УДК 004.457
DOI 10.21685/2587-7704-2020-5-2-9

Open Access | RESEARCH ARTICLE

Обзор служб сертификации Active Directory для защиты сценариев PowerShell при управлении виртуальной инфраструктурой

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

Р. В. Баляснико́в
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Проведен анализ служб сертификации Active Directory операционной системы Windows Server для защиты сценариев PowerShell при управлении виртуальной инфраструктурой, применяемых для обеспечения безопасности виртуальной инфраструктуры. Проведенный анализ показал, что функциональные возможности операционной системы Windows Server могут применяться для обеспечения безопасности среды виртуализации и выполнения требований по защите среды виртуализации.

Ключевые слова: виртуальная инфраструктура, службы сертификации Active Directory, сценарии PowerShell, виртуальная машина, Windows Server.

An overview of Active Directory Certificate Services to protect PowerShell scripts for virtual infrastructure management

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

R. V. Baljasnikov
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. Windows Server Active Directory Certificate Services for protecting PowerShell scripts in managing virtual infrastructure to provide its security have been analyzed. The analysis has shown that the functionality of the Windows Server operating system can be used to secure a virtualized environment and to meet the requirements for its protection.

Keywords: virtual infrastructure, Active Directory Certificate Services, PowerShell scripts, virtual machine, Windows Server.

В настоящее время все большую популярность набирают технологии виртуализации. И это не случайно: вычислительные мощности компьютеров растут. Растет пропускная способность интерфейсов компьютеров, а также емкость и отзывчивость систем хранения данных. В результате возникает такая ситуация, что, имея такие мощности на одном физическом сервере, можно перенести в виртуальную среду все серверы, функционирующие в организации. Это возможно сделать с помощью современной технологии виртуализации.

Технологии виртуализации в настоящее время становятся одним из ключевых компонентов современной ИТ-инфраструктуры крупных предприятий (организаций). Сейчас уже сложно представить построение нового серверного узла компании без использования технологии виртуализации.

Определяющими факторами такой популярности, несмотря на некоторые недостатки, можно назвать экономию денег и времени, а также высокий уровень безопасности и обеспечение непрерывности бизнес-процессов [1].

С распространением технологий виртуализации увеличилось использование служб каталогов Windows Server, а именно Active Directory. Active Directory (AD) – это служебные программы, разработанные для операционной системы Microsoft Server, которые первоначально создавались в качестве облегченного алгоритма доступа к каталогам пользователей. Active Directory хранит сведения об объектах в сети и предоставляет эту информацию администраторам и пользователям, которые могут легко найти и использовать ее. Active Directory использует структурированное хранилище данных в качестве основы для логической иерархической организации сведений в каталоге [2].

Одной из самых используемых и полезных служб Active Directory является служба сертификации. Службы сертификации выполняют две основные функции: выдачу и обслуживание цифровых сертификатов на основе ключей. Сертификаты применяются:

– для аутентификации – пользователь подписывает пакет приватным ключом из выданного ему сертификата, а сервер аутентификации проверяет подпись публичным ключом этого же сертификата, который опубликован в доступном серверу месте;

– для подписи документов и сценариев – пользователь подписывает пакет приватным ключом из выданного ему сертификата, а другие пользователи, у которых есть доступ к публичному ключу сертификата подписывающего, используя публичный ключ, могут убедиться, что именно владелец сертификата подписал документ или сценарий;

– для шифрования каналов – клиент шифрует пакеты публичным ключом сервера, таким образом, только сервер, обладающий приватным (закрытым) ключом, сможет расшифровать информацию от клиента;

– для шифрования данных – два сотрудника, обменявшись открытыми (публичными) ключами, могут шифровать с их помощью файлы. Таким образом, расшифровать файл сможет только владелец приватного ключа. Или другой пример: для шифрования диска система использует публичный ключ, в то время как приватный хранится на флешке, без которой невозможно дешифрование [3].

В настоящее время системные администраторы и администраторы безопасности все чаще пользуются сценариями Windows PowerShell. Средство PowerShell [4] было разработано как оболочка с полным доступом ко всем компонентам Windows с помощью .NET Framework, объектов COM (Component Object 3Model – модель составных объектов) и других методов. Кроме того, в PowerShell предусмотрена среда выполнения. Сценарий PowerShell – это обычный текстовый файл с расширением .ps1. Файл содержит одну или несколько инструкций PowerShell, которые выполняются при вызове сценарного файла с консоли. PowerShell дает пользователю возможность определять, допустимо ли выполнение сценариев и, если да, указывать, какие сценарии могут выполняться. При управлении сценариями PowerShell администраторы выполняют ряд некоторых действий, а именно сформировывают политику выполнения PowerShell и удостоверяют сценарии цифровой подписью.

Политика выполнения PowerShell определяет, допустимо ли выполнение сценариев и будут ли загружаться файлы конфигурации при запуске оболочки PowerShell. Для формирования политики выполнения нужно воспользоваться составной командой Set-ExecutionPolicy и указать с ее помощью один из следующих параметров выполнения:

– Restricted: файлы конфигурации PowerShell не загружаются, и сценарии не выполняются. Этот обеспечивающий самые жесткие ограничения параметр применяется по умолчанию. В результате, после того как вы установили PowerShell, непреднамеренное выполнение сценариев, а также загрузка данных конфигурации исключаются. В то же время вы можете выполнять отдельные команды с консоли PowerShell.

– AllSigned: все сценарии и файлы конфигурации должны быть удостоверены цифровой подписью пользующегося доверием издателя. Для подписи сценария вы должны задействовать сертификат подписи кода. Как будет показано ниже, такой сертификат можно создать самостоятельно.

– RemoteSigned: все сценарии и файлы конфигурации, загруженные из Интернета, должны быть удостоверены цифровой подписью. Однако сценарии, хранящиеся на вашем компьютере, могут выполняться, а локальные файлы конфигурации загружаться и в том случае, если они не имеют цифровой подписи.

– Unrestricted: выполняются все сценарии, и загружаются все файлы конфигурации. Этот вариант связан с наименьшими ограничениями и, следовательно, сопряжен с наибольшим риском.

Добавление цифровой подписи к скрипту подразумевает, чтобы такой скрипт был подписан сертификатом с цифровой подписью «Сертификат подписи кода» (Code Signing Certificate). Для ре-

шения этой задачи существует три метода: покупка сертификата у доверенного центра сертификации, использование самозаверяющего сертификата, а также использование инфраструктуры открытого ключа.

Покупка сертификата у доверенного центра сертификации представляет собой самый простой метод.

Если скрипты предназначены для использования исключительно внутри организации, то чаще всего применяется второй метод, а именно создание и самостоятельная подписью сертификата. Самозаверяющий сертификат представляет собой специальный тип сертификата, подписанный самим его субъектом. Технически данный тип ничем не отличается от сертификата, заверенного при помощи подписи удостоверяющего центра, однако вместо передачи на подпись в такой центр пользователь создает свою собственную сигнатуру. Для самозаверяющего сертификата назначенным компьютером является орган, создающий сертификат. Преимущества самоподписывания заключаются как минимум в его нулевой стоимости, а также в скорости и удобстве создания. Такой сертификат администратор может создать при помощи инструмента MakeCert. Недостатком этого метода является то, что такой сертификат должен быть установлен на каждом компьютере, на котором будут выполняться скрипты, поскольку изначально другие компьютеры не будут доверять компьютеру, используемому для создания сертификата.

При помощи третьего метода можно создать шаблон сертификата подписи кода и использовать его для создания скриптов PowerShell от доверенного издателя. Этот метод считается наиболее трудоемким, так как для его реализации требуется развернутая инфраструктура доменных служб. К основному требованию для данного метода относится наличие центра сертификации внутри вашего домена. Условно всю операцию можно разбить на четыре этапа, а именно:

– создание шаблона сертификата подписи кода на выдающем сервере сертификации;
– запрос сертификата подписи кода пользователем;
– подписание скрипта Windows PowerShell;
– распространение сертификата подписи кода как доверенного издателя в среде Active Directory [5].

В результате обзора служб сертификации Active Directory операционной системы Windows Server для защиты сценариев PowerShell при управлении виртуальной инфраструктурой, применяемых для обеспечения безопасности виртуальной инфраструктуры, следует отметить, что они позволяют гибко реализовать контроль за использованием сценариев и являются важной функциональной возможностью при управлении виртуальной инфраструктурой.

Библиографический список

1. Анализ современных технологий виртуализации. – URL: https://habr.com/ru/company/southbridge/blog/212985
2. Что такое Active Directory – как установить и настроить. – URL: http://composs.ru/active-directory-chto-eto/
3. Службы сертификации Active Directory. Базовые знания. – URL: https://system-admins.ru/sluzhby-sertifikacii-active-directory-bazovye-znaniya
4. Что такое PowerShell? – URL: https://docs.microsoft.com/ru-ru/powershell/scripting/overview?view=powershell-7
5. Подпись скриптов PowerShell в доменной среде. – URL: http://gpo-planet.com/?p=4621

Образец цитирования:

Фатеев, А. Г. Обзор служб сертификации Active Directory для защиты сценариев PowerShell при управлении виртуальной инфраструктурой / А. Г. Фатеев, Р. В. Балясников // Инжиниринг и технологии. – 2020. – Vol. 5(2). – С. 1–3. – DOI 10.21685/2587-7704-2020-5-2-9.