ДОВЕРЕННАЯ СРЕДА

УДК 004.056.2

Доверенная загрузка и менеджмент логических дисков. Роскошь или необходимость

Д. И. Девятилов
Закрытое акционерное общество "ОКБ САПР", Москва, Россия

Описана система менеджмента логических дисков (LVM). Дано объяснение необходимости контроля целостности файлов на данных системах.

Ключевые слова: доверенная загрузка, модуль доверенной загрузки, средство доверенной загрузки, резидентный компонент безопасности, доверенная вычислительная среда, доверенные вычисления, контроль целостности, менеджмент логических дисков, менеджер логических дисков.

Парадигма доверенных вычислений начала развиваться с конца XIX столетия. Наблюдая за эволюцией парадигмы (от функционально-замкнутой среды — ФЗС до доверенного сеанса связи — ДСС) [1], можно с уверенностью сказать, что ее основа — это концепция доверенной вычислительной среды (ДВС), для создания которой одним из условий является наличие резидентного компонента безопасности (РКБ). РКБ осуществляет проверку целостности технических и программных средств ПК и может быть реализован в виде аппаратного модуля доверенной загрузки (АМДЗ). Доверенная загрузка — загрузка операционных систем (ОС) только с заранее определенных носителей и после успешного прохождения специальных процедур контроля целостности (КЦ) программных и аппаратных средств ПК [2]. Конечно же, уместно говорить не о доверенной загрузке ОС, а о доверенной загрузке загрузчика ОС, т. к. после прохождения процедур КЦ управление передается не коду ОС, а коду загрузчика [3]. Доверенная загрузка будет считаться выполненной только после успешного прохождения всех процедур КЦ.

В силу того что информационные технологии постоянно развиваются, усовершенствуются старые и создаются новые программные и аппаратные компоненты, в частности операционные и файловые системы, необходимо для обеспечения функций безопасности доверенной загрузки поддерживать появляющиеся удобства цивилизации, уметь с ними работать. Ответом на такой вызов становятся как усовершенствование самих фундаментальных парадигм доверенных вычислений [4—9] и новых взглядов на реализацию РКБ [6—14], так и поддержка новых технологий в существующих и уже зарекомендовавших себя подходах [7].

Необходимость более гибкого управления памятью запоминающих устройств ПК подталкивает к созданию новых систем управления дисковым пространством [10]. Часто возникает необходимость в разбиении или, наоборот, соединении отдельных блоков памяти жесткого диска с сохранением при этом всех установленных ОС, данных и программ. Кроме того, не хочется прибегать к резервному копированию имеющихся файлов. С этой задачей отлично справляется LVM (*Logical Volume Manager*) — система управления дисковым пространством, абстрагирующаяся от физических устройств [4].

Другими словами, LVM — это дополнительный слой абстракции от аппаратной части ПК, с помощью которого можно эффективно и легко управлять дисковым пространством, объединяя множество разнородных жестких дисков в один или, наоборот, отделяя их друг от друга. При этом все операции можно выполнить, не прибегая к перезагрузке компьютера. В современном администрировании рабочих станций это очень важно, т. к. излишние простои могут привести к финансовым потерям.

Несомненными плюсами использования LVM являются:

- использование любого количества жестких дисков или их разделов как одного большого раздела;
- логические диски могут быть распределены на несколько жестких дисков;
- можно производить создание, изменение и удаление логических томов в любом виде, независимо от физического расположения тома; также это можно делать в режиме реального времени;

Девятилов Дмитрий Игоревич, программист 3-й категории группы программирования ПО СЗИ.
E-mail: 9tilov@okbsapr.ru

Статья поступила в редакцию 26 июня 2016 г.

- возможность создавать резервную копию файловой системы практически "на лету";
- использование прозрачного шифрования файловой системы и кэширование часто используемых данных;
- динамическое увеличение размеров томов по мере их заполнения.

Бесспорным недостатком LVM считается то, что данный менеджер дисков реализован только для Unix-подобных операционных систем. Также к недостаткам можно отнести и сложность настройки.

В ОС семейства Windows аналогом LVM является технология динамических дисков, что еще раз говорит о востребованности таких типов систем гибкого менеджмента жестких дисков.

Несмотря на существующие недостатки, LVM является мощным инструментом для управления дисковым пространством СВТ. И для создания ДВС необходимо, чтобы РКБ "умел" работать с LVM. Например, в таких средствах защиты информации (СЗИ), как ПАК Соболь, не поддерживается контроль целостности файлов, расположенных на дисках с виртуальными файловыми системами и дисках, являющихся наборами томов LVM [15].

В средствах защиты информации от несанкционированного доступа (НСД) семейства Аккорд [5, 12] поддержка LVM и динамических дисков реализована в полном объеме. Если смотреть с практической точки зрения, то в Аккорде есть список, в котором отображаются группы и тома LVM. Пользователь может работать с томами так же, как и с разделами: выбирать нужный файл и ставить его на контроль. Пользователи могут быть спокойны за свои данные, которые обрабатываются в файловой системе, поддерживающей менеджер логических томов. Процедуры контроля целостности здесь осуществляются так же, как и на системах без LVM, и только после успешного их прохождения выполняется доверенная загрузка операционной системы.

Система LVM — мощный инструмент, обеспечивающий удобство и массу возможностей для работы с дисковыми накопителями. Поэтому для того, чтобы идти в ногу со временем, необходимо уметь осуществлять контроль целостности файлов и программ, обрабатываемых в данной системе.

Литература

1. *Конявский В. А.* Доверенный сеанс связи. Развитие парадигмы доверенных вычислительных систем — на старт, внимание, МАРШ! В: Комплексная защита информации. Сб. материалов XV Межд. науч.-прак. конф. Иркутск, 1—4 июня 2010 г. — М., 2010. С. 166—169.
2. *Алтухов А. А.* Концепция персонального устройства контроля целостности вычислительной среды // Вопросы защиты информации. 2014. № 4. С. 64—68.
3. *Каннер А. М.* Linux: о доверенной загрузке загрузчика ОС // Безопасность информационных технологий. 2013. № 2. С. 41—46.
4. *Lewis A. J.* LVM HOWTO. [Электронный ресурс]. URL: http://www.tldp.org/HOWTO/LVM-HOWTO/ (дата обращения 13.04.2016).
5. СЗИ НСД Аккорд-АМДЗ. [Электронный ресурс]. URL: http://www.accord.ru/amdz.html (дата обращения 14.04.2016).
6. *Алтухов А. А.* Неатомарный взгляд на РКБ как на композицию перехвата управления и контроля целостности. Межд. конф. "Комплексная защита информации". Беларусь, 2015. С. 53—55.
7. *Борисова Т. М., Романенко Н. В.* Аккорд-АМДЗ: Next Generation. Межд. конф. Суздаль, 2012. С. 57, 58.
8. *Конявский В. А.* Организация безопасного ДБО на основе СОДС "МАРШ!" // Национальный банковский журнал. 2011. № 9. С. 88, 89.
9. *Кравец В. В.* Доверенная вычислительная среда на планшетах Dell. "МАРШ!" // Вопросы защиты информации. 2014. № 4 (107). С. 32—33.
10. *Kim Ch.-S., Kim G. B., Shin B. J.* Method for managing logical volume in order to support dynamic online resizing and software raid and to minimize metadata and computer readable medium storing the same. Заявитель и патентообладатель. Electronics And Telecommunications Research Institute. № US6718436 B2. Заявлен 07.12.2001. Опубликован 06.04.2004.
11. *Конявский В. А.* Эпохе бурного развития — компьютер с динамической архитектурой // Национальный банковский журнал. 2016. № 3. С. 102, 103.
12. Способ защиты от несанкционированного доступа к информации, хранимой на персональной ЭВМ. Патент на изобретение № 2475823. 20.02.2013. Бюл. № 5.
13. *Алтухов А. А.* Контроль доступа на основе атрибутов и оптимизация управления множеством АПМДЗ. Мат. XX науч.-прак. конф. Минск, 19—21 мая 2015 г. — Минск: РИВШ, 2015. С. 55—60.
14. *Конявский В. А., Гадасин В. А.* Основы понимания феномена электронного обмена информацией. Библиотека журнала "УЗИ". Кн. 2. — Мн.: Беллитфонд, 2004. — 282 с.
15. ПАК "Соболь". Версия 3.0. Комментарии к версиям 2.0.88 ПО Windows, 3.0.41/40 ПО Linux и 1.0.180 BIOS. [Электронный ресурс]. URL: http://www.securitycode.ru/_upload/ editor_files/documentation/sobol_2/Sobol_FSB_ReleaseNotes.pdf (дата обращения 18.04.2016).

Trusted download and Logical Volume Manager. Luxury or necessity

D. I. Devyatilov

Closed Joint Stock Company "OKB SAPR", Moscow, Russia

The thesis describes LVM system and explain the need of file integrity monitoring on these systems.

Keywords: secure boot, trusted boot module, trusted boot means, resident security component, trusted computing environment, trusted computing, integrity control, Logical Volume Manager, Logical Disk Manage.

Bibliography — 15 references. *Received June 26, 2016*