УДК 004.42

А. В. Челнокова[1]*

Разработка метода автоматизированного развертывания безопасной виртуальной инфраструктуры предприятия

[1] Национальный исследовательский ядерный университет «МИФИ», г. Москва, Российская Федерация
* e-mail: chelalex1511@gmail.com

Аннотация. На обзор выносится проблема обеспечения надежности, отказоустойчивости и информационной безопасности виртуальной инфраструктуры предприятия с использованием технологии автоматизированного развертывания и конфигурирования клиентских и серверных решений. С целью решения данной проблемы разработан метод автоматизированного развертывания инфраструктуры предприятия. Утверждается, что представленный метод позволяет предприятию реализовать автоматизацию настройки виртуальных машин, исключив при этом ошибки ручного конфигурирования. В качестве стека технологий выбрана система управления конфигурациями Ansible и инструмент управления внешними ресурсами Terraform. Тестовый стенд развертываемой инфраструктуры представлен на базе аппаратного гипервизора VMware ESXi. Проанализированы достоинства и недостатки приведенного решения с точки зрения информационной безопасности при помощи модульного тестирования. Областью применения представленной работы являются корпоративные вычислительные сети, функционирующие на основе стека протоколов TCP/IP.

Ключевые слова: виртуализация, виртуальная инфраструктура, среда виртуализации, VMware ESXi, VMware vCenter, VMware vSphere

A. V. Chelnokova[1]*

Developing of the Method for the Automated Deployment of the Virtual Secure Enterprise Infrastructure

[1] National Research Nuclear University MEPhI
* e-mail: chelalex1511@gmail.com

Abstract. The problem of providing reliability, resiliency and information security of enterprise virtual infrastructure using the technology of automated deployment and configuration of client and server solutions is reviewed. In order to solve this problem, a method of automated deployment of enterprise infrastructure was developed. It is argued that the presented method allows the enterprise to automate the configuration of virtual machines, while eliminating the errors of manual configuration. The configuration management system Ansible and the external resource management tool Terraform were chosen as the technology stack. The test bed of the deployed infrastructure is presented on the basis of VMware ESXi hardware hypervisor. The advantages and disadvantages of this solution in terms of information security are analyzed using unit testing. The area of application of the presented work is corporate computer networks based on the TCP/IP protocol stack.

Keywords: virtualization, virtual infrastructure, virtualization environment, VMware ESXi, VMware vCenter, VMware vSphere

Введение

В современную эпоху наблюдается стремительный рост объема информации, который требует комплексной обработки. При обработке этого объема необходимы значительные вычислительные ресурсы. Одной из проблем, с которой сталкиваются предприятия, является нехватка мощности персональных компьютеров. Решение данной проблемы требует проведения различных исследований в области развития технологий виртуализации, в том числе для корпоративных сетей. Проблематикой комплексной методологии интеллектуально-адаптивного управления информационной инфраструктурой предприятия занимается научная школа Басыни Е. А. [1, 2].

Разграничение доступа к ресурсам виртуальной инфраструктуры является одной из важных задач в данной области. На этом акцентируют внимание такие ученые, как Журов П. М., Ружанская А. А., Переспелов А. В. и другие [3–5]. Проблема разграничения доступа нарушает безопасность виртуальной инфраструктуры: пользователь, неправомерно повысивший права доступа, может нарушить целостность и конфиденциальность данных виртуальных машин (ВМ). Никольский А. В. в автореферате диссертации приводит архитектуру многодоменного гипервизора, решающего проблему ограничения привилегий для пользователей ВМ, однако применение такого гипервизора не отменяет возможности ошибок ручного конфигурирования виртуальных инфраструктур, что повышает риск атак на среды виртуализации [6].

Развитие технологий виртуализации оказало влияние на законодательный аспект данной области. К примеру, Федеральная служба технического и экспортного контроля (ФСТЭК) 5 февраля 2021 года выпустила Методический документ «Методика оценки угроз безопасности информации» [7]. В разделе 4.3 указаны категории информационных ресурсов, которые могут быть атакованы, в том числе системы виртуализации. Таким образом, обеспечение защиты средств виртуализации является значимым не только для коммерческих организаций, но и для государственных учреждений. Это подчеркивает актуальность разработки метода для безопасной конфигурации виртуальной инфраструктуры предприятия.

В связи с существующей проблематикой становится актуальным решение класса задач по автоматизации развертывания виртуальной инфраструктуры предприятия.

Исследование предметной области

Несколько групп ученых занимаются исследованием проблем в области виртуализации. В работе, проведенной Лапшином Д. В., Кабанцовым Ю. Е. и Баулиным А. В., был проведен сравнительный анализ нескольких существующих систем виртуализации, таких как *VMware Horizon 7*, *Citrix XenDesktop 7.5*, *Microsoft RDS* (*Windows Server 2012 R2*), *Red Hat Enterprise Virtualization 3.3* и ПК Горизонт-ВС [8]. Результаты исследования показали, что лучшим решением для виртуализации является *VMware Horizon 7*. Однако, следует отметить, что

работа содержит субъективную экспертную оценку и не учитывает промежуточные результаты по каждому из критериев, что является значительным недостатком данного исследования. Не принимая во внимание недочеты, которые могут быть присущи оцениваемой системе по другим критериям, нельзя однозначно говорить о ее безопасности.

Ученые Зима В. М. и Крюков Р. О. занимаются исследованием проблемы ошибок, возникающих в процессе ручного конфигурирования виртуальной инфраструктуры (ВИ) в рамках центра обработки данных (ЦОД) [9]. В своей работе они предложили использовать математический аппарат для выявления уязвимостей конфигурации ВИ и для создания корректных и эффективных сценариев кибератак для тестирования защищенности ВИ. Авторы также рекомендовали устранять выявленные недостатки и уязвимости. В данной работе описывается разработанный метод с математическим обоснованием. Однако в работе не представляют экспериментальных данных на примере гипервизоров, которые могут использоваться в центрах обработки данных. Такие эксперименты могли бы повысить надежность, отказоустойчивость и информационную безопасность ЦОД.

В другой статье авторы предложили методику формирования защищенной виртуальной инфраструктуры для автоматизированных систем специального назначения [10]. В процессе разработки этой методики были определены требования к защите виртуальной инфраструктуры, перечень актуальных угроз для ВИ и различные уровни защиты. В исследовании подчеркивается важность использования данной методики, поскольку она позволяет предотвратить угрозы информационной безопасности путем устранения слабых мест в автоматизированной системе. Одним из преимуществ работы является демонстрация практического применения разработанной методики и соответствующих экспериментальных данных.

Таким образом, в исследуемой области можно выделить несколько значимых проблем, а именно:

– наличие уязвимостей в существующих гипервизорах различных типов;

– отсутствие возможности разграничения доступа в виртуальной среде;

– наличие ошибок ручного конфигурирования при развертывании виртуальных инфраструктур.

Постановка задачи

Целью настоящей работы является обеспечение надежности, отказоустойчивости и информационной безопасности виртуальной инфраструктуры предприятия с использованием технологии автоматизированного развертывания и конфигурирования клиентских и серверных решений.

Проведена декомпозиция цели на следующие задачи:

– исследование предметной области;

– проектирование метода автоматизированного развертывания безопасной виртуальной инфраструктуры предприятия;

– программная реализация спроектированного метода;

– проведение автоматизированного тестирования разработанного решения.

Предлагаемое решение

В целях решения поставленной задачи предлагается реализовать топологию сети виртуальной инфраструктуры и дальнейшей автоматизации ее конфигурации. Развертывание инфраструктуры, в первую очередь, требует создания и настройки виртуальных коммутаторов (ВК) – сетевых устройств уровня *L2+*, обеспечивающих передачу данных между ВМ внутри сети в рамках сервера ESXi, а также передачу данных во внешнюю сеть через физическую сетевую карту, предоставляющую сетевой интерфейс. В качестве первого шага реализации локальной сети необходимо сконфигурировать два ВК: один с подключением к глобальной сети и другой – без такого подключения. На рис. 1 и 2 представлена топология сети развертываемой инфраструктуры.

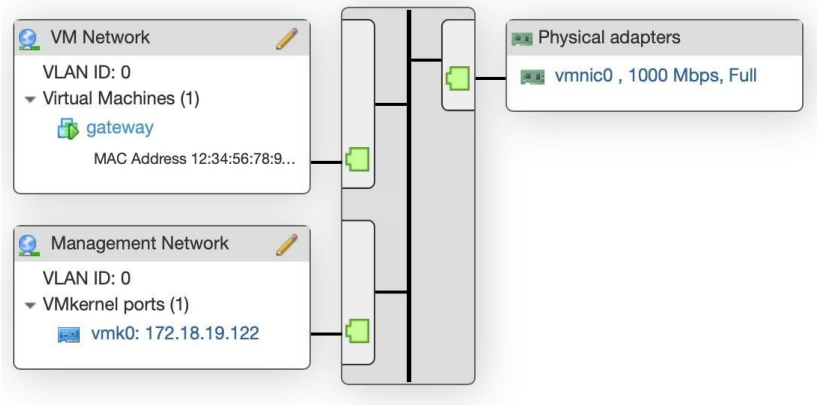

Рис. 1. Топология виртуального коммутатора
с доступом к глобальной сети Интернет

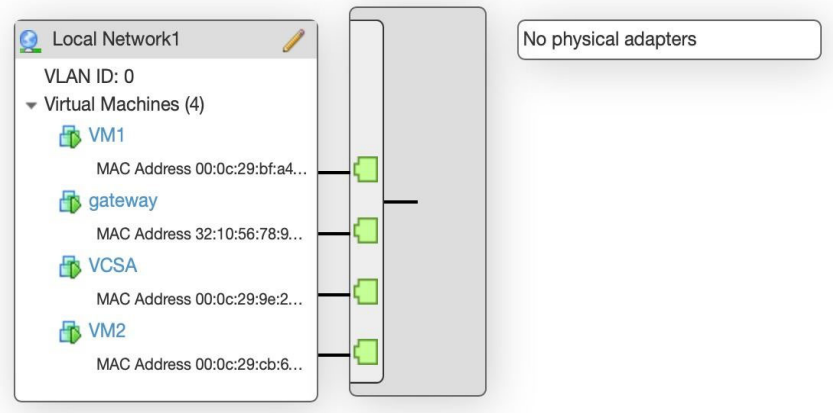

Рис. 2. Топология виртуального коммутатора без доступа к Интернету

В целях развертывания виртуальной инфраструктуры были разработаны *Ansible*-роли для конфигурации виртуального шлюза и сервера *VMware ESXi* и *Terraform*-сценарий управления внешними ресурсами для создания виртуальных машин. На рис. 3 представлен метод автоматизированного развертывания виртуальной инфраструктуры в виде блок-схемы.

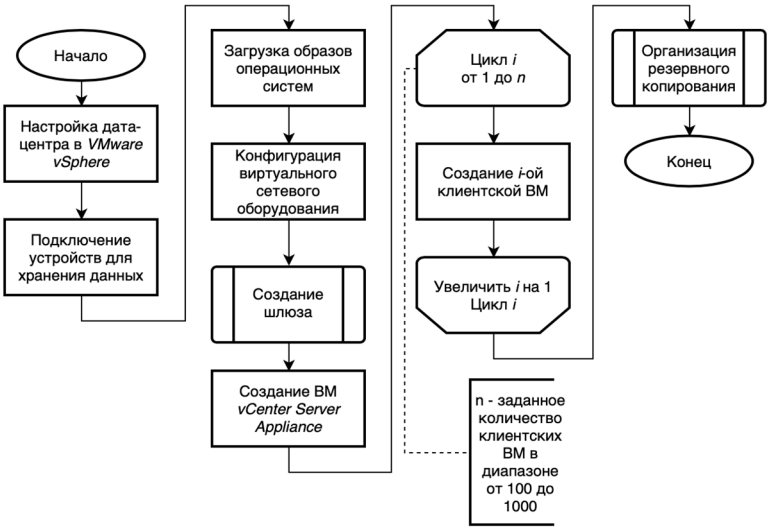

Рис. 3. Блок-схема метода развертывания безопасной виртуальной инфраструктуры

Данный метод отражает все три этапа, представленные ранее, а именно: создание ВИ, конфигурация виртуальных машин (включая ВМ *Gateway*) для обеспечения безопасности и организация резервного копирования (РК) виртуальной инфраструктуры для обеспечения надежности и отказоустойчивости. Создание шлюза и настройка РК являются подпрограммами, блок-схемы которых приведены на рис. 4.

Рис. 4. Блок-схемы подпрограмм «Создание шлюза» и «Организация резервного копирования»

Подпрограмма «Создание шлюза» описывает метод развертывания виртуальной машины *Gateway*, который включает в себя настройку *DHCP*-сервера для локальной сети и реализацию правил пакетного фильтра для внешних подключений и преобразования сетевых адресов при обращении в глобальную сеть. Резервное копирование виртуальных машин производится путем создания копий ВМ с последующим шифрованием. Затем полученные данные передаются на сервер резервного копирования, а старые копии удаляются для обеспечения максимальной эффективности и минимизации затрат на хранение информации.

Экспериментальное исследование

С целью апробации достоверности результатов исследования был создан тестовый стенд (ТС, рис. 5) виртуальной инфраструктуры, включающий в себя четыре ключевых элемента, необходимых для развертывания ВИ:

– master-сервер – основной сервер, который запускает наборы задач для настройки других компонентов ТС;

– сервер ESXi – аппаратный гипервизор, используемый для комплексного управления виртуальными машинами;

– сервер резервного копирования – сервер, развертываемый в виде отдельного физического устройства или изолированной среды на master-сервере.

– шлюз – ВМ Gateway, выполняющий функции маршрутизатора и DHCP-сервера.

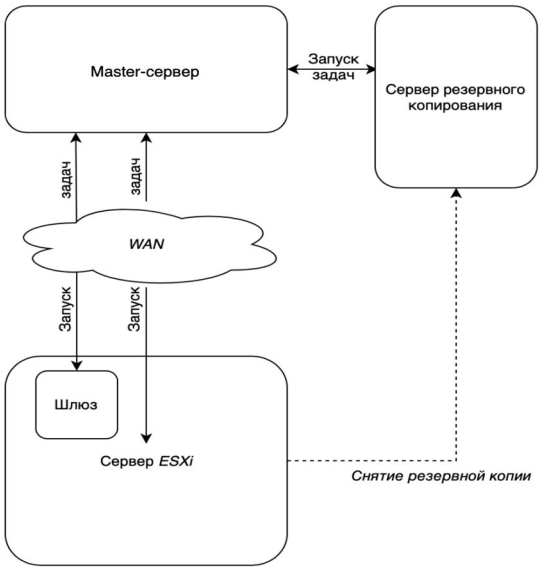

Рис. 5. Тестовый стенд развертываемой инфраструктуры

Взаимодействие между сервером *ESXi* и *master*-сервером, а также отдельно со шлюзом осуществляется через глобальную сеть Интернет по протоколу *SSH*. На каждый из представленных элементов главный сервер запускает задачи по конфигурированию отдельных структур и получению новых данных о текущем состоянии всего тестового стенда.

Запуск задач выполняется путем применения разработанных ролей Ansible и сценариев Terraform. Базируясь на данной тестовой системе, были проведены эксперименты для проверки достоверности полученных результатов.

Экспериментальное исследование проводилось с использованием инструментов для статического анализа кода *MegaLinter*, а также применялось модульное тестирование при помощи встроенных механизмов и дополнительного программного средства (ПС) *Molecule*.

Модульное тестирование – процесс тестирования отдельных модулей (или функций) программного обеспечения (ПО) для проверки их корректности и соответствия спецификации. Главная особенность данных тестов заключается в том, что каждый блок ПО проверяется независимо от других модулей, и результаты тестирования анализируются отдельно.

На рис. 6 представлен положительный результат модульного тестирования для *Ansible*-ролей.

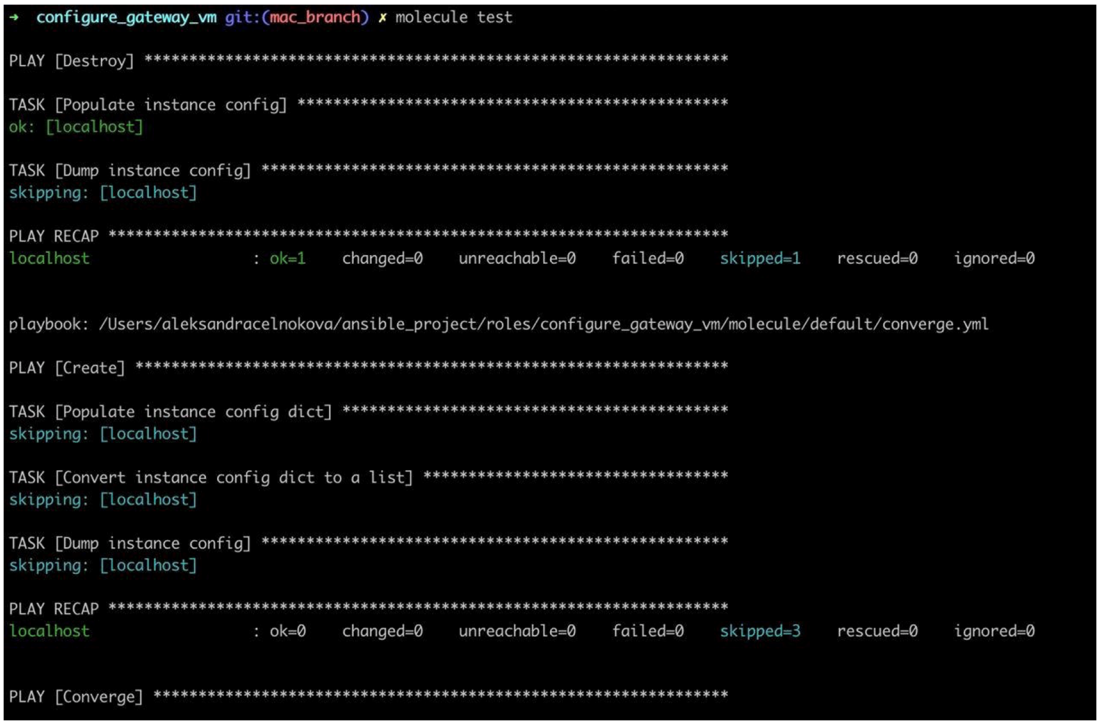

Рис. 6. Результат модульного тестирования *Ansible*-ролей

Аналогично была проведена проверка для *Terraform*-сценариев. По результатам тестирования предлагаемое решение успешно продемонстрировало реализацию метода развертывания виртуальной инфраструктуры, а также показало отсутствие уязвимостей исходного кода.

Заключение

В рамках данной работы был предложен метод, автоматизирующий развертывание безопасной виртуальной инфраструктуры предприятия, который был реализован программно и успешно показал себя на этапе тестирования.

Экспериментальное исследование представленной работы включало в себя статический анализ кода с применением набора инструментов *MegaLinter* и модульное тестирование исходного кода. Проведенный эксперимент завершился положительным результатом, что говорит о жизнеспособности и готовности к использованию разработанного решения.

Практическая значимость работы заключается в повышении безопасности виртуальной инфраструктуры предприятия и в устранении ошибок ее ручного конфигурирования.

Новизна данной работы заключается в предложении нового метода развертывания виртуальной инфраструктуры и ее дальнейшего сопровождения, повышающего надежность, отказоустойчивость и информационную безопасность развертываемой виртуальной инфраструктуры предприятия.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Басыня Е. А. Комплексная методология интеллектуально-адаптивного управления информационной инфраструктурой предприятия = Comprehensive Methodology of Intelligently Adaptive Management of an Enterprise Information Infrastructure / Е. А. Басыня. - Текст : непосредственный // Защита информации. Инсайд = Zasita informacii. Inside. - 2021. - № 5 (101). - С. 16-25.

2. Basinya E. A. Enterprise information infrastructure management [Electronic resource] / E. A. Basinya, D. S. Khudiakov // International multi-conference on industrial engineering and modern technologies (FarEastCon) : [proc.], Vladivostok, 6–9 Oct. 2020. – Vladivostok : IEEE, 2020. – 6 p. - Mode of access: https://ieeexplore.ieee.org/document/9271463/authors#authors. - Title from screen - DOI: 10.1109/FarEastCon50210.2020.9271463.

3. Журов П. М. Особенности контроля взаимодействия клиента VMware vSphere 6.5 с vCenter / П. М. Журов // Вопросы защиты информации. – 2018. – № 3(122). – С. 31-34.

4. Ружанская А. А. Особенности разграничения доступа при управлении виртуальной инфраструктурой на базе гипервизора KVM / А. А. Ружанская // Вопросы защиты информации. – 2018. – № 2(121). – С. 25-29.

5. Переспелов А. В. Применение технологии виртуализации для организации разграничения доступа / А. В. Переспелов, П. Ю. Богданов, Е. В. Краева // Известия высших учебных заведений. Приборостроение. – 2021. – Т. 64. – № 5. – С. 364-369.

6. Никольский А. В. Защита облачных вычислений от атак на средства виртуализации : специальность 05.13.19 "Методы и системы защиты информации, информационная безопасность" : автореферат диссертации на соискание ученой степени кандидата технических наук / Никольский Алексей Валерьевич. – Санкт-Петербург, 2013. – 18 с.

7. Методический документ. Методика оценки угроз безопасности информации : дата введения 5 февраля 2021 года. – Москва : ФСТЭК России, 5 февраля 2021 года. – 83 с.

8. Анализ защищенности систем виртуализации / Д. В. Лапшин, Ю. Е. Кабанцов, А. В. Баулин [и др.] // Colloquium-Journal. – 2020. – № 10-2(62). – С. 63-66.

9. Зима В. М. Метод выявления уязвимостей конфигурации виртуальной инфраструктуры на основе эквивалентных преобразований схем Янова / В. М. Зима, Р. О. Крюков // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. – 2020. – № 11-12(149-150). – С. 38-47.

10. Зима В. М. Методика формирования защищенной виртуальной инфраструктуры в автоматизированных системах специального назначения / В. М. Зима, Р. О. Крюков // Труды Военно-космической академии имени А. Ф. Можайского. – 2019. – № 667. – С. 213-223.