Инструмент контроля доступа к средствам управления виртуальной инфраструктурой

Светлана Конявская, *заместитель генерального директора ЗАО "ОКБ САПР", к.ф.н.*
Дмитрий Угаров, *руководитель группы разработки СЗИ для систем виртуализации, ЗАО "ОКБ САПР"*
Дмитрий Постоев, *программист группы разработки СЗИ для систем виртуализации, ЗАО "ОКБ САПР"*

Казалось бы, нам следовало закрыть вопрос защиты виртуальных инфраструктур (далее ВИ) на базе VMware, создав Аккорд-В., но мы испытывали смутную неудовлетворенность тем, как решили в нем задачу разграничения доступа к средствам управления ВИ: разграничение на уровне предоставления или запрета доступа к средствам управления казалось нам слишком уже недетализированным. А необходимость контролировать организационными мерами, наличие средств разграничения доступа на АРМ Администратора ВИ (далее АРМ АВИ) – слишком уж зависимой от человеческого фактора.

Из этого неудовольствия и желания расширить (детализировать) функционал разграничения и перейти от организационного подхода ("следите, чтобы на всех АРМ было СПО Аккорд-Winxx") к техническому ("с любого АРМ запрос пройдет через наш модуль") и вырос наш новый продукт "Сегмент-В.". Он также предназначен для VMware vSphere.

С точки зрения Сегмента-В., vCenter является внутренним элементом по отношению к ВИ, а администратор ВИ – внешним.

Применение продукта требует дополнительной настройки ВИ так, чтобы все запросы к vCenter и ESXi проходили через Сегмент-В. (см. рис.). Аргументом в пользу того, что данная реорганизация сети не является обременяющей, может служить требование к усилению ЗСВ.4: в информационной системе, построенной с применением технологии виртуализации, должна быть обеспечена единая точка подключения к виртуальной инфраструктуре (при необходимости резервирования каналов связи точка подключения должна рассматриваться как комплексное решение, включающее в себя средства взаимодействия с основным и резервными каналами связи).

Что контролируем

Контролировать все возможные действия пользователей не имеет смысла. Более того, избыточность функционала усложняет работу с ПО. Интерес представляют в первую очередь действия, выделяемые регулятором, + специфичные функции конкретных платформ, которые им не учтены (например: lockdown mode). По результатам анализа 17/21 приказов и всех функций в API vClient мы выделили 23 операции:

1. Вход.
1.1. Вход в систему (вход в систему по паролю или с учетными данными текущей сессии).
2. ВМ.
2.1. Доступ к файлам ВМ (просмотр хранилища и файлов виртуальных машин на нем).
2.2. Удаление ВМ (удаление ВМ и ее файлов с диска).
2.3. Создание ВМ (создание, импорт, а также добавление в инфраструктуру ВМ).
2.4. Запуск ВМ/vApp (запуск виртуальной машины/vApp).
2.5. Останов ВМ/vApp (выключение, Suspend, перезапуск ВМ/vApp).
2.6. Создание копий ВМ (клонирование в ВМ/шаблон, разворачивание ВМ из шаблона).
2.7. Изменение конфигурации ВМ/vApp (изменение конфигурации оборудования ВМ/vApp).
2.8. Доступ к консоли ВМ (доступ к консоли – экрану ВМ по VNC).
2.9. Контроль подключаемых к ВМ устройств (контроль подключаемых к ВМ USB, CD, FDD).
2.10. Экспорт ВМ (экспорт ВМ в OVF-формат).
2.11. Миграция ВМ (миграция/перемещение ВМ со сменой хоста и/или хранилища).
3. Сетевые устройства.
3.1. Работа с сетью (изменение настроек сети хоста и сетевых устройств: свитчей, групп портов и их распределенных вариантов).
4. Хосты.
4.1. Базовые операции с хостом (запуск, остановка, перезапуск, подключение, отключение, Maintenance Mode хоста).
4.2. Работа со службами хоста (запуск, остановка, перезапуск сервисов хоста).
4.3. Изменение настроек сетевого экрана (открытие, закрытие портов, ограничение диапазона IP).

Рис. Настройка маршрутизации

4.4. Работа с Lockdown Mode (включение, отключение Lockdown Mode).
4.5. Конфигурация автостарта (включение, отключение автостарта, изменение порядка запуска ВМ).
4.6. Настройка DNS и маршрутизации хоста (настройка DNS и маршрутизации хоста).
4.7. Настройка домена на хосте (ввод сервера в домен и вывод из него).
4.8. Настройка времени на хосте (ручное изменение времени, добавление NTP-сервера, включение и отключение NTP-сервиса).
5. Снапшоты.
5.1. Работа со снапшотами (создание, откат – к предыдущему состоянию и удаление снапшотов).
6. Роли.
6.1. Управление правами (управление ролями, назначение и удаление прав).

Также есть ряд действий, которые по ряду причин приходится всегда запрещать:

- полное [delete] удаление папок/vApp (включая ВМ внутри);
- экспорт vApp;
- клонирование vApp.

Важно, что Сегмент-В. – это не часть Аккорда-В., и их можно использовать по отдельности. Если по какой-то причине получилось так, что в системе уже установлено другое средство контроля запуска виртуальных машин, установить и использовать в ней Сегмент-В. все равно возможно и правильно: это позволит закрыть ЗСВ.1, ЗСВ.2, ЗСВ.3, ЗСВ.6, ЗСВ.10.

NM
АДРЕСА И ТЕЛЕФОНЫ ЗАО "ОКБ САПР" см. стр. 80