошедшего в систему, и применяют максимальную метку безопасности (уровень конфиденциальности, категория конфиденциальности и уровень целостности) пользователя на исполняющийся процесс ВМ в конкретном узле виртуализации. Для того чтобы поставить более точную метку в настройках следует выбрать статическую модель PARSEC. МРД и МКЦ позволяют добиться многократного уменьшения риска реализации вирусных атак, случайного или преднамеренного изменения файлов и процессов, утечки информации. На всех серверах был настроен межсетевой экран ufw на запрет

всех неиспользуемых портов. Стенд виртуальной облачной инфраструктуры представлен на рис. 3.

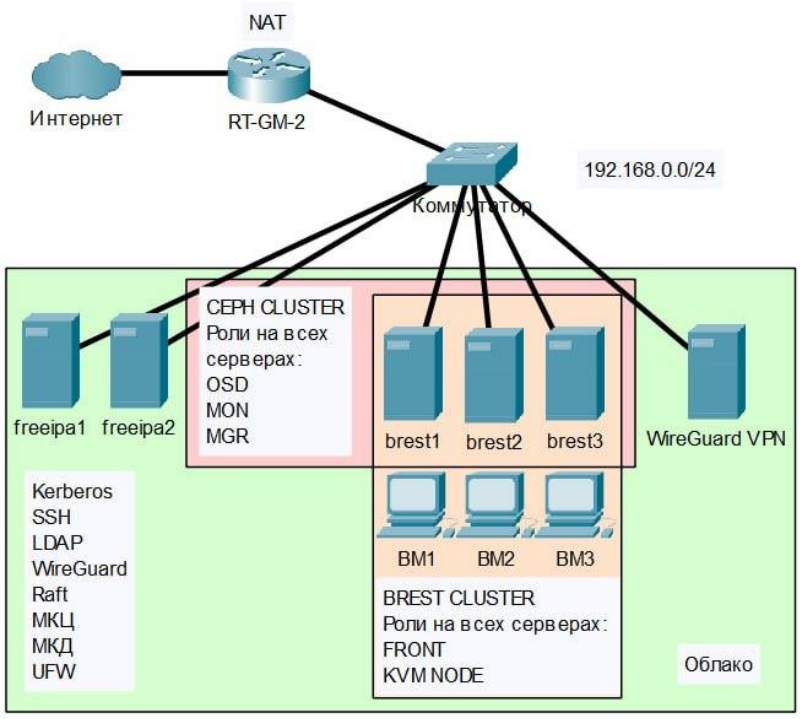

Рис. 3. Схема организации стенда

По мере создания инфраструктуры возникли проблемы со скоростью и удобством работы, так как приходилось дублировать команды для серверов облачной инфраструктуры, а некоторые процессы занимали длительное время. С целью ускорения и простоты развертывания были разработаны следующие bash-скрипты и Ansible-плейбуки:

1. Первоначальная настройка системы и конфигурация службы SSH на всех виртуальных машинах:

– обновление операционной системы;

– изменение имен компьютеров и добавление локальных доменных имен в /etc/hosts;

– конфигурация сетевых параметров интерфейсов ВМ (IP-адрес, шлюз по умолчанию, DNS);

– настройка конфигурационных файлов ssh и генерация ключей.

2. Организация отказоустойчивого кластера ПК СВ Брест в дискреционном режиме:

– установка серверных пакетов на трех серверах ПК СВ Брест и двух контроллерах домена FreeIPA;

– настройка конфигурационных файлов ПК СВ Брест и контроллеров домена FreeIPA;

– установка клиентских пакетов FreeIPA на сервера ПК СВ Брест и их введение в домен;

– настройка конфигурационных файлов RAFT на серверах ПК СВ Брест и объединение их в кластер;

– добавление новых серверов виртуализации в кластер ПК СВ Брест.

3. Создание распределенной файловой системы Ceph и ее подключение к ПК СВ Брест:
- установка пакетов и настройка конфигурационных файлов на трех серверах CEPH;
- создание пула и хранилища CEPH в системе виртуализации.

Заключение. В результате исследования были изучены основные термины и понятия виртуализации, проанализированы особенности отечественных систем виртуализации, создан стенд облачной инфраструктуры, в котором особое внимание уделяется вопросам информационной безопасности, разработаны скрипты по автоматизации развертывания облака.

СПИСОК ЛИТЕРАТУРЫ

1. Comnews — Текст: электронный // comnews.ru: [сайт]. — URL: https://www.comnews.ru/digital-economy/content/229154/2023-10-02/2023-w40/1016/virtualizacii-serverov-vyzovy-rynka (дата обращения: 28.03.2024).
2. Сысоев М.А. Особенности внедрения систем виртуализации в Российской Федерации / М.А. Сысоев, Е.А. Наташкина. — Тула, 2023. — С. 135-139. — EDN LCGZKT. — URL: https://elibrary.ru/item.asp?id=50420910 (дата обращения: 05.04.2024).
3. Кузнецов Н.М. Безопасность средств виртуализации облачной инфраструктуры / Н.М. Кузнецов // Вестник современных исследований: Учредители: ИП Соловьев В.А. — Москва, 2019. — С. 62-64. — EDN BBFCAQ. — URL: https://elibrary.ru/item.asp?id=37127050.
4. Лазарев А.В. Основные проблемы импортозамещения программного обеспечения в Российской Федерации / А.В. Лазарев // Студенческий: Учредители: Общество с ограниченной ответственностью «Сибирская академическая книга». — Астрахань, 2022. — С. 8-14. — EDN QTUJQY. — URL: https://elibrary.ru/item.asp?id=49114022 (дата обращения: 05.04.2024).
5. Овчинников М.А. Облачная инфраструктура и ее характеристики / М.А. Овчинников, К.В. Гусев. — Москва, 2021. — С. 75-77. — EDN MBCJFF. — URL: https://elibrary.ru/item.asp?id=45725641
6. Поддубный М.И. Анализ и особенности настройки средств централизованного администрирования FreeIPA в ОС Astra Linux Special Edition 1.6 / М.И. Поддубный, В.А. Бугаев, А.И. Очередько, Е.В. Филипчак, О.В. Бухарина. — Анапа, 2021. — С. 378-387. — EDN PUFFPJ. — URL: https://elibrary.ru/item.asp?id=47322312 (дата обращения: 05.04.2024).