УДК 004.056.2

Контроль целостности виртуальной инфраструктуры и ее конфигурации

Н. В. Мозолина
Московский физико-технический институт (государственный университет),
г. Долгопрудный, Московская область, Россия

Дано определение предмета контроля целостности виртуальной инфраструктуры и ее конфигурации и способ контроля целостности объекта с помощью представления конфигурации виртуальной инфраструктуры графом специального вида.

Ключевые слова: контроль целостности, виртуальная инфраструктура, конфигурация виртуальной инфраструктуры.

Для защиты среды виртуализации требуется выполнение множества мер [1], в том числе должен выполняться контроль целостности виртуальной инфраструктуры и ее конфигураций. Для обеспечения контроля в первую очередь следует определить, что является предметом контроля и каким способом можно его осуществить.

Целостность — одно из трех основных свойств информации с точки зрения безопасности [2], обеспечение которых является общепринятой практикой защиты информации.

Целостность информации определяется как свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право [1].

При таком определении целостности информация рассматривается исключительно как неделимый объект в том смысле, что нельзя разбить его на контролируемые и неконтролируемые части.

Например, есть некоторый текст, целостность которого контролируется. Безусловно, в нем можно выделить отдельные абзацы, предложения, слова, но при этом изменения в любой части текста могут повлечь за собой искажение смысла информации в целом, а потому нельзя пренебрегать контролем целостности любой из частей.

На практике данный подход не может быть применен, так как реальные объекты имеют сложную структуру и чаще всего являются динамическими, т. е. содержат в себе части, изменяющиеся в процессе работы. Например, файловая система хранит на диске в составе директории атрибуты файлов, в том числе меняющиеся данные о дате последнего открытия файла [3], а работа операционной системы и компьютера в целом невозможна без изменений в оперативной памяти. В таких случаях принято выделять критически важные части сложного объекта и контролировать их целостность [4].

Для защиты виртуальных инфраструктур подход, при котором контролируется целостность абсолютно всех частей инфраструктуры, также не подходит. Виртуальная инфраструктура должна рассматриваться как система, состоящая из различных объектов: виртуальных машин, хостов, хранилищ и других объектов в зависимости от конкретной реализации. При этом каждый объект также не является неделимым, и потому вопрос о контроле целостности виртуальной инфраструктуры сводится к контролю целостности только критически важных объектов виртуальной инфраструктуры и их частей.

Вместе с тем такой подход имеет и недостаток: он не учитывает связи между объектами виртуальной инфраструктуры и различные параметры настройки, т. е. конфигурацию.

Для различных виртуальных сред общими будут связи, характеризующие принадлежности одних объектов другим (например, виртуальная машина принадлежит хосту в том смысле, что запущена на нем), связи, характеризующие управление (например, в рамках решения vSphere компании VMware возможно управление множеством хостов-гипервизоров ESXi с помощью vCenter Server), связи, отражающие передачу данных (например, подключение виртуальных машин к сети).

Игнорирование связей между объектами может повлечь за собой возникновение угроз безопасности. Пусть в виртуальной инфраструктуре существуют 2 сегмента, предназначенные для работы

Мозолина Надежда Викторовна, инженер группы разработки СЗИ для систем виртуализации.
E-mail: nmozolina@okbsapr.ru

Статья поступила в редакцию 26 июня 2016 г.

с информацией различного уровня доступа. Первый сегмент — для работы с информацией ограниченного доступа, включает в себя хост-гипервизор № 1 с работающими на нем виртуальными машинами; второй сегмент — только для работы с общедоступной информацией, состоит из хоста-гипервизора № 2, на котором запущены некоторые виртуальные машины. Если через некоторое время виртуальные машины, работающие на гипервизоре № 1, окажутся включенными на гипервизоре № 2, то возникнет угроза безопасности, связанная со смешением двух различных сегментов, что может повлечь за собой и смешение информации различного уровня доступа. Несмотря на возникновение угрозы и нарушение целостности системы в целом, целостность каждого хоста-гипервизора и каждой виртуальной машины может быть сохранена.

Помимо связей, контроль целостности виртуальной инфраструктуры должен учитывать также параметры настройки виртуальной среды. Они значительно разнятся в зависимости от конкретного программного обеспечения, используемого для виртуализации. Примером параметра настройки для среды виртуализации, построенной на платформе vSphere, могут служить разрешение или запрет на управление гипервизором ESXi напрямую, в обход vCenter Server (*lockdown mode*).

Таким образом, необходимо контролировать не только целостность выделенных (критически важных) объектов (частей объектов) виртуальной инфраструктуры, но и целостность ее конфигурации, связей между объектами, а также параметры настройки среды виртуализации. Как и в случае с объектами, следует рассматривать лишь критически важные связи и настройки. Минимальный набор наиболее значимых для контроля объектов, связей и настроек должен быть основан на требованиях государственных регуляторов [5, 6] и рекомендациях производителей сред виртуализации [7, 8].

Вопрос обеспечения целостности виртуальных инфраструктур на платформах vSphere и Hyper-V решен с помощью ПАК Аккорд-В и ПАК СЗИ НСД ГиперАккорд, которые обеспечивают доверенную загрузку виртуальных машин, контролируя целостность оборудования, операционной системы, BIOS и MBR виртуальных машин [9, 10]. Входящий в их состав аппаратный модуль доверенной загрузки Аккорд-АМДЗ контролирует целостность технических и программных средств физических серверов (гипервизоров, хранилищ) [11]. Эти средства защиты позволяют обеспечить целостность всех объектов виртуальной инфраструктуры.

Вопрос контроля конфигурации требует выбора способа представления связей между объектами. Если каждый объект виртуальной инфраструктуры представить в виде вершины графа, то связи между объектами будут представляться ребрами. Такой способ представления конфигурации инфраструктуры не является новым, привычен для пользователей сред виртуализации [12] и вместе с тем удобен как для визуального восприятия, так и для хранения в памяти компьютера [13].

В отличие от привычного определения графа, когда ребра отличаются друг от друга только вершинами, которые они связывают (и, возможно, порядком вершин в случае ориентированного графа), для представления конфигурации виртуальной инфраструктуры стоит назначить каждому ребру некоторое свойство, тип связи, которую данное ребро отражает.

Учитывать различие между связями следует по той причине, что изменение типа связи влечет за собой изменения в работе инфраструктуры. Например, на хосте-гипервизоре ESXi работает виртуальная машина, целостность которой контролируется. После установки на эту машину vCenter Server целостность как виртуальной машины, так и хоста может быть сохранена, связь между объектами, если не учитывать ее тип, также останется прежней, но вместе с тем произойдет существенное изменение в работе системы: появится возможность управлять хостом-гипервизором ESXi с этой виртуальной машины. Если учитывать тип связи между объектами, то такое преобразование повлечет за собой нарушение целостности конфигурации, что отражает реальные изменения в системе.

Каждый контролируемый параметр настройки можно соотнести с одним или несколькими объектами виртуальной инфраструктуры и хранить свойство соответствующих вершин графа.

Представление конфигурации виртуальной инфраструктуры в виде графа изложенным способом возможно в любой момент жизни виртуальной инфраструктуры, и такой граф однозначно определен критически важными объектами, связями и параметрами. Это позволяет сравнивать текущую конфигурацию системы с некоторой эталонной (фиксированной) через сравнение двух графов и тем самым контролировать целостность конфигурации системы.

Таким образом, при применении предложенного подхода предметом контроля целостности виртуальной инфраструктуры и ее конфигурации являются критически важные объекты инфраструктуры, связи между ними и параметры настройки. Обеспечение контроля целостности

объектов осуществляется с помощью соответствующих средств защиты информации, а для контроля связей и настроек могут использоваться представление виртуальной инфраструктуры с помощью графа специального вида и последующее сравнение текущего графа с эталонным.

Литература

1. Методический документ ФСТЭК России от 11.02.2014 "Меры защиты информации в государственных информационных системах".
2. *Девянин П. Н.* Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. — М.: Академия, 2005. — С. 5.
3. *Карпов В. Е., Коньков К. А.* Основы операционных систем. Курс лекций. Учеб. пособие. — М.: Интернет-университет информационных технологий, 2005. — С. 173.
4. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией. 3.1.4. Свойства документа — доступность, целостность, легитимность. [Электронный ресурс]. URL: http://www.okbsapr.ru/docs/books/opf/37_opf.htm (дата обращения 12.04.2016).
5. Приказ № 17 ФСТЭК России от 11.02.2013 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".
6. Приказ № 21 ФСТЭК России от 18.02.2013 "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных".
7. VMware Security Hardening Guides. [Электронный ресурс]. URL: http://www.vmware.com/ru/security/hardening-guides (дата обращения 12.04.2016).
8. Security guide for Hyper-V in Windows Server 2012. [Электронный ресурс]. URL: https://technet.microsoft.com/en-us/library/dn741280.aspx (дата обращения 12.04.2016).
9. ПАК СЗИ НСД "ГиперАккорд". [Электронный ресурс]. URL: http://www.accord.ru/hyper-accord.html (дата обращения 12.04.2016).
10. ПАК АККОРД-В. [Электронный ресурс]. URL: http://www.accord.ru/accord-v.html (дата обращения 12.04.2016).
11. *Конявская С. В., Мищенко М. Г., Синякин С. А.* Аппаратные СЗИ НСД. Повторение пройденного. [Электронный ресурс]. URL: http://www.okbsapr.ru/konyavskaya_2007_3.html#_ftn2 (дата обращения 12.04.2016).
12. Using VirtualCenter maps to display VMware Infrastructure relationships. [Электронный ресурс]. URL: http://searchvmware.techtarget.com/tip/Using-VirtualCenter-maps-to-display-VMware-Infrastructure-relationships (дата обращения 12.04.2016).
13. *Кормен Т. Х., Лейзерсон Ч. И., Ривест Р. Л., Штайн К.* Алгоритмы: построение и анализ. Изд. 3-е / Пер. с англ. — М.: Вильямс, 2013. — 626 с.

Integrity monitoring of the virtual infrastructure and its configuration

N. V. Mozolina
Moscow institute of physics and technology (state university),
Dolgoprudny, Moscow region, Russia

The thesis offers the definition of integrity monitoring object of the virtual infrastructure and its configuration and the method of control by representing virtual infrastructure configuration as graph of a special kind.

Keywords: integrity monitoring, virtual infrastructure, virtual infrastructure configuration.

Bibliography — 13 references. *Received June 26, 2016*