


«Сегмент-В.»



Угаров Дмитрий
dugarov@okbsapr.ru

Что это?

**ПАК «Сегмент-В.» предназначен для
разграничения доступа к функциям
управления виртуальных
инфраструктур на базе VMware
vSphere***

**версий 5.x и 6.x*

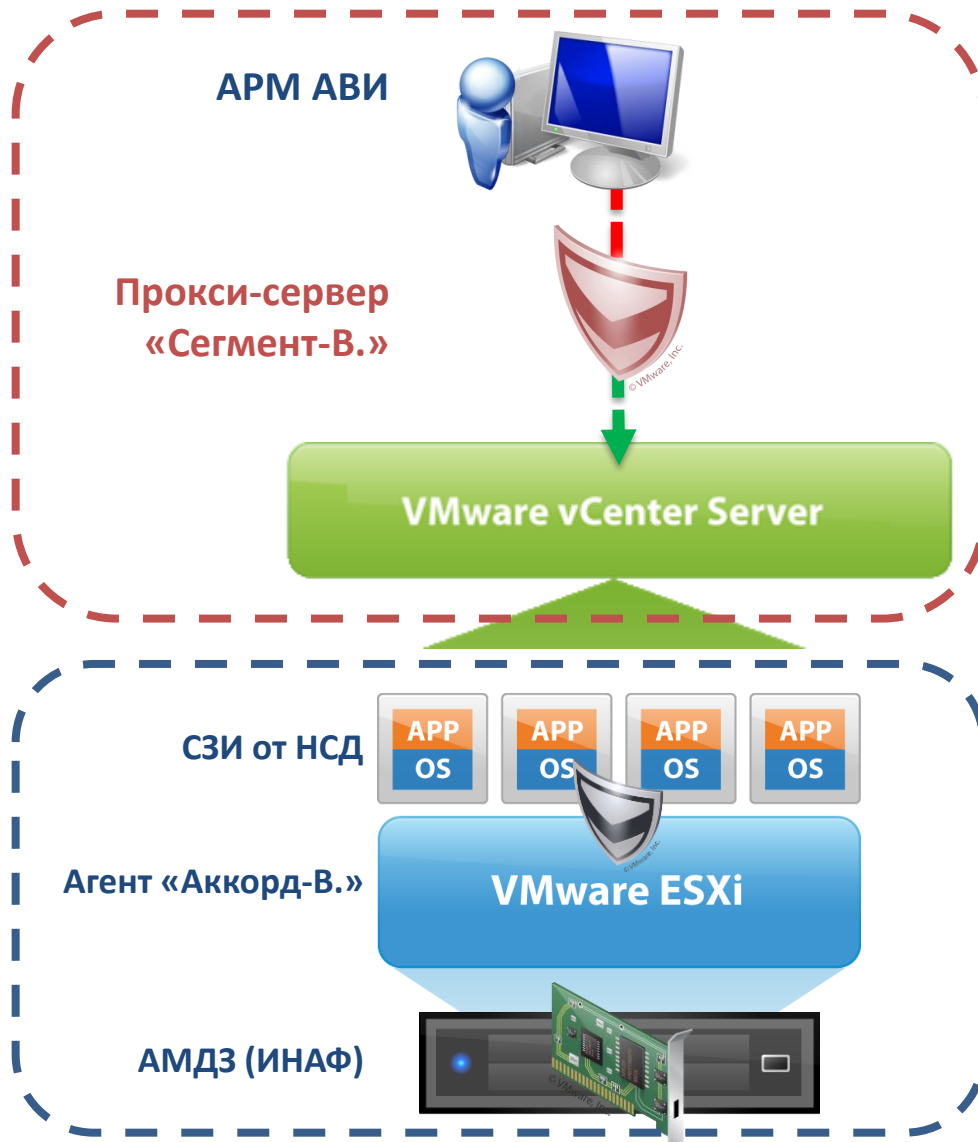


Зачем? (Аналогия)

	Физическая среда	Виртуальная среда
«Опорная точка»	АМДЗ	Аккорд-В.
Защита во время исполнения	Аккорд-Win Аккорд-Х	?



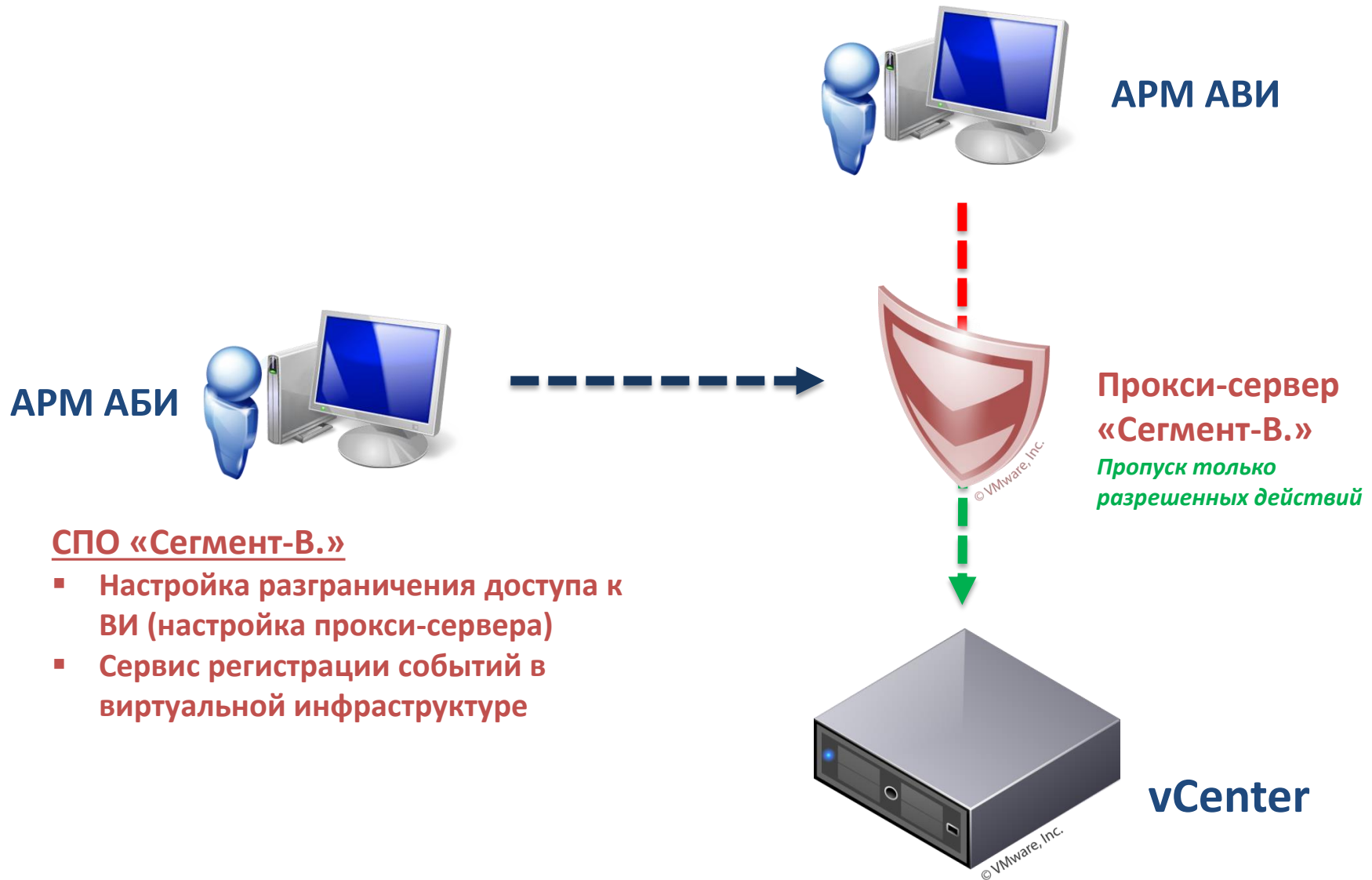
Зачем?



«Сегмент-В.»
*Разграничение
доступа к ВИ*

ПАК «Аккорд-В.»
*Построение
доверенной среды*

Обобщенная архитектура «Сегмент-В.»



- **Разграничение доступа к объектам ВИ:**
 - **Мандатное (иерархические и неиерархические метки)**
 - **Дискреционное (Более 20 действий)**
- **Отказоустойчивость (использование нескольких серверов)**
- **Поддержка нескольких vCenter (в том числе Linked режим)**
- **Запрет смешивания информации из различных сегментов**

Пример применения (1)

Дано:

АВИ имеет максимальный уровень доступа ко всем объектам vCenter (в числе которых VM обрабатывающие общедоступные данные и сов. секретные)

Задача:

Исключить для АВИ возможность переключения сов. секретной VM в подсеть общедоступных VM (по ошибке или умышленно), оставив при этом у него максимальный уровень прав доступа.



Пример применения (2)

Решение:

Вариант 1 – полное физическое разделение (отдельные ESXi сервера не имеющие связи между собой).

Минус – дорого (уменьшается эффективность DRS и HA)

Вариант 2 – создание отдельных учетных записей для каждого типа доступа.

Минус – все же потребует урезания прав АВИ (для исключения возможности изменения прав, что противоречит условию)

Вариант 3 – при помощи ПАК «Сегмент-В.» назначить соответствующие метки для VM соответствующих категорий (тем самым избежать возможности смешивания информации различного уровня доступа)

Решение позволяет избежать проблем вариантов 1 и 2



Самостоятельный продукт

«Сегмент-В.»



Совместное использование

«Сегмент-В.» + «Аккорд-В.»



Вариации исполнения и состав



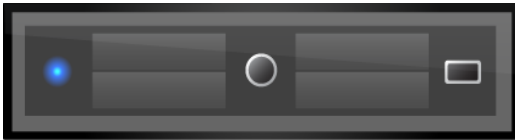
Программная

ISO образ

Аппаратная

Сервер Aquarius

+ ПО Управления



© VMware, Inc.

2 версии:

- НДСВ-2
- НДСВ-4

И/А в ВИ	(ЗСВ. 1)
Управление доступом	(ЗСВ. 2)
Регистрация событий	(ЗСВ. 3)
Управление миграцией	(ЗСВ. 6)
Сегментирование ВИ	(ЗСВ.10)
Вместе с «Аккорд-В.»	
Доверенная загрузка	(ЗСВ. 5)
Контроль целостности	(ЗСВ. 7)

Исключения*:

Управление потоками	(ЗСВ.4)
Резервирование	(ЗСВ.8)
Антивирусная защита	(ЗСВ.9)

**закрываются существующими решениями на рынке*



Ключевые моменты

Законченное решение

«Сегмент-В.» - самодостаточное решение. Требуется лишь настроить приобретенный сервер или «развернуть» новую VM. Отсутствуют скрытые затраты (например, на ОС).

Отказоустойчивое решение

«Сегмент-В.» поддерживает кластерную конфигурацию, что обеспечивает автоматическое переключение на резервный сервер в случае непредвиденных ситуаций.

Простое решение

«Сегмент-В.» поддерживает любые исполнения виртуальной инфраструктуры: VCSA / Linked Mode / Standalone ESXi. При этом решение не усложняет работу АВИ (отсутствуют какие-либо агенты).

Вопросы?

help@okbsapr.ru

