БЕЗОПАСНОСТЬ НРС ДЛЯ ИНТЕЛЛЕКТУАЛЬНЫХ МЕСТОРОЖДЕНИЙ

А.А. Захаров, А.В. Бойко

Под термином «интеллектуальное месторождение», обычно понимают комплекс состоящий из устройств находящихся на скважинах (многофазного контроля притока, датчиками забойного давления и температур), средств коммуникации и управляющим программно-аппаратном комплексом, который позволяет оперативно, в идеале в автоматическом режиме, принимать решения по оптимизации режимов работы скважин, пластов и системы разработки и/или эксплуатации месторождения всего месторождения.

Принципиально важно отметить, что вывести скважину на оптимальный режим добычи нефти по всему месторождению естественно невозможно без моделирования с использованием геологии, гидродинамических моделей и истории разработки. Иными словами интеллектуальное нефтяное месторождение это система автоматического управления операциями по добыче нефти, предусматривающая непрерывную оптимизацию двух моделей - интегрированной (геологической и гидродинамической) модели месторождения и модели управления добычей [1].

Нами был сделан анализ как декларируемых, так и внедренных проектов, связанных с интеллектуальным месторождением в РФ, на основании которого можно сделать выводы:

1. Все системы интеллектуального месторождения сходны по целям и задачам – они призваны моделировать различные сценарии развития ситуации на производстве и давать возможность выбрать оптимальное решение, в том числе и по более эффективному использованию высококвалифицированных специалистов компании. Несмотря на широкомасштабное обсуждение новых идей по созданию интеллектуальных скважин и интеллектуальных месторождений, практическое воплощение подобных подходов не столь масштабно.

2. Список компаний ведущих работы по развитию технологий, связанных с интеллектуальным месторождением, показывает, с одной стороны, высокую актуальность тематики, а с другой стороны, позволяет сделать вывод о хорошей перспективе найти в этой области свою нишу практически для каждого IT-направления.

В рамках сотрудничества с ТННЦ ТНК-ВР нами выполнен пилотный проект по использованию облачных технологий для решения задач, связанных с подсчетом запасов и геологическим моделированием. В качестве облачной платформы выбран продукт VMware Private Clouds, использующий в своей основе систему виртуализации VMware vSphere. Разработан программный комплекс на базе ПО Irap RMS, который дополнен библиотекой процедур, позволяющих реализовать:

- новый математический метод двухмерного геологического моделирования литологии с использованием квазитрехмерного подхода;
- метод прогнозирования положения межфлюидных контактов в скважинах, вскрывающих залежи углеводородов (на основе численного метода Бройдена#Флетчера#Гольдфарба#Шанно);
- усовершенствованный метод решения задачи комплексирования одно# и двухмерных геологических трендов в виде трехмерного куба.

Пилотное внедрение комплекса показало, что одна из самых распространенных причин, по которым организации не спешат внедрять облачные IT услуги, является безопасность исходных данных и результатов расчетов. Действительно, облачные вычисления не дают заказчику возможности контролировать не только технологические, но и собственные информационные ресурсы, а следовательно, в такой области как подсчет запасов, где информация напрямую связана с налогообложением добывающих компаний, вопросы информационной безопасности выходят на первое место.

Применение ПО виртуализации как основы облачных технологий требует существенного изменения в подходах к обеспечению информационной безопасности систем [2-3]. Необходимо отметить появление нового, принципиально важного объекта виртуальной инфраструктуры - гипервизора, который на практике часто игнорируется и не защищается при помощи специализированных средств. Отметим, что за счет компрометации одного только гипервизора возможен вариант получения контроля над всеми подконтрольными ему виртуальными машинами и даже всей инфраструктурой виртуализации.

В качестве методов защиты виртуальных сред применялись: интеграция хост-серверов со службой каталога Active Directory, использование политик сложности и устаревания паролей, стандартизация процедур доступа к управляющим средствам хост-сервера, встроенный брандмауэр хоста виртуализации, отключение таких служб, как веб-доступ к серверу виртуализации.

Следует отметить, что при внедрении технологий виртуализации происходят серьезные изменения в физической инфраструктуре. С точки зрения организации сети возникает такое новое понятие как виртуальный коммутатор, который обеспечивает сетевое взаимодействие виртуальных машин в пределах одного хоста виртуализации. Проблема виртуальных коммутаторов заключается в неподконтрольности внутрисетевого трафика, а также в возможности прослушивания всего сетевого трафика между виртуальными машинами.

Для решения проблемы прослушивания портов использован подход к организации сетей VLAN на базе виртуальных коммутаторов, где тегирование кадров происходит на уровне хоста виртуализации еще до попадания пакетов в физическую сеть.

Виртуальная машина является самым потенциально опасным объектом виртуальной инфраструктуры с точки зрения информационной защиты ввиду ее изначальной полной незащищенности и простоты модификации данных. Кроме того, такие технологии как «живая миграция» и «мгновенные снимки» способны послужить отличным инструментом сокрытия следов присутствия в руках злоумышленника. В частности, злоумышленник, проникнув в гостевую операционную систему виртуальной машины и имея достаточный контроль над системой управления хостом виртуализации, может скрыть следы своего пребывания путем возврата к предыдущему снимку диска виртуальной машины (snapshot). Наконец, кража самих файлов мгновенных снимков виртуальной машины способна привести к серьезной утечке информации, поскольку они содержат в себе все последующие изменения данных на виртуальном диске и полный снимок оперативной памяти виртуальной машины с момента создания снимка.

Исходя из выше сказанного, были выделены следующие основные типы угроз безопасности виртуальных сред:

атака на виртуальную машину
- из другой виртуальной машины,
- на диск и файлы конфигурации виртуальной машины,
- на сеть репликации виртуальных машин,
- на сеть и систему хранения данных содержащей файлы виртуальной машины,
- на средства резервного копирования виртуальной машины;

атака на хост виртуализации
- из физической сети,
- средствами скомпрометированного сервера управления виртуальной инфраструктурой,
- через внутренние сервисы гипервизора SSH, WEB, TELNET и.т.д.,
- через агенты гипервизора от сторонних производителей;

атака на сервер управления виртуальной инфраструктуры
- через ОС, обеспечивающую функционирование управляющих сервисов,
- через СУБД сервера управления,
- через базу учетных записей,
- через сервис взаимодействия и мониторинга с хостами виртуализации;

атака на ресурсы хоста виртуализации путем
- неконтролируемого роста числа виртуальных машин,
- некорректного планирования разграничения пулов ресурсов,
- некорректного планирования растущих по мере заполнения виртуальных дисков ВМ,
- некорректного разграничения прав пользователей и групп виртуальной инфраструктуры.

Для автоматизированного аудита виртуальной среды на предмет наличия ошибок в конфигурации безопасности виртуальной инфраструктуре VMware vSphere нами разработан программный продукт, который использует для взаимодействия с компонентами платформы виртуализации VMware vSphere стандартный VMware vSphere SDK интерфейс. На вход программе подается адрес конкретного хоста виртуализации VMware ESX либо сервера управления всей инфраструктурой VMware vCenter и учетные данные пользователя с правами на чтение. На выходе программа генерирует отчет по состоянию защиты исследуемого объекта и выставляет общий рейтинг защищенности на соответствие одному из 3-х уровней защищенности, предложенных компанией производителем VMware Inc:

1. Уровень предприятия (Enterprise) Этот уровень предназначен для защиты от большинства типичных атак на виртуальную инфраструктуру и обеспечения высокого уровня защищенности конфиденциальной информации.
2. Уровень демилитаризованной зоны (DMZ). Этот уровень позволяет обеспечить надежную защиту хостов и виртуальных машин, имеющих подключение к Интернет.
3. Уровень специализированной зоны с ограниченной функциональностью (SSLF). Этот уровень призван обеспечить максимально возможную степень защиты виртуальной инфраструктуры, в том числе за счет потери определенной функциональности виртуальной инфраструктуры в пользу защищенности от самых ухищренных атак.

Отчет представляет собой детализированную таблицу, разделенную по типам угроз, свойственных виртуальной инфраструктуре, которые были предложены выше. В качестве тестов на защищенность используется отслеживание параметров конфигурации хостов, виртуальных машин, сервера управления и

другие, основанные на рекомендуемых регламентах производителя платформы. В основе этих рекомендаций лежит технический документ VMware vSphere Hardening Guide, описывающий 3 уровня защищенности виртуальной инфраструктуры VMware vSphere, где каждому из этих уровней соответствует более 100 параметров объектов системы виртуализации. Все эти параметры аккумулируются и анализируются движком программы в автоматическом режиме и накладываются на заранее созданный шаблон угроз по уровню защищенности. В результате пользователь (администратор) может детально отследить, какому уровню защищенности соответствует данная виртуальная инфраструктура и на какие параметры системы следует обратить внимание для приведения ее в соответствие.

Предлагаемый программный комплекс в значительной мере повышает безопасность виртуальной инфраструктуры, однако, естественно, он не в состоянии обеспечить абсолютную защиту виртуальной среды. Следовательно, необходимо выработать и стандартизовать единый подход к обеспечению информационной безопасности в виде регламентов и стандартов, обязательно учитывая рекомендации производителя платформы виртуализации, поскольку именно технологические особенности платформы определяют необходимые меры по обеспечению безопасности.

ЛИТЕРАТУРА:

1. Батурин А. Ю. Геолого#технологическое моделирование разработки нефтяных и газонефтяных месторождений. – М.: Издательство ВНИИОЭНГ, 2008. – 111 с.
2. Дериева Е. «Облака»: преимущества и риски безопасности // Компьютерное обозрение. 2009. № 44 (710). [Электронный ресурс] Режим доступа: http://ko.com.ua/kompyuternoe_obozrenie_44_710_ 2009_46653, свободный.
3. В.М. Шишкин. Безопасность облачных вычислений – проблемы и возможности риск-анализа//Transactions. Georgian technical university. Automated control systems - no 1(10), 2011c. 100-104.