ВИРТУАЛИЗАЦИЯ В СКУД И IP-ВИДЕО: КЛЮЧЕВЫЕ ХАРАКТЕРИСТИКИ И ВОЗМОЖНОСТИ ПРИМЕНЕНИЯ

Значение программного обеспечения для современных систем контроля и управления доступом и IP-видеонаблюдения трудно переоценить. Многие концепции пришли в индустрию безопасности из сферы информационных технологий, и направление виртуализации не является исключением. Термин «виртуализация» имеет множество различных значений, поэтому важно понимать возможности и ограничения данной технологии для использования в системах безопасности. При соблюдении определенных условий виртуализация позволяет повышать эффективность использования аппаратного обеспечения и снижать затраты на сервера и рабочие станции.

В общем случае можно выделить следующие основные два типа виртуализации, которые используются в системах безопасности: виртуализация представлений и виртуализация серверов. Виртуализация представлений позволяет выполнять приложение на сервере, а пользователю на экран рабочей станции или мобильного устройства выводятся результаты его выполнения. Представителем виртуализации представлений являются службы удаленных рабочих столов Microsoft (прежнее название — «Службы терминалов»). Принцип этого типа виртуализации состоит в том, что пользователь видит экран удаленного сеанса, а на сервер передаются данные о нажатиях клавиш на клавиатуре и перемещении мыши. Для пользователя это выглядит так, как будто он работает с обычным рабочим столом на своем компьютере. Виртуализация рабочего стола подходит для программного обеспечения СКУД, позволяя получить следующие преимущества:

- Снижение затрат на приобретение рабочих станций. При использовании технологии виртуализации представлений вместо полноценных рабочих станций могут использоваться недорогие устройства («тонкие» клиенты), которые не нужно будет обновлять многие годы. «Тонкие» клиенты включают в себя маломощный процессор и видеокарту с пассивным охлаждением, не содержат жесткого диска и т.п.

- Снижение затрат на приобретение программного обеспечения (операционных систем, антивирусов) для рабочих станций. «Тонкие» клиенты не требуют приобретения этого ПО, нужно только иметь лицензии на подключение к серверу удаленных рабочих столов, стоимость которых существенно ниже.
- Сокращение затрат на обслуживание рабочих станций, администрирование и обновление ПО. Требуется обслуживать только сервер удаленных рабочих столов и один экземпляр приложения.
- Безопасность передачи данных. Поскольку автономные функции «тонкого» клиента сильно ограничены, то минимизируются риски, связанные с некорректными или неразрешенными действиями оператора: несанкционированная установка приложений, подключение USB-устройств и т.п. Весь трафик между «тонким» клиентом и сервером полностью зашифрован.

Примером программного обеспечения комплексной интегрированной системы безопасности, реализующей возможности службы удаленных рабочих столов, является ПО Honeywell Pro-Watch. Оно может использоваться как в варианте с полноценными клиентскими рабочими станциями, так и с «тонкими» клиентами и веб-интерфейсом.

Важно отметить, что из-за ограничений производительности рабочих станций по отображению большого количества видеопотоков в мегапиксельном разрешении, виртуализация представлений для рабочих станций с отображением (рендерингом) видео в настоящее время используется редко. Для высокоэффективного рендеринга мегапиксельных видеоизображений на рабочих станциях производители сетевых видеорегистраторов (NVR) и VMS используют новую технологию, которая задействует

ресурсы графических карт (GPU). Современные графические адаптеры имеют значительные вычислительные ресурсы, которые можно задействовать для декодирования и отображения видеопотоков H.264 от NVR, получив прямой доступ к аппаратному обеспечению видеокарты. Рабочая станция с процессором Intel Core i7 и Intel HD Graphics, использующая технологию GPU-рендеринга, может декодировать и отображать 18–25 видеопотоков с разрешением Full HD в реальном масштабе времени. В качестве примера можно привести ПО для систем IP-видеонаблюдения Honeywell MAXPRO NVR и MAXPRO VMS, реализующее рендеринг с использованием графического адаптера.

Вторым типом виртуализации, используемым в системах безопасности, является виртуализация серверов. Виртуализация серверов подразумевает запуск на одном физическом сервере нескольких виртуальных машин. Виртуальные машины представляют собой приложения, запущенные на операционной системе физического сервера (обычно это Microsoft Hyper-V или VMware vSphere), которые эмулируют физические устройства сервера. На каждой виртуальной машине устанавливается операционная система, в которой выполняются приложения и службы. Виртуализация серверов при правильном планировании позволяет получить следующие преимущества:

- Снижение затрат на оборудование. Благодаря объединению нескольких виртуальных серверов на одном физическом сервере, виртуализация позволяет сократить затраты на серверное оборудование. На одном физическом сервере могут одновременно функционировать несколько виртуальных серверов.
- Снижение затрат на программное обеспечение. Производители программного обеспечения имеют схемы лицензирования, экономически эффективные для реализации виртуальных сред.
- Снижение затрат на обслуживание серверов и потребляемую электроэнергию.
- Повышение удобства администрирования. Виртуализация позволяет программному обеспечению абстрагироваться от физического оборудования, что дает возможность перемещать виртуальные машины между физическими серверами. Это упрощает процедуру восстановления виртуальной машины в случае неисправности физического сервера.
- Повышение уровня отказоустойчивости. Виртуализация предоставляет средства кластеризации целого сервера, независимо от работающего на нем программного обеспечения. Физические сервера, на которых запускаются виртуальные машины, могут быть объединены в кластер и, в случае отказа одного из серверов, автоматически перемещаться на другой сервер.

В качестве примера ПО для систем безопасности, поддерживающего виртуализацию серверов, можно привести Honeywell Pro-Watch, WIN-PAK и MAXPRO VMS/NVR.

Необходимо правильно рассчитывать аппаратные ресурсы физического сервера при виртуализации видеосерверов, осуществляющих работу с видеопотоками. Процессы записи и трансляции мегапиксельного видео создают высокую нагрузку на процессор, память, сетевую карту и систему хранения данных. Использование NVR в виртуальной среде не всегда реализуемо, поскольку он может задействовать практически все имеющиеся ресурсы физического сервера.

Следует отметить, что виртуализация превратилась из технологии для лабораторных тестовых сред в неотъемлемый элемент центров обработки данных и инфраструктур виртуальных рабочих столов. При выборе решения по виртуализации серверов СКУД и IP-видео следует учитывать, что ощутимый экономический эффект может быть достигнут прежде всего для серверов, работающих с базами данных, таких как сервера СКУД и VMS. Важно обеспечить надлежащую безопасность виртуальных серверов, поскольку скопировать целую виртуальную машину не представляет труда. Простота копирования является ключевой причиной неконтролируемого размножения виртуальных машин. Если физическая безопасность виртуальных машин не обеспечена, их виртуальные или физические диски должны быть зашифрованы, чтобы предотвратить потерю конфиденциальных данных. Централизованное размещение носителей виртуальных машин и хранилищ в безопасных местах может минимизировать как размножение виртуальных систем, так и угрозу потери данных.

Резюмируя, стоит отметить, что компания, которая выпускает ПО с поддержкой виртуализации, имеет больше конкурентных преимуществ на современном рынке систем безопасности, так как данная технология позволяет достигать экономической эффективности при использовании конечным потребителем. Компания Honeywell предлагает полный функциональный ряд оборудования с ПО, поддерживающим виртуализацию.

Honeywell

АО «ХОНЕВЕЛЛ»
121059, Москва, ул. Киевская, д. 7
тел.: (495) 797-9371, (495) 796-9800
191123, Санкт-Петербург,
ул. Шпалерная, д. 36
тел.: (812) 329-5722
e-mail: securityrussia@honeywell.com
www.security.honeywell.com/ru