УДК 004.456
DOI 10.21685/2587-7704-2020-5-2-3

Open Access | RESEARCH ARTICLE

Обзор механизмов безопасности операционной системы Windows Server, применяемых для обеспечения доступности виртуальной инфраструктуры

А. Г. Фатеев
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Е. С. Архипов
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Проведен анализ механизмов безопасности операционной системы Windows Server, применяемых для обеспечения доступности виртуальной инфраструктуры. Проведенный анализ показал, что функциональные возможности операционной системы Windows Server могут применяться для обеспечения доступности среды виртуализации и выполнения требований по защите среды виртуализации.

Ключевые слова: виртуальная инфраструктура, мера защиты, доступность виртуальной инфраструктуры, виртуальная машина, Windows Server.

Overview of Windows Server operating system security mechanisms used to ensure availability of virtual infrastructure

A. G. Fateev
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

E. S. Arkhipov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. An analysis of security mechanisms for the Windows Server operating system used to ensure the availability of virtual infrastructure is carried out. The analysis has shown that the functionality of the Windows Server operating system can be used to ensure the availability of a virtualized environment and to meet the requirements for its protection.

Keywords: virtual infrastructure, security control, availability of virtual infrastructure, virtual machine, Windows Server.

В настоящее время одним из ключевых компонентов современной информационной инфраструктуры организаций является технология виртуализации. Развитие технологии виртуализации произошло во многом благодаря увеличению мощностей аппаратного обеспечения, позволившего создавать эффективные платформы виртуализации как для серверных систем, так и для пользовательских компьютеров. Технологии виртуализации позволяют запускать на одном физическом компьютере несколько виртуальных экземпляров операционных систем в целях обеспечения их независимости от аппаратной платформы и сосредоточения нескольких виртуальных машин на одной физической.

Виртуализация используется для построения инфраструктур, которые применяются для предоставления доступа к хранимой и обрабатываемой информации, доступа к услугам (сервисам), к средствам обработки данных. Во всех этих случаях одним из основных требований является время доступа, допустимое время ожидания доступа, допустимое время перерывов. Примеры таких инфраструктур – центры обработки данных (ЦОД), которые применяются для организации файловых хранилищ, также примерами являются сервисы по проведению электронных платежей, приобретению товаров (билетов). Во всех этих примерах важным является обеспечение доступности сервиса, так как, если будет перерыв в работе сервиса, он скажется на работе клиентов, чья деятельность (бизнес) может зависеть от работы сервиса. Поэтому компании, которые владеют виртуальной инфраструктурой и предоставляют ее ресурсы в аренду клиентам, в первую очередь обеспечивают бесперебойную работу виртуальной инфраструктуры в соответствии с соглашением об уровне услуг (SLA – Service Level Agreement). В противном случае могут быть репутационные, а далее и финансовые потери [1].

При обеспечении безопасности с использованием технологий виртуализации на первое место ставится такое свойство безопасности информации, как доступность, а также целостность виртуальной инфраструктуры, при этом конфиденциальность, как правило, обеспечивается при наличии соответствующих требований и не рассматривается как основное свойство.

Развитие технологии виртуализации, а следовательно, и применение таких технологий привело к тому, что стали разрабатываться нормативные документы, которые устанавливают требования к обеспечению информационной безопасности в государственных информационных системах (ГИС) и в информационных системах персональных данных (ИСПДн). Такими нормативными документами являются Приказы ФСТЭК № 17 и № 21, устанавливающие требования по обеспечению информационной безопасности в информационных и автоматизированных системах, использующих в своем составе технологии виртуализации [2, 3]. В данных приказах приведен перечень защитных мер среды виртуализации. Для обеспечения доступности виртуальной инфраструктуры могут использоваться следующие защитные меры: ЗСВ.4, ЗСВ.6, ЗСВ.8. Данные защитные меры могут быть реализованы с помощью встроенных механизмов безопасности операционной системы Windows Server.

Основными функциями, которые применяются для обеспечения доступности виртуальной инфраструктуры и информации, которая в ней обрабатывается, являются:

– миграция виртуальных машин;
– репликация виртуальных машин;
– дедупликация информации;
– резервное копирование виртуальных машин и других файлов.

В операционной системе Windows Server данные функции реализованы с помощью встроенных механизмов безопасности. Также данная операционная система реализует платформу виртуализации Hyper-V, которая обеспечивает создание изолированных программных окружений для использования в качестве виртуальных машин, одновременно работающих на одном физическом сервере [4]. В частности, Hyper-V предоставляет возможность выполнять виртуализацию оборудования. Это означает, что каждая виртуальная машина работает на виртуальном оборудовании. Hyper-V позволяет создавать виртуальные жесткие диски, виртуальные коммутаторы и ряд других виртуальных устройств, каждое из которых можно добавить в виртуальную машину [5].

Для управления механизмами безопасности, обеспечивающими доступность виртуальной инфраструктуры, в операционной системе Windows Server администратору предоставляются возможности таких графических консолей, как «Диспетчер серверов» (для управления дедупликацией информации и резервным копированием виртуальных машин и других файлов) и «Hyper-V Manager» (для управления механизмами миграции и репликации виртуальных машин).

Также для управления механизмами безопасности, обеспечивающими доступность виртуальной инфраструктуры, разработчики Windows предлагают использовать оболочку PowerShell. Оболочка PowerShell – это кроссплатформенная система для автоматизации задач и управления конфигурацией, состоящая из оболочки командной строки и языка сценариев. Для работы с объектами в данной оболочке используются командлеты. Каждый командлет можно применять отдельно, но наиболее эффективным является их совместное использование для выполнения сложных задач [6].

В результате обзора механизмов безопасности операционной системы Windows Server, применяемых для обеспечения доступности виртуальной инфраструктуры, следует отметить, что они позволяют реализовать все меры, связанные с доступностью виртуальной инфраструктуры, установленные приказами ФСТЭК [2, 3]. Данных механизмов достаточно, и применение специальных средств защиты информации не требуется.

Библиографический список

1. Соглашение об Уровне Услуг (SLA). – URL: https://www.smlogic.ru/g-it-s/itsm/soglashenie-ob-urovne-uslug-sla
2. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК России от 11 февраля 2013 г. № 17. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702
3. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных : Приказ ФСТЭК России от 18 февраля 2013 г. № 21. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691
4. Виртуализация Hyper-V: что это такое, цены, сравнение. Подробный обзор. – URL: https://market.cnews.ru/news/top/2020-04-08_virtualizatsiya_hyperv_chto_eto
5. Знакомство с Hyper-V в Windows 10. – URL: https://docs.microsoft.com/ru-ru/virtualization/hyper-v-on-windows/about
6. Что такое PowerShell? – URL: https://docs.microsoft.com/ru-ru/powershell/scripting/overview?view=powershell-7

Образец цитирования:

Фатеев, А. Г. Обзор механизмов безопасности операционной системы Windows Server, применяемых для обеспечения доступности виртуальной инфраструктуры / А. Г. Фатеев, Е. С. Архипов // Инжиниринг и технологии. – 2020. – Vol. 5(2). – С. 1–3. – DOI 10.21685/2587-7704-2020-5-2-3.