Symantec NetBackup с Nirvanix-сервисами для облачного хранения. Основные преимущества NetBackup 5000:

- простота использования – не требуется покупка, тестирование какого-либо ПО и оборудования. Развертывание менее чем за 20 мин.;
- гибкость и масштабируемость – до 96 Тбайт используемой емкости с дедупликированием;
- высокая производительность бэкапирования – 4,3 Тбайт/час на узел;
- экономия ресурсов – от 10 до 50 раз снижается требуемая емкость хранения и на 99% уменьшаются требования к полосе пропускания;
- поддержка виртуальных сред – VMware и Microsoft Hyper-V.

NetBackup 5000 может масштабироваться от 1 до 6 узлов. Каждый узел представляет из себя 4U устройство с 2 Intel CPUs, 24 GB DDR2 памяти, 24 x 1 TB дисками, LSI disk management, 4 GB Ethernet портами.

Программное решение Symantec VirtualStore *(доступность с начала 2011 г., прим. ред.)* дает возможность создавать высокопроизводительные NFS NAS-СХД (на любых стандартных серверах с использованием существующих SAN- и DAS-развертываний от любого вендора) для высокомасштабируемых VMware развертываний, в частности, для VDI-инфраструктур (Virtual Desktop Infrastructure) с числом виртуальных машин более 10 тыс. В отличие от классических двухконтроллерных NAS, VirtualStore позволяет разворачивать 64-узловые кластерные СХД с линейно масштабируемой производительностью и сотни виртуальных машин (ВМ) за минуты.

В данном случае дедупликация с эффективностью 80% использовалась для устранения избыточности VMDK-файлов при создании ВМ.

Тестирование показало, что 1150 ВМ было развернуто менее чем за 3 минуты с использованием 40 ESX серверов и одного VirtualStore узла *(по данным Symantec, прим. ред.)*. В этом тесте узким местом была IP-сеть между VirtualStore и ESX кластером.

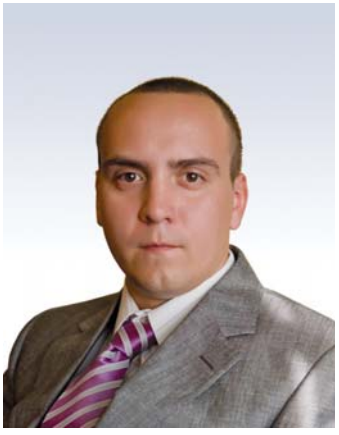
Подобные проблемы с развертыванием ВМ могут возникать, например, в утренние часы в больших организациях, перешедших на VDI-инфраструктуру, когда сотни сотрудников одновременно активируют свои рабочие столы.

Заключение

Технологии дедупликации постепенно становятся базовой опцией как в составе РКВ-решений, так и в составе продуктивных систем. Эффективность дедупликации, уровень ее масштабируемости и консолидации управления сейчас доступны во всех ценовых диапазонах. Основной вектор ее развития связан с более глубокой интеграцией в технологии виртуализации и в решения для развертывания облачных сервисов. В качестве примера можно привести РКВ-сервисы (со встроенной дедупликацией) как SaaS, которые стала предлагать с конца 2010 г. компания "Ай-Теко" на базе своего центра "Траст-Инфо" и платформы Netbackup 7 в результате заключения договора с Symantec. Благодаря тому, что права на лицензии не передаются потребителю, РКВ-сервисами можно пользоваться на условиях аренды, т.е. к сервису можно подключаться и платить за него только по мере использования.

SIEM-системы: мониторинг ИБ, оптимизация ИТ, контроль соответствия

На вопросы журнала отвечает Алексей Федоров, ведущий специалист НТЦ "Вулкан", сертифицированный инженер RSA enVision.



Алексей Федоров – ведущий специалист НТЦ "Вулкан".

SN. Тема SIEM (системы управления событиями и информацией о безопасности корпоративных IT-инфраструктур – Security Information and Event Management) периодически поднимается на страницах нашего журнала. В чем, по-Вашему, современная специфика решений этого класса?

А.Ф. Современные ИТ-инфраструктуры – это технически сложные системы. При этом их уровень сложности (как с архитектурной точки зрения, так и с точки зрения изощренности возможных угроз информационной безопасности) с развитием технологий только возрастает. Это связано, в том числе, с увеличением количества поддерживаемых платформ, приложений, клиентов. Например, число серверов/виртуальных машин в ИТ-инфраструктуре большой организации может уже достигать нескольких тысяч единиц. При таком значительном количестве источников событий наблюдение за состоянием инфраструктуры с точки зрения безопасности и стабильности работы становится сложнейшей задачей, поскольку речь идет об обработке потока событий до сотен тысяч EPS от огромного числа источников.

Когда в большой ИТ-инфраструктуре начинает теряться информация о событиях, возникает масса рисков. И здесь на помощь приходят системы управления событиями и информацией о безопасности – решения, позволяющие принять и обработать информацию о событиях от бесчисленного множества источников: серверов, рабочих станций, операционных систем, телекоммуникационного оборудования, приложений, средств защиты. Моя специализация – решение RSA enVision, одна из лучших современных SIEM-систем, в которой воплощено множество новейших тенденций. Так, enVision способен интегрироваться не только с самими источниками событий (рис. 1), но и со штатными средствами управления компонентов ИТ-инфраструктуры, а также с системами управления конфигурациями, сетью и т.п. Если говорить о решениях EMC, то примером может служить интеграции RSA enVision со SMARTS и Ionix Cofiguration Manager. Кроме того, сам enVision может являться источником информации для комплексной платформы управления рисками на базе RSA Archer eGRC. Как видно, современная SIEM-система – это уже не просто средство поддержки процессов Log/Event Management и анализа состояния ИБ. В лучших образцах реализованы возможности ведения аналитики и визуализации информации с точки зрения оптимизации ИТ, а также – контроля на соответствие нормативным требованиям (Compliance). Таким образом, очевидно, что системы SIEM способны стать ключевым элементом управления ИБ и ИТ с точки зрения своевременного выявления и предотвращения угроз ИБ, оптимизации работы оборудования и приложений, обеспечения соответствия.

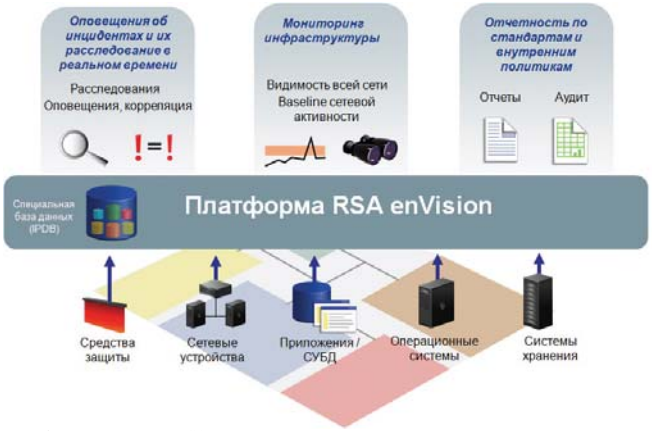


Рис. 1. Интеграции RSA enVision с множеством источников и другими средствами управления позволяет проводить более комплексный корреляционный анализ на угрозы ИБ с возможностью ретроспективы за многие годы.

SN. Согласитесь, RSA enVision – не самый распространенный SIEM-продукт в России?

А.Ф. Действительно, будучи одним из лидеров в мировом масштабе, решение от RSA пока не снискало должной популярности в нашей стране. Тем значительнее потенциал продукта и интереснее его перспективы. Уверен, что по целому ряду параметров enVision стоит на несколько ступеней выше конкурентов.

SN. Уточните, о чем именно идет речь?

А.Ф. Постараюсь быть кратким. К ключевым моментам я отнес бы следующее. Во-первых, широкие, практически ничем не ограниченные возможности по обработке информации о событиях. Мы с коллегами говорим, "что захочешь, то и настроишь". Во-вторых, способность работать с любым объектом, который генерирует события. Технология доступа к информации о событиях в каком-то роде здесь вторична. Сообщения отправляются по syslog? Берем. Используется SNMP? Понимаем. Запись в базу данных или в файл? Нет проблем. Для большинства распространенных устройств и приложений вендор предусмотрел поддержку соответствующих форматов регистрации служебной информации. Если же мы имеем дело с нестандартным источником, мощные встроенные средства RSA enVision позволят "подружить" систему хоть с высокотехнологичным холодильником, лишь бы он вел "логи". Наконец, никакой другой продукт не обладает такими возможностями масштабирования, как enVision. И последнее. Сбор событий enVision осуществляет без использования программ-агентов – согласитесь, это важное преимущество.

SN. Масштабирование – свойство, особенно ценное для растущих компаний. Если говорить о линейке RSA enVision, что для этого предлагается?

А.Ф. Линейка решений RSA enVision многообразна. В ней есть продукты "для начинающих", скажем, модель ES-560 с лицензией на обработку до 500 событий в секунду не более чем от 100 источников событий. А есть конфигурации, про которые можно смело сказать: "производительность и количество источников – не ограничены". Обратите внимание, я упомянул слово "лицензия". Это означает, что RSA enVision может "расти" вместе с владельцем. При увеличении количества источников или при росте потока событий имеется возможность просто обновить лицензии, а не перестраивать все решение с нуля. Существует и аппаратное масштабирование. Оно очень часто применяется в территориально-распределенных сетях многофилиальных компаний или холдингов.

SN. Название нашего издания обязывает задать вопрос о возможностях RSA enVision по взаимодействию с системами хранения данных.

А.Ф. Компания RSA, разработчик enVision, является подразделением безопасности корпорации EMC – мирового лидера в производстве решений для хранения данных. Это означает, что владельцы систем хранения от EMC, желающие построить комплексную систему безопасности вокруг своих данных, могут легко и просто воплотить эти идеи. Пользователи СХД других вендоров – также не в обиде. Механизмы RSA enVision, позволяющие подключить любые источники событий, обеспечат интеграцию SIEM с самым разным оборудованием. Также возможна и интеграция с линейкой EMC Ionix for IT Operations Intelligence, куда, в частности, вошло и решение Storage Insight for Availability (определение первопричины события, вызвавшего отклонение от заданного регламента, на уровне СХД и сети хранения).

SN. Что могут увидеть эксплуатанты систем хранения данных в RSA enVision?

А.Ф. Все, что может передать система хранения данных в качестве информации о событиях! RSA enVision способен принимать весь поток сообщений, как с систем хранения, так и с любых других источников – без предварительной фильтрации событий. На основе полученной информации могут формироваться отчеты разного уровня детализации, генерироваться уведомления, строиться диаграммы.

S.N. А что есть в enVision "из коробки" для СХД?

А.Ф. RSA enVision имеет целый ряд стандартных отчетов, которыми можно воспользоваться "как есть" либо модифицировать их под свои нужды, либо – написать новые оригинальные отчеты; для этого имеются все необходимые инструменты. На сегодняшний день существует порядка пятидесяти стандартных отчетов, ориентированных на системы хранения. Ежеквартально производитель выпускает пакет обновлений с поддержкой новых источников событий, а также предлагает новые отчеты – в том числе и для СХД. Откровенно говоря, enVision не является "коробочным" продуктом. Его внедрение зачастую требует большого объема работ по реализации именно тех задач, которые стоят перед конкретным заказчиком. Зато после того, как эти задачи реализованы, система долго и стабильно работает без вмешательства высококвалифицированного персонала. Отсюда – возможности по снижению TCO.

S.N. Можно ли использовать enVision для мониторинга работы СУБД?

А.Ф. Да, RSA enVision поддерживает достаточно много СУБД: Oracle, Microsoft SQL Server, IBM DB2, MySQL Enterprise, Sybase ASE. Стандартный набор отчетов по указанным СУБД удовлетворит потребность большинства пользователей. Если же необходимо реализовать дополнительную обработку – что ж, без проблем можно модифицировать имеющиеся шаблоны или запрограммировать новые алгоритмы анализа данных.

S.N. Чем еще силен RSA enVision?

А.Ф. Однозначно, это – поддержка VMware. Виртуализация быстро завоевывает рынок. И здесь enVision опережает всех конкурентов по возможностям взаимодействия с виртуальными инфраструктурами. Это является закономерным результатом интеграции в составе EMC большой группы активов, в числе которых есть и VMware, и RSA.

S.N.: Какие именно специалисты могут быть заинтересованы в использовании RSA enVision?

А.Ф. Ответ на этот вопрос, как мне кажется, гораздо шире, нежели принято ожидать. Скажу так: в один момент времени результаты работы enVision могут находиться и на столе у президента компании, и на консоли администратора безопасности. Разумеется, уровень представления будет отличаться - в первом случае это сводный отчет или группа диаграмм, во втором – "сырые" данные о событиях "как они есть" – важное подспорье например для проведения расследований. Кстати, не только специалисты по ИБ являются основными "потребителями" результатов работы RSA enVision. Ориентация этой системы на работу с самыми разными событиями делает ее полезной для всех без исключения ИТ-специалистов.

S.N. Ваш прогноз относительно развития технологии SIEM?

А.Ф. Думаю, что системы управления событиями и информацией о безопасности пойдут по пути усиления синергии ИТ и ИБ (уже сейчас тот же RSA enVision реализует возможности обработки событий как в интересах "автоматизации", так и "безопасности"). Они будут еще глубже интегрироваться с большинством ИТ/ИБ-процессов (рис. 2). Возрастет производительность, улучшатся аналитические возможности. Визуализация станет более интерактивной. В конечном итоге, SIEM станут незаменимым элементом корпоративного SOC/NOC (Security/Network Operation Center). И еще более широкие горизонты повышения эффективности управления ИТ откроются, когда SIEM-

Рис. 2. RSA enVision: обеспечение ИБ, оптимизация ИТ, контроль соответствия нормативным требованиям.

решения будут на уровне данных интегрироваться с системами управления сетью. Разумеется, не снимается со счетов и традиционное расширение функциональных возможностей подобных средств. Так что у систем управления событиями и информацией о безопасности большое будущее.

S.N. Спасибо, и успехов Вам и Вашим коллегам!