УДК 004.056.5

Особенности применения средств защиты информации в виртуальных системах

Д. А. Постоев
ЗАО «ОКБ САПР», Москва, Россия

Рассмотрены проблемы создания и использования средств защиты информации для систем виртуализации. Предлагается подход, основанный на автоматическом построении системы защиты, учитывающий архитектурные особенности виртуализации.

Ключевые слова: виртуализация, разработка средств защиты информации, автоматизация, контроль целостности, управление доступом.

Использование виртуальных систем требует не только создания новых средств защиты информации, но и пересмотра самого подхода к проектированию и управлению ими. Существующие средства защиты (СЗИ) не учитывают особенностей сред виртуализации и являются статическими, со строгими, заранее определенными, параметрами контроля и политиками безопасности, характерными для физических систем. Процесс добавления и изменения элементов физической системы довольно сложен, связан с появлением новых аппаратных компонентов, а также проходит при участии администратора системы и обслуживающего персонала. Именно поэтому он жестко регламентирован и требует обязательного согласования вопросов безопасности, что в данном случае оправдывает вмешательство администратора безопасности в процесс изменения настроек СЗИ.

В отличие от физических систем, виртуальная инфраструктура представляет собой динамически меняющуюся информационную систему, позволяющую модифицировать собственные параметры налету, в том числе и в автоматизированном режиме. Также автоматизируется сам процесс создания новых элементов – виртуальных машин. Все это, при использовании старого подхода к защите, требует вмешательства администратора безопасности и постоянного изменения параметров безопасности системы, что усложняет работу и лишает преимуществ виртуализации.

Для того чтобы решить данную проблему, необходимо сформировать новый подход к построению системы защиты. Сформулируем некоторые его принципы:

Постоев Дмитрий Александрович, программист 2-й категории.
E-mail: postoev@okbsapr.ru

Статья поступила в редакцию 14 июня 2014 г.

- в информационной системе существует, как минимум два вида администраторов: администратор безопасности информации (АБИ) и администратор виртуальной инфраструктуры (АВИ);
- роль АБИ заключается в назначении прав пользователям системы и выработке политик безопасности, которые затем автоматически назначаются новым сущностям;
- в процессе работы системы управление виртуальной инфраструктурой осуществляет АВИ, причем все изменения виртуальной системы, корректные в рамках выбранной политики, происходят без участия АБИ, его вмешательство в работу АВИ требуется только при физических изменениях системы, например, при добавлении нового хранилища или сервера.

На основе описанных выше правил сформулируем функциональные требования к СЗИ для виртуальных сред. В большинстве существующих комплексах защиты виртуальных систем можно выделить две подсистемы: подсистема контроля целостности и подсистема управления доступом. Рассмотрим каждую из них по отдельности.

Под подсистемой контроля целостности будем понимать программную проверку целостности компонентов виртуальных машин перед их запуском. К контролируемым компонентам обычно относят: файлы конфигурации и BIOS, MBR и критичные системные файлы ОС. При появлении в системе новой виртуальной машины для нее не существует записи о контролируемых компонентах, и, как следствие, при существующем подходе возможны два варианта: запретить включение таким машинам или, наоборот, разрешить. Оба варианта имеют недостатки: первый лишает нас преимущества автоматического разворачивания системы из предварительно настроенных шаблонов (мастер-образов), требуя вмешательства АБИ, второй делает такие машины уязвимыми, так как не проверяет их контрольные суммы.

В случае использования шаблонов необходимо сверять контрольные суммы новых машин систем с контрольной суммой мастер-образа, однако стоит учитывать, что новые виртуальные машины не имеют файла настроек BIOS, который появляется после включения, и не все параметры vmx-файла проинициализированы. Таким образом, необходимо исключить их из проверки при старте новой виртуальной машины.

Подсистема управления доступом в большинстве существующих средств защиты для виртуальных сред реализует мандатную политику безопасности на основе уровней доступа. Метки безопасности назначаются элементам, имеющим непосредственно доступ к данным: хостам, хранилищам, сетевым устройствам и виртуальным машинам.

Как уже было замечено раннее, процесс создания новых виртуальных машин может быть автоматизирован. По этой причине необходимо назначать политики безопасности новым виртуальным машинам во избежание блокирования работы с ними. Это можно реализовать с помощью наследования метки безопасности с родительской сущности, которой для виртуальной машины является хост. Назначение меток должно предполагать то, что сущности, разделяющие аппаратные компоненты, должны иметь одинаковый уровень доступа. Существует 3 вида связей сущностей:

- общая оперативная память (хост и виртуальные машины на нем);
- общая внешняя память (хранилища и виртуальные машины на нем);
- общая сеть (сетевые устройства, хосты и виртуальные машины в рамках одного сетевого адаптера).

Таким образом, для настройки уровней доступа достаточно присвоить метку хосту, который является центральным элементом виртуальной системы, остальные метки будут розданы связанным объектам (рисунок).

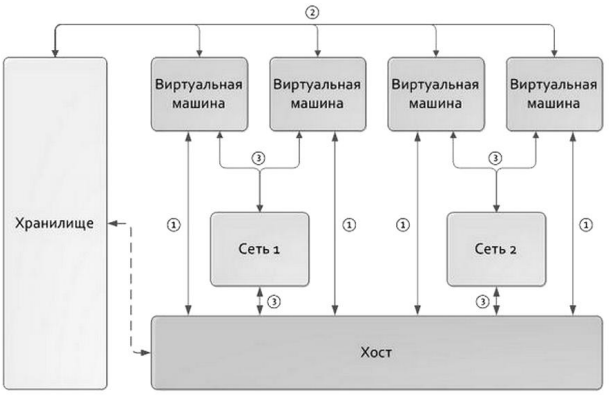

Схема подключения объектов в виртуальной среде

Стрелками на схеме обозначены связи, каждая из которых помечена цифрой в зависимости от вида. Сеть 1 и 2 принадлежат одному физическому общему сетевому адаптеру хоста. Хранилище связано с хостом с помощью локального подключения или специального устройства — *HBA* (***H**ost **B**us **A**dapter*).

Из выше описанного следует, что существующие на хосте виртуальные машины, подключенные к нему хранилища, сетевые адаптеры хоста и назначенные им сети получают одинаковый с ним уровень автоматически после настройки меток хоста. Дальнейшая детализация политики безопасности с помощью категорий и разрешения (запрещения) отдельных действий пользователям происходит в ручном режиме.

Современные системы становятся все более сложными в управлении и настройке, виртуализация помогает упростить эти действия, однако использование старых подходов к защите уменьшает ее эффективность. Применение автоматизированных способов управления средствами защиты помогает сократить время развертывания системы, уменьшить вероятность ошибки в процессе настройки системы и избежать необоснованного пересмотра вопросов безопасности.

Special aspects of using data protection tools in virtualized systems

D. A. Postoev
OKB SAPR JSC, Moscow, Russia

The article deals with problem of developing and use of data protection tools for virtualized systems. The author proposes approach based on automatic protection system building, which takes into account features of virtualization.

Keywords: virtualization, data protection tools development, automation, integrity check, access control.

Received June 14, 2014