ОКБ АПР
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

Программно-аппаратный комплекс «Сегмент-В.»
(версия 1.3)

Руководство по установке

11443195.4012.069 98

Листов 98

Москва
2017

АННОТАЦИЯ

Настоящий документ является руководством по установке модуля разграничения доступа к vCenter и ESXi – программно-аппаратного комплекса (ПАК) «Сегмент-В.» v.1.3 (далее по тексту – «Сегмент-В.» или комплекс), предназначенного для защиты инфраструктуры виртуализации на основе VMware vSphere версий 5.1, 5.5, 6.0.

Документ предназначен для администраторов – должностных лиц, обладающих знаниями и полномочиями достаточными для того, чтобы настраивать и управлять инфраструктурой виртуализации VMware vSphere.

В документе приведены описания этапов установки и настройки комплекса «Сегмент-В.».

Перед установкой и эксплуатацией «Сегмент-В.» рекомендуется внимательно ознакомиться с настоящим руководством.

Применение модуля «Сегмент-В.» должно дополняться общими мерами предосторожности и физической безопасности.

ПРИНЯТЫЕ ТЕРМИНЫ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

Администратор БИ (или АБИ) – администратор безопасности информации, привилегированный пользователь - должностное лицо, имеющее особый статус и абсолютные полномочия (супервизора). Администратор БИ организует установку комплекса в ПЭВМ, настройку защитных механизмов комплекса в соответствии с правами доступа пользователей, осуществляет контроль за правильным использованием ПЭВМ с установленным комплексом и периодическое тестирование средств защиты комплекса.

Администратор ВИ (или АВИ) – администратор виртуальной инфраструктуры, привилегированный пользователь - должностное лицо, отвечающее за настройку и обслуживание виртуальной инфраструктуры.

АРМ - автоматизированное рабочее место.

Виртуальная машина (или ВМ) – полностью изолированный программный контейнер, который работает с собственной операционной системой и приложениями подобно физическому компьютеру.

Сервер виртуализации (или хост) – объект виртуальной инфраструктуры, предоставляющий доступ к платформе виртуализации (гипервизору) посредством команд управления.

Сервер управления виртуальной инфраструктурой (vCenter) – сервер со специализированным программным обеспечением, отвечающий за распределение нагрузки в автоматическом режиме, перемещение виртуальных машин (миграцию) и настройку всех компонентов виртуализации посредством посылки команд управления остальным элементам виртуальной инфраструктуры.

Сетевое устройство (сеть, группа портов) – сеть, разделяемая между хостами и/или виртуальными машинами; может быть физической (подключена к физической сетевой карте) или логической (VLAN).

Хранилище – виртуальное представление физического хранилища, является местом хранения файлов виртуальных машин. Хранилище скрывает особенности своей физической реализации и предоставляет единую модель для хранения виртуальных машин.

Пользователь – субъект доступа к объектам (ресурсам) виртуальной инфраструктуры.

Ошибки – информация, выводимая на дисплей, указывающая на неправильность действий, сбои, аварии комплекса.

Примечания – замечания в описании некоторых команд, содержащие рекомендации администратору БИ по порядку использования этих команд. Пояснения выделены мелким шрифтом.

Сообщения - информация, выводимая на дисплей, которая сообщает о действиях, требуемых от пользователя, о состоянии программы и о корректно завершенных действиях.

СОДЕРЖАНИЕ

1. Общие сведения

1.1. Назначение комплекса

Программно-аппаратный комплекс «Сегмент-В.» предназначен для защиты инфраструктур виртуализации, построенных на базе платформ виртуализации:

- VMware vSphere 5.1;
- VMware vSphere 5.5;
- VMware vSphere 6.0.

Комплекс представляет собой совокупность технических и программных средств, предназначенных для выполнения основных функций защиты от НСД на основе:

- идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации.
- управления доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре.
- регистрации событий безопасности в виртуальной инфраструктуре.
- управления перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных.
- разбиения виртуальной инфраструктуры на сегменты (сегментирования виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

1.2. Состав ПАК «Сегмент-В.»

1.2.1. Общие сведения

ПАК «Сегмент-В.» представляет собой комплекс программных и аппаратных средств, предназначенный для разграничения доступа пользователей к объектам инфраструктуры виртуализации VMware vSphere. При этом комплекс обеспечивает защиту от утечек информации, предоставляя возможность работы под одной учетной записью с различными сегментами виртуальной инфраструктуры (ВИ), запрещая их смешивание.

Основу комплекса составляет прокси-сервер, устанавливаемый в разрыв между vCenter сервером и рабочим местом администратора виртуальной инфраструктуры (АВИ).

Возможны два режима работы прокси-сервера:

- **двухинтерфейсный режим** – для работы с комплексом необходимо выделение двух сегментов сети: внешней и внутренней (организованы разные подсети, рисунок 1);

– **одноинтерфейсный режим** – для работы с комплексом не требуется выделение двух сегментов сети: и АРМ АВИ, и vCenter/ESXi, и прокси-сервер принадлежат одному сегменту сети (рисунок 2).

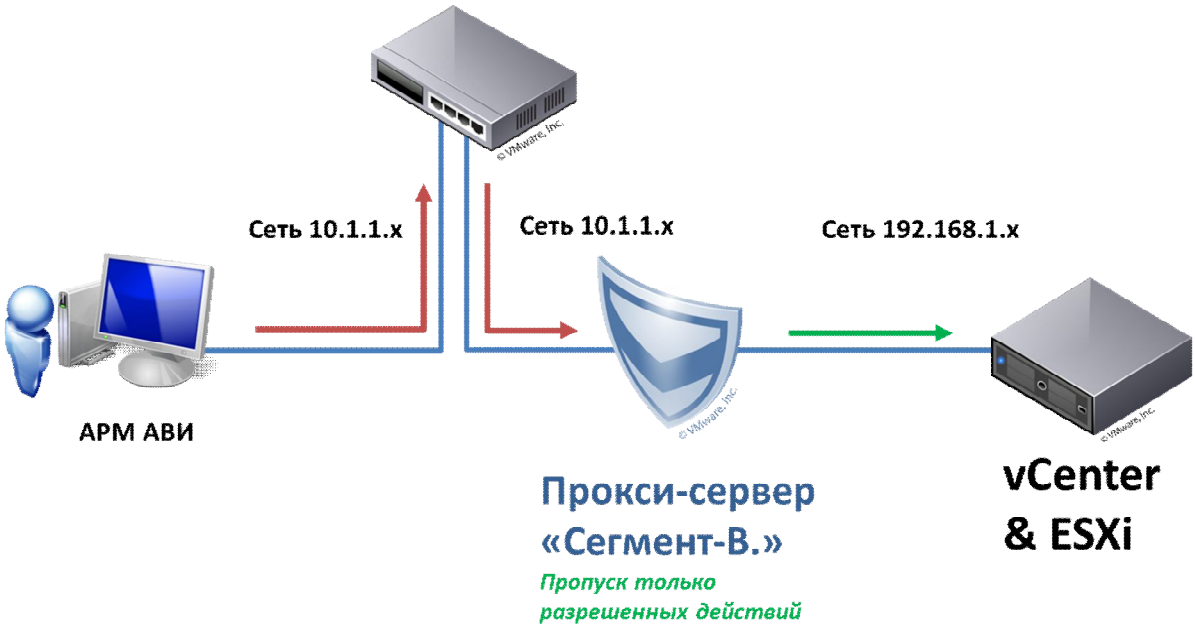


Рисунок 1 - Схема организации сети при использовании «Сегмент-В.» (двухинтерфейсный режим)

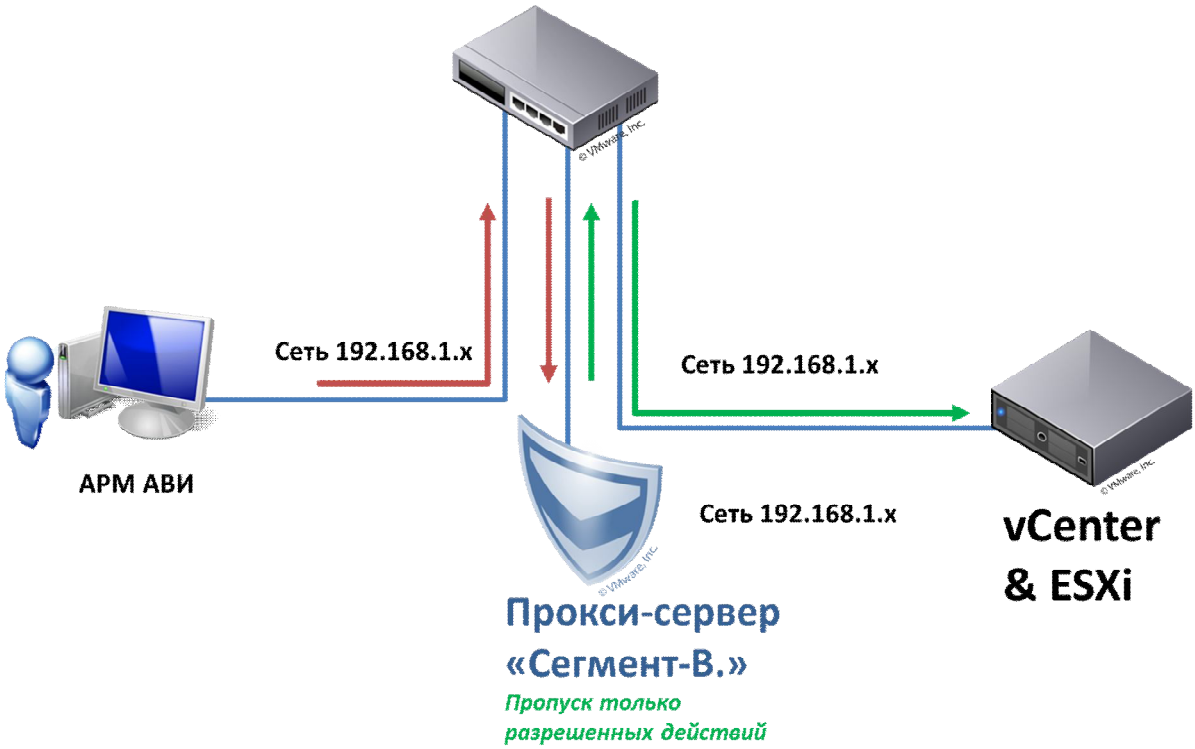


Рисунок 2 - Схема организации сети при использовании «Сегмент-В.» (одноинтерфейсный режим)

Прокси-сервер представлен в следующих исполнениях:

1) аппаратное исполнение: физический сервер с предустановленным ПО;
2) программное исполнение: ISO-образ, предназначенный:

- для установки в ВМ;
- для установки на сторонний сервер организации-Заказчика.

ВНИМАНИЕ! В случае использования варианта исполнения, предназначенного для установки на сторонний сервер организации-Заказчика, следует учитывать, что аппаратная часть стороннего сервера должна быть совместима с базовой сборкой CentOS 6.5 и поддерживать работу с «Аккорд-АМДЗ».

«Сегмент-В.» не требует установки дополнительного ПО на АРМ администраторов виртуальной инфраструктуры и позволяет «бесшовно» интегрировать систему защиты в инфраструктуру виртуализации vSphere. При этом поддерживается режим Linked mode для vCenter, а также сохраняется возможность использования vCenter в качестве ВМ (в том числе VCSA – VMware vCenter Server Appliance).

ПАК «Сегмент-В.» состоит из аппаратных и программных средств.

1.2.2. Аппаратные средства

Аппаратные средства ПАК «Сегмент-В.» включают в себя следующие компоненты:

- физический сервер Aquarius T40 S24 (опционально; возможны варианты использования собственных серверов);
- установленная в сервер (Aquarius T40 S24 или собственный сервер) плата «Аккорд-АМДЗ» семейства GX (подробнее см. документацию на «Аккорд-АМДЗ»);
- usb -> Ethernet адаптер – поставляется (опционально) в составе решения для использования функционала отказоустойчивости (High Availability).

1.2.3. Программные средства

Программные средства ПАК «Сегмент-В.» включают в себя следующие компоненты:

1) модули СПО «Сегмент-В.»:

а) *ПО управления комплексом* **Segment-V. (exe)**, устанавливаемое на АРМ Администратора БИ (АРМ АБИ), предназначенное для настройки разграничения доступа к виртуальной инфраструктуре. Может устанавливаться отдельно или как расширение «СПО Аккорд-В.». Включает в себя следующие утилиты:.

- «Segment-V.» – утилита управления комплексом «Сегмент-В.»;
- «Installer-V.» – утилита настройки соединения с vCenter, а также точек сбора событий с прокси-серверов (в случае совместного использования с «Аккорд-В.» используется также для установки агентов «Аккорд-В.» на ESXi);
- «LogViewer-V.» – утилита просмотра зарегистрированных событий.

б) *сервис регистрации событий,* устанавливаемый на АРМ АБИ или в ОС отдельного сервера (рекомендуемый вариант), предназначенный для сбора событий инфраструктуры VMware vSphere, а также с агентов «Аккорд-В.» на ESXi (для установки сервиса регистрации событий в ОС предназначена вспомогательная утилита LogServiceInstaller);

2) Segment-V. Module (iso) – *прокси-сервер* – специально настроенный образ операционной системы, устанавливаемый на физический сервер или внутрь ВМ, предназначенный для перехвата команд управления vCenter/ESXi и организации разграничения доступа на основе заранее заданных правил. Segment-V. Module включает в себя СПО *«Аккорд-X»*, применение которого на прокси-сервере обеспечивает выполнение процедур идентификации и аутентификации пользователей root и accord, а также выполнение динамического контроля целостности исполняемых файлов из состава ПАК «Сегмент-В.».

Примечание: В случае программного исполнения (ВМ), в силу невозможности использования контроллеров «Аккорд-АМДЗ», рекомендуется использовать ПАК «Аккорд-В.».

1.3. Технические условия применения комплекса

Для установки комплекса «Сегмент-В.» требуется следующий минимальный состав технических и программных средств:

- наличие инфраструктуры виртуализации, построенной на базе одной из поддерживаемых платформ виртуализации, список которых приведен в подразделе 1.1;
- реализация АРМ АБИ в виде физической машины под управлением ОС Windows, в которой установлены:
  - программная платформа Microsoft .NET Framework 3.5;
  - распространяемые пакеты (Redistributable Package) Microsoft Visual C++ 2008 (x86) и Microsoft Visual C++ 2010 (x86)[1];
- наличие ресурсов на сервере для создания ВМ и установки в нее ОС прокси-сервера или наличие x86-64 совместимого сервера[2] с требованиями, аналогичными предъявляемым к ВМ.

Минимальные системные требования к ВМ указаны в таблице 1.

Таблица 1 - Минимальные системные требования к ВМ

	Работа в одноинтерфейсном режиме	Работа в двухинтерфейсном режиме
1	двухъядерный процессор, 2 Гб ОЗУ, 16 Гб свободного места на диске	
2	USB контроллер – для подключения устройства хранения с сертификатами	
3	одна сетевая карта (E1000) – в случае использования одного прокси-сервера	две сетевые карты (E1000) – в случае использования одного прокси-сервера
4	две сетевые карты (E1000) – в случае использования механизмов резервирования	три сетевые карты (E1000) – в случае использования механизмов резервирования

[1)] Данные компоненты включены в комплект поставляемого ПО ПАК «Сегмент-В.»

[2)] В зависимости от варианта исполнения ПАК «Сегмент-В.», может входить в комплект поставки

Для корректной работы сервиса регистрации событий может потребоваться (подробнее см. 3.8.3), чтобы АРМ, на котором он запущен, был включен в домен (если АРМ совпадает с vCenter, то возможно использование локальной учетной записи).

Необходимо организовать схему подключения, при которой все запросы к vCenter и ESXi будут проходить через прокси-сервер (чтобы не существовало путей в обход модуля «Сегмент-В.»).

2. Начало работы

2.1. Архитектура системы безопасности

ВНИМАНИЕ! АРМ АБИ не может быть реализовано в виде виртуальной машины.

Перед началом установки и настройки ПАК «Сегмент-В.» необходимо определиться с архитектурой развертываемой инфраструктуры виртуализации, а также провести ряд подготовительных мероприятий.

Для этого следует ответить на следующие вопросы:

1. В виртуальной инфраструктуре используется vCenter или она построена на отдельных (standalone) ESXi? Применяются ли vCenter в режиме Linked Mode?

В случае если инфраструктура виртуализации построена на отдельных ESXi (более одного) или в ней используются vCenter, связанные режимом Linked Mode, при инициализации модуля на прокси-сервере необходимо включить режим Linked Mode (подробнее см. 3.5.2, пункт 3. Настройка сетевых интерфейсов).

Примечание: В случае нескольких несвязанных vCenter необходимо использовать отдельные прокси-серверы.

2. Каким образом, в случае использования vCenter, предполагается ограничить доступ АВИ к ESXi?

В силу того что уникальные идентификаторы одних и тех же объектов при доступе через ESXi и через vCenter различаются, рекомендуется использовать только один тип доступа АВИ к виртуальной инфраструктуре, а второй – блокировать (в первую очередь, для упрощения процесса настройки).

Примеры реализации:

1) использование механизма Lockdown Mode (примечание, «Сегмент-В.» позволяет ограничивать использование данного механизма администраторами ВИ);

2) перенаправление трафика управления ESXi через прокси-сервер и блокирование входа учетным записям пользователей, зарегистрированных на ESXi.

3. Совпадают ли АРМ АБИ и АРМ АВИ, или для работы Администратора БИ предполагается отдельное АРМ?

Рассмотрим вариант, когда АРМ АВИ/АБИ совмещено и на нем установлено СПО «Сегмент-В.».

ВНИМАНИЕ! **На АРМ АБИ** (вне зависимости от того, совмещен он с АРМ АВИ или нет) для осуществления разграничения доступа к СПО управления комплексом «Сегмент-В.» и ПО управления виртуальной инфраструктурой

должны быть установлены «Аккорд-АМДЗ» и ПАК «Аккорд-Win32»/ ПАК «Аккорд-Win64».

При такой реализации возможны два варианта работы:

1) АВИ и АБИ работают локально на данном СВТ;

2) АВИ и АБИ работают удаленно, подключаясь к СВТ по протоколам RDP или ICA. В таком случае, при использовании СПО разграничения доступа (ПАК «Аккорд-Win32 TSE»/ ПАК «Аккорд-Win64 TSE») на АРМ, с которого будет происходить подключение, должен быть установлен терминальный клиент «Аккорд-ТК».

При этом на совмещенном АРМ необходимо чтобы:

- доступ к ПО администрирования ПАК «Аккорд-Win32 TSE»/ ПАК «Аккорд-Win64 TSE», ПО «Сегмент-В.» был только у АБИ;
- доступ к vClient был у АВИ (при необходимости, и у АБИ).

Примечание: пример настройки разграничения доступа на совмещенном АРМ АБИ/АВИ см в разделе 3.10.

4. Какие средства будут использоваться для перенаправления трафика, идущего на защищаемые сервера через прокси-сервер?

Требование к реализации подключений к vCenter через прокси-сервер «Сегмент-В.» может быть выполнено различными способами, в частности:

- настройкой route-map на оборудовании Cisco;
- прописыванием маршрутов в командной строке;
- указыванием IP-адреса прокси-сервера в качестве default gateway.

Подробнее с механизмами реализации можно ознакомиться в подразделе 3.11.

5. Прокси-сервер предполагается в аппаратном исполнении или в качестве ВМ?

Вне зависимости от варианта исполнения прокси-сервера необходимо предварительно выделить:

- внешнюю сеть, из которой будут подключаться АВИ;
- внутреннюю сеть – сеть управления, которая предназначена для «management»-трафика vCenter и ESXi.

Дополнительно (опционально) рекомендуется предварительно настроить правила маршрутизации (примеры см. в подразделе 3.11).

ВНИМАНИЕ! Вне зависимости от варианта исполнения прокси-сервера (аппаратное или ВМ) рекомендуется заранее записать MAC-адреса сетевых карт, т.к. эти данные потребуются при первоначальной инициализации!

В случае аппаратного исполнения прокси-сервера необходимо выделить место в стойке под сервер, а также, в случае необходимости, подвести дополнительную сеть для удаленного управления сервером.

Поскольку аппаратное исполнение прокси-сервера поставляется с комплексом «Аккорд-АМДЗ» (ТУ 4012-038-11443195-2011), перед началом работы необходимо ознакомиться с базовыми принципами работы с ним (см. комплект эксплуатационной документации, входящий в комплект поставки «Аккорд-АМДЗ»).

В случае установки прокси-сервера в ВМ необходимо создать портгруппы для внешней и внутренней сетей (и сети отказоустойчивости – в случае необходимости), а также создать саму ВМ с ресурсами, указанными в подразделе 1.3.

6. Будет ли осуществляться резервирование/отказоустойчивость прокси-сервера?

Существуют различные способы построения отказоустойчивого решения (в том числе для различных целей). Под рассматриваемой отказоустойчивостью подразумевается защита от сбоев оборудования. Если обеспечение отказоустойчивости будет осуществляться с помощью средств «Сегмент-В.», то требуются два прокси-сервера, каждый из которых имеет:

- три сети (в случае исполнения на ВМ) или
- три сетевых адаптера (в случае аппаратного исполнения).

Подробнее см. подраздел 3.6.

7. «Сегмент-В.» используется отдельно или совместно с ПАК «Аккорд-В.»?

ВНИМАНИЕ! Совместная установка «Сегмент-В.» и «Аккорд-В.» возможна только при совпадении версий их дистрибутивов.

Если предполагается совместное использование «Сегмент-В.» и «Аккорд-В.», необходимо сначала произвести установку «Аккорд-В.», изучив соответствующую документацию, а затем перейти к установке «Сегмент-В.».

8. Каким образом будет осуществляться сбор событий? В случае использования средств «Сегмент-В.» где будет располагаться сервис регистрации событий: на vCenter/ на отдельном АРМ (например, на АРМ АБИ)/ в ВМ)?

В состав комплекса «Сегмент-В.» входит сервис регистрации событий, предназначенный для сбора событий:

- с vCenter;
- с прокси-сервера «Сегмент-В.».

Кроме того, события «Сегмент-В.» и агентов «Аккорд-В.» на ESXi также дублируются в syslog. В связи с этим, если в инфраструктуре используются централизованные системы регистрации событий (в том числе умеющие собирать события от vCenter), от сервиса регистрации событий можно отказаться.

В случае использования сервиса регистрации событий комплекса «Сегмент-В» возможны различные варианты его расположения:

1. На одном АРМ с АРМ АБИ;
2. На отдельном АРМ от АРМ АБИ (в том числе это может быть и vCenter).

ВНИМАНИЕ! При определении месторасположения сервиса регистрации событий необходимо учитывать следующее требование: необходимо (в том числе организационными мерами) *обеспечить бесперебойность работы АРМ, на котором будет установлен сервис регистрации событий* (данный сервис никогда не должен выключаться), поскольку в противном случае события, полученные с vCenter, могут быть пропущены.

2.2. Пример развертываемой инфраструктуры

Пример типовой инфраструктуры (до внедрения СЗИ) представлен на рисунке 3.

ВНИМАНИЕ! В процессе создания виртуальных машин следует учитывать, что имя виртуальной машины не должно содержать символов кириллицы.

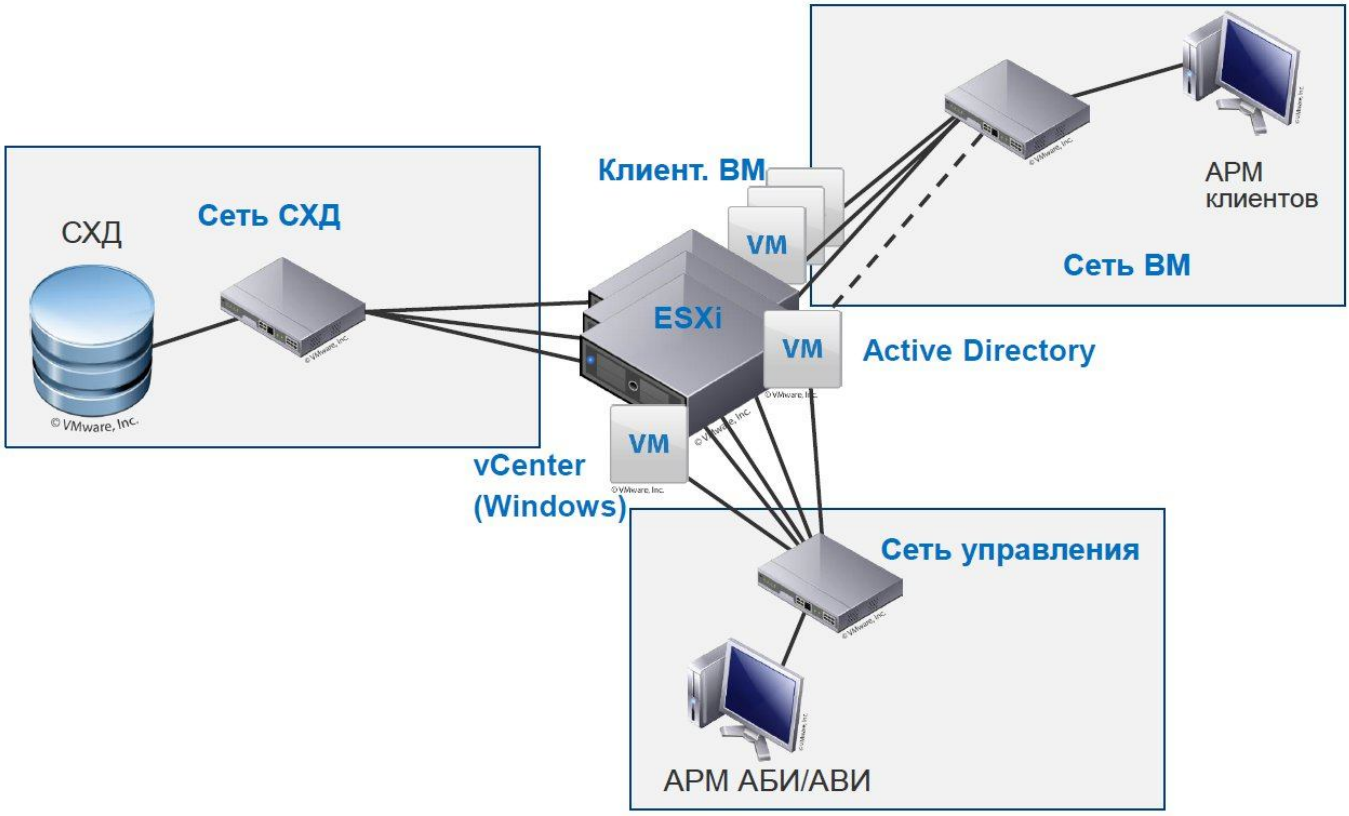


Рисунок 3 - Пример развертываемой инфраструктуры

2.3. Особенности работы с комплексом

При работе с «Сегмент-В.» необходимо учитывать следующие особенности:

- действия пользователей разграничиваются только при организации доступа через vClient/PowerCLI/vCLI; в случае доступа с помощью WebClient разграничения не происходит, поэтому следует заблокировать доступ к ESXi/vCenter через WebClient (соответствующая настройка «Сегмент-В.» задается при первоначальной инициализации модуля);
- доступ к отдельным ESXi, если они развернуты и работают совместно с vCenter, по умолчанию не разграничивается (предполагается использование Lockdown Mode, подробнее см. подраздел 2.1 пункт 8). При этом возможен вариант защиты Standalone ESXi (без vCenter), для которого работает только дискреционная политика разграничения доступа;
- разграничение доступа при работе со снапшотами ВМ, назначение прав в vClient осуществляется с помощью полного запрещения/разрешения, а не на основе мандатной политики;
- оповещения о запрете доступа не появляются в vClient при запрете включения ВМ, а также при изменении настроек портгрупп;
- для незарегистрированных в ПО «Сегмент-В.» объектов их имена в событиях не отображаются (по умолчанию такие действия также блокируются) – указывается только тип объектов.

3. Установка и настройка компонентов комплекса

3.1. Общие сведения

ПО, входящее в состав комплекса «Сегмент-В.», должно быть установлено на АРМ АБИ и прокси-сервер следующим образом (см. рисунок 4):

1)**на АРМ АБИ** должна быть установлена система администрирования «Сегмент-В.»;

2)**на прокси-сервер** «Сегмент-В.» устанавливается предварительно настроенная операционная система, содержащая модули принятия решения, сервис работы с событиями и сервис настройки ПО «Сегмент-В.».

Рисунок 4 - Общая схема решения

3.2. Порядок установки и настройки комплекса «Сегмент-В.»

Установка и настройка компонентов ПАК «Сегмент-В.» осуществляется в соответствии с порядком, указанным в таблице 2.

Таблица 2 – Порядок установки и настройки ПАК «Сегмент-В.»

№	Где найти подробное описание	Где выполняется действие		
		Общее	АРМ АБИ	Прокси-сервер
1	Подраздел 3.3	Предварительные действия		
2	Подраздел 3.4		Установка ПО управления комплексом «Сегмент-В.»	
3	Подраздел 3.5			Установка «Сегмент-В.» на прокси-сервер
4	Подраздел 3.6		Настройка отказоустойчивости решения	Настройка отказоустойчивости решения
5	Подраздел 3.7			Установка и конфигурирование СПО «Аккорд-Х»
6	Подраздел 3.8		Настройка ПО управления комплексом «Сегмент-В.»	
7	Подраздел 3.9		Настройка разграничения доступа к ВИ	
8	Подраздел 3.10		Настройка разграничения доступа на совмещенном АРМ АБИ/АВИ	
9	Подраздел 3.11	Пример настройки сетевого оборудования (или маршрутизации в сети)		

3.3. Предварительные действия

После рассмотрения базовых вопросов в разделе 2 (определения расстановки элементов защиты и их режима работы) для уменьшения затрачиваемого времени в процессе развертывания необходимо провести ряд дополнительных превентивных действий:

0. Рассмотреть вопросы из раздела 2, если он был пропущен.

1. Предварительно выделить IP-адреса для прокси-сервера:

а) в двухинтерфейсном режиме (рисунок 5):

- внешний интерфейс (по одному на каждый сервер – интерфейсы 1, 2);
- внутренний интерфейс (по одному на каждый сервер – интерфейсы 4, 5);

- виртуальный внутренний и внешний интерфейсы в режиме отказоустойчивости (общие – интерфейсы 3, 6) – необходимы при обеспечении отказоустойчивости прокси-сервера;

б) в одноинтерфейсном режиме (рисунок 6):

- интерфейсы в сети для каждого сервера – интерфейсы 1, 2;
- виртуальный интерфейс в режиме отказоустойчивости (общий – интерфейс 3) – необходим при обеспечении отказоустойчивости прокси-сервера;

в)создать сеть репликации между прокси-серверами (при использовании режима отказоустойчивости). Рекомендуется объединять серверы напрямую. Выделить в созданной сети по одному IP-адресу для каждого прокси-сервера (интерфейсы 7, 8 на рисунках 5 и 6).

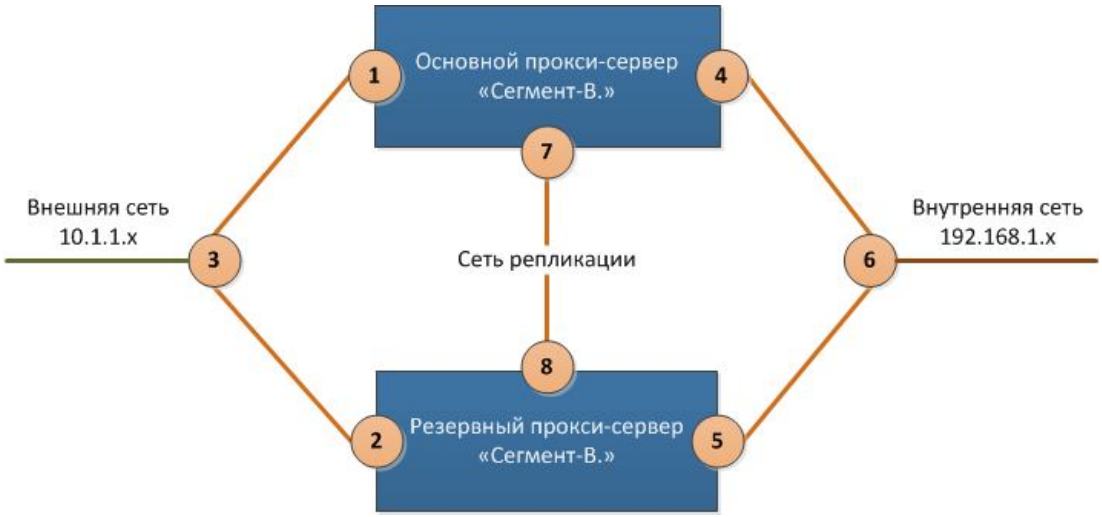


Рисунок 5 - Необходимые IP-адреса (двухинтерфейсный режим)

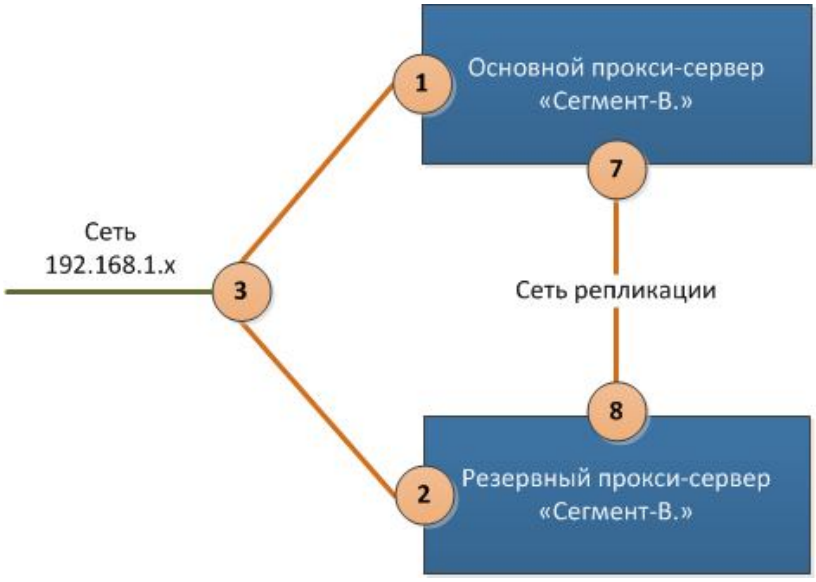


Рисунок 6 - Необходимые IP-адреса (одноинтерфейсный режим)

2. Настроить маршрутизацию в соответствии с выбранным механизмом (примеры в подразделе 3.11).

3. Создать необходимых для начальной настройки и работы комплекса пользователей в рамках VMware vSphere:

- **локального (обязательно!) - accord**. Возможны следующие варианты выполнения процедуры создания локального пользователя:

  – в случае vCenter на Windows – создать пользователя в ОС;

  – в случае VCSA версий 5.x – в shell использовать команду *useradd accord –p [пароль]*;

  – в случае VCSA версии 6 – в shell использовать команду *user.add –username accord –password*.

  – в случае использования отдельных (standalone) ESXi – создать пользователя через соответствующую вкладку в vClient (Local Users & Groups).

  В рамках vSphere необходимо назначить пользователю accord права «Read Only» с наследованием на корневой каталог (vCenter).

ВНИМАНИЕ! Первоначальный запуск утилит управления комплексом возможен только от имени учетной записи accord. Ее создание является обязательным условием установки и настройки комплекса «Сегмент-В.».

- **доменного (необязательно)[1] – logservice** (или любое другое имя). Создание этого пользователя необходимо в том случае, если планируется использование сервиса регистрации событий в составе комплекса «Сегмент-В.», – от его имени будет работать сервис (сервисная учетная запись).

  В рамках vSphere назначить этому пользователю права «Read Only» с наследованием на корневой каталог (на vCenter, в случае его использования, или на каждый из отдельных ESXi). Также рекомендуется заранее создать пользователей АБИ/АВИ (не важно, будут они локальными или доменными).

4. Выделить защищаемые сегменты (см. пример в подразделе 3.9) и описать входящие в них объекты (ВМ/шаблоны/портгруппы/хранилища/хосты). Провести соответствие пользователей доступным им сегментам. Указать, какие им отведены роли, и в соответствии с этим указать перечень прав, необходимых и достаточных пользователю для выполнения их должностных обязанностей.

5. Подготовить USB-носитель (файловая система NTFS) для копирования сертификатов.

6. В заключение, настоятельно рекомендуется сформировать способ именования объектов в виртуальной инфраструктуре (naming convection) в соответствии с сегментацией и придерживаться его в дальнейшем (это упростит

[1] подробнее см. 3.8.3

не только настройку через ПО управления «Сегмент-В.», но и работу с виртуальной инфраструктурой).

Например: для всех элементов, относящихся к персональным данным, использовать приставку *_PD (Datastore_PD, WinServer_VM_PD, Net_PD)*

3.4. Установка и настройка ПО управления комплексом

3.4.1. Начало процедуры установки

ВНИМАНИЕ! Предполагается, что система виртуализации уже установлена и соответствующим образом сконфигурирована администратором виртуальной инфраструктуры.

ВНИМАНИЕ! ПО управления «Сегмент-В.» использует для соединения протокол SSL, поэтому, если время между ним и прокси-сервером рассинхронизировано, компоненты не смогут установить соединение между собой!

В случае если время не синхронизировано, необходимо на прокси-сервере переключиться на новую консоль (<Alt>+<F2>) и выполнить вход от имени системной учетной записи root. После успешной операции логина следует выполнить команду *date –s [верное время]*. Например, *«date -s="20151019 09:17:00"»*. После этого завершить сессию, выполнив команду *exit*.

Чтобы начать установку системы управления, необходимо запустить с правами администратора исполняемый файл **Segment-V.exe**, который находится на диске с дистрибутивом, и дать согласие на внесение программой изменений в компьютере.

Вначале на экран выводится окно выбора языка (рисунок 7). В данный момент поддерживается вариант инсталляции (и дальнейшей работы всех программных компонентов) на двух языках – русском и английском. Необходимо определиться с выбором и нажать кнопку <OK>.

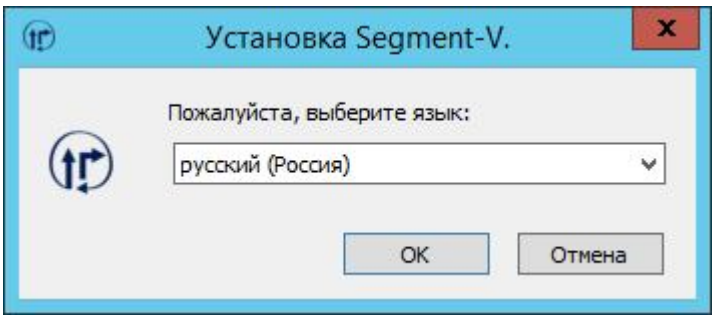


Рисунок 7 - Выбор языка

После выбора языка начнется процесс установки ПО.

В появившихся в процессе установки окнах установки распространяемого пакета Microsoft Visual C++ 2010 (x86)[1] следует ознакомиться с лицензионным соглашением, принять его посредством установки галочки в соответствующем поле, нажать кнопку <Установить> (рисунок 8), дождаться окончания процесса установки пакета и нажать кнопку <Готово> (рисунок 9).

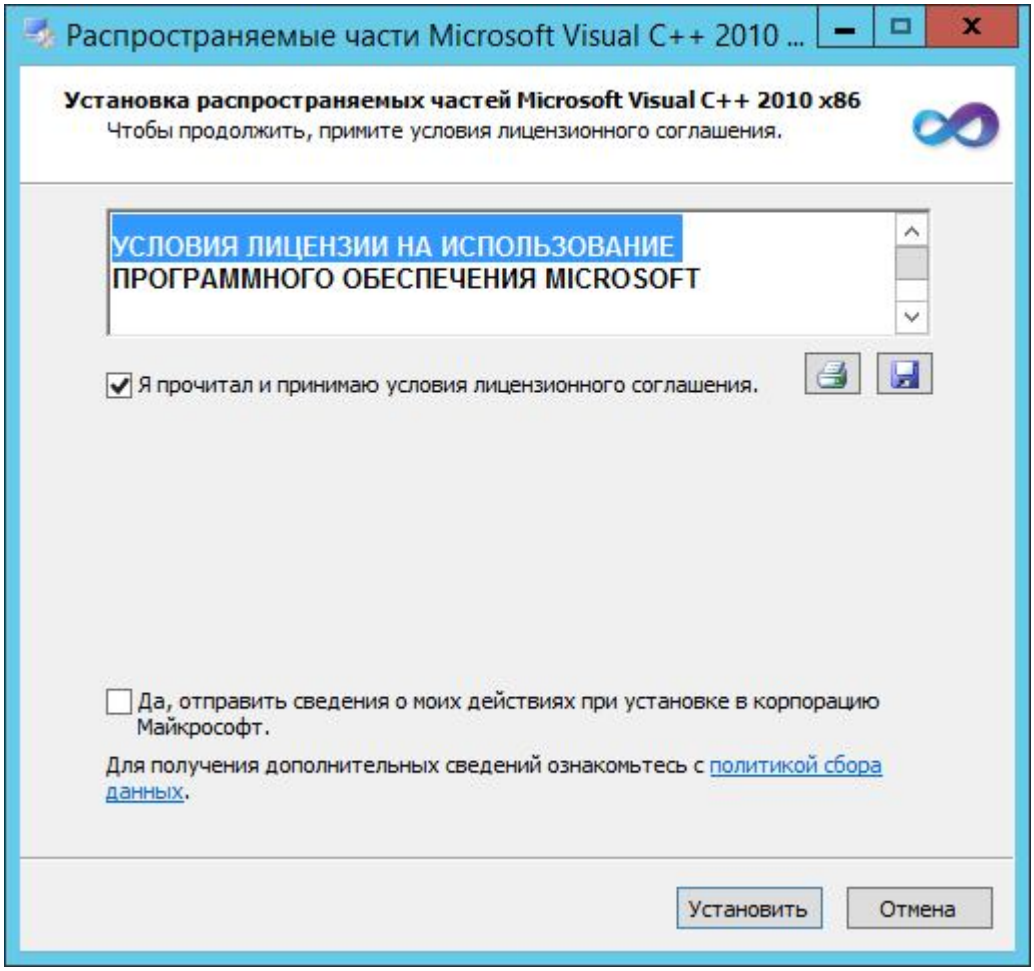


Рисунок 8 - Установка распространяемых пакетов Windows

[1)] Распространяемые пакеты (Redistributable Package) Microsoft Visual C++ 2008 (x86) и Microsoft Visual C++ 2010 (x86) включены в комплект поставляемого ПО ПАК «Сегмент-В.»

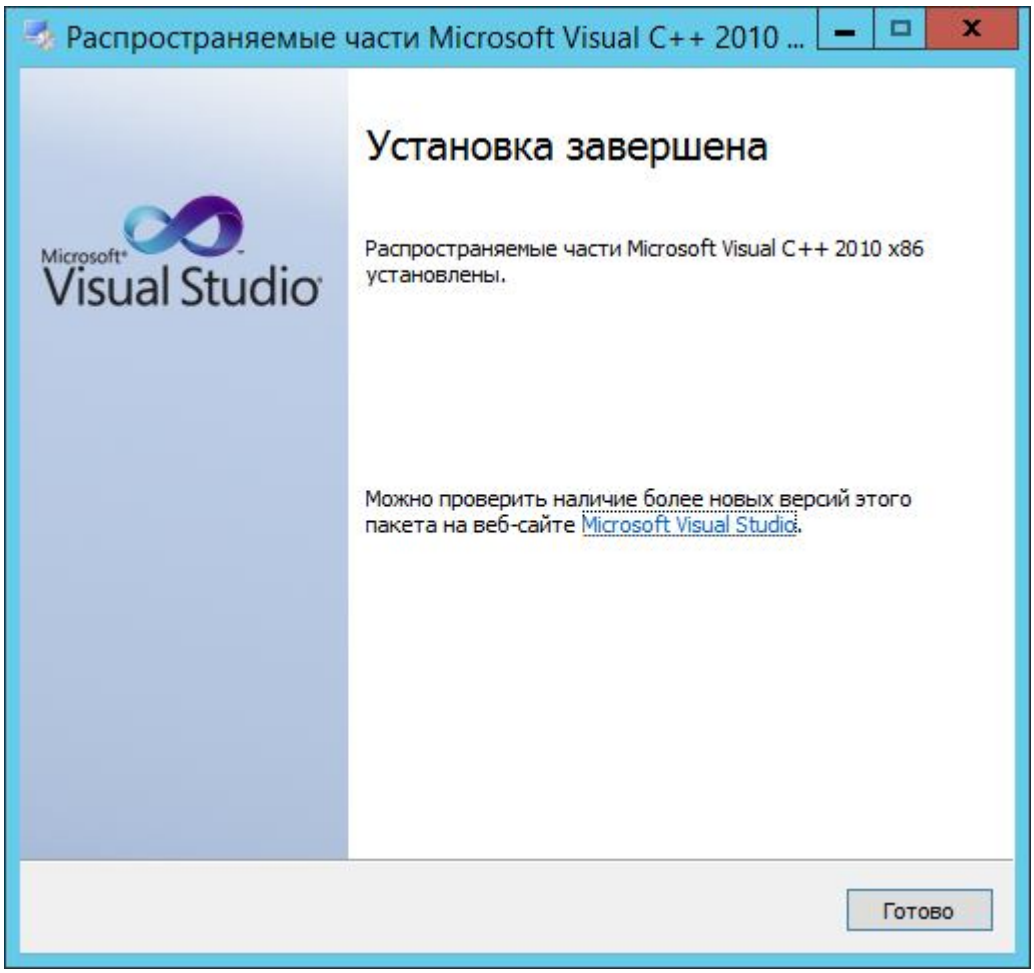


Рисунок 9 - Завершение процедуры установки распространяемых пакетов Windows

Далее следует перейти к процедуре установки модулей «Сегмент-В.».

3.4.2. Установка модулей «Сегмент-В.»

В появившемся далее окне следует ознакомиться с лицензионным соглашением, принять его посредством установки галочки в соответствующем поле и нажать кнопку <Далее> (рисунок 10).

Рисунок 10 - Окно принятия условий лицензионного соглашения

Далее следует выбрать режим установки (рисунок 11).

Установка возможна в двух вариациях: в качестве самостоятельного продукта или в качестве расширения «Аккорд-В.».

ВНИМАНИЕ! Установка «Сегмент-В.» в качестве расширения «Аккорд-В.» возможна только после установки «Аккорд-В.» и только при совпадении версий сборок «Аккорд-В.» и «Сегмент-В.».

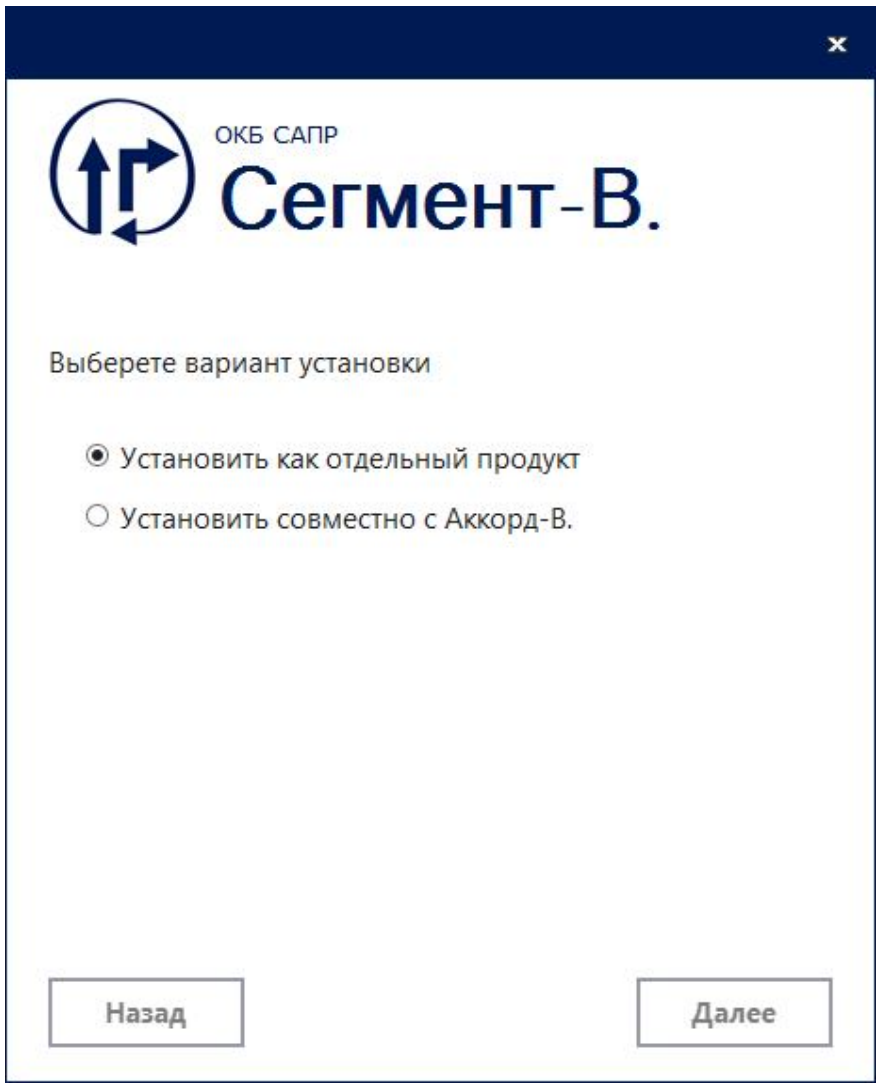


Рисунок 11 - Выбор режима установки

Далее необходимо указать путь к каталогу установки (рисунок 12).

По умолчанию установка всех программных компонентов выполняется в каталог **C:\Program Files (x86)\OKB SAPR\Segment-V**.

В случае установки **совместно с «Аккорд-В.»** в качестве каталога установки должен быть выбран каталог, в котором расположен «Аккорд-В.». Установка «Аккорд-В.» по умолчанию выполняется в каталог **C:\Program Files (x86)\OKB SAPR\Accord-V.**

Каталог, предлагаемый по умолчанию, может быть изменен посредством ручного редактирования или задан с помощью стандартного диалога ОС Windows, вызываемого по нажатии кнопки <Обзор…>. Если указанный каталог не существует, он будет создан программой установки автоматически.

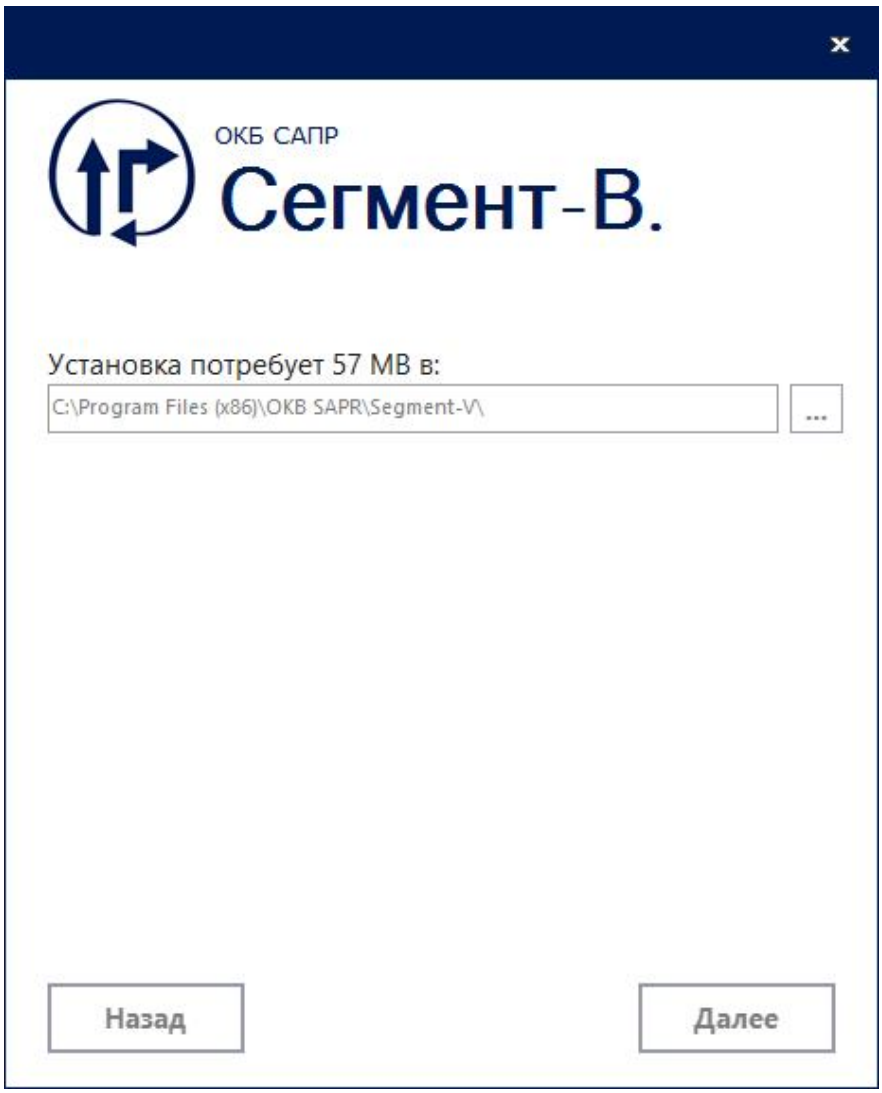


Рисунок 12 - Выбор пути установки

Далее необходимо выбрать компоненты устанавливаемого ПО и нажать кнопку <Установить> (рисунок 13).

Если в качестве расположения сервиса регистрации событий было выбрано отдельное АРМ (не АРМ АБИ), на данном этапе следует выполнить установку ПО без сервиса регистрации событий (данная процедура будет выполнена позже – см. 3.8.3).

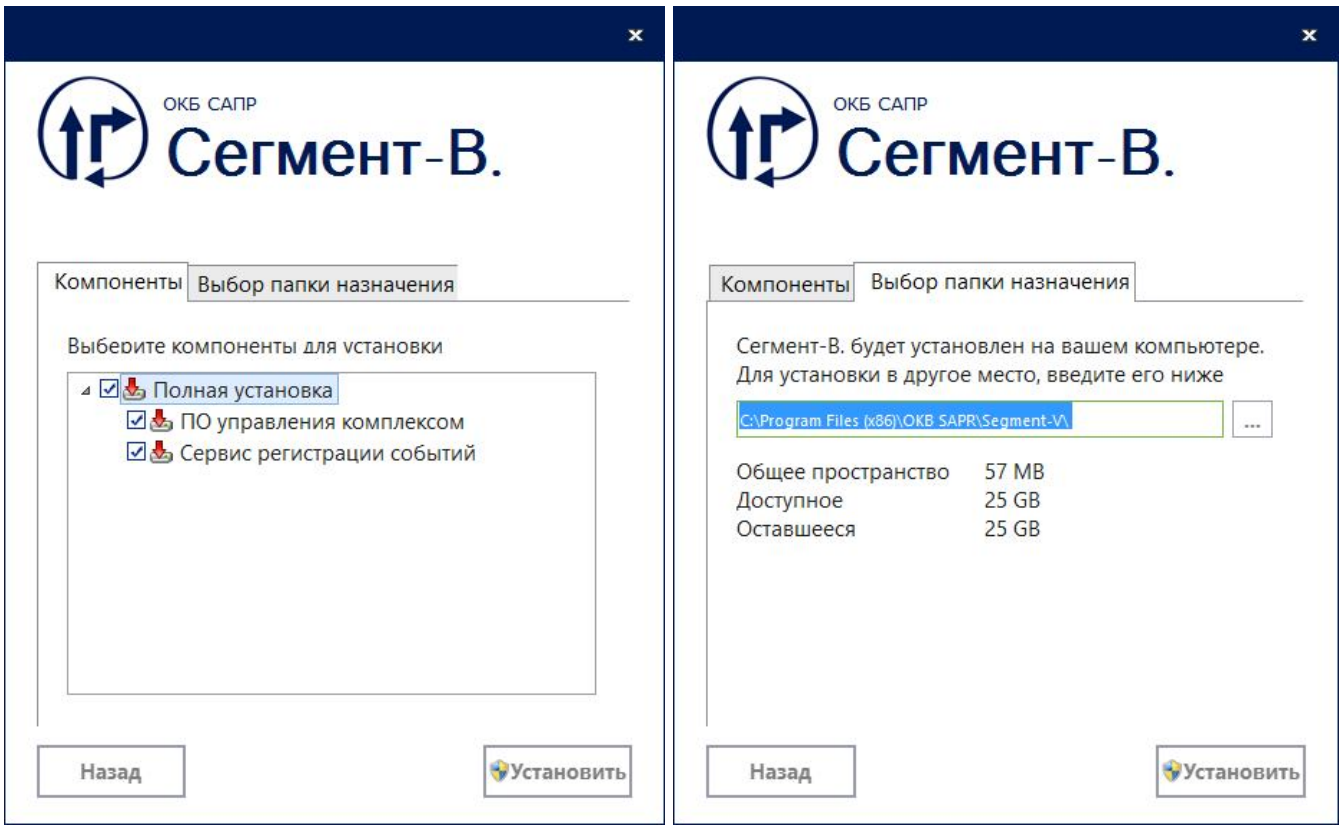


Рисунок 13 - Выбор компонентов установки и папки назначения

Начнется установка ПО, по завершении которой на рабочем столе ОС создаются ярлыки следующих утилит:

- **«Installer-V.»** – утилита настройки соединения с vCenter, а также точек сбора событий с прокси-серверов (в случае совместного использования с «Аккорд-В.» используется также для установки агентов «Аккорд-В.» на ESXi);
- **«Segment-V.»** – утилита управления комплексом «Сегмент-В.»;
- **«LogViewer-V.»** – утилита просмотра зарегистрированных событий.

По окончании процесса установки на экран выводится окно с соответствующим сообщением, в котором следует нажать кнопку <Готово>.

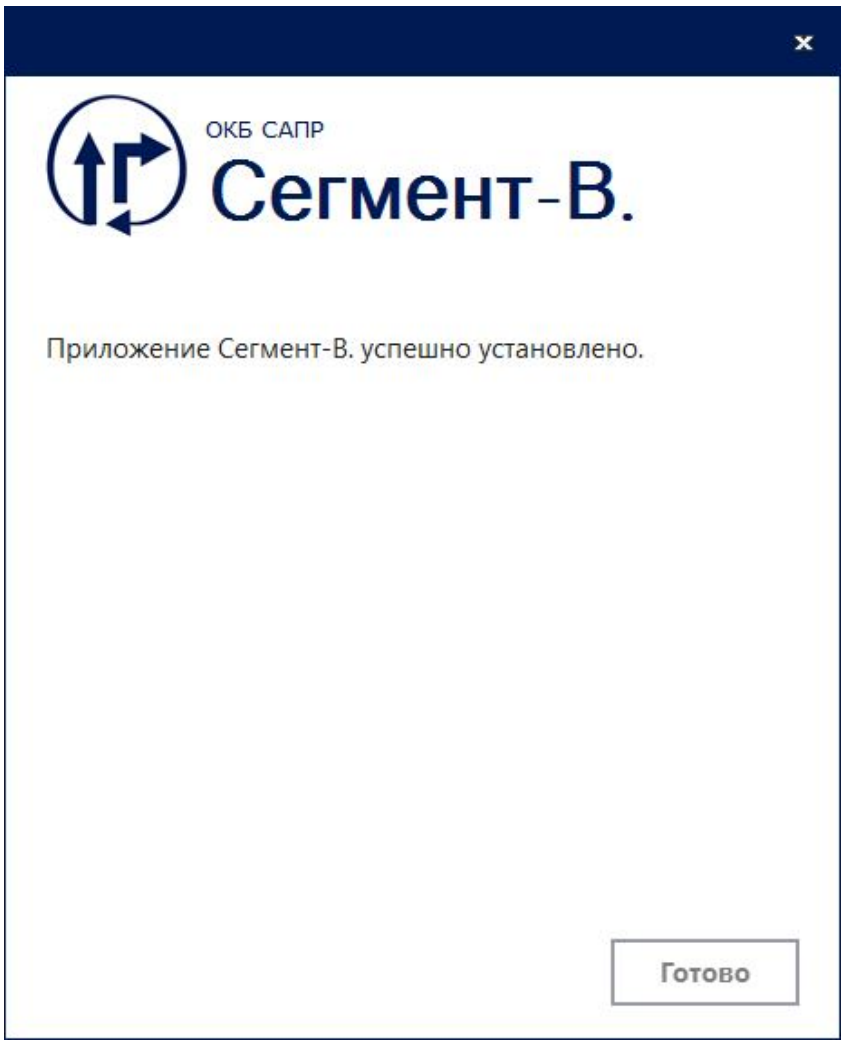


Рисунок 14 - Окончание процесса установки ПО «Сегмент-В.»

После установки необходимо настроить права доступа администраторам безопасности, учитывая следующее:

1) пользователь, запускающий «LogViewer-V.», должен иметь права на запись в файл LogConfig.xml и чтение/исполнение файлов в каталоге с установленным ПО «Сегмент-В.»;

2) пользователь, запускающий «Segment-V.», должен иметь права на запись в ManagedDatabase.db, на чтение и создание файлов в каталоге с установленным ПО «Сегмент-В.»;

3) запуск утилиты установки сервиса (LogServiceInstall) требует административных прав;

4) пользователь, запускающий «Installer-V.», должен иметь права на запись в файл Config.xml, а также на чтение/исполнение файлов в каталоге с установленным ПО «Сегмент-В.»;

5) для входа в «Segment-V.» должна использоваться учетная запись АБИ, имеющая полный доступ к инфраструктуре в режиме только для чтения (для vCenter в разделе настроек «Permissions» следует установить тип доступа «Read only» с флагом «Propagate»).

3.4.3. Предъявление лицензии на работу с комплексом

Для работы с ПО «Сегмент-В.» требуется лицензия. Она выдается производителем и поставляется на компакт-диске в составе комплекта поставки продукта или иным способом (файл license-v.lic).

Для предъявления лицензии потребуется скопировать с диска файл лицензии license-v.lic в корень папки с установленным ПО: **C:\Program Files (x86)\OKB SAPR\Segment-V** (или C:\Program Files (x86)\ OKB SAPR\Accord-V).

Подробнее о системе лицензирования см. в разделе 5.

3.4.4. Сбор необходимых сертификатов на USB-носитель

Перед тем как перейти к установке ПО на прокси-сервер, необходимо подготовить выделенный ранее USB-носитель (он должен использовать файловую систему NTFS!). Для этого требуется скопировать на устройство два вида сертификатов: сертификаты «Сегмент-В.» и сертификаты vCenter.

Таким образом, данный этап состоит из следующих частей:

А) Копирование сертификатов «Сегмент-В.».

Следует выполнить вход на АРМ АБИ и перейти в папку, в которую был установлен «Сегмент-В.»:

- по умолчанию: C:\Program Files (x86)\OKB SAPR\Segment-V;
- в случае установки совместно с «Аккорд-В.»: C:\Program Files (x86)\ OKB SAPR\Accord-V.

Далее необходимо создать сертификаты, запустив утилиту **GenCerts.exe** из командной строки с параметром *–h (GenCerts.exe –h)*, после этого скопировать папку certs из текущей директории на USB-устройство.

Б) Копирование сертификатов vCenter.

Б.1 В случае vCenter на Windows:

Следует выполнить вход на vCenter, перейти *в случае vCenter версии 5.x* в папку C:\Program Data\VMware\VMware VirtualCenter\SSL или *в случае vCenter версии 6.0* – в папку C:\Program Data\VMware\vCenterServer\cfg\vmware-rhttpproxy\ssl, скопировать из нее файлы rui.crt и rui.key на USB-устройство в папку certs (в которой уже находятся сертификаты «Сегмент-В.»).

Б.2 В случае VCSA версии 5.x:

Следует удостовериться, что ssh на VCSA открыт. Для этого необходимо открыть в браузере панель управления VCSA: *https://[ip или fqdn vcsa]:5480*, авторизоваться и в открывшемся окне перейти во вкладку admin; параметр «*Administrator SSH login enabled*» должен быть установлен в значение «*yes*» (рисунок 15).

Далее из папки /etc/vmware-vpx/ssl в уже созданную на USB-носителе папку certs следует скопировать файлы rui.crt и rui.key.

По завершении копирования закрыть ssh (параметр «*Administrator SSH login enabled*» должен быть установлен в значение «*no*»).

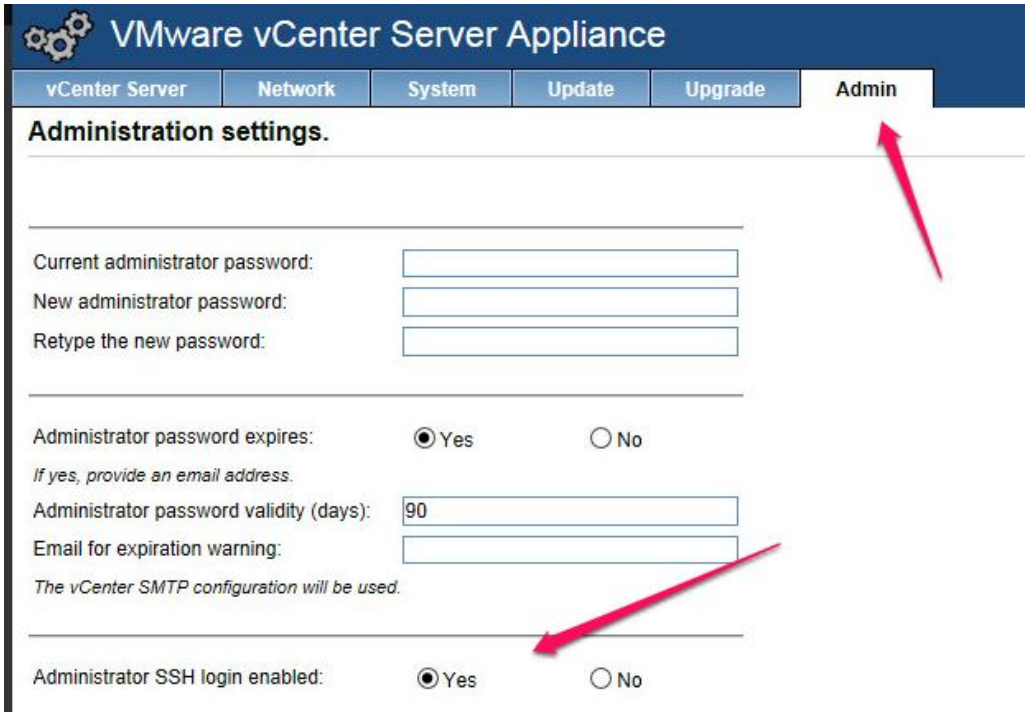


Рисунок 15 - Включение ssh на VCSA 5.x

Б.3 В случае VCSA версии 6.0:

Следует открыть консоль VCSA, перейти в пункт «Troubleshooting options», открыть shell и ssh. Затем, нажав клавиши <Alt>+<F1>, переместиться в shell и авторизоваться от пользователя root. Набрать команду *shell* и переместиться в соответствующий режим. Затем активировать возможность подключения с использованием протокола sftp (команда *chsh –s "/bin/sh" root*) и подключиться при помощи соответствующего ПО (например WinSCP) к Вашему VCSA. Далее в уже созданную на USB-носителе папку certs следует скопировать файлы rui.crt и rui.key (из папки /etc/vmware-vpx/ssl).

По окончании копирования вернуться в консоль VCSA и вернуть всё в исходное положение: набрать команду chsh –s "/bin/appliancesh" root ; затем exit (2 раза) и отключить во вкладке troubleshooting options shell и ssh.

3.5. Установка модуля «Сегмент-В.» на прокси-сервер

Установка модуля «Сегмент-В.» выполняется непосредственно на каждый прокси-сервер путем установки соответствующего образа операционной системы (в аппаратном исполнении комплекса модуль предустановлен!).

3.5.1. Установка ОС на прокси-сервер

Для установки ОС на прокси-сервер необходимо смонтировать образ операционной системы **Segment-V. Module.iso** или вставить диск с операционной системой в CD/DVD-привод сервера, установить в настройках

BIOS порядок загрузки с CD/DVD, дождаться появления окна выбора варианта установки.

После появления списка следует удостовериться в том, что выбран вариант «Install Segment-V Module», и нажать клавишу <Enter> – начнется процесс установки операционной системы.

Рисунок 16 - Начало установки ОС на прокси-сервер

В процессе установки в графическом режиме будет запрошен пароль для учетной записи root, который будет использоваться в дальнейшем для входа в ОС только в случае внештатных ситуаций, – в соответствующих полях для ввода необходимо задать и подтвердить пароль (рисунок 17).

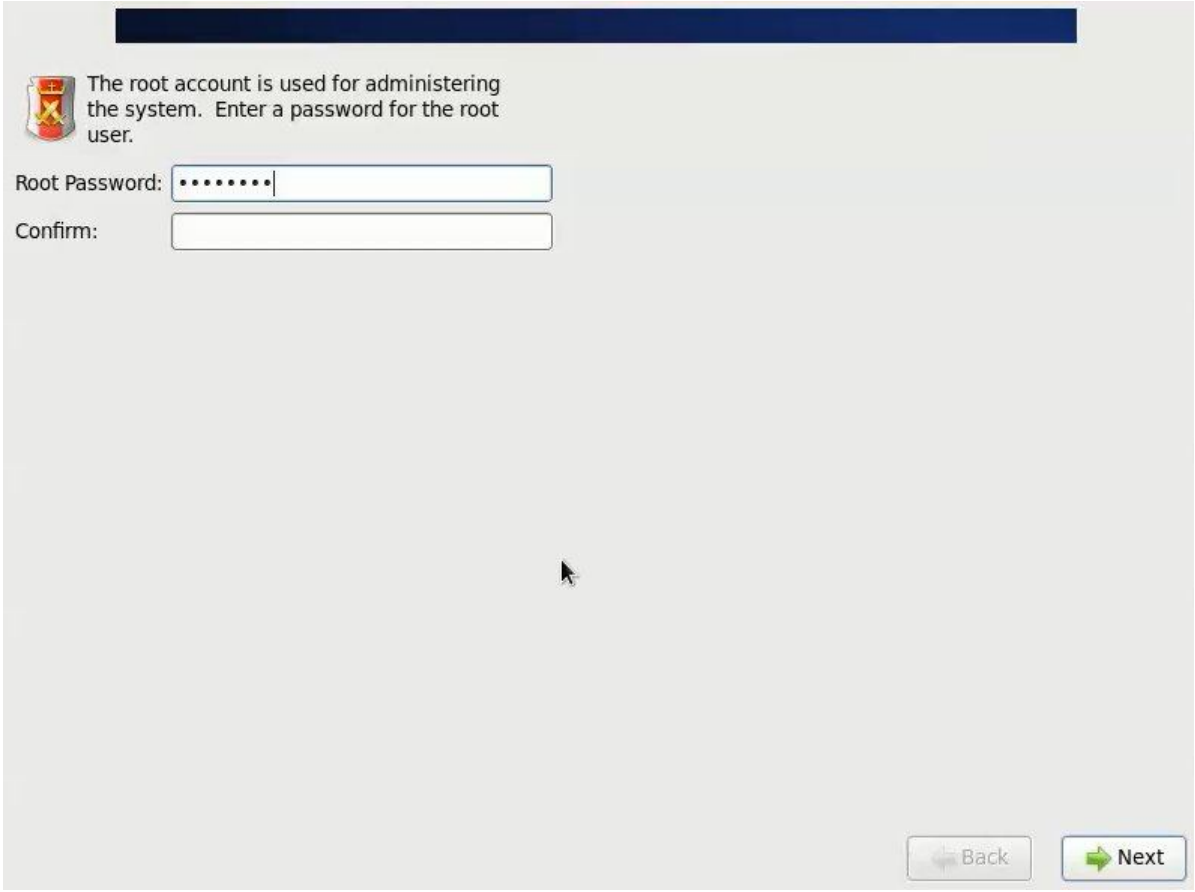


Рисунок 17 - Установка пароля учетной записи root

ВНИМАНИЕ! После завершения установки не забудьте сменить порядок загрузки в BIOS или извлечь диск из CD/DVD-привода.

По окончании процесса установки модуля необходимо перезагрузить ОС (кнопка <Reboot>, см. рисунок 18) и дождаться запроса на авторизацию пользователя (см. 3.5.2).

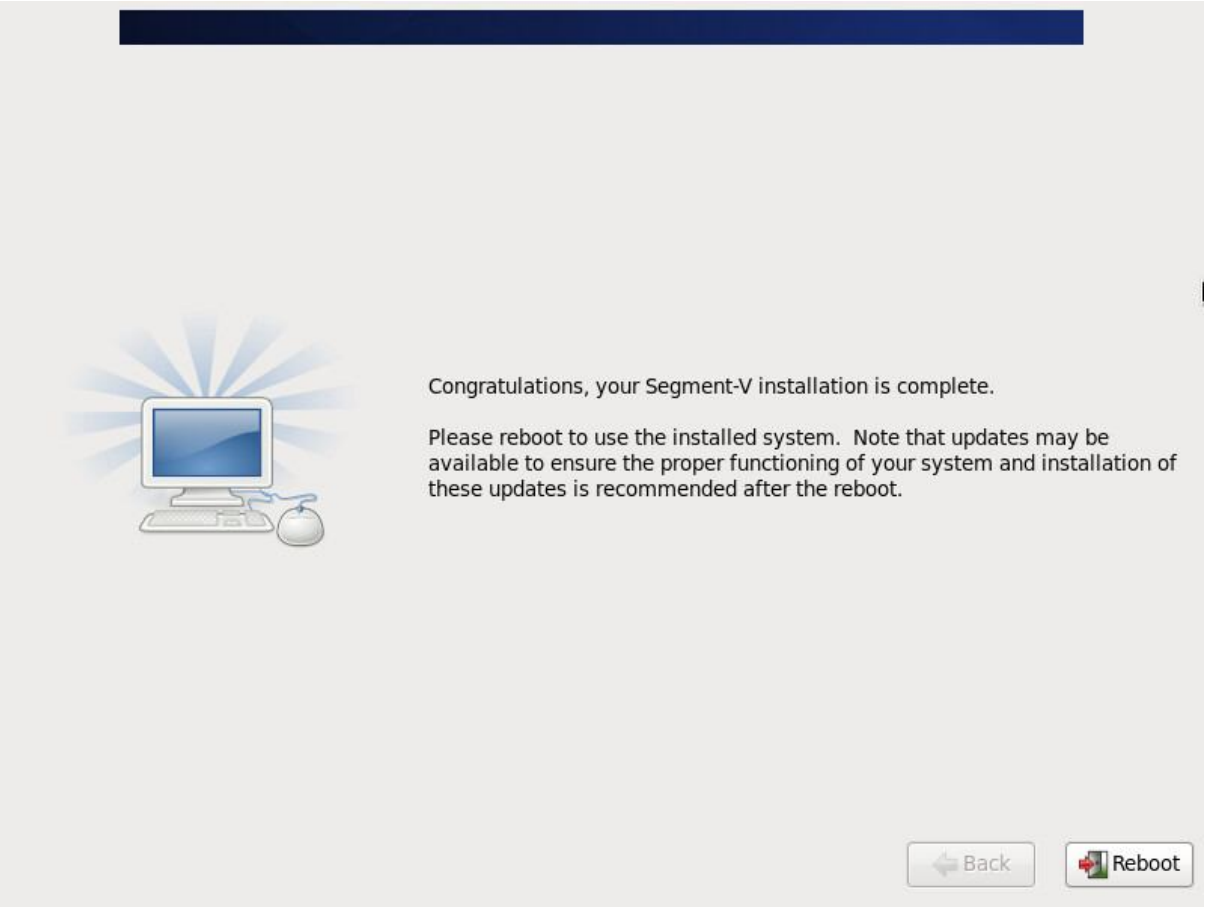


Рисунок 18 - Сообщение об окончании процесса установки ОС на прокси-сервер

3.5.2. Первичная инициализация прокси-сервера

По завершении установки и перезагрузки сервера на экран выводится запрос на вход в систему, требующий ввода данных учетной записи accord, предустановленной в образе.

ВНИМАНИЕ! Для учетной записи accord по умолчанию установлен пароль **P@ssw0rd**, который следует использовать для первого входа в систему и **необходимо сменить**.

После успешного входа в систему выполняется автоматический запуск скрипта настройки прокси-сервера. При первичной установке необходимо выбрать пункт *«0 – Full Installation»*.

Начинается процесс установки и настройки, включающий в себя несколько этапов:

1. Изменение пароля учетной записи accord.

После выбора пункта *«0 – Full Installation»* на экран выводится запрос на смену пароля для учетной записи accord:

Do you want to change Segment-V. user password? (Y/N)

Следует выбрать *«Y»* и выполнить процедуру смены пароля, введя новый пароль пользователя. Данную процедуру можно выполнить и позднее, по

завершении настройки ПО (см. 3.5.3). Однако в любом случае следует помнить о том, что **оставлять пароль по умолчанию небезопасно!**

2. Установка дополнительных пакетов, необходимых для работы прокси-сервера.

Данный этап выполняется в автоматическом режиме.

3. Настройка сетевых интерфейсов.

Первым этапом необходимо **выбрать режим работы прокси-сервера:**

Do you want to use 1-interface or 2-interfaces mode?

Следует выбрать «1», если планируется применять только один интерфейс, или «2», если будут применяться два сетевых интерфейса.

В случае если **выбран одноинтерфейсный режим**, необходимо выполнить установку параметров одиночного интерфейса (*«Enter single interface name»*). Для этого следует выполнить установку следующих параметров:

- **имя интерфейса** (обычно *eth0* или *eth1*), которое должно совпадать с именем внутреннего интерфейса сервера (для того чтобы определить необходимую для этого сетевую карту, следует сравнить отображаемые в процессе настройки MAC-адреса для каждого интерфейса с параметрами, записанными ранее);
- **тип получения настроек** *(«Enter inner interface type»)*: статический или DHCP.

В случае *static* следует указать IP-адрес для выбранного интерфейса *(«Enter ip for ethX»)* и маску подсети *(«Enter netmask for ethX»).* Также при статическом типе получения настроек может быть задан шлюз по умолчанию *(«Do you want to set default gateway for ethX? (Y/N»))*. В случае удовлетворительного ответа следует ввести IP-адрес шлюза для внутреннего интерфейса *(«Enter default gateway for ethX:»)*.

В случае если **выбран двухинтерфейсный режим**, необходимо выполнить последовательно настройку **внутреннего** *(«Enter inner interface name»)* и **внешнего** *(«Enter outer interface name»)* **интерфейсов**. Их настройка выполняется аналогичным одиночному интерфейсу образом.

ВНИМАНИЕ! Рекомендуется задавать статические IP-адреса внутреннего, внешнего и одиночного интерфейсов прокси-сервера.

Далее следует выполнить настройку IP-адресов защищаемых серверов (vCenter или отдельные ESXi), к которым разграничивается доступ.

Примечание: указывать IP адреса ESXi, связанных с vCenter, не нужно. Достаточно указать адрес vCenter.

В ответ на запрос *«Enter vCenter ip»* следует ввести IP-адрес защищаемого сервера.

В случае если в инфраструктуре используются несколько vCenter в режиме Linked Mode или несколько отдельных (standalone) ESXi без связи с vCenter (см. подраздел 2.1, вопрос 1), необходимо подтвердить использование режима Linked Mode (в ответ на запрос *«Do you want to use vCenter in Linked Mode?»*).

Далее следует указать число vCenter и/или ESXi, для которых необходимо разграничить доступ, и их IP адреса.

Например, если в инфраструктуре используется три vCenter в режиме Linked Mode, следует сначала задать IP-адрес первого (любого) vCenter, затем указать число vCenter, информация о которых еще не задана на прокси-сервере (2), после чего задать адреса оставшихся двух vCenter.

Далее следует указать, есть ли необходимость в блокировке доступа к vCenter при помощи WebClient (в ответ на запрос *«Do you want to block WebClient Access to vCenter?»*).

ВНИМАНИЕ! ПАК «Сегмент-В.» версии 1.3 не разграничивает доступ к WebClient! Возможен либо полный запрет, либо полное разрешение на работу АВИ через WebClient.

В случае блокировки доступа через WebClient необходимо указать число серверов, на которых установлен vSphere Web Client и доступ к которым следует заблокировать (запрос «How many WebClient Server are there?»).

Далее для каждого сервера следует указать:

- IP-адрес сервера, на котором установлен vSphere Web Client (запрос «*Enter WebClient Server ip*»);
- порт (запрос «*Enter WebClient Server port*») – по умолчанию это 9443.

ВНИМАНИЕ! IP-адрес Web Client может отличаться от IP-адреса vCenter (если он установлен отдельно).

В завершение настройки сетевой части необходимо указать IP-адрес DNS-сервера во внутренней сети (запрос «Enter DNS server ip:»).

ВНИМАНИЕ! В случае отсутствия DNS-сервера необходимо добавить записи для vCenter и ESXi в файл hosts на прокси-сервере и на АРМ АБИ.

4. Копирование сертификатов.

По завершении настройки сети на экран выводится запрос на подключение USB-устройства, с которого будут скопированы сертификаты (описание подготовки устройства рассмотрено в подразделе 3.4.4):

Please, insert USB device, with certs folder

Следует подключить устройство и дождаться завершения процесса копирования.

Обратите внимание: если в процессе копирования сертификаты не обнаружены (например, если они отсутствуют на USB-устройстве или USB-устройство некорректно считалось при первом подключении), на экран выводится сообщение *«Error: certs wasn't copied!»* и запрос:

Do you want to try another device? (Y/N)

Следует удостовериться, что на USB-устройстве присутствуют необходимые сертификаты, выбрать *«Y»* и дождаться корректного завершения процесса копирования сертификатов. Если в данный момент нет возможности произвести копирование сертификатов, данную операцию можно выполнить по окончании процесса установки, вызвав её в разделе Reconfigure Segment-V (см. пункт 3.5.4).

Если сертификаты копируются вручную, папку certs с требуемыми сертификатами следует переместить в директорию /etc/accord-v/.

5. Настройка сервиса управления.

Далее на экран выводится запрос IP-адреса, который будет использоваться для подключения к сервисам управления модуля «Сегмент-В.» из ПО управления комплексом с АРМ АБИ (обычно это IP-адрес внешнего интерфейса):

Enter ip for accordservice management:

6. Настройка отказоустойчивого решения.

На данном этапе на экран выводится запрос на настройку режима High Availability:

Do you want to configure High Availability?

Конфигурирование данного режима возможно и позже, подробнее про настройку см. отдельный подраздел 3.6.

7. Установка и начальная конфигурация СПО «Аккорд-X»

На данном этапе на экран выводится запрос на установку «Аккорд-X»:

Do you want to install Accord-X? (Y/N)

Установка и конфигурирование «Аккорд-X» возможны и позже: подробнее см. подраздел 3.7.

8. Проверка статуса сервисов.

На этом инициализация модуля «Сегмент-В.» завершена.

По нажатии любой клавиши выполняется переход в основное меню настройки (запрос *«Press any key to continue»*).

После завершения установки необходимо убедиться в том, что сервисы запущены и работают корректно, выбрав третий пункт скрипта установки – *«Print current settings»* (все сервисы должны находиться в состоянии Running).

3.5.3. Настройки безопасности прокси-сервера

После завершения процедуры первичной инициализации прокси-сервера необходимо перейти в раздел «Change security settings» (выбрать пункт 2 скрипта установки) и выполнить следующие изменения (рисунок 19):

0 – Change default Accord-V user password – изменить пароль пользователя accord (если по каким-либо причинам данная процедура не была выполнена ранее: перед началом настроек, описанных в п. 3.5.2). **Оставлять пароль по умолчанию небезопасно!**

1 – Change ssh service status – отключить досуп по ssh (рекомендуется, но не является необходимым; **ssh должен быть включен в момент настройки High Availability!**).

What operation do you want to perform? -> stop

2 – GRUB password - Установить пароль на grub. Выполнить команду:

Do you want to add grub password or delete? -> ADD и ввести пароль.

Рисунок 19 - Изменение настроек безопасности прокси-сервера

Далее следует переместиться в пункт 4 скрипта установки и выполнить команду *0 Logout* (при необходимости проверки пароля на grub выбрать *1 – restart,* т.е. выполнить перезагрузку).

Модуль защищен и готов к работе!

Обратите внимание на необходимость выполнения также действий, направленных на защиту данного модуля «снаружи», – настройки доверенной загрузки (подробнее см. документацию на комплекс «Аккорд-АМДЗ» и на ПАК «Аккорд-В.»), отключения в настройках ВМ возможности использования CD/DVD-дисков, дискет и USB-контроллеров.

3.5.4. Изменение настроек прокси-сервера

Помимо полной настройки прокси-сервера, скрип установки позволяет (рисунок 20):

1)*Reconfigure Segment-V* – в случае необходимости перенастроить параметры прокси-сервера (например, если в процессе при базовой инициализации была совершена ошибка);

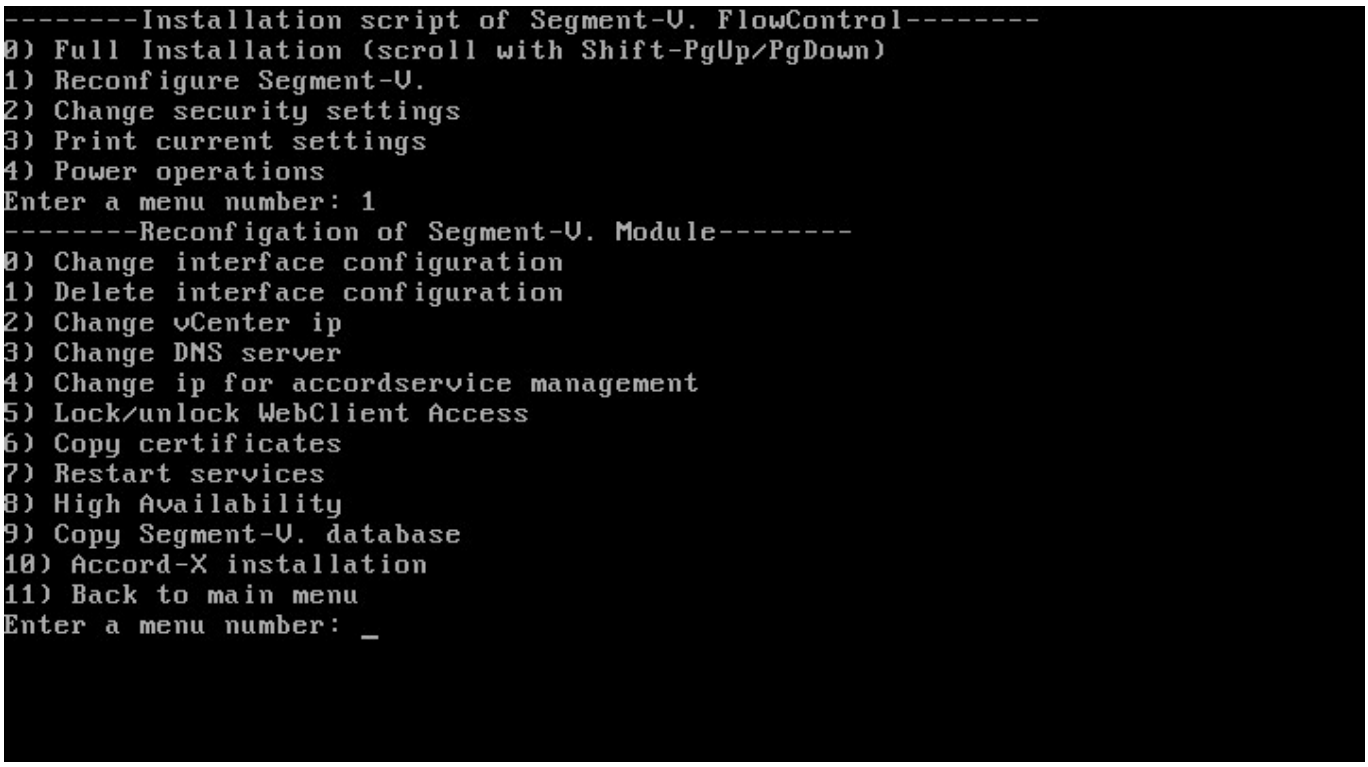


Рисунок 20 - Изменение параметров прокси-сервера

2)*Change security settings* – изменить настройки безопасности модуля. НЕОБХОДИМО ВОСПОЛЬЗОВАТЬСЯ ПОСЛЕ ИНИЦИАЛИЗАЦИИ! (см. пункт 3.5.3);

3)*Print current settings* – отобразить текущие настройки модуля;

4)*Power operations* – выполнить операции по перезагрузке системы, в том числе операцию завершения сессии (logout).

Чтобы удостовериться, что все настройки были выполнены правильно и все необходимые службы запустились, следует выбрать пункт 3 – на экране отобразятся основные параметры модуля (рисунок 21):

- настройки сетевых интерфейсов с указанием режима работы прокси-сервера (*«1-interface mode»* – для одноинтерфейсного режима, *«2-interface mode»* – для двухинтерфейсного режима);
- IP-адреса защищаемого/защищаемых vCenter;
- IP-адреса и номера портов серверов с установленным vSphere Web Client, доступ к которым заблокирован;
- статус SSH и сервисов «Сегмент-В.»;
- информация об использовании режима отказоустойчивости;
- информация о том, установлено ли СПО «Аккорд-Х».

Наибольший интерес при этом представляет раздел *«Segment-V. services status»* со следующими сервисами:

- *Segment-V Service* – сервис, отвечающий за взаимодействие с ПО управления на АРМ АБИ;

- *Segment-V LogCollector* – предназначен для взаимодействия с сервисом регистрации событий с целью сбора событий;
- *Segment-V Proxy* – данный сервис отвечает за разграничение доступа. Если он остановлен, выполнить подключение к vCenter невозможно.

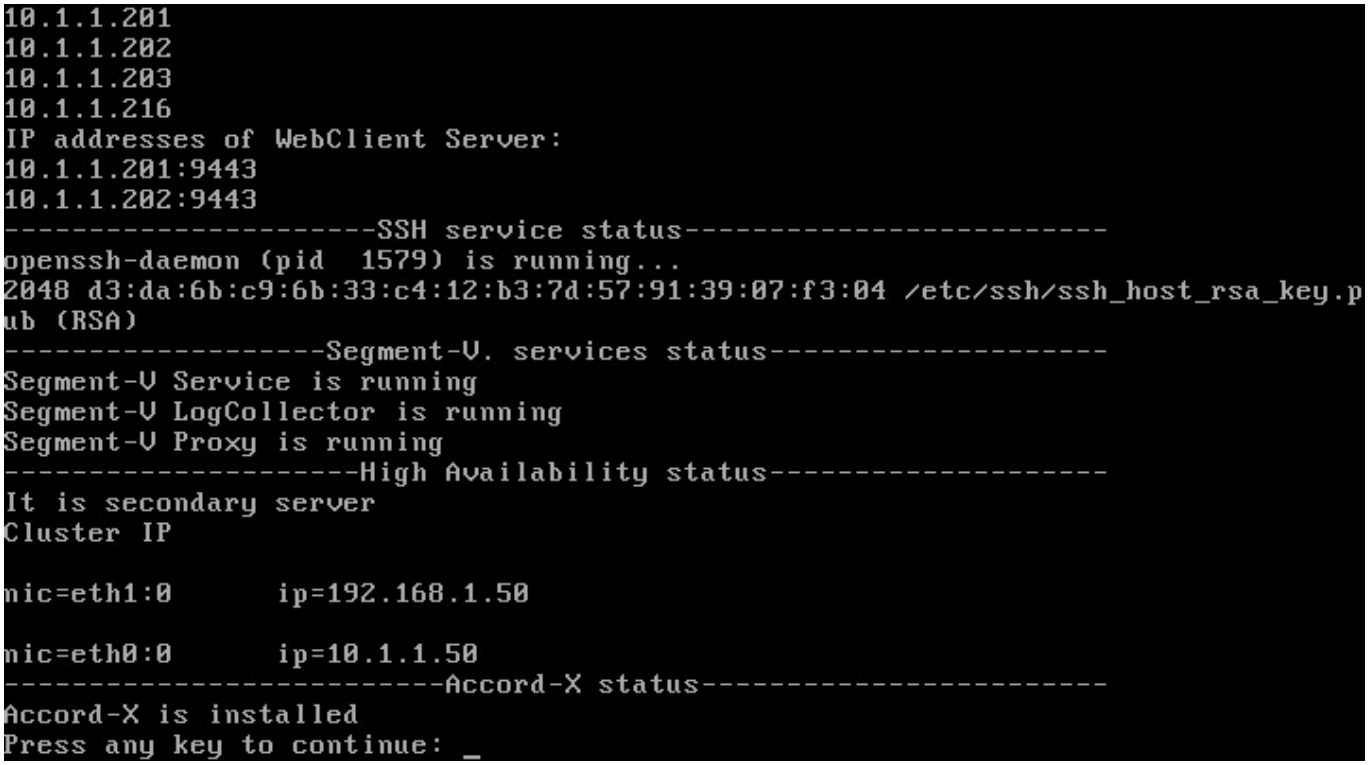


Рисунок 21 - Основные параметры модуля

Дополнительно рекомендуется запомнить отпечаток ключа (key fingerprint) для High Availability или использования ssh в дальнейшем.

3.6. Настройка отказоустойчивого решения (при использовании двух прокси-серверов)

Существуют различные способы построения отказоустойчивого решения (в том числе для различных целей). Под рассматриваемой отказоустойчивостью в данном разделе подразумевается защита от сбоев оборудования.

3.6.1. Защита с помощью средств VMware vSphere (вариант для ВМ)

Для защиты прокси-сервера, реализованного в виде ВМ, существует возможность использовать стандартные средства отказоустойчивости, предлагаемые в рамках комплекса VMware vSphere, а именно:

1) High Availability;

2) Fault Tolerance (актуально для vSphere 6, где отсутствует ограничение на 1 vCPU).

В рамках данного руководства подробно настройка этих вариантов не рассматривается, т.к. не относится непосредственно к описанию работы с комплексом «Сегмент-В.».

3.6.2. Защита с помощью комбинирования внешних средств, а также функционала «Сегмент-В.»

За отказоустойчивость отвечают внешние сетевые устройства (проверяют доступность интерфейсов прокси-серверов для передачи трафика), в случае необходимости они меняют маршруты.

Прокси-серверы дополнительно не настраиваются, каждый прокси-сервер использует свой IP-адрес, а за переключение отвечает внешнее устройство.

Со стороны «Сегмент-В.» необходимо только подключить оба прокси-сервера к ПО управления комплексом (см. п. 3.6.3.2).

3.6.3. Защита с помощью функционала «Сегмент-В.» (вариант подходит и для ВМ, и для аппаратных исполнений)

3.6.3.1. Настройка прокси-сервера

High Availability

Два прокси-сервера (основной/резервный – primary/secondary) могут быть объединены в кластер для повышения доступности прокси-серверов.

ВНИМАНИЕ! Оба прокси-сервера, входящие в кластер отказоустойчивости, должны функционировать в одном режиме: либо в одноинтерфейсном, либо в двухинтерфейсном.

В кластере каждый прокси-сервер выполняет одну из двух ролей: основной (primary) сервер или резервный/вторичный (secondary).

На основном прокси-сервере поднимаются виртуальные IP-адреса (*outer/inner interface of cluster* – **в двухинтерфейсном режиме**; *single interface of cluster* – **в одноинтерфейсном режиме**), через которые проходит управляющий трафик (его обработка происходит на основном сервере).

При потере связи с внешней/внутренней сетями основного прокси-сервера (например, по причине отказа сетевой карты или потери сигнала), те же виртуальные IP-адреса будут подняты на резервном сервере, который после этого станет основным (primary), а вышедший из строя – резервным/вторичным (secondary).

Проверка подключения сервера к сети при работе **в двухинтерфейсном режиме** осуществляется посредством проверки доступности проверочных IP-адресов внешней/внутренней сети (*IP for check connection in outer/inner network*), при работе **в одноинтерфейсном режиме** – на основании доступности только одного проверочного IP-адреса (*IP for check connection in network*).

В качестве проверочных адресов внешней/внутренней сети рекомендуется использовать шлюз (Gateway) соответствующей сети.

Информацию об изменении ролей кластера при различных изменениях сетевых подключений серверов кластера см. в таблице 3.

Таблица 3 - Изменение ролей кластера при различных изменениях сетевых подключений серверов кластера

Изменение сетевых подключений серверов кластера	Изменение ролей серверов кластера
Потеря подключения к внешней/внутренней[1] сети, отключение резервного сервера	Роли серверов остаются без изменений
Потеря подключения к внешней/внутренней сети, отключение основного сервера	Основной сервер –> резервный. Резервный сервер –> основной
Потеря подключения к НА сети резервным/основным сервером	Оба сервера становятся основными. Для корректного продолжения работы требуется исправление ошибок подключения к сети
Потеря подключения к НА сети и внутренней/внешней сетям резервного сервера	Основной сервер -> основной. Резервный сервер -> попеременно меняет роль с основного на резервный. Для корректного продолжения работы требуется исправление ошибок подключения к сети
Потеря подключения к НА сети и внутренней/внешней сетям основного сервера	Основной сервер -> попеременно меняет роль с основного на резервный. Резервный сервер -> основной. Для корректного продолжения работы требуется исправление ошибок подключения к сети
Потеря подключения к проверочному IP-адресу внешней/внутренней сети	Оба сервера попеременно меняют роль с основного на резервный. Для корректного продолжения работы требуется исправление ошибок подключения к сети

Общие требования для использования High Availability:

1 .Два ВМ/сервера (на которые будет установлен «Сегмент-В.»), функционирующие в одном режиме:

- с тремя сетевыми адаптерами – при работе **в двухинтерфейсном режиме**;
- с двумя сетевыми адаптерами – при работе **в одноинтерфейсном режиме.**

2. Три свободных IP-адреса (по одному для каждого сервера, а также виртуальный IP-адрес кластера):

- во внешней и внутренней сетях – при работе **в двухинтерфейсном режиме**;
- в сети – при работе **в одноинтерфейсном режиме**.

3. Дополнительная сеть (сеть High Availability, далее – НА) для построения кластера, репликации данных между серверами.

[1)] Здесь и далее в этой таблице: для двухинтерфейсного режима – внешняя/внутренняя сеть; для одноинтерфейсного режима – одна, общая, сеть.

Требование к подключению прокси-серверов к внешней/внутренней сети:

При работе **в двухинтерфейсном режиме** внутренняя и внешняя сети на серверах должны быть подключены к интерфейсам с одинаковыми именами. Например, если для подключения к внешней сети на основном прокси-сервере используется интерфейс eth0, то и на резервном подключение к внешней сети должно осуществляться по этому интерфейсу.

При работе **в одноинтерфейсном режиме** серверы должны быть подключены к сети с помощью интерфейсов с одинаковыми именами.

Установка «Сегмент-В.» с использованием High Availability

После выполнения процедуры настройки сервисов управления, перед выполнением процедуры проверки статуса сервисов, на экран выводится запрос на настройку High Availability (см. 3.5.2, пункт «6. Настройка отказоустойчивого решения»).

Настройка High Availability (HA configuration)

Следует подтвердить настройку:

Do you want to configure High Availability? y

и указать, какую роль в кластере будет выполнять данный сервер. После чего выполнить настройку в соответствии с выбранной ролью.

ВНИМАНИЕ! Необходимо заранее выбрать, какой из двух серверов будет выполнять роль основного.

Примечание: во время первоначальной (полной) установки «Сегмент-В.» можно отказаться от настройки High Availability, выполнив ее позднее с помощью реконфигурации «Сегмент-В.» (Reconfigure Segment-V -> High Availability -> Full Configuration).

ВНИМАНИЕ! В момент выполнения настройки ssh должен быть включен! По завершении процедуры настройки ssh можно отключить (если далее в нем нет необходимости).

ВНИМАНИЕ! Используйте полную настройку High Availability (Reconfigure Segment-V -> High Availability -> Full Configuration) только для первоначальной конфигурации данной опции.

Порядок настройки серверов кластера:

1. Настройка резервного сервера.
2. Настройка основного сервера.

Настройка резервного сервера:

1. Указать, что это не основной сервер (*Is it primary host? n*).
2. Выбрать номер ноды в кластере (Enter the number of node in cluster: (1/2)).

ВНИМАНИЕ! Серверы в кластере должны иметь различные номера нод.

3. Задать настройки подключения к сети HA: указать имя интерфейса, подключенного к сети HA, IP-адрес сетевого устройства и маску подсети.

4. Убедиться в правильности настройки резервного сервера.

При отображении текущих настроек *"High Availability status" должен иметь следующий вид: "There is no High Availability configuration on this server. This server is ready to be secondary server". Имя сервера изменится в соответствии с выбранным номером ноды ("segment-v-fc1" для ноды 1 и @segment-v-fc2" для ноды 2).*

Настройка основного сервера:

ВНИМАНИЕ! Настройка основного сервера должна осуществляться только после настройки резервного.

Проверить, что настройка резервного сервера уже была выполнена. Выполнить проверку можно с помощью отображения текущих настроек резервного сервера. "High Availability status" должен иметь следующий вид: *"There is no High Availability configuration on this server. This server is ready to be secondary server".*

1. Указать, что это основной сервер (*Is it primary host? y*).

2. Подтвердить, что начальная конфигурация резервного сервера уже была выполнена (*Did you configure the secondary host? y*).

3 .Выбрать номер ноды в кластере (Enter the number of node in cluster: (1/2)).

4. Задать настройки подключения к сети HA: указать имя интерфейса, подключенного к сети HA, IP-адрес сетевого устройства и маску подсети.

5. Указать IP-адрес резервного сервера в сети HA. Узнать IP-адрес можно с помощью отображения текущих настроек резервного сервера.

6. Выполнить настройку виртуальных IP-адресов кластера (*interface of cluster(virtual IP)*) и проверочных IP-адресов (*IP for check connection in outer/inner network*).

В случае **двухинтерфейсного режима работы** сначала выполняется настройка виртуального IP-адреса кластера (с указанием имени интерфейса) и проверочного IP-адреса во внутренней сети, после – во внешней сети.

В случае **одноинтерфейсного режима работы** настраивается один виртуальный IP-адрес кластера и один проверочный адрес.

ВНИМАНИЕ! Подключение к внешней/внутренней сети как основного, так и резервного сервера должно осуществляться через интерфейсы с одинаковыми именами.

6. Убедиться в правильности настройки основного и резервного серверов.

При отображении текущих настроек в "High Availability status" будет указана роль сервера (*primary/secondary*), а также виртуальные IP-адреса кластера и имена соответствующих интерфейсов.

Переход от работы отдельного прокси-сервера к кластеру:

Вариант 1. Без изменения настроек подключения уже существующего прокси-сервера к внешней/внутренней сетям:

1. Выполнить реконфигурирование уже существующего сервера в качестве резервного сервера: полная конфигурация High Availability (*Reconfigure Segment-V -> High Availability -> Full Configuration*).

2. Выполнить полную установку второго сервера в качестве основного.

3. На сетевых устройствах удалить старые и прописать новые правила перенаправления управляющего трафика из внешней сети (управляющий трафик должен быть перенаправлен на соответствующий виртуальный IP-адрес кластера).

Вариант 2. Без изменения конфигурации сетевых устройств:

1. Выполнить реконфигурирование уже существующего сервера в качестве резервного: изменение настроек внутреннего и внешнего интерфейсов (для двухинтерфейсного режима) или одиночного интерфейса (для одноинтерфейсного режима) (*Reconfigure Segment-V -> Change inner interface, Change outer interface;* полная конфигурация HA).

2. Выполнить полную установку для второго сервера (виртуальные IP-адреса для кластера – IP-адреса «старого» сервера) в качестве основного.

Примечание: для любого варианта возможна настройка уже существующего сервера в качестве основного с предварительной установкой нового (второго) сервера в качестве резервного.

Изменение настроек и отключение High Availability

ВНИМАНИЕ! В момент выполнения настройки ssh должен быть включен! По завершении процедуры настройки ssh можно отключить (если далее в нем нет необходимости).

Для изменения настроек High Availability следует перейти в меню реконфигурирования: Reconfigure Segment-V -> High Availability.

ВНИМАНИЕ! Изменение настроек кластера следует выполнять только при наличии соединения между серверами по сети HA.

Если не указано иное, изменения настроек могут выполняться на любом (основном или резервном) сервере.

Изменение проверочных IP адресов

1) выбрать пункт меню «Change IP for check connection state»;

2) в случае **двухинтерфейсного режима** – указать, проверочный адрес какой сети, внешней или внутренней, планируется изменить. В случае **одноинтерфейсного режима** – перейти к выполнению п.3;

3) ввести новый проверочный адрес из соответствующей сети.

Изменение сетевого подключения сервера к сети HA

1) выбрать пункт меню *«Change IP of this server in High Availability network»*;

2) задать новые параметры подключения к сети HA: имя интерфейса, подключенного к сети HA, IP адрес сетевого устройства и маску подсети.

Замена одного из серверов кластера

1) убедиться, что заменяемый сервер выполняет роль резервного;

2) отключить заменяемый сервер или остановить использование на нем High Availability (см. далее «Отключение High Availability»);

3) подготовить новый сервер для использования в качестве резервного (см. «Настройка резервного сервера»);

ВНИМАНИЕ! Серверы в кластере должны иметь различные номера нод.

4) на основном сервере в меню реконфигурирования High Availability выбрать пункт *«Change secondary server»*;

5) указать IP-адрес нового резервного сервера в сети HA.

Изменение IP адреса кластера

1) выбрать пункт меню *«Change IP of cluster»*;

2) в случае **двухинтерфейсного режима** – указать, IP-адрес кластера в какой сети, внешней или внутренней, планируется изменить. В случае **одноинтерфейсного режима** – перейти к выполнению п.3;

3) задать новые имя интерфейса и виртуальный IP-кластера.

Изменение роли серверов

На основном сервере выбрать пункт меню *«Restart cluster»*. В результате бывший основной сервер начнет выполнять роль резервного, а виртуальные IP-адреса кластера поднимутся на бывшем резервном сервере, который, таким образом, становится основным.

Отключение High Availability

Выбрать пункт меню *«Stop use High Availability on this node»* на том сервере, на котором планируется остановить использование High Availability.

3.6.3.2. Настройка ПО управления «Сегмент-В.» для взаимодействия с прокси-серверами в режиме отказоустойчивости

Необходимо добавить два прокси-сервера в утилите управления «Сегмент-В.». Подробнее данные действия рассматриваются в подразделе 3.8.

3.7. Установка и конфигурирование СПО «Аккорд-Х»

Применение «Аккорд-Х» на прокси-сервере обеспечивает выполнение процедур идентификации и аутентификации пользователей root и accord, а также выполнение динамического контроля целостности исполняемых файлов из состава ПАК «Сегмент-В.».

ВНИМАНИЕ! Перед началом установки «Аккорд-Х» на прокси-сервер на USB-устройство должен быть скопирован файл лицензии license.accord.

Установка и настройка «Аккорд-X» выполняется в два этапа:

1. Начальная конфигурация: установка необходимых пакетов, создание пользователей root и accord, создание списков контроля целостности, настройка разграничения доступа, копирование лицензии. *После начальной конфигурации «Аккорд-X» работает в мягком режиме (soft-mode).*

ВНИМАНИЕ! Начальная конфигурация может быть осуществлена как в процессе полной установки (см. п. 3.5.2), так и после неё (пункт «10) Accord-X installation» меню реконфигурирования – см. п. 3.5.4, рисунок 20).

После подтверждения начала установки «Аккорд-X»:

Do you want to install Accord-X? (Y/N) y

начнётся исполнение начальной конфигурации, включающей в себя выполнение следующих процедур:

а) Установка дополнительных пакетов, необходимых для работы «Аккорд-X». Данный этап выполняется в автоматическом режиме.

б) Выбор типа идентификаторов и установка соответствующего пакета.

```
acx-remote-1.2-0.x86_64.rpm
acx-tmid-amdz-1.2-0.x86_64.rpm
acx-tmid-cards-1.2-0.x86_64.rpm
acx-tmid-shipka-1.2-0.x86_64.rpm
acx-tmid-tokens-1.2-0.x86_64.rpm
acx-tmid-usb-1.2-0.x86_64.rpm
Preparing...                ########################################### [100%]
   1:acx-admin              ########################################### [100%]

AccordX security framework administration utilities installed successfully

Preparing...                ########################################### [100%]
   1:acx-core-remote        ########################################### [100%]

AccordX security framework core with remote access installed successfully

Which type of identifier do you want to use?
0) Smartcard
1) Token (etoken, etoken-pro, laser)
2) Shipka
3) TM-identifier
Enter a menu number: 3
Preparing...                ########################################### [100%]
   1:acx-tmid-usb           ########################################### [100%]
_
```

Рисунок 22 - Выбор типа идентификатора и установка соответствующего пакета

в) Создание пользователя accord.

По соответствующему запросу администратор, производящий установку и настройку «Аккорд-X», вводит пароль и идентификатор, которые «привязываются» к пользователю accord.

ВНИМАНИЕ! Пароль, заданный пользователю в «Аккорд-X», должен совпадать с паролем в ОС.

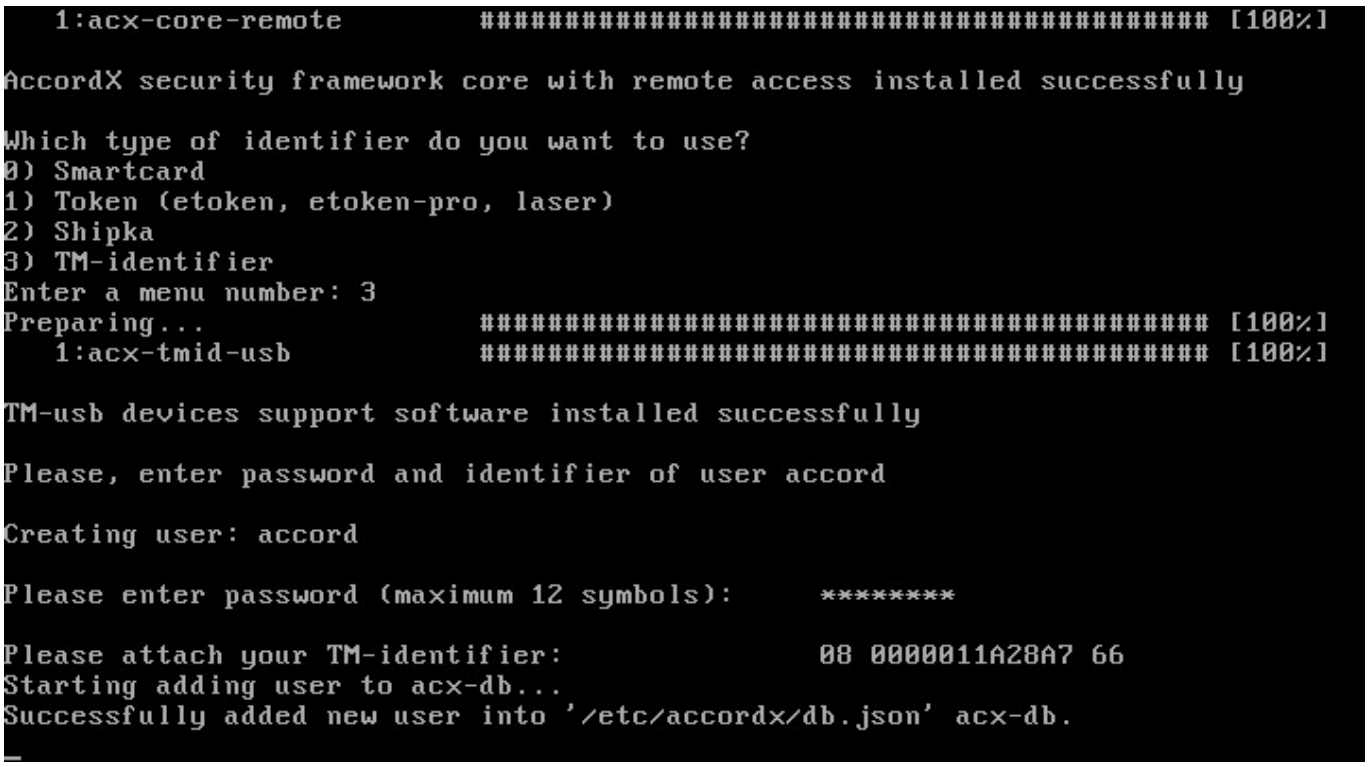


Рисунок 23 - Создание пользователя accord

г) Настройка разграничения доступа и создание списка контроля целостности. Данный этап выполняется в автоматическом режиме.

д) Создание пользователя root.

По соответствующему запросу администратор, производящий установку и настройку «Аккорд-X», вводит пароль и идентификатор, которые «привязываются» к пользователю root.

ВНИМАНИЕ! Пароль, заданный пользователю в «Аккорд-X», должен совпадать с паролем в ОС.

ВНИМАНИЕ! В случае если настройка отказоустойчивости (HA) будет выполняться после установки «Аккорд-X», потребуется xid идентификатора пользователя, т.к. в этом случае используется подключение по SSH.

Для работы без ввода xid используйте пакет acx-remote; подробнее см. раздел «Настройка PAM» «Руководства администратора» на ПАК «Аккорд-X» (11443195.4012.026 90)).

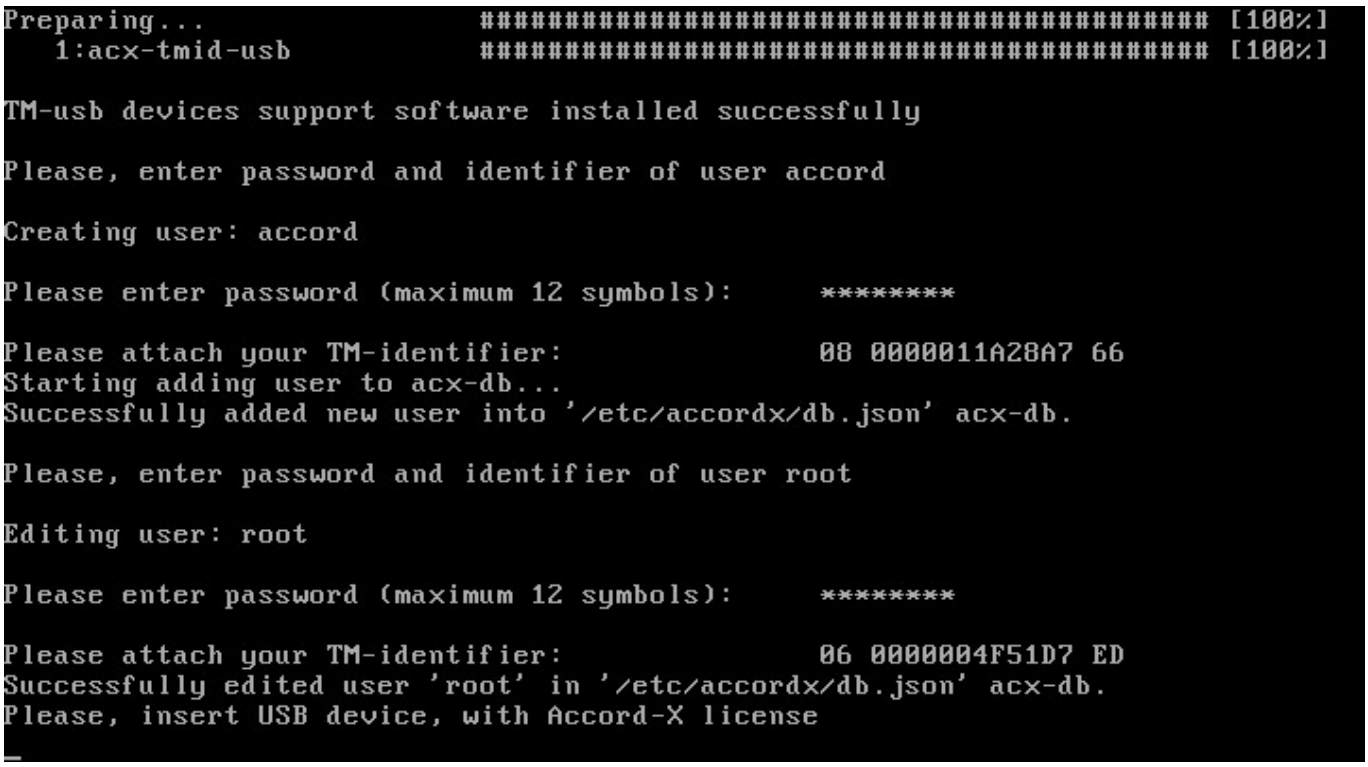


Рисунок 24 - Создание пользователя root

e) Копирование лицензии.

На экран выводится запрос на подключение USB-устройства, с которого будет скопирован файл лицензии. Следует подключить устройство и дождаться завершения процесса копирования. В случае успешного копирования появится соответствующее сообщение и запрос на перезагрузку прокси-сервера.

Accord-X license was copied. Please, reboot.

Do you want to reboot now? (Y/N)

Примечание: перезагрузку можно осуществить и позднее, воспользовавшись разделом «4) Power operations» меню скрипта установки. Но перезагрузка является обязательным условием ввода Аккорд-X в эксплуатацию.

В том случае, если файл лицензии не был скопирован в автоматическом режиме, сделайте это вручную, поместив файл лицензии в директорию /etc/accord/, после чего выполните перезагрузку прокси-сервера.

ВНИМАНИЕ! Не перезагружайте прокси-сервер до завершения копирования лицензии.

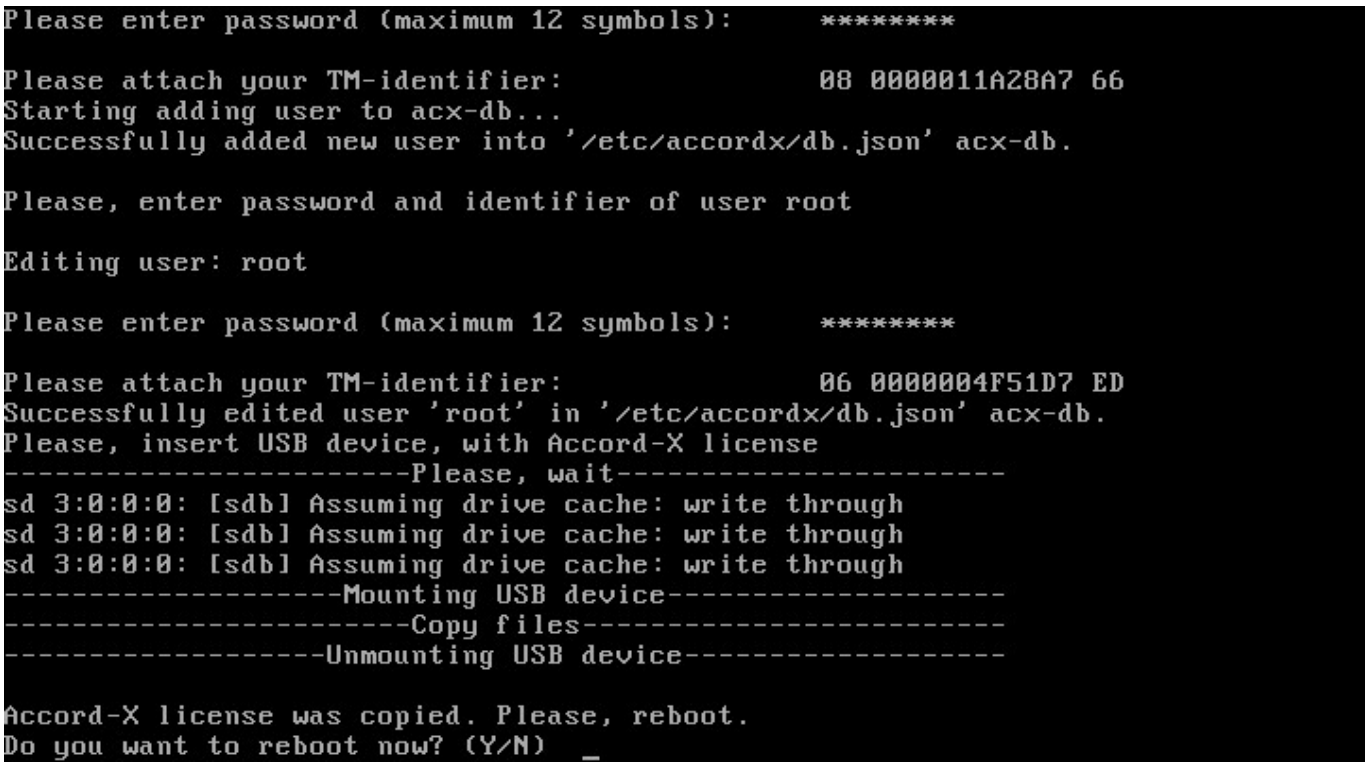


Рисунок 25 - Копирование лицензии

После перезагрузки «Аккорд-X» работает в «мягком» режиме (подробнее о режимах работы см. документацию на ПАК «Аккорд-X»), а также не задана И/А при подключениях по SSH выбранным ранее идентификатором пользователей.

2. Финальная настройка: отключение мягкого режима, настройка разграничения доступа по SSH.

Для завершения конфигурирования «Аккорд-X» (выполнения финальной настройки) выберите пункт *«10) Accord-X installation»* меню реконфигурирования, и данный этап выполнится в автоматическом режиме.

Особенность подключения по SSH

В качестве пароля необходимо использовать строку следующего вида:

XX XXXXXXXXXXX XX@password

где *XX XXXXXXXX XX* – xid идентификатора пользователя, а *password* – его пароль.

3.8. Настройка ПО управления комплексом «Сегмент-В.»

После инициализации прокси-сервера «Сегмент-В.» необходимо настроить ПО управления для взаимодействия с ним, а также сервис регистрации для сбора событий. Рассмотрим эти действия по порядку.

ВНИМАНИЕ! Убедитесь, что процедура предъявления файла лицензии уже выполнена (см. пункт 3.4.3).

3.8.1. Настройка ПО управления

3.8.1.1. Настройка защищаемых серверов (ESXi/vCenter)

Для начала процедуры настройки защищаемых серверов следует запустить от имени администратора утилиту «**Installer-V.**» и в появившемся главном окне утилиты нажать кнопку <Добавить сервер> (рисунок 26).

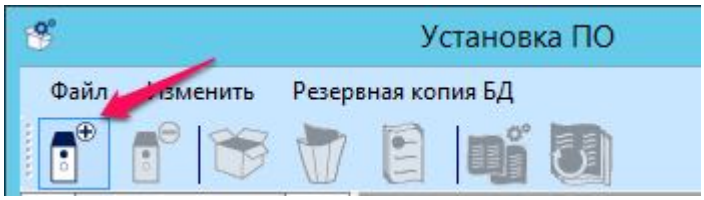


Рисунок 26 - Кнопка <Добавить сервер> в главном окне программы

В появившемся далее окне (рисунок 27), *в случае использования vCenter в виртуальной инфраструктуре*, следует ввести адрес добавляемого vCenter (IP-адрес или FQDN vCenter), а также имя и пароль для созданной ранее учетной записи accord (см. подраздел 3.3, этап 3), в качестве роли сервера указать **«vCenter»** и нажать кнопку <Добавить>.

ВНИМАНИЕ! Используемые отдельные (standalone) ESXi также должны быть добавлены в инфраструктуру. При этом, в качестве роли добавляемого сервера следует указывать «ESXi». Агенты на отдельные (standalone) ESXi следует устанавливать только в случае совместного использования с «Аккорд-В.».

Примечание: В случае vCenter в Linked Mode режиме необходимо добавлять все vCenter по отдельности.

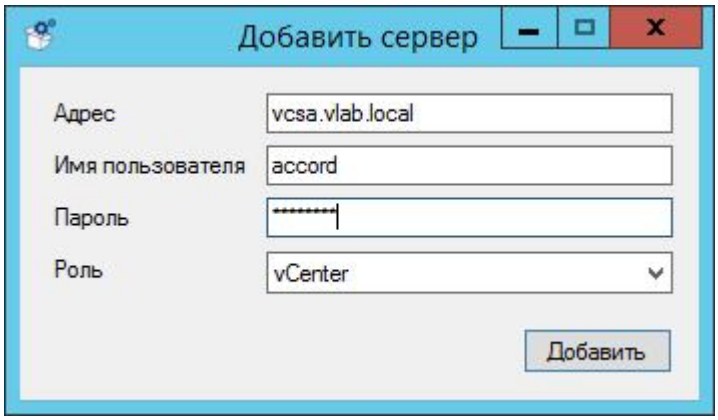


Рисунок 27 - Ввод параметров добавляемого vCenter

Если маршрутизация на модуле настроена верно и учетная запись accord существует, на экран выводится сообщение о том, что сервер успешно добавлен (рисунок 28).

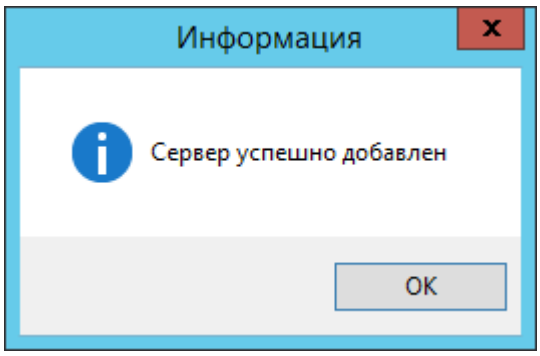


Рисунок 28 - Сообщение об успешном добавлении сервера

При этом в главном окне программы появляется соответствующая запись о добавленном vCenter (рисунок 29).

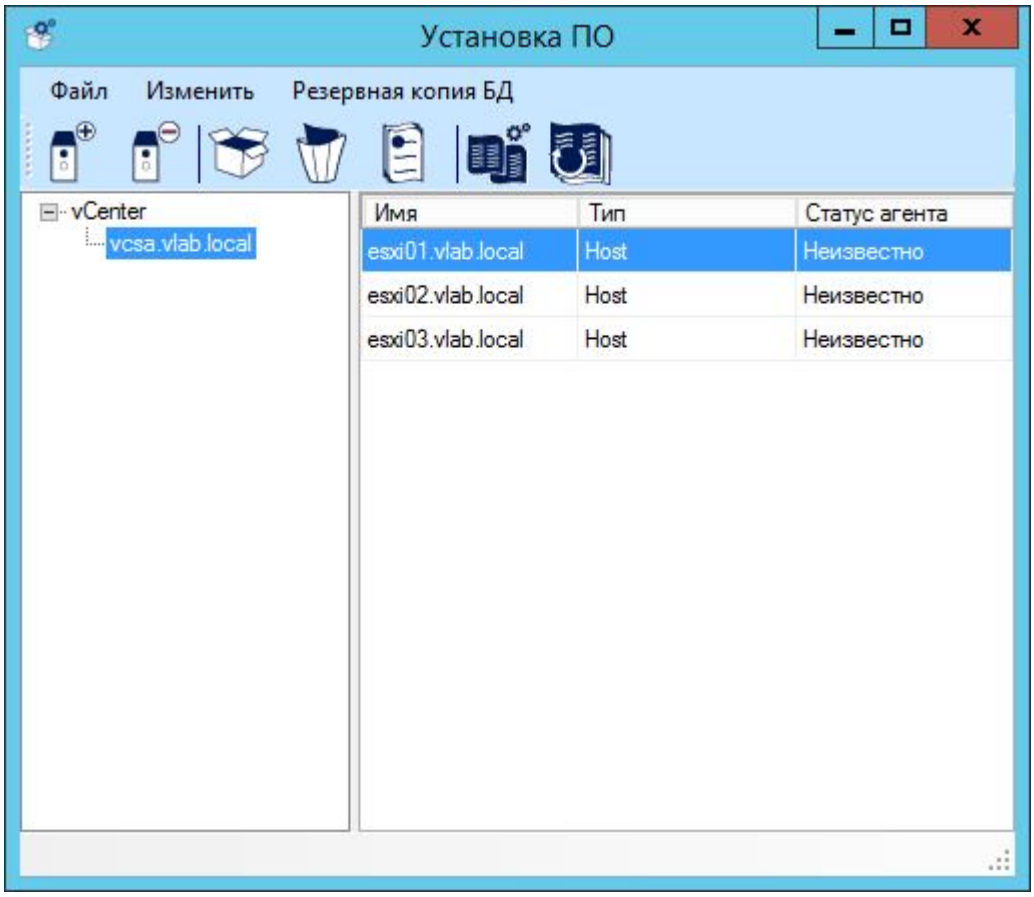


Рисунок 29 - Главное окно программы

Также в главном окне программы вместе с vCenter отображаются все связанные с ним ESXi (рисунок 29). Устанавливать агенты на них необходимо только в случае совместного использования с «Аккорд-В.».

3.8.1.2. Настройка для сбора событий с прокси-сервера

Следующим этапом необходимо указать информацию о прокси-серверах для сервиса регистрации событий.

Для этого в главном окне программы **«Installer-V.»** следует снова нажать кнопку <Добавить сервер> (рисунок 26), в появившемся далее окне (рисунок 30) выбрать роль **«Прокси-сервер»** и указать IP-адрес интерфейса управления прокси-сервера (обычно IP-адрес внешнего интерфейса, см. пункт 3.5.2, этап «5. Настройка сервиса управления»).

Примечание: в случае одновременного использования нескольких прокси-серверов (например, в случае резервирования) необходимо добавить каждый прокси-сервер!

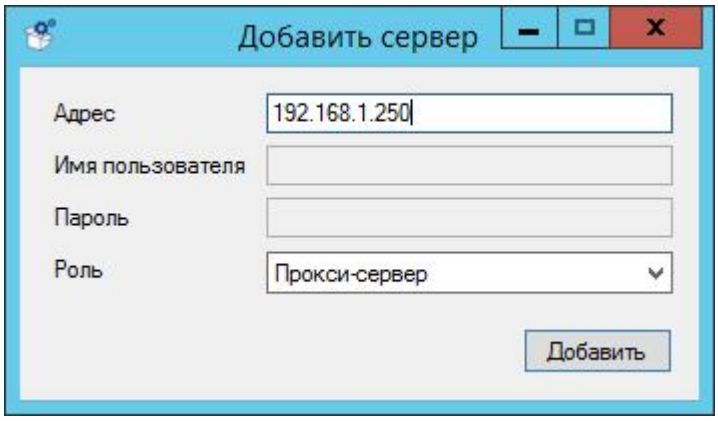


Рисунок 30 - Добавление прокси-сервера

3.8.1.3. Настройка связи между прокси-серверами и ПО управления «Сегмент-В.»

ВНИМАНИЕ! Перед тем как начать настройку прокси-сервера, убедитесь, что он установлен и настроен корректно, а сервисы управления на нем запущены.

ВНИМАНИЕ! Убедитесь, что хотя бы один vCenter или ESXi добавлены в перечень защищаемых серверов (с помощью утилиты **«Installer-V.»**).

Для настройки связи между прокси-серверами и ПО управления «Сегмент-В.» следует запустить утилиту **«Segment-V.»**.

В появившемся окне уже будет заполнено поле «Сервер», содержащее IP-адрес защищаемого сервера (vCenter и/или отдельные ESXi, добавленные ранее в утилите «Installer-V.»), с которым будет происходить работа. Необходимо заполнить параметры учетной записи accord (см. подраздел 3.3, этап 3), и нажать кнопку <Вход> (рисунок 31).

Далее нужно авторизоваться на каждом защищаемом сервере.

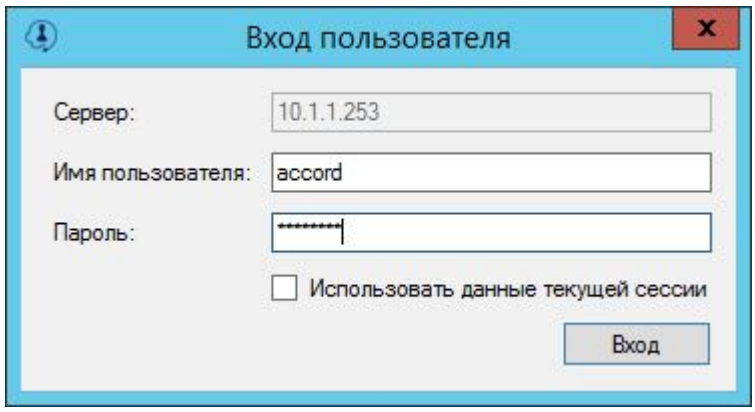


Рисунок 31 - Окно авторизации пользователя accord

Далее необходимо перейти в режим отображения прокси-серверов (выбрать раздел «Прокси-сервера» инфраструктуры в главном окне программы) и выполнить процедуру добавления прокси-сервера. Для этого в главном окне программы следует нажать кнопку <Добавить сервер> (или выбрать пункт меню «Прокси-сервера» -> «Добавить»).

Рисунок 32 - Кнопка <Добавить сервер>

По умолчанию создается прокси-сервер с именем localhost. Следует изменить данное имя на IP-адрес интерфейса управления прокси-сервера (обычно это IP-адрес внешнего интерфейса прокси-сервера, см. подраздел 3.5.2, этап «5. Настройка сервиса управления»), нажав на имя сервера в списке правой кнопкой мыши и выбрав пункт меню <Переименовать> (рисунок 33).

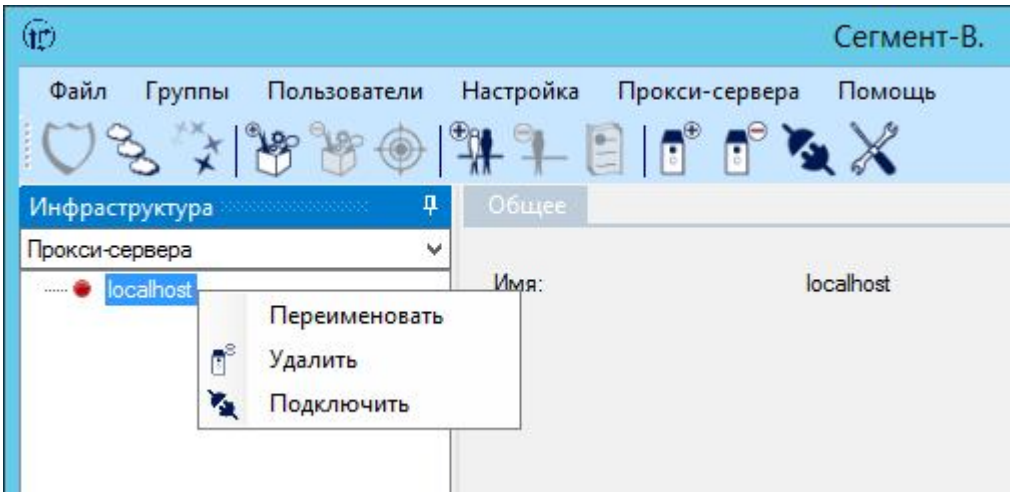


Рисунок 33 - Переименование сервера

В появившемся далее окне следует ввести IP-адрес настроенного прокси-сервера и нажать кнопку <Применить> (рисунок 34).

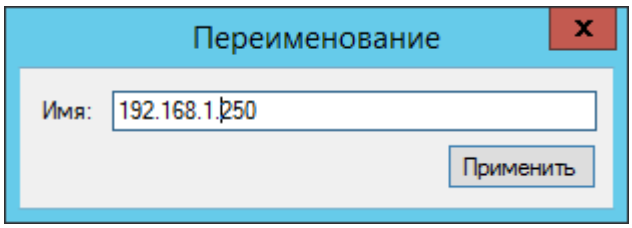


Рисунок 34 - Окно переименования сервера

После того как сервер переименован, следует выполнить его подключение. Для этого нужно выбрать сервер в списке (рисунок 35) и нажать кнопку <Подключить сервер> (или выбрать пункт меню «Прокси-сервера» –> «Подключить»; или выбрать пункт контекстного меню «Подключить», вызываемого по правому нажатию кнопкой мыши на имени сервера в списке, – рисунок 33).

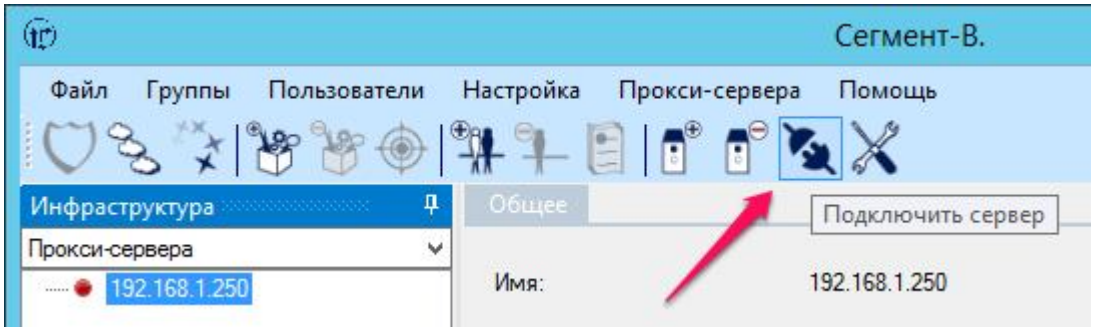


Рисунок 35 - Подключение сервера

В случае успешного выполнения действия цвет маркера прокси-сервера сменится на зеленый (рисунок 36).

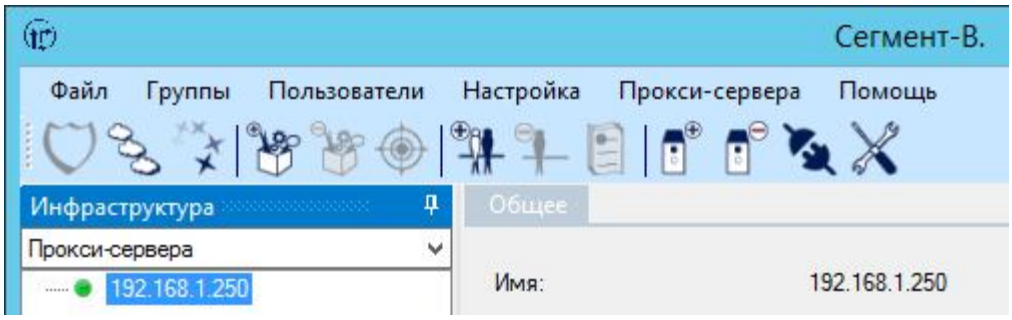


Рисунок 36 - Подключенный сервер в списке

ВНИМАНИЕ! В случае одновременного использования нескольких прокси-серверов (например, в случае резервирования) необходимо добавить каждый сервер!

ВНИМАНИЕ! Добавление прокси-серверов в количестве, большем предусмотренного лицензией, невозможно. Подробнее о лицензировании см. разделе 5 данного руководства.

ВНИМАНИЕ! При потере соединения между утилитой управления «Сегмент-В.» и прокси-сервером статус соединения не обновится! Для обновления статуса соединения необходимо перезапустить утилиту!

ВНИМАНИЕ! Перед тем как перейти к дальнейшим действиям, убедитесь, что в разделе «Прокси-сервера» инфраструктуры все элементы подключены (у всех элементов имеется зеленый маркер).

Подробнее о работе с утилитой **«Segment-V.»** см. в подразделе 3.9 данного руководства и в «Руководстве администратора» на комплекс.

3.8.2. Добавление учетной записи АБИ

ВНИМАНИЕ! Предполагается, что учетная запись АБИ уже создана и ей заданы соответствующие права (как минимум, “Read Only”) в vSphere.

Для настройки комплекса рекомендуется пользоваться специальной учетной записью АБИ. Для этого необходимо перейти в режим отображения пользователей (выбрать раздел «Пользователи» инфраструктуры в главном окне программы) и добавить соответствующего пользователя в систему, нажав в главном окне программы на кнопку <Добавить пользователя> или выбрав пункт меню «Пользователи»–> «Создать» (рисунок 37).

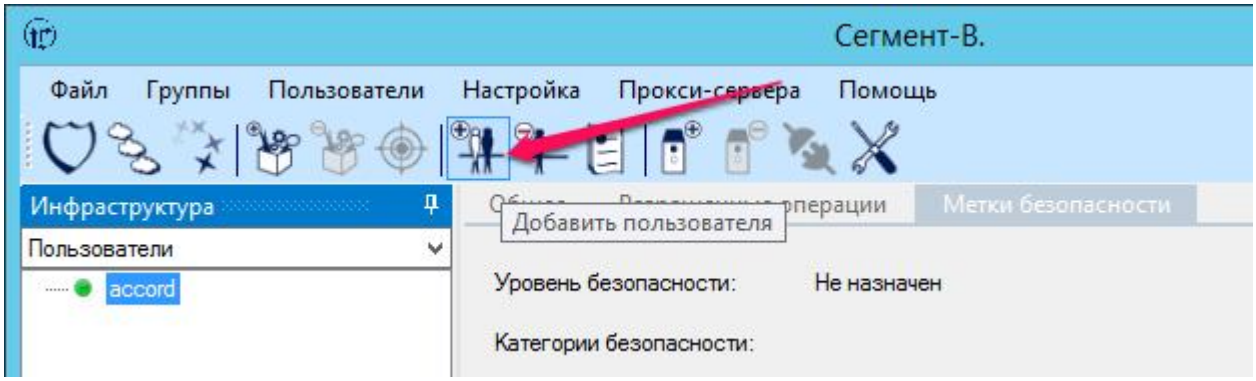


Рисунок 37 - Кнопка <Добавить пользователя>

В разделе «Пользователи» инфраструктуры появится пользователь «user». Нажав по нему правой кнопкой мыши и выбрав пункт контекстного меню <Редактировать> (рисунок 38), следует изменить для него параметры учетной записи.

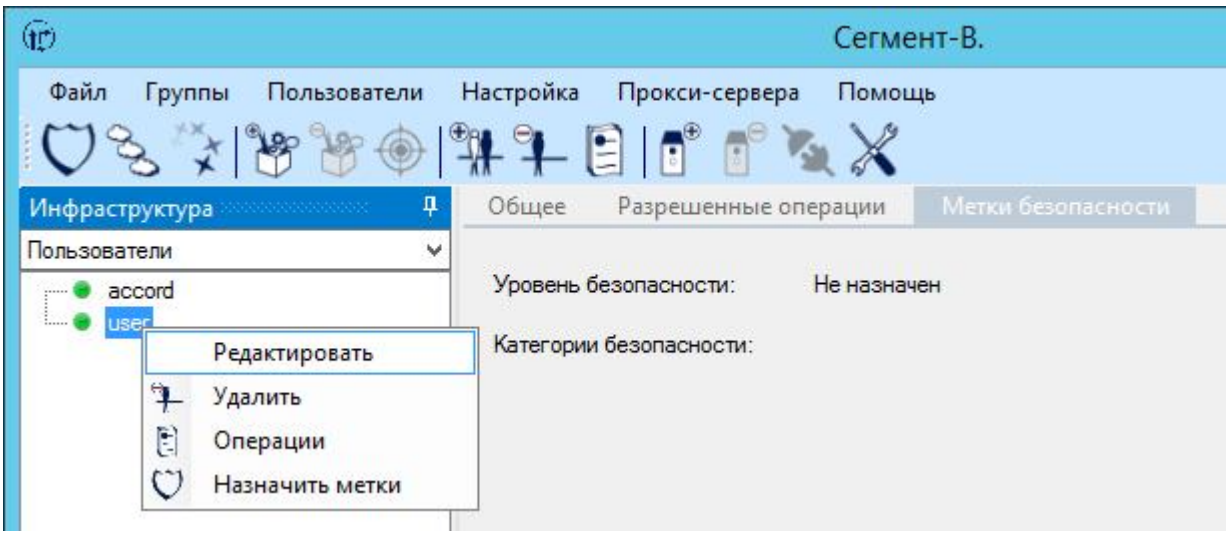


Рисунок 38 - Редактирование параметров учетной записи пользователя

В появившемся далее окне следует ввести имя пользователя, а также, если это доменный пользователь, NetBIOS имя домена (например, в случае vlab.local необходимо указывать только vlab!) и нажать кнопку <Применить> (рисунок 39).

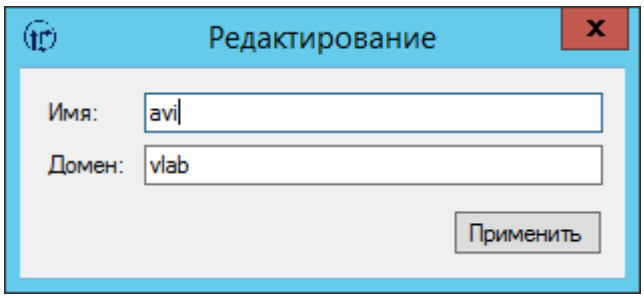


Рисунок 39 - Окно редактирования параметров учетной записи пользователя

В дальнейшем все настройки разграничения прав доступа необходимо производить от имени АБИ. Учетную запись accord рекомендуется удалить.

Подробнее о добавлении пользователей см. в пункте 3.9.2 данного руководства.

3.8.3. Установка и настройка сервиса регистрации событий

3.8.3.1. Установка и настройка сервиса регистрации событий

ВНИМАНИЕ! Предполагается, что местоположение сервиса уже заранее определено (на начальном этапе), а также проведены настройки, описанные в подразделе 3.8.1.

ВНИМАНИЕ! Если сервис регистрации событий устанавливается отдельно, то необходимо предварительно скопировать папку **«certs»** (убедившись при этом, что в ней уже содержатся сертификаты openssl.cfg, host_cert, host_key,

cacert) и файл конфигурации **Config.xml** с АРМ АБИ (см. подраздел 3.4.4), на котором установлено ПО управления, в корень папки с сервисом регистрации событий (взамен аналогичных, появившихся в папке после установки сервиса)!

Файл конфигурации содержит список хостов и vCenter, с которых будут собираться события. Если их количество увеличилось или изменились их IP-адреса или имена, необходимо обновить данный конфигурационный файл (вручную или скопировав повторно с АРМ АБИ) и перезапустить сервис!

Установка сервиса регистрации событий осуществляется при помощи утилиты **LogServiceInstall.exe** (расположена в папке с установленным ПО «Сегмент-В.», по умолчанию C:\Program Files (x86)\OKB SAPR\Segment-V\LogServiceInstall.exe).

Созданному ранее пользователю, от имени которого будет работать сервис регистрации событий (сервисная учетная запись – см. подраздел 3.3, этап 3), необходимо назначить полные права на папку с установленным ПО. Подробнее о правах этого пользователя см. в пункте 3.8.3.2 данного руководства.

После этого следует запустить утилиту **LogServiceInstall.exe** с правами администратора и начать установку сервиса регистрации событий, настроив при этом следующие параметры (рисунок 41):

- *поля «Пользователь» и «Пароль»* – параметры учетной записи, от имени которой будет работать сервис регистрации событий;
- *поле «IP адрес»* – содержит значение IP-адреса, который будет использовать сервис (в дальнейшем в утилите просмотра журнала событий **«LogViewer-V.»** необходимо будет указывать именно этот адрес). Данный пункт реализован в виде выпадающего списка, в котором отображаются IP-адреса всех доступных сетевых интерфейсов;
- *поле «Режим»* – выбор способа авторизации сервиса. По умолчанию предлагается использовать режим *SSPI* – в этом случае учетные данные пользователя, от имени которого работает сервис, используются только один раз, в процессе настройки. **При этом требуется, чтобы учетная запись существовала на АРМ, с которого выполняется авторизация, и была доступна vCenter.** В некоторых случаях целесообразно вместо режима SSPI использовать режим *CredentialStore* (например, в случае работы с VCSA, когда не работает авторизация при помощи vClient с использованием опции *use windows session credentials*). Данный режим позволяет использовать АРМ, не состоящий в домене (и при этом использовать для авторизации доменную учетную запись). В таком случае сервис запускается от имени локальной службы. Поэтому перед установкой в данном режиме необходимо предоставить полные права на папку с установленным ПО («Аккорд-В.» или «Сегмент-В.») пользователю «LOCAL SERVICE» (рисунок 40).

ВНИМАНИЕ! При выборе режима CredentialStore запрещается использовать учетные записи vSphere, имеющие права, отличные от «Read only». Предполагается также, что доступ к папке с установленным ПО

разграничивается средствами ОС или наложенными средствами разграничения доступа (ПАК «Аккорд-Win32»/ «Аккорд-Win64»).

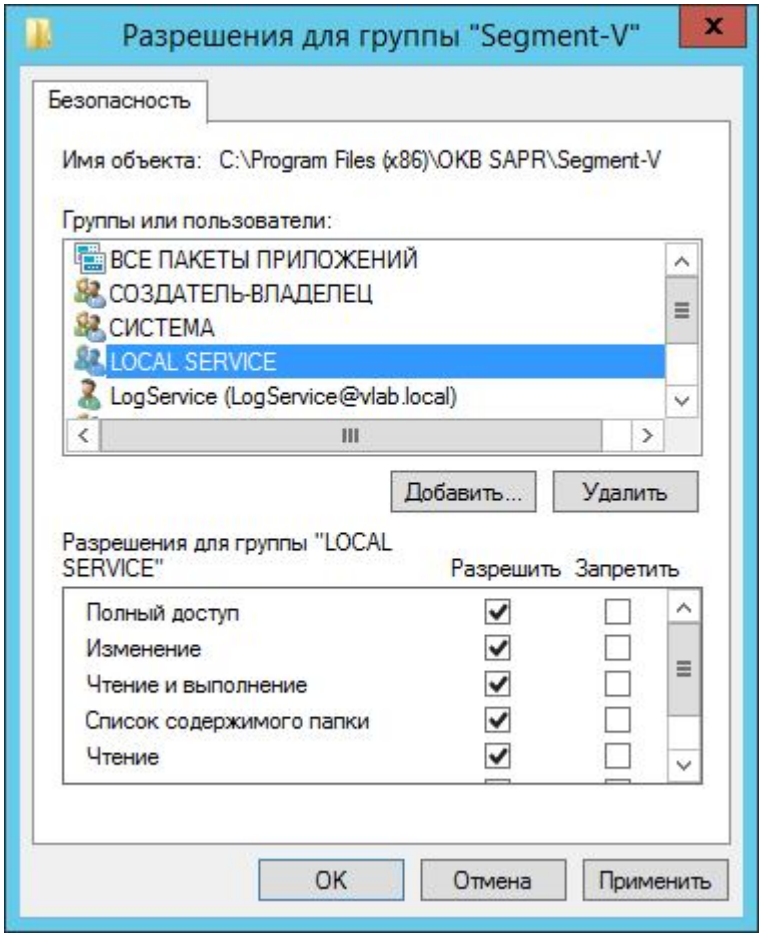


Рисунок 40 - Назначение прав сервисной учетной записи на папку с установленным ПО

- *поле «Статус»* – содержит сведения о текущем состоянии сервиса регистрации событий. Для данного поля доступны состояния «Не установлен», «Устанавливается», «Установлен». Если при попытке установки утилита не обнаружит необходимых элементов (файл конфигурации, сертификаты, база данных), будет выдано соответствующее предупреждение;
- *галочка «Сервис на одном сервере с vCenter».* Данную опцию необходимо активировать, если сервис регистрации событий установлен на одном сервере с vCenter. В этом случае для данного сервиса будет добавлена соответствующая зависимость по запуску: сначала запускается сервис «vpxd» (т.е. vCenter), затем – сервис регистрации событий.

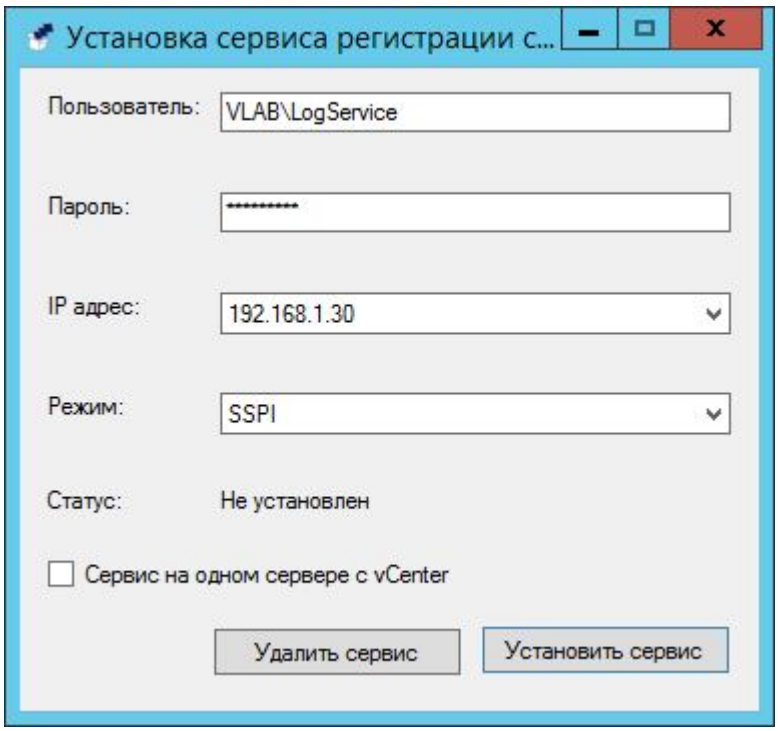


Рисунок 41 - Установка сервиса регистрации событий

По нажатии кнопки <Установить сервис> значение поля «Статус» сменится на «Устанавливаем...», затем, если все условия были выполнены, утилита отобразит сообщение «Сервис успешно установлен и готов к работе!» и в списке сервисов добавится «LogService-V» (рисунок 42).

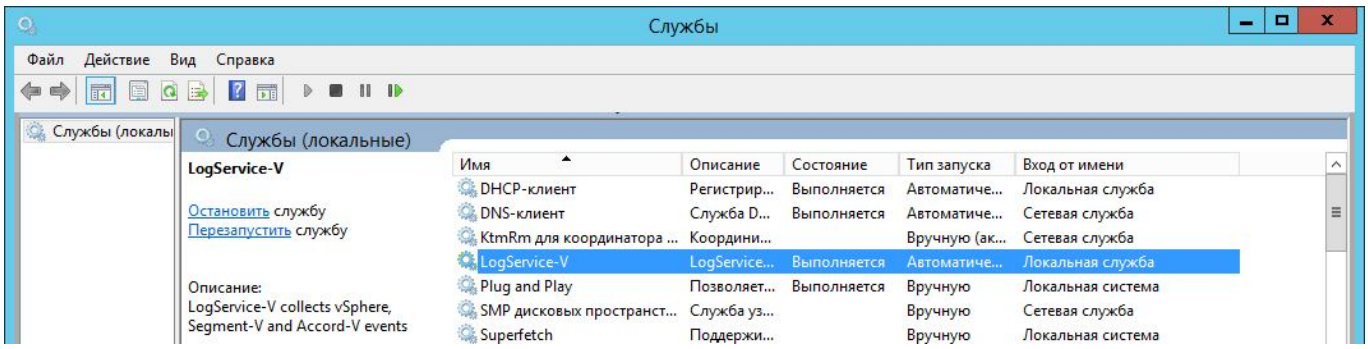


Рисунок 42 - Проверка запуска сервиса

Далее для настройки работы с сервисом регистрации событий следует запустить с правами администратора утилиту «**LogViewer-V»** на АРМ АБИ и открыть окно настроек, нажав на кнопку <Настройки>.

Рисунок 43 – Кнопка <Настройки>

В появившемся далее окне следует указать IP-адрес сервиса регистрации событий (выбранный ранее в утилите LogServiceInstall) и выполнить подключение, нажав кнопку <Принять>.

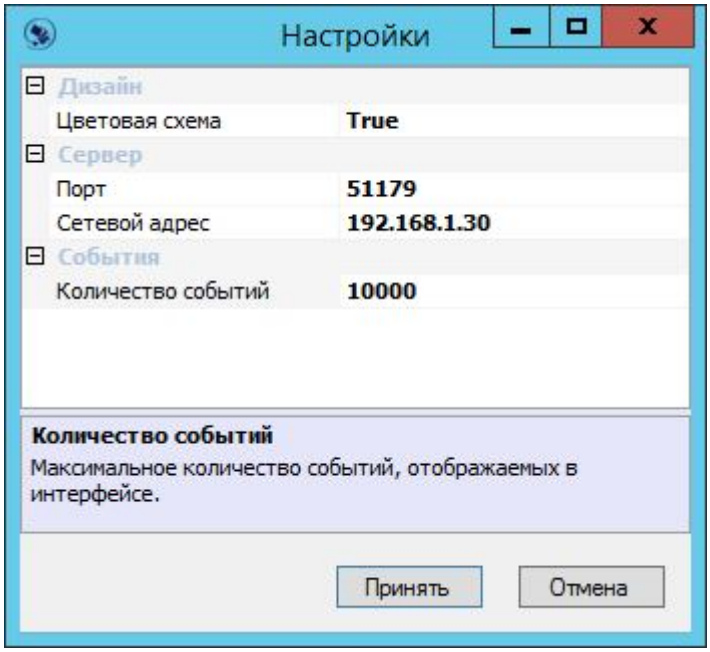


Рисунок 44 - Настройка IP-адреса сервиса регистрации событий

ВНИМАНИЕ! При задании IP-адреса сервера с установленным сервисом регистрации событий значения «127.0.0.1» и «localhost» не поддерживаются!

Далее в главном окне журнала регистрации событий следует нажать кнопку <Получить события> (либо выбрать пункт меню «Файл»/ «Получить события» или нажать кнопку F5).

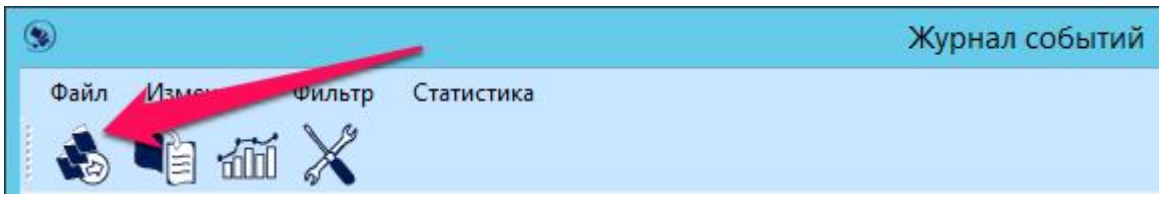


Рисунок 45 – Кнопка <Получить события>

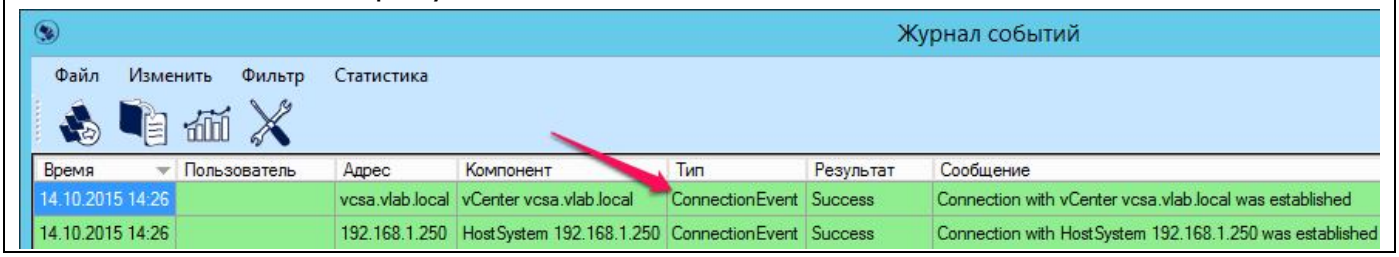
На экран выводится список всех выполненных событий.

ВНИМАНИЕ! События в журнале регистрации событий не обновляются автоматически – для получения актуальной информации необходимо выполнять процедуру их получения.

ВНИМАНИЕ! В списке полученных событий после первого старта сервиса отображаются события о подключении к vCenter и прокси-серверам «Сегмент-В.» (тип «ConnectionEvent» – показывает, что соединение с указанными в файле конфигурации элементами прошло успешно). Необходимо удостовериться, что события подключения существуют для всех заданных элементов (всех прокси-серверов и vCenter)!

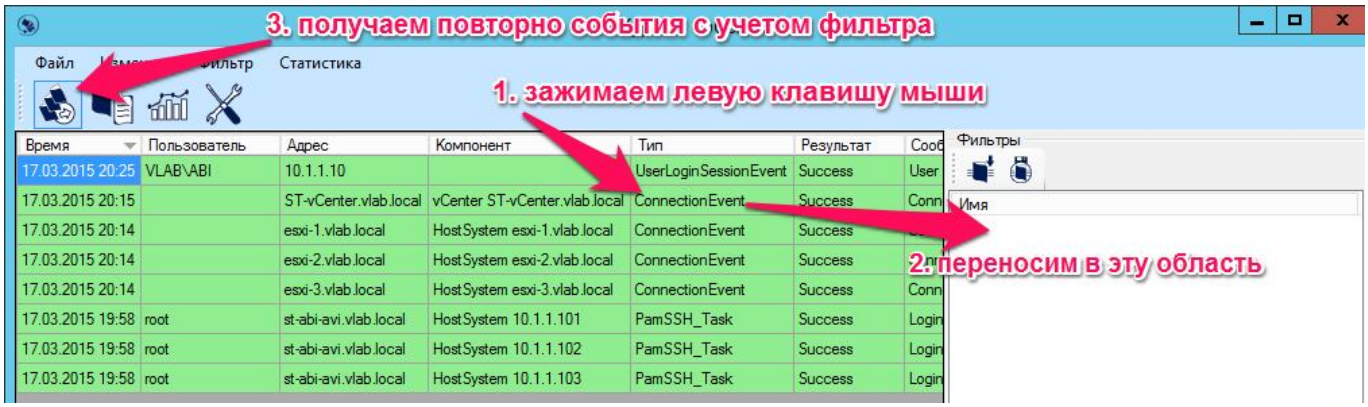
Возможной причиной, по которой соединение может быть не установлено, является рассинхронизированное время (подробнее см. 3.4.1).

В дальнейшем, если соединение потеряно, сгенерируется событие с типом «ConnectionEvent» и результатом «Error».



ВНИМАНИЕ! Конфигурационный файл считывается только при запуске сервиса! Если в процессе работы изменились IP-адреса прокси-серверов (или их количество), необходимо перезапустить сервис (в случае отдельно установленного сервиса необходимо заменить конфигурационный файл на новый).

Примечание: В дальнейшем для работы удобно пользоваться фильтрами. Можно загружать существующие фильтры или создавать и сохранять собственные. Для создания фильтра достаточно перетащить из ячейки слева значение в область фильтра и повторно получить список событий.



Работа с сервисом регистрации событий выполняется администратором безопасности информации и более подробно описана в «Руководстве администратора» на комплекс.

Примечание: Причины возникающих неполадок в процессе работы сервиса регистрации событий «Сегмент-В.» выводятся также в стандартную утилиту просмотра событий операционной системы: Start -> Administrative tools -> Event Viewer.

3.8.3.2. Сервисная учетная запись

Сервисная учетная запись, предназначенная для запуска сервиса регистрации событий, должна обладать следующими правами:

1) учетная запись должна быть доменной в случае использования режима подключения «SSPI» (в случае установки на одном АРМ с vCenter допускается локальная учетная запись), в случае использования режима «CredentialStore» сервис запускается от учетной записи «Локальная служба»;

2) на vCenter (в случае его использования) и на ESXi-хостах (в случае standalone) для данной учетной записи должны быть заданы ReadOnly Permissions;

3) на АРМ, на котором работает сервис регистрации событий, учетная запись, от имени которой он запускается, должна обладать полными правами на папку с установленным ПО «Сегмент-В.»;

4) рекомендуется запретить локальный и удаленный вход на ПК для сервисной учетной записи.

3.9. Настройка правил разграничения доступа пользователей

3.9.1. Общие сведения

Настройка разграничения прав доступа к элементам виртуальной инфраструктуры осуществляется при помощи утилиты управления комплексом **«Segment-V»**.

ВНИМАНИЕ! В «Сегмент-В.» по умолчанию включена политика запрета входа незарегистрированным пользователям. Всем пользователям, созданным в рамках vCenter, но не зарегистрированным в «Сегмент-В.», запрещается доступ через vClient.

По умолчанию в ПО зарегистрирован только пользователь accord.

ВНИМАНИЕ! Перед началом процедуры настройки правил разграничения доступа необходимо поместить полученный при заказе файл лицензии license-v.lic в папку с установленным ПО «Сегмент-В.» (подробнее см. раздел 5).

Для начала процедуры настройки разграничения доступа следует на рабочем столе АРМ АБИ запустить утилиту **«Segment-V.»** (у учетной записи АБИ, от имени которой запускается утилита, должны быть права на запись в папку с установленным ПО управления.

В появившемся окне уже будет заполнено поле «Сервер», содержащее IP-адрес vCenter, с которым будет происходить работа. Необходимо заполнить параметры учетной записи АБИ, и нажать кнопку <Вход>.

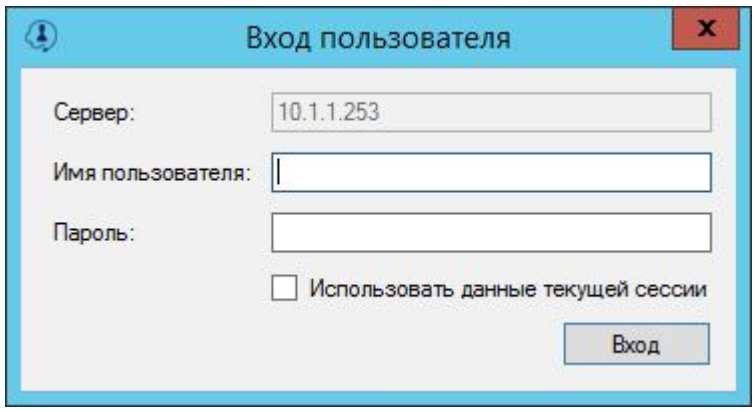


Рисунок 46 - Авторизация АБИ

При запуске утилиты автоматически происходит подключение ко всем добавленным прокси-серверам.

Если подключение по каким-либо причинам не удалось, задача «Подключение к серверу» будет завершена с состоянием «Ошибка». Если подключение прошло успешно, но выбранный режим работы сервера не является рекомендуемым, задача будет завершена с состоянием «Предупреждение». Если же подключение к прокси-серверу с безопасным режимом работы было завершено успешно, задача завершится с состоянием «Завершено».

Сервер, к которому относится задача подключения, указан в описании данной задачи.

Примечание! Информацию о добавлении прокси-сервера см. в п. 3.8.1, этап 2.

Примечание! Информацию о безопасном режиме работы прокси-сервера см. в п. 3.9.4.

Далее на экран выводится главное окно утилиты управления комплексом (рисунок 47).

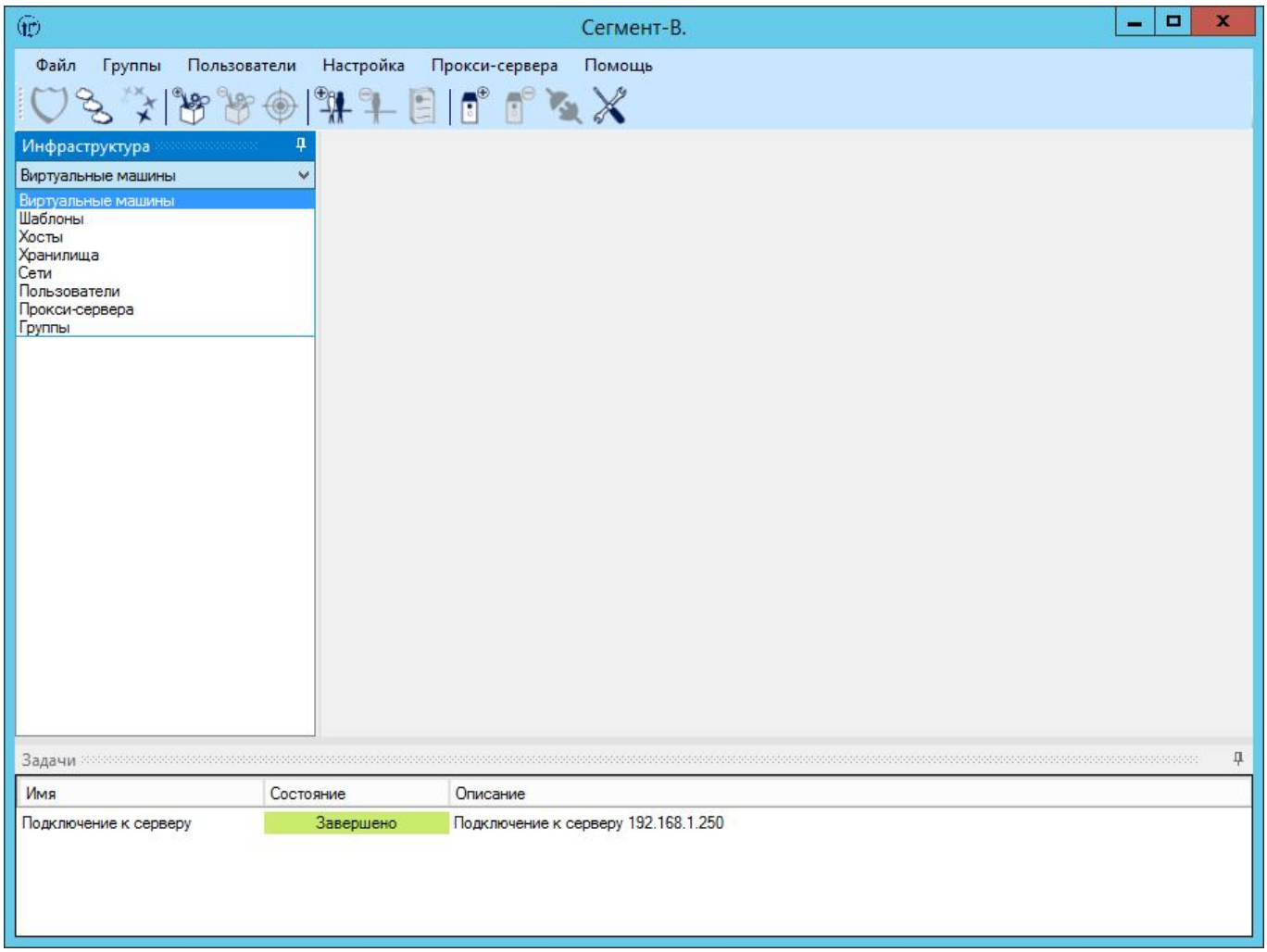


Рисунок 47 - Главное окно утилиты управления комплексом

Главное окно содержит следующие кнопки на панели задач:

- <Назначить метки> – назначение меток безопасности пользователям и объектам виртуальной инфраструктуры;
- <Настроить уровни> – создание, изменение, удаление уровней доступа (иерархических меток безопасности);
- <Настроить категории> – создание, изменение, удаление категорий доступа (неиерархических меток безопасности);
- <Добавить группу> – создание групп объектов для назначения им одинаковых меток;
- <Удалить группу> – удаление группы;
- <Добавить в группу> – добавление объектов виртуальной инфраструктуры (ВМ, пользователи, сети, хосты, хранилища, шаблоны);
- <Добавить пользователя> – создание пользователя;
- <Удалить пользователя> – удаление пользователя;
- <Операции> – настройка операций, разрешенных пользователю;
- <Добавить сервер> – создание прокси-сервера;

- <Удалить сервер> – удаление прокси-сервера;
- <Подключить> – подключение прокси-сервера;
- <Настройка> – выбор режима работы прокси-серверов.

В разделе <Инфраструктура> отображаются все доступные для изменения и настройки элементы виртуальной системы. К ним относятся:

- виртуальные машины;
- шаблоны;
- хосты;
- хранилища;
- сети (группы портов и распределенные группы портов);
- пользователи;
- прокси-серверы (серверы безопасности);
- группы.

Для элементов инфраструктуры предусмотрены индикаторы состояний:

1. Для виртуальных машин:

- зеленый маркер – назначение меток разрешено, ВМ выключена;
- красный маркер – назначение меток ВМ разрешено, ВМ включена;
- желтый маркер – назначение меток ВМ разрешено, ВМ в состоянии «Suspend»;
- имя ВМ отмечено серым – ВМ удалена или конвертирована в шаблон;
- имя ВМ отмечено красным – недостаточно информации о ВМ (например, ВМ находится в одном из статусов orphaned, inaccessable, unknown, disconnected).

2. Для шаблонов:

- зеленый маркер – назначение меток разрешено;
- имя отмечено серым – шаблон удален или конвертирован в ВМ;

3. Для хостов, хранилищ и сетей:

- всегда зеленый маркер;
- имя отмечено серым – объект удален;
- имя отмечено красным – недостаточно информации об объекте (например, находится в одном из статусов orphaned, inaccessable, unknown, disconnected).

4. Для пользователей:

- всегда зеленый маркер.

5. Для серверов безопасности (прокси-серверов):

- зеленый маркер – соединение с сервером установлено;
- красный маркер – соединение с сервером не установлено.

В случае если ВМ, шаблон, хранилище, сеть или хост были удалены, они помечаются серым цветом как неактивные. При следующем включении ПО управления они уже не будут отображаться в списке.

3.9.2. Добавление пользователей

ВНИМАНИЕ! ПО «Сегмент-В.» не создает своих пользователей в инфраструктуре VMware, а только разрешает/запрещает доступ пользователям, уже созданным в рамках VMware.

По умолчанию в ПО «Сегмент-В.» добавлен пользователь «accord» (соответствует пользователю «accord», созданному ранее в инфраструктуре VMware, – см. 3.3, п. 3), от учетной записи которого производится первоначальная настройка остальных пользователей.

ВНИМАНИЕ! После выполнения процедуры добавления пользователей учетную запись accord рекомендуется удалить.

Добавить пользователя можно двумя способами:

1)добавить пользователя вручную;

2)загрузить пользователей из домена.

Далее рассмотрены оба случая.

3.9.2.1. Добавление пользователя вручную

Для ручного добавления пользователя в ПО «Сегмент-В.» следует в главном окне программы нажать кнопку <Добавить пользователя> (рисунок 48) или выбрать пункт меню «Пользователи» -> «Создать».

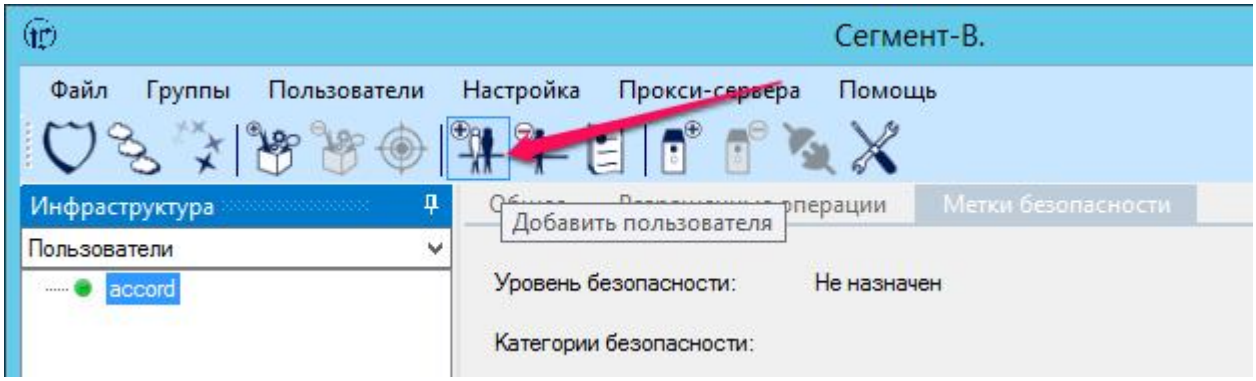


Рисунок 48 - Кнопка <Добавить пользователя>

В разделе «Пользователи» инфраструктуры появится пользователь «user». Нажав по нему правой кнопкой мыши и выбрав пункт контекстного меню <Редактировать> (рисунок 49), следует изменить для него параметры учетной записи.

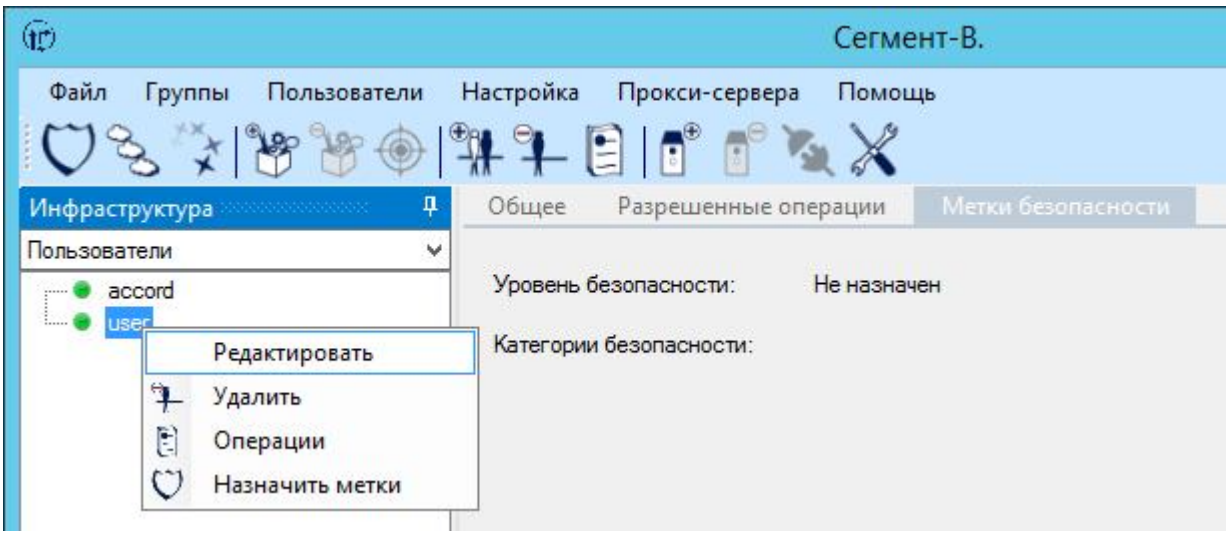


Рисунок 49 - Редактирование параметров учетной записи пользователя

В появившемся далее окне следует изменить имя учетной записи на соответствующее добавляемому пользователю VMware vSphere. Если добавляемая учетная запись является доменной, следует также указать NetBIOS имя домена в поле «Домен».

Имя пользователя должно содержать не менее трех символов (кириллица поддерживается, регистр букв не имеет значения).

После заполнения необходимых данных следует нажать кнопку <Применить> (рисунок 50).

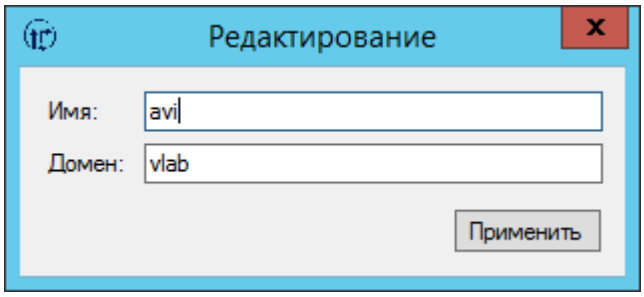


Рисунок 50 - Окно редактирования параметров учетной записи пользователя

3.9.2.2. Импорт пользователей из домена

Для выполнения процедуры импорта пользователей из домена следует в главном окне утилиты управление комплексом выбрать пункт меню «Пользователи» –> «Импорт из AD...». В появившемся окне «Загрузка пользователей» (рисунок 51) необходимо указать NetBIOS имя домена (до первой точки), из которого планируется добавить пользователей.

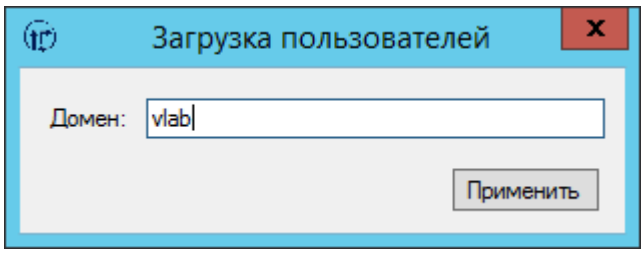


Рисунок 51 - Окно «Загрузка пользователей»

По нажатии кнопки <Применить> на экран выводится окно «Импорт пользователей» (рисунок 52), в левом списке которого отображаются все пользователи домена.

Для того чтобы импортировать пользователей из домена, следует выделить в левом списке всех необходимых пользователей и поместить их в правый список, нажав кнопку <+> (поддерживается множественное выделение с использованием клавиш <Ctrl> или <Shift>). После того как правый список будет окончательно сформирован, следует нажать кнопку <Применить> (рисунок 52).

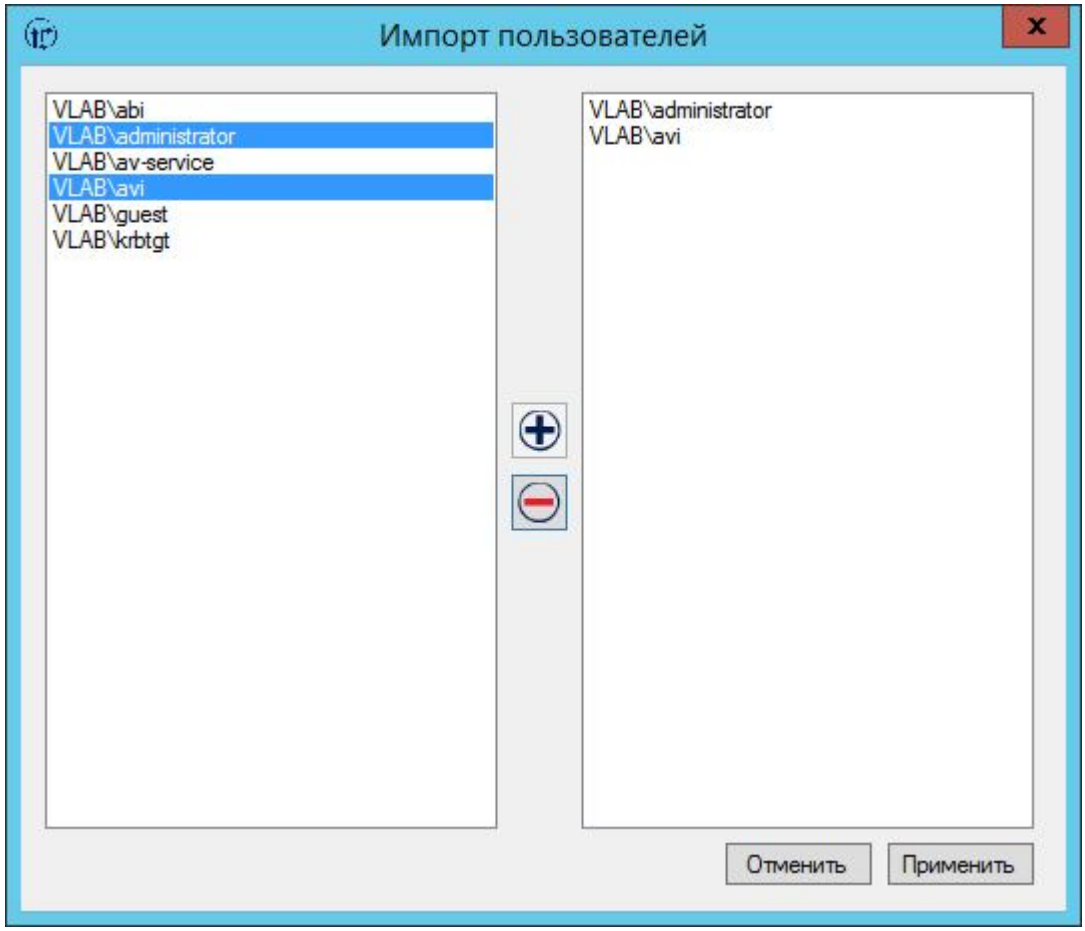


Рисунок 52 - Импорт пользователей

ВНИМАНИЕ! Импорт пользователей из AD возможен только в том случае, если утилита «Segment-V.» запущена от имени доменного пользователя. Кроме того, данный пользователь должен обладать правами администратора на папку с

установленным ПО управления комплексом (по умолчанию: C:\Program Files (x86)\OKB SAPR\Segment-V).

Если требуется удалить пользователя из ПО «Сегмент-В.», следует в главном окне утилиты управления комплексом выделить его в списке пользователей, а затем нажать кнопку <Удалить пользователя> на панели задач (или выбрать пункт меню «Пользователи» -> «Удалить», или, щелкнув по пользователю правой кнопкой мыши, выбрать пункт контекстного меню «Удалить»).

ВНИМАНИЕ! Удаление всех пользователей из ПО «Сегмент-В.» полностью заблокирует вход в виртуальную инфраструктуру из внешней сети и в само ПО «Сегмент-В.»! Если это произошло, необходимо пересоздать базу данных «Сегмент-В.» на АРМ АБИ прокси-сервере. Для этого на клиенте следует вызвать из папки с ПО утилиту **Repair.exe** с параметром *–db*, на сервере безопасности запустить из папки */etc/accord-v* утилиту **accordguard** с параметром *–n*. Данное действие восстановит настройки по умолчанию (пользователя «accord»), однако удалит назначенные политики безопасности и созданные метки.

3.9.3. Настройка меток безопасности

Данная версия «Сегмент-В.» позволяет создавать и работать с иерархическими (уровнями) и неиерархическими метками (категориями).

Разрешено создание 64 различных уровней иерархии (при создании иерархической метки задается его имя и уровень: от 1 до 64) и неограниченное количество категорий (для которых задается имя и цвет).

3.9.3.1. Настройка уровней

ВНИМАНИЕ! Хотя бы один уровень обязательно должен быть создан.

Даже если для разграничения доступа не предполагается использование иерархических меток, нужно создать один уровень (с любым «порядком») и назначить его всем объектам виртуальной инфраструктуры.

Для того чтобы создать уровень, следует в главном окне программы нажать кнопку <Настроить уровни> (рисунок 53) (или выбрать пункт меню «Настройка» -> «Уровни...») и в появившемся окне нажать кнопку <Добавить> (рисунок 54).

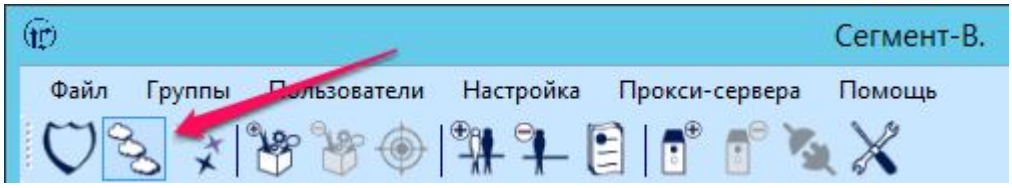


Рисунок 53 - Кнопка <Настроить уровни>

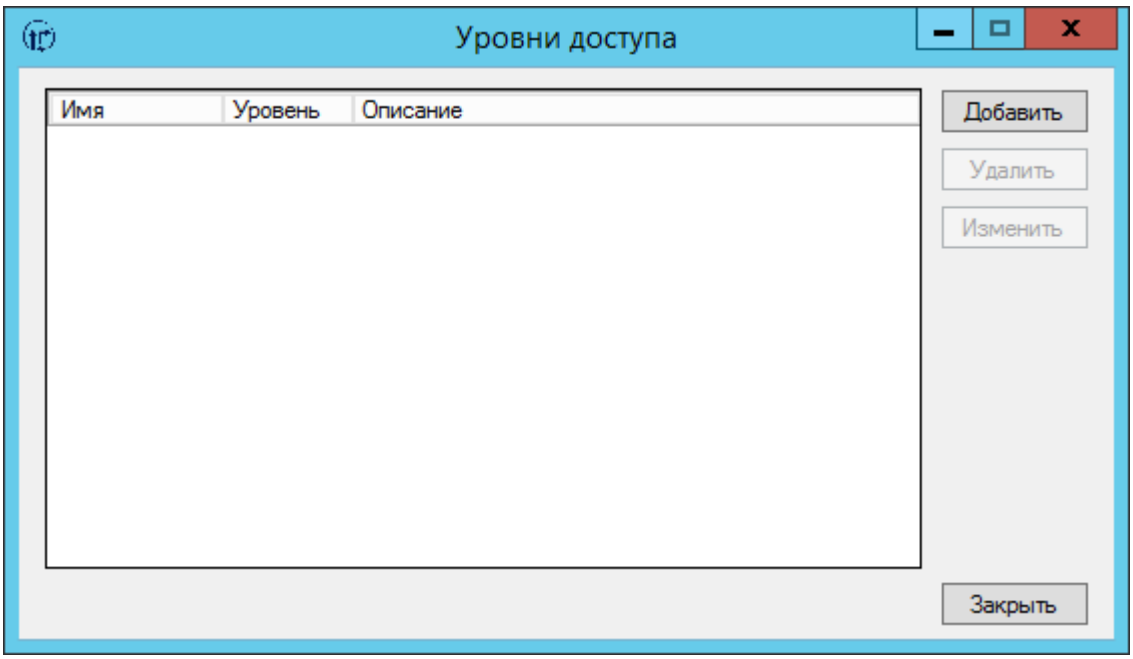


Рисунок 54 - Уровни доступа

В появившемся далее окне (рисунок 55) следует задать имя уровня, его уровень иерархии и, опционально, описание (кириллица поддерживается).

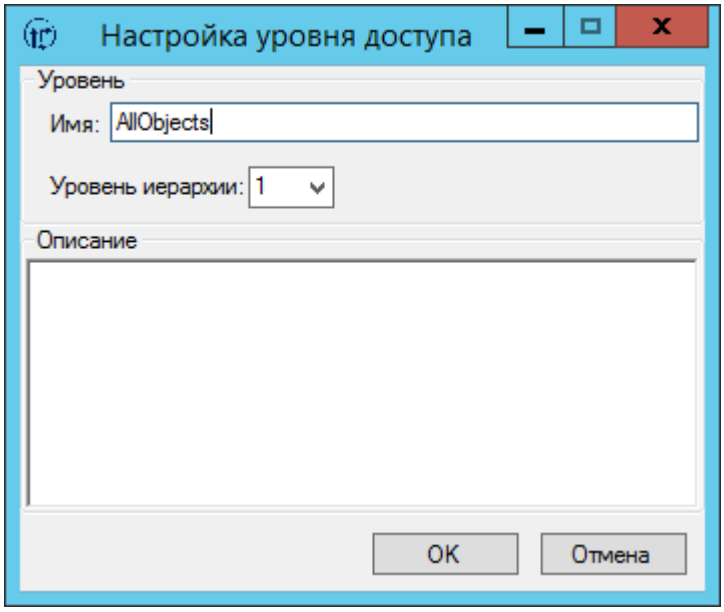


Рисунок 55 - Настройка уровня доступа

ВНИМАНИЕ! Создание уровней с одинаковыми именами и/или уровнями иерархии запрещено.

Если требуется изменить параметры уровня, следует в окне «Уровни доступа» (рисунок 56) выбрать из списка соответствующий элемент и нажать кнопку <Изменить>. В появившемся далее окне «Настройка уровня доступа» (рисунок 55) поля «Имя», «Уровень иерархии»> и «Описание» будут заполнены текущими значениями элемента.

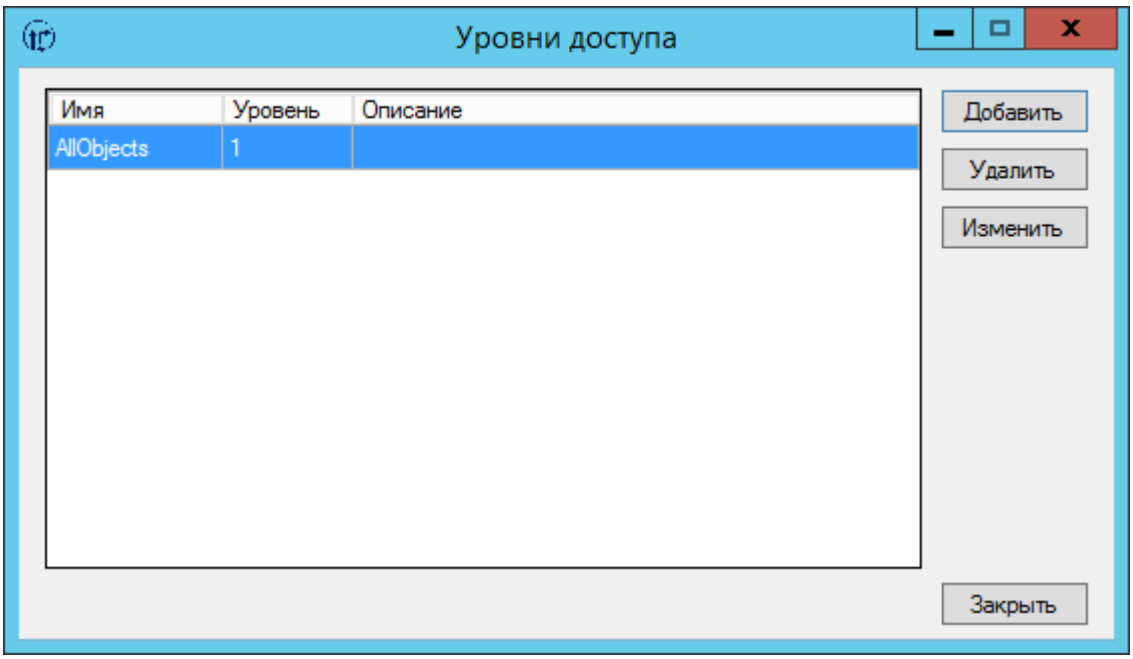


Рисунок 56 - Уровни доступа

ВНИМАНИЕ! При изменении уровня иерархии метки изменяется уровень конфиденциальности объектов и уровень доступа пользователей, которым данная метка была назначена. Это может привести к нарушению политики безопасности.

Если требуется удалить уровень, следует в окне «Уровни доступа» (рисунок 56) выбрать из списка соответствующий элемент и нажать кнопку <Удалить>.

ВНИМАНИЕ! После удаления метки уровень конфиденциальности объектов и уровень доступа пользователей, которым данная метка была назначена, будет отсутствовать. Это может привести к нарушению политики безопасности.

3.9.3.2. Настройка категорий

Для того чтобы создать категорию, следует в главном окне программы нажать кнопку <Настроить категории> (рисунок 57) или выбрать пункт меню «Настройка» -> «Категории...» и в появившемся окне нажать кнопку <Добавить> (рисунок 58).

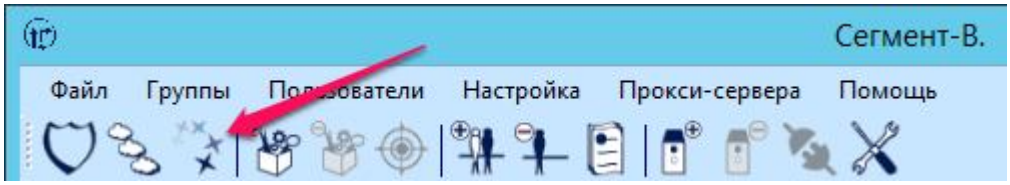


Рисунок 57 - Кнопка <Настроить категории>

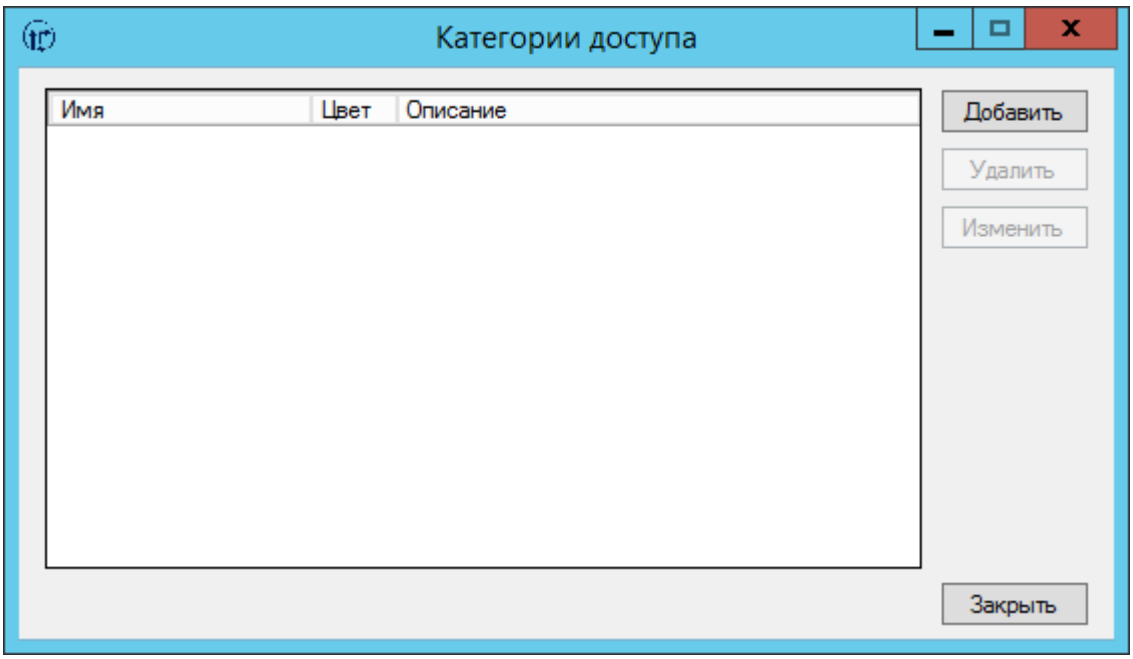


Рисунок 58 - Категории доступа

В появившемся далее окне (рисунок 59) следует задать имя категории, ее цвет и, опционально, описание (кириллица поддерживается).

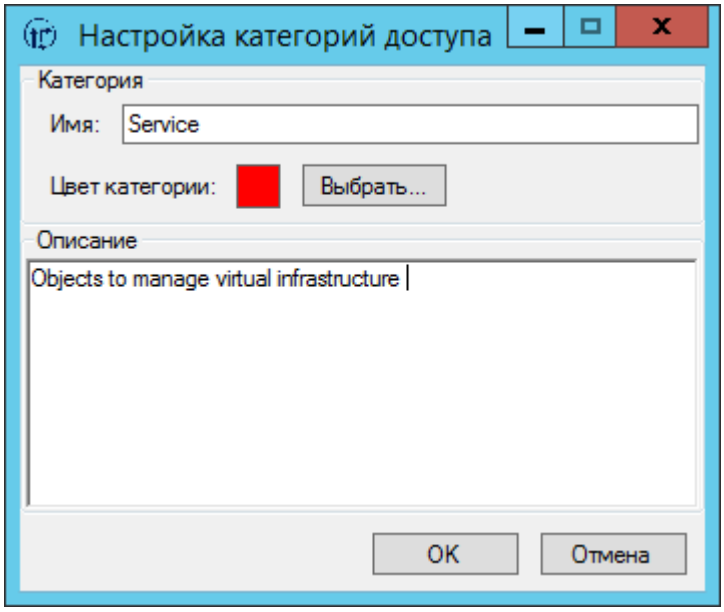


Рисунок 59 - Настройка категорий доступа

ВНИМАНИЕ! Создание категорий с одинаковыми именами и/или цветами запрещено.

Если требуется изменить параметры категории, в окне «Категории доступа» (рисунок 60) следует выбрать из списка соответствующий элемент и нажать кнопку <Изменить>. В появившемся далее окне «Настройка категорий доступа» (рисунок 59) поля «Имя», «Цвет» и «Описание» будут заполнены текущими значениями элемента.

ВНИМАНИЕ! Переименование стандартных портгрупп (не распределенных) во время и после настройки политик безопасности приводит к потере назначенных для данной сети меток!

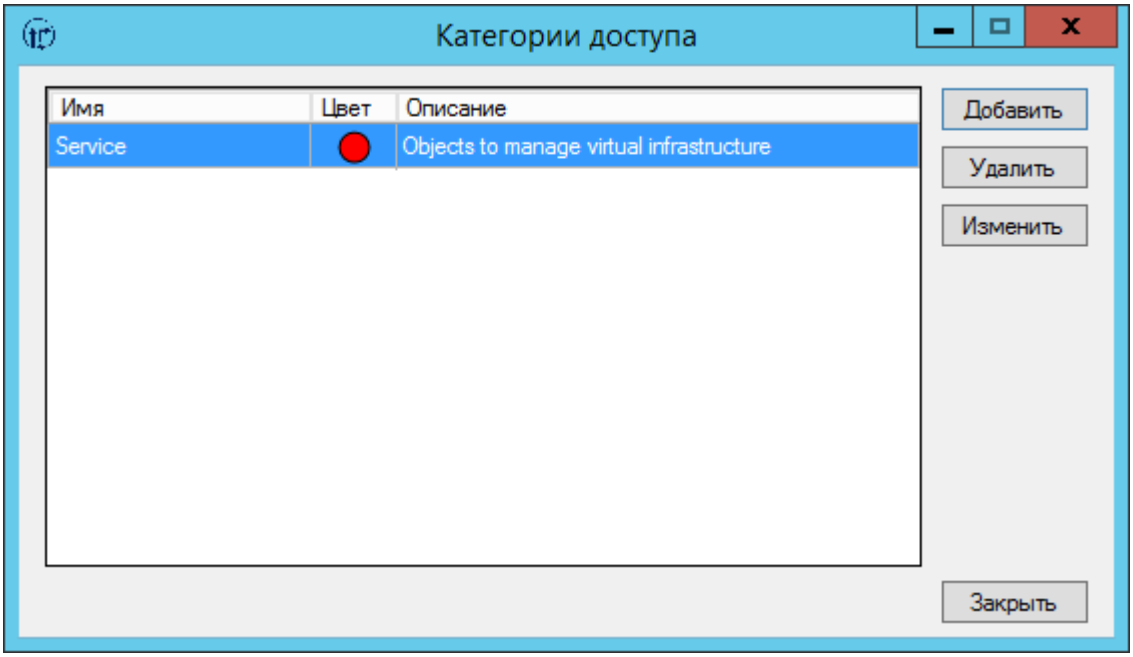


Рисунок 60 - Категории доступа

Если требуется удалить категорию, следует в окне «Категории доступа» (рисунок 60) выбрать из списка соответствующий элемент и нажать кнопку <Удалить>.

ВНИМАНИЕ! После удаления категории из списка категорий, у объектов и пользователей, которым данная метка была назначена, будет удалена соответствующая категория. Это может привести к нарушению политики безопасности.

3.9.4. Назначение политик безопасности

3.9.4.1. Общие сведения

Работа через vClient подразумевает в качестве действий операции, которые могут затрагивать один или несколько объектов доступа. Объектами доступа в ПО «Сегмент-В.» являются хосты, ВМ, шаблоны, сети (группы портов, распределенные группы портов) и хранилища. Примерами операций могут служить: включение ВМ, миграция ВМ со сменой хоста и/или хранилища, переименование и так далее.

Все действия, с точки зрения их разрешения или запрета на исполнение пользователем, можно разделить на три категории:

- разграничиваемые;
- всегда разрешенные;

– всегда запрещенные.

Из разграничиваемых действий для каждого пользователя создается свой список разрешенных операций пользователя.

Примечание: список разграничиваемых действий пользователя см. в пункте 3.9.4.4.

Решение о разрешении или запрете на исполнение разграничиваемых действий принимается на основе списка разрешенных пользователю операций (см. 3.9.4.4) и на основе меток, назначенных пользователю и всем объектам доступа, участвующим в операции (см. 3.9.4.3). Кроме того, свое влияние оказывает также политика прокси-сервера (см. 3.9.4.2).

Настройки прокси-сервера позволяют задать различные варианты работы:

1) **Работа с незарегистрированными объектами.** Возможные значения параметра: «Запрещено», «Разрешено».

При запрете на работу с незарегистрированными объектами любому пользователю будут запрещены все разграничиваемые действия (вне зависимости от списка разрешенных операций пользователя) над объектами, которым не назначен уровень.

При значении параметра «Разрешено» любому пользователю будут разрешены все разграничиваемые действия над незарегистрированными объектами.

2) **Мягкий режим.** Возможные значения параметра: «Включен», «Выключен».

Если мягкий режим включен, то всем пользователям разрешаются все операции над любыми объектами; при этом данные о совершенных действиях собираются сервисом регистрации событий.

3) **Проверка уровня сессии.** Возможные значения параметра: «Включена», «Выключена».

Если проверка уровня сессии включена, разрешены будут лишь те операции, в которых участвуют объекты одного уровня доступа.

ВНИМАНИЕ! Даже если проверка уровня сессии выключена, для разрешения выполнения операции уровень пользователя должен быть больше или равен уровню объекта/объектов.

4) **Проверка категорий сессии.** Возможные значения параметра: «Включена», «Выключена».

Если проверка категорий сессии включена, разрешены будут лишь те операции, в которых участвуют объекты, пересечение множеств категорий которых не пусто.

ВНИМАНИЕ! Даже если проверка категорий сессии выключена, для разрешения выполнения операции множество категорий объектов должно быть подмножеством множества категорий пользователя.

Рекомендуемым режимом работы прокси-сервера считается: запрет на работу с незарегистрированными объектами, отключенный мягкий режим и включенные проверки уровня и категорий сессии. Таким образом, в рамках

«Сегмент-В.» реализована политика безопасности, предусматривающая следующие правила (мягкий режим отключен):

1) Если пользователь не зарегистрирован в ПО «Сегмент-В.», **доступ** ему **запрещается**.

2) Если объект не зарегистрирован и работа с незарегистрированными объектами запрещена, **доступ запрещается**.

3) Если уровень доступа пользователя меньше уровня конфиденциальности хотя бы одного из объектов, участвующих в операции, **доступ запрещается**.

4) Если существует хотя бы одна категория объекта, участвующего в операции, которая не назначена пользователю, **доступ запрещается**.

5) Если уровень хотя бы одного объекта отличен от уровня других объектов, участвующих в операции, и включена проверка уровня сессии, **доступ запрещается**.

6) Если пересечение множеств категорий объектов, участвующих в действии, пусто и включена проверка категорий сессии, **доступ запрещается**.

7) Если данная операция не входит в список разрешенных пользователю, **доступ запрещается**.

8) Если данная операция находится в списке всегда запрещенных действий, **доступ запрещается**.

9) В остальных случаях **доступ разрешается**.

ВНИМАНИЕ! Запрет или разрешение на доступ зависит от объектов, участвующих в операции, и неверное представление о том, какие объекты вовлечены в операцию, может привести к неверному построению системы виртуальной инфраструктуры с помощью «Сегмент-В.».

3.9.4.2. Настройка политики прокси-сервера

Для того чтобы выполнить настройку политики прокси-сервера, следует в главном окне утилиты управления нажать кнопку <Настройка> (рисунок 61) (или выбрать пункт меню «Прокси-сервера» -> «Настройка…»).

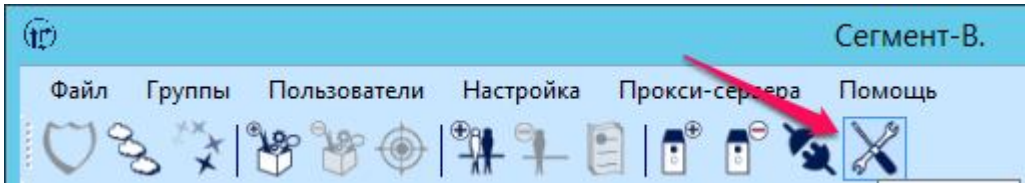


Рисунок 61 - Кнопка <Настройка>

Откроется окно «Настройка» со списком всех подключенных прокси-серверов и указанием их статуса и режимов работы. Из выпадающего списка в соответствующих столбцах следует выбрать нужные значения параметров прокси-сервера и нажать кнопку <Применить> (рисунок 62).

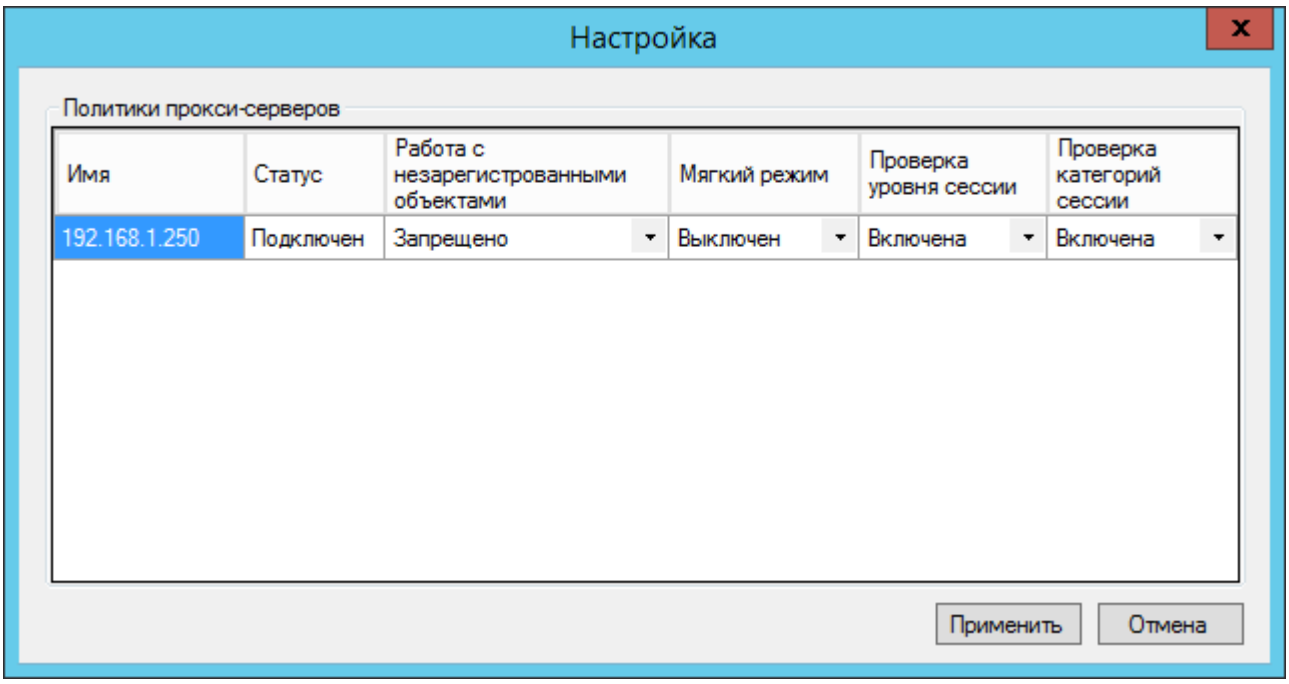


Рисунок 62 - Настройка политик прокси-сервера

ВНИМАНИЕ! Для корректной работы в режиме отказоустойчивости прокси-серверы должны иметь одинаковые настройки политики.

3.9.4.3. Настройка меток

Для того чтобы назначить политики безопасности выбранному в списке объекту доступа, следует в главном окне утилиты управления нажать кнопку <Назначить метки> (рисунок 63), в появившемся далее окне (рисунок 64) выбрать необходимый уровень и категории из списка созданных и нажать <OK>.

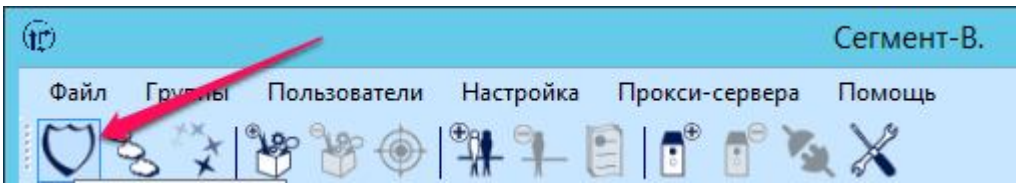


Рисунок 63 - Кнопка <Назначить метки>

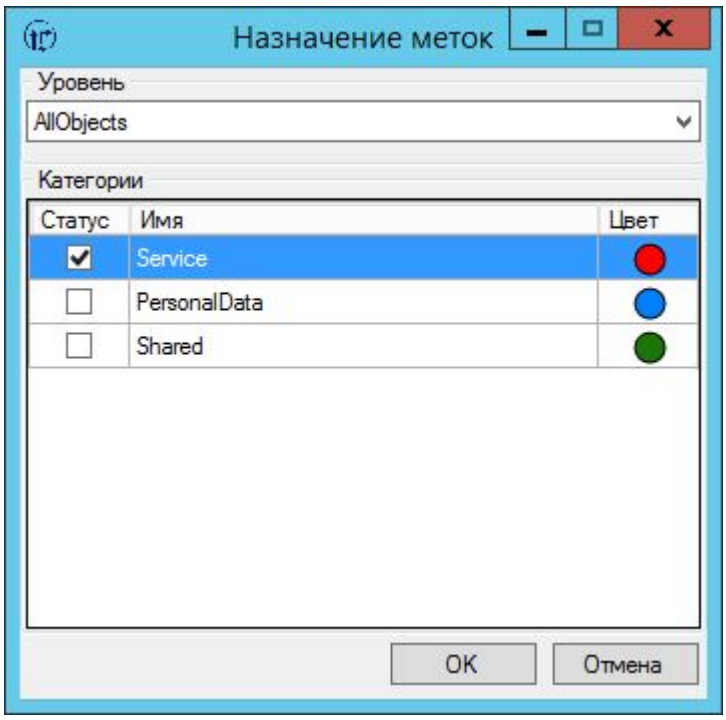


Рисунок 64 - Назначение меток

ВНИМАНИЕ! Если данному элементу ранее были назначены какие-либо метки, они будут переназначены согласно выбранным правилам после нажатия кнопки <OK>.

3.9.4.4. Настройка разрешенных пользователю операций

Общие сведения

«Сегмент-В.» использует дискреционную политику для запрета/разрешения пользователям некоторых действий.

К таким разграничиваемым действиям пользователя относятся 24 операции (группы операций), выполняемые через vClient и(или) с помощью vCLI/PowerCLI.

ВНИМАНИЕ! Действия, совершаемые пользователем через Web Client, не разграничиваются. Возможна только полная блокировка доступа к Web Client.

ВНИМАНИЕ! Политика безопасности, построенная на проверке уровня и категорий пользователей и объектов, работает «поверх» дискреционной политики. Подробнее см. пункт 3.9.4 данного руководства.

Помимо разграничиваемых операций есть всегда разрешенные операции (Read-only действия) и всегда запрещенные операции.

Всегда запрещенные операции:

- удаление элементов вместе с папкой (если выставлена галочка Delete from disk);

- экспорт, удаление (Delete from disk для входящих в состав ВМ) и клонирование vApp.

Разграничиваемые действия

Вход:

- *вход в систему* – вход в систему по паролю или с учётными данными текущей сессии.

Виртуальные машины:

- *доступ к файлам ВМ* – просмотр хранилища и файлов виртуальных машин в нем;
- *удаление ВМ* – удаление ВМ и её файлов с диска;
- *создание ВМ* – создание, импорт, а также добавление в инфраструктуру ВМ;
- *запуск ВМ (vApp)* – запуск ВМ/vApp;
- *останов ВМ (vApp)* – выключение, suspend, перезапуск ВМ (vApp), в том числе гостевой ОС;
- *создание копий ВМ* – копирование в ВМ (шаблон), разворачивание ВМ из шаблона;
- *изменение конфигурации ВМ (vApp)* – изменение конфигурации оборудования ВМ (vApp);
- *доступ к консоли ВМ* – доступ к консоли ВМ по VNC;
- *контроль подключаемых к ВМ устройств* – контроль подключаемых к ВМ USB, CD, FDD;
- *экспорт ВМ* – экспорт ВМ в формат OVF/OVA;
- *миграция ВМ* – миграция/перемещение ВМ со сменой хоста и(или) хранилища.

Сетевые устройства:

- *работа с сетью* – изменение настроек сети хоста и сетевых устройств: свитчей, групп портов и их распределенных вариантов.

Хосты:

- *базовые операции с хостом* – запуск, остановка, перезапуск, подключение, отключение, maintenance mode хоста;
- *работа со службами хоста* – запуск, остановка, перезапуск сервисов хоста (изменение политик запуска/остановки сервисов всегда разрешено);
- *изменение настроек сетевого экрана* – открытие, закрытие портов, ограничение диапазона IP;
- *работа с Lockdown Mode* – включение, отключение Lockdown Mode;
- *конфигурация автостарта* – включение, отключение автостарта, изменение порядка запуска ВМ;
- *настройка DNS и маршрутизации хоста* – настройка DNS и маршрутизации хоста;
- *настройка домена на хосте* – ввод сервера в домен и вывод из него;

- *настройка времени на хосте* – ручное изменение времени, добавление NTP сервера и его включение и отключение.

Другое:

- *работа со снапшотами* – создание, откат и удаление снапшотов (вне зависимости от доступа пользователя к ВМ, со снапшотом которой он работает);
- *управление правами* – управление ролями, назначение и удаление прав;
- *исполнение команд esxcli* – исполнение команд esxcli с использованием vCLI/PowerCLI.

Создание списка разрешенных операций пользователя

По умолчанию при создании пользователей в ПО «Сегмент-В.» список разрешенных им операций пуст.

Для создания списка разрешенных выбранному пользователю операций следует в главном окне утилиты управления нажать кнопку <Операции> (рисунок 65) (либо выбрать пункт «Операции» контекстного меню, вызываемого нажатием правой кнопки мыши по пользователю в списке; либо выбрать пункт главного меню «Пользователи»–> «Операции»).

Рисунок 65 - Кнопка <Операции>

В появившемся далее окне (рисунок 66) следует отметить те действия из списка (по нажатии на действие в списке, в нижней части окна «Разрешение действий» выводится его описание), которые требуется внести в список Разрешенных для данного пользователя (при выполнении правил политик безопасности 1-4), и нажать кнопку <Установить>.

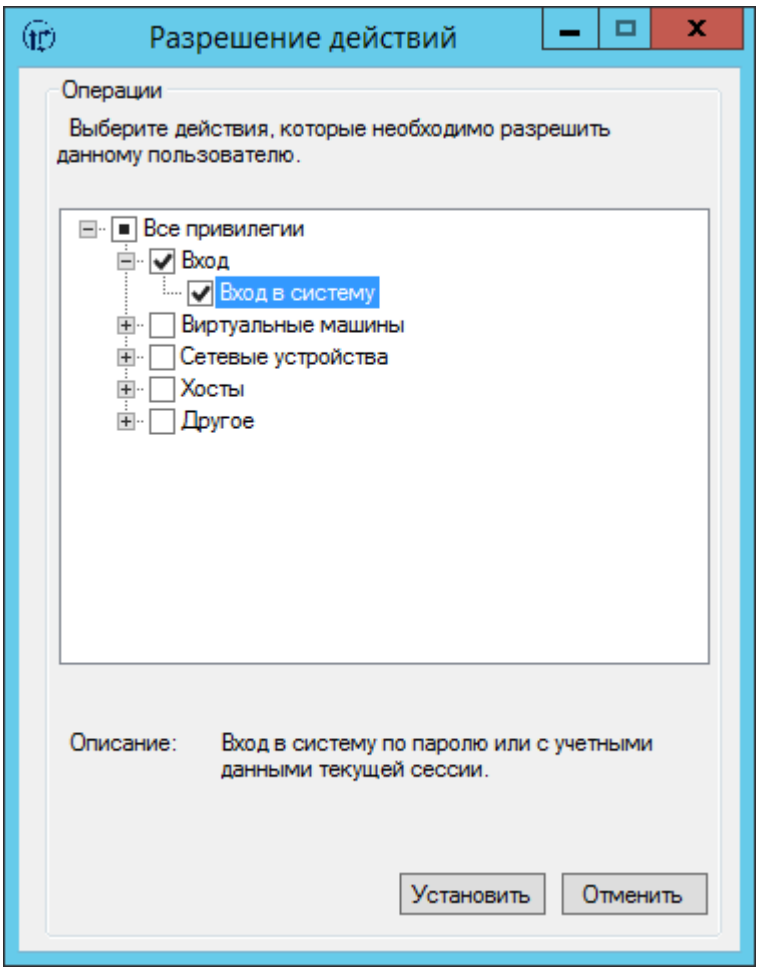


Рисунок 66 - Разрешение действий

ВНИМАНИЕ! Если данному пользователю ранее были разрешены какие-либо операции, они будут переназначены согласно выбранным правилам после нажатия кнопки <OK>.

Список разрешенных пользователю операций отображается в соответствующей вкладке главного окна утилиты управления (рисунок 67).

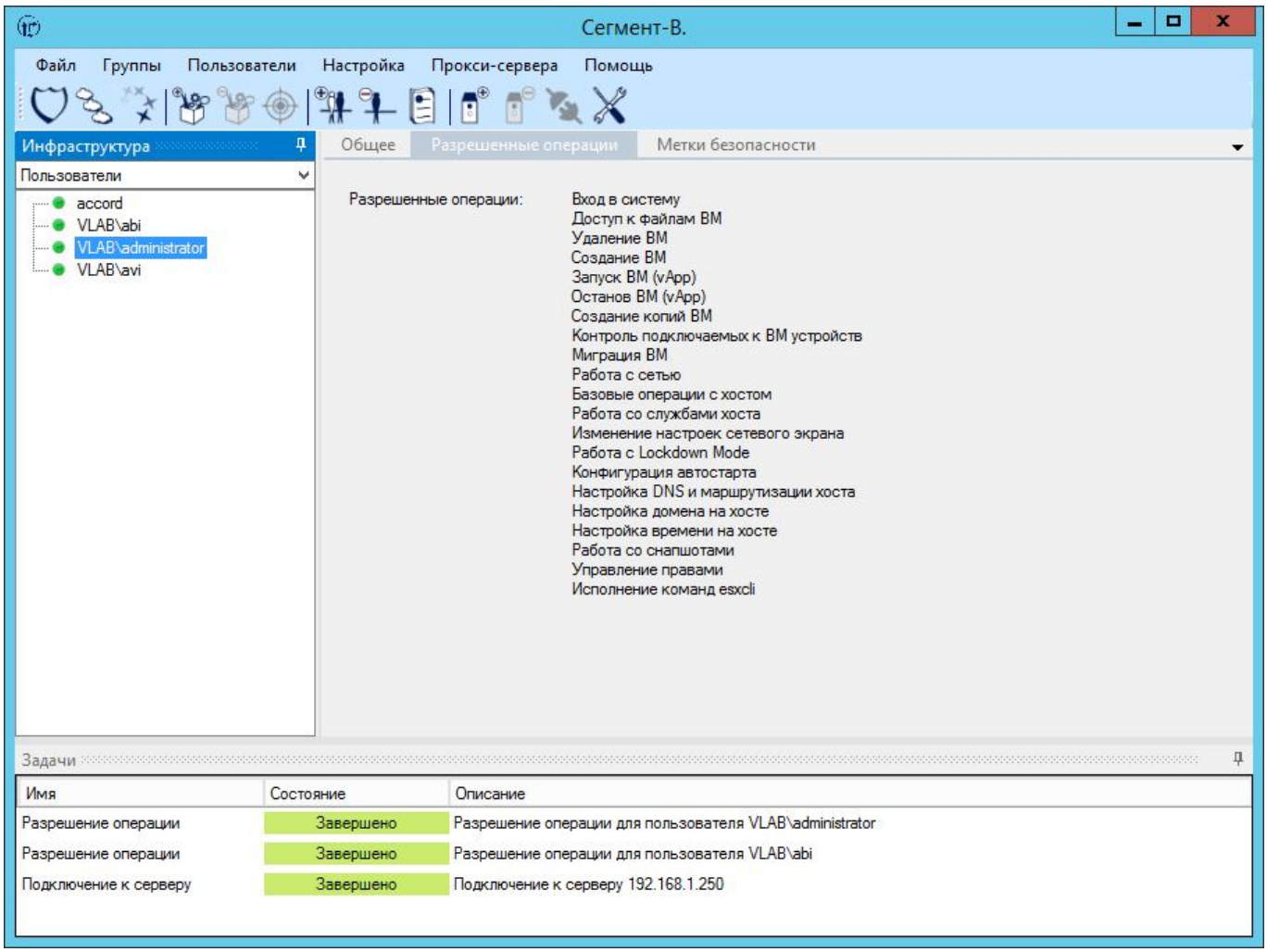


Рисунок 67 - Разрешенные операции

ВНИМАНИЕ! Даже после создания списка Разрешенных операций пользователь считается незарегистрированным в системе, если ему не назначен какой-либо уровень (см. 3.9.3.1). В отчете такой пользователь будет выделен красным цветом. При этом вход в систему будет разрешен (если это действие входит в список разрешенных пользователю).

3.9.5. Работа с группами

Любые объекты и субъекты могут быть объединены в группы – наборы элементов, для которых возможно одновременное назначение меток безопасности.

Использование групп позволяет ускорить процесс назначения меток безопасности, реализовать сегментирование ВИ более наглядным и понятным образом, а также упростить контроль за назначенными метками.

ВНИМАНИЕ! Группы существуют только в рамках ПАК «Сегмент-В.»; при создании группы виртуальная инфраструктура не меняется.

Для создания группы следует в главном окне утилиты управления нажать кнопку <Добавить группу> (или выбрать пункт меню «Группы» -> «Создать»).

Рисунок 68 – Кнопка <Добавить группу>

Добавленную группу (по умолчанию она имеет название «Folder») можно переименовать, нажав на нее правой клавишей мыши и выбрав пункт контекстного меню «Переименовать».

Для добавления объектов в группу следует выделить в списке нужную группу и нажать кнопку <Добавить в группу> (рисунок 69) (либо выбрать пункт контекстного меню «Добавить в группу»).

Рисунок 69 - Кнопка <Добавить в группу>

В появившемся далее окне (рисунок 70) с помощью кнопки <+> или простым перетаскиванием следует перенести выбранные объекты или пользователей в правую часть окна и нажать кнопку <Применить>.

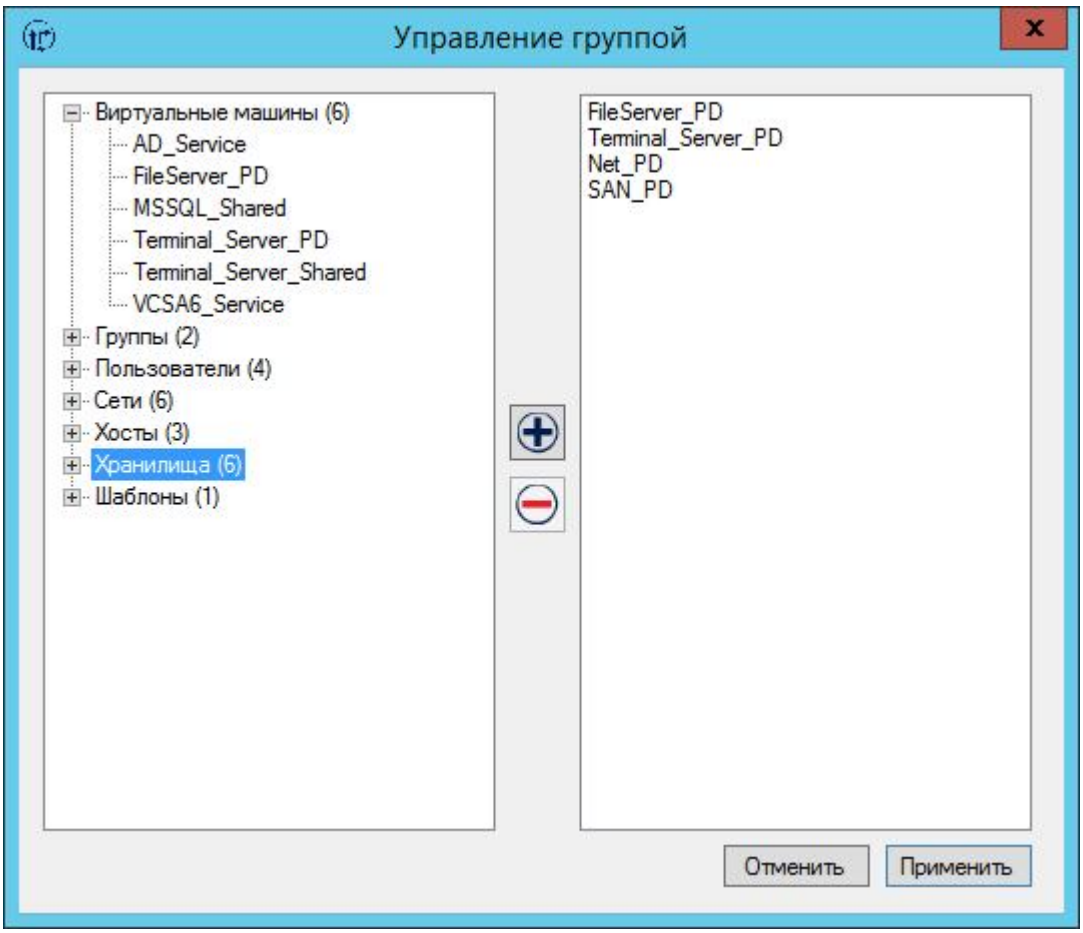


Рисунок 70 - Окно управления группой

Необходимо убедиться в том, что все объекты и субъекты добавлены в группу. После этого с помощью кнопки <Назначить метки> следует задать требуемые уровень и категории (рисунок 64). Выбранные метки будут назначены всем объектам и пользователям, входящим в группу.

ВНИМАНИЕ! При изменении меток безопасности объектов или пользователей, входящих в группу, такие элементы из группы автоматически удаляются.

ВНИМАНИЕ! Группа автоматически не объединяет в себе все объекты и пользователей с одинаковыми метками безопасности. Добавление элементов в группу выполняется только вручную.

Для того чтобы удалить группу, следует нажать на неё правой кнопкой мыши и выбрать пункт контекстного меню «Удалить группу» (либо нажать одноименную кнопку на панели задач).

ВНИМАНИЕ! Удаление группы не удаляет элементы ВИ, входящие в нее.

ВНИМАНИЕ! Метки безопасности, назначенные элементам, входящим в группу, после ее удаления остаются.

ВНИМАНИЕ! Если в базе данных обнаружатся несоответствия между назначенными метками группе и назначенными метками объекту, входящему в эту группу, при открытии утилиты «Segment-V.» появится окно с сообщением об ошибке. После закрытия окна работа с утилитой продолжится, необходимо выявить несоответствия и устранить их.

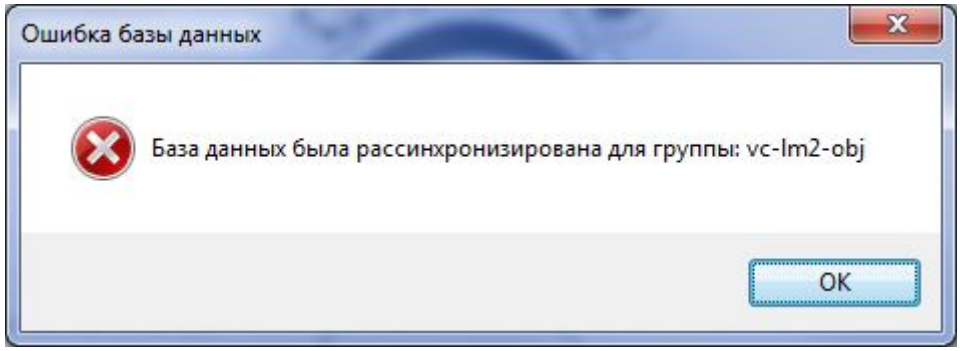


Рисунок 71 - Сообщение об ошибке в базе данных

3.9.6. Работа с шаблонами

Работа с шаблонами аналогична работе с другими типами объектов виртуальной инфраструктуры за тем исключением, что шаблон может быть конвертирован в виртуальную машину и обратно.

В связи с этим при первом изменении («ВМ -> шаблон» или обратно) в ПО управления объект будет помечен как новый и для него не будет отображаться метка (однако разграничение по заданным ранее уровням и категориям останется на прокси-сервере, поскольку шаблон в vSphere также является ВМ). Для исправления данной ситуации достаточно повторно указать объекту метку или вернуть объект в исходное состояние.

3.9.7. Работа с отчетами

Отчеты позволяют увидеть, какие метки назначены объектам доступа и пользователям, а также обнаружить незарегистрированные объекты и пользователей, для которых не назначены ни уровни, ни категории.

Для просмотра отчета следует в главном окне утилиты управления выбрать пункт меню «Файл» -> «Создать отчет...».

В открывшемся окне «Просмотр отчета» (рисунок 72) отображена таблица с указанием имени объекта или пользователя, его типа (Виртуальные машины, Шаблоны, Хосты, Сети, Хранилища, Пользователи), назначенных уровня и категорий.

В правой части окна можно настроить фильтры отображаемых объектов и пользователей по имени, типу, назначенному уровню или категории объекта.

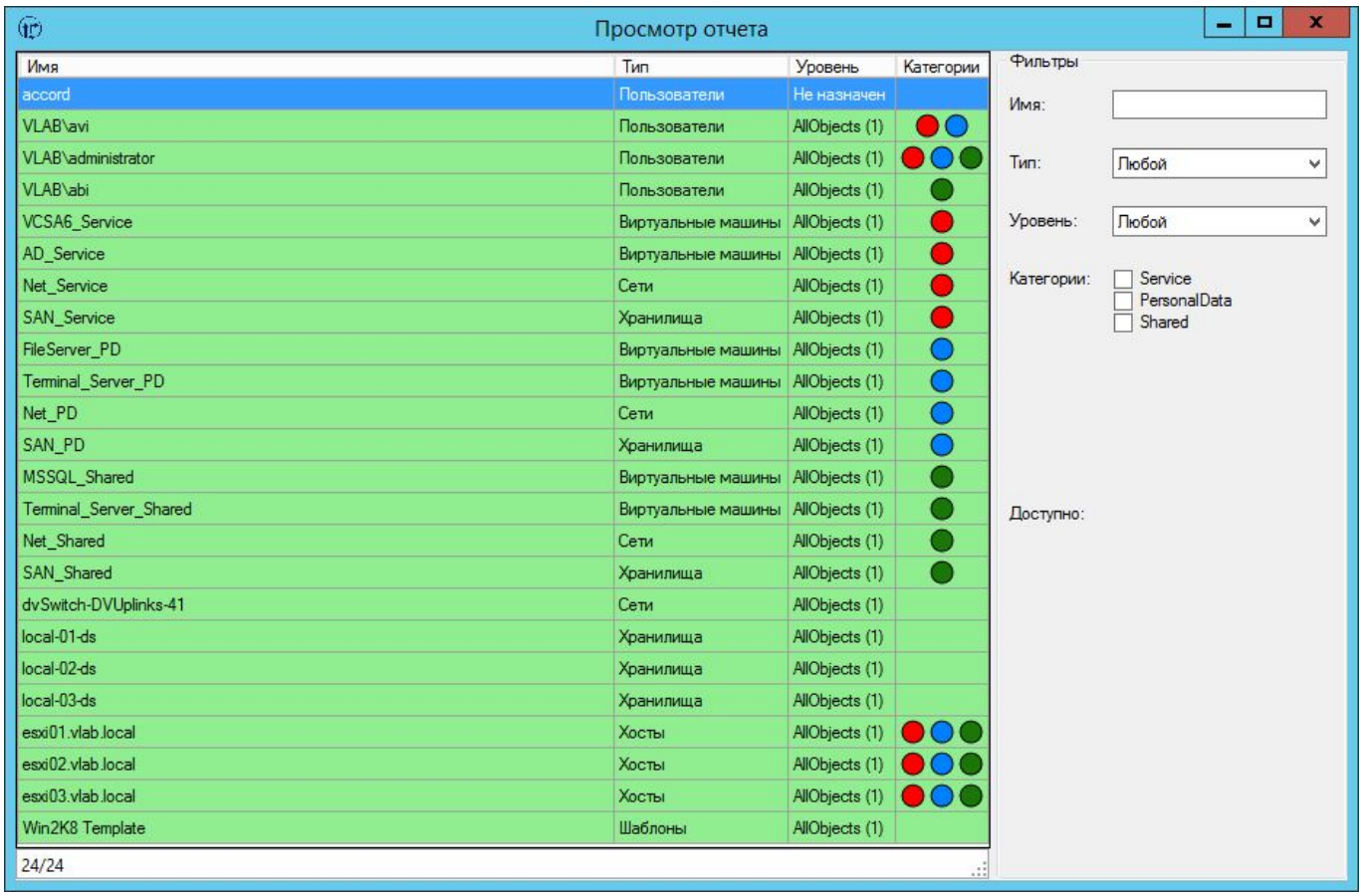


Рисунок 72 - Просмотр отчета

Красным будут выделены записи незарегистрированных объектов, для которых метки безопасности не были назначены.

Если для объекта был определен уровень, то запись объекта выделена зеленым (объект зарегистрирован).

По нажатии на такую запись, в правой части окна «Просмотра отчетов» выводится список доступных объектов для выделенного пользователя или список пользователей, которым выделенный объект доступен (рисунок 73).

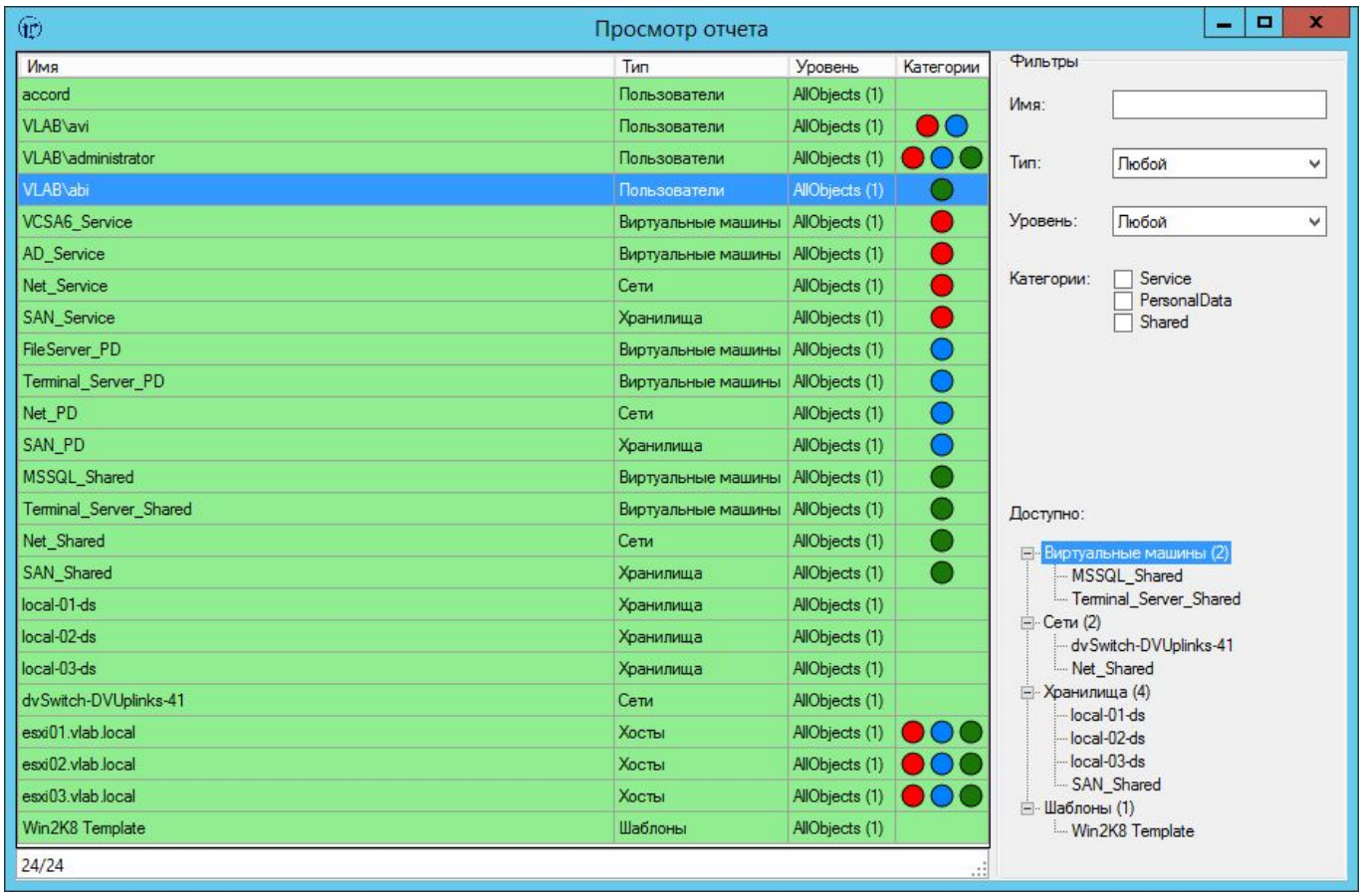


Рисунок 73 - Просмотр отчета

ВНИМАНИЕ! В отчете отображаются те объекты, к которым у пользователя есть доступ при одновременном выполнении следующих условий:

– работа с незарегистрированными пользователями запрещена;

– выключен Мягкий режим.

При этом не учитываются случаи одновременного обращения к нескольким объектам (например, миграция или назначение сети), в которых осуществляются проверки уровня и категорий сессии, и разрешенные пользователю операции.

В столбце «Уровень» отображается значение «Не назначен» для незарегистрированных объектов и имя уровня (с указанием иерархического номера) для зарегистрированных объектов.

Категории объекта отображаются в соответствующем столбце в виде кружка определенного цвета (если категория не указана – ячейка пуста).

3.9.8. Поведение в случае блокировки доступа

Если пользователю был заблокирован доступ к объекту, операция не выполняется и на экран выводится следующее уведомление: *«Task was blocked by Segment-V.».*

ВНИМАНИЕ! Окно ошибки не показывается в случае блокировки доступа на включение ВМ и изменения настроек портгрупп, операция в этом случае просто

не выполняется. Информацию о запрете доступа можно найти в журналах ПО «Сегмент-В.».

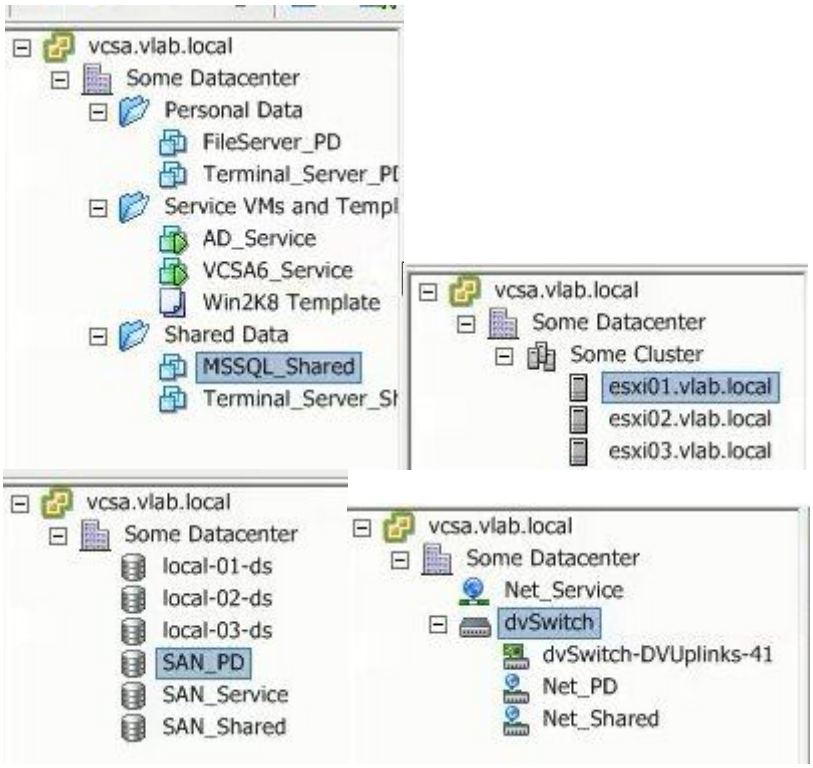
Для выяснения причины, по которой действие запрещено, необходимо открыть утилиту **«LogViewer-V.» –** для просмотра событий с прокси-сервера «Сегмент-В.».

3.9.9. Пример настройки «Сегмент-В.»

Рассмотрим ВИ, состоящую из трех ESXi-хостов, объединенных в кластер и находящихся под управлением vCenter (ВМ VCSA). Каждый из ESXi обладает собственным локальным хранилищем (под гипервизор), а также к нему подключено общее хранилище (SAN) с тремя разделами (LUN), на каждом из которых хранятся данные определенного типа. АБИ в данной ВИ выделяет три сегмента: общедоступный, персональные данные, а также сервисные ВМ.

Для сети управления (Net_Service) используются стандартные портгруппы, для остальных сетей – распределенные.

Примечание! Для удобства работы представленной ВИ, применяются правила именования, указывающие на принадлежность объектов к определенному сегменту (_PD, _Service, _Shared).



Задача: АБИ необходимо предоставить АВИ возможность работы со всеми объектами ВИ, но при этом исключить возможность «утечки» данных из одного сегмента в другой.

Для выделения сегментов создадим три соответствующих группы в утилите **«Segment-V.»**: *Personal Data, Shared Data, Service Data*. Так как за сегментацию отвечает прокси-сервер, имеется возможность обрабатывать все типы информации на каждом из серверов. Поэтому создадим также группу *hosts*.

Объединим объекты в группы следующим образом:

Service Data:

Виртуальные машины: *AD_Service, vCenter_Service*

Сети: *Net_Service*

Хранилища: *SAN_Service*

Шаблоны: *Win2k8 template*

Personal Data:

Виртуальные машины: *FileServer_PD, Terminal_Server_PD*

Сети: *Net_PD*

Хранилища: *SAN_PD*

Shared Data:

Виртуальные машины: *MSSQL_Shared, Terminal_Server_Shared*

Сети: *Net_Shared*

Хранилища: *SAN_Shared*

Hosts:

Серверы: *esxi1.vlab.local, esxi2.vlab.local, esxi3.vlab.local*

Создадим один уровень (общий для всех пользователей и объектов, т.к. хотя бы один уровень должен быть создан всегда) и три категории, соответствующие категориям обрабатываемых данных: *Shared Data (зеленая), Service Data (желтая) и Personal Data (красная)*.

Назначим всем группам один уровень (AllInOne) и соответствующую категорию (группы по названиям считаем идентичными категориям).

Администратору виртуальной инфраструктуры (VLAB\avi) и группе *Hosts* назначим уровень 1 и все три категории: *«Service Data», «Personal Data», «Shared Data»*.

В результате такого назначения меток пользователь сможет работать со всеми объектами виртуальной инфраструктуры (изменять конфигурацию ВМ, перезагружать хост в случае необходимости, настраивать параметры vSwitch и другое), а ВМ может быть запущена на любом ESXi.

Вместе с тем, мы гарантируем, что храниться и обрабатываться информация определенного типа будет лишь в своем сегменте. Таким образом, пользователь не сможет инициировать, например, миграцию ВМ *Terminal_Server_PD* на хранилища *SAN_Shared* или *SAN_Service*, подключение ВМ *MSSQL_Shared* к сети *Net_PD* и другие действия, которые могут привести к смешению данных.

3.10. Настройка разграничения доступа на совмещенном АРМ АБИ/АВИ

В том случае если АРМ, на который устанавливается комплекс «Сегмент-В.», является совмещенным, то есть на нем работают и Администратор БИ, и Администратор ВИ, необходимо разграничить доступ этих

администраторов к утилитам управления комплексом и утилитам управления VMware.

С помощью ПО ПАК «Аккорд-Win32»/ ПАК «Аккорд-Win64» это можно сделать следующим образом:

1) создание пользователей в Active Directory: Администратора БИ, Администратора ВИ и специальной учетной записи для запуска LogService (при применении режима сервиса «SSPI»);

2) на АРМ АБИ/АВИ: установка ПО ШИПКА на АРМ АБИ (вариант установки «Обычная», дать согласие с установкой драйверов от неизвестного источника);

3) на АРМ АБИ/АВИ: установка ПАК «Аккорд-Win32»/ ПАК «Аккорд-Win64» (в конце установки – настройка идентификаторов, основной – ТМ-идентификатор (АМДЗ), дополнительный – ШИПКА);

4) на АРМ АБИ/АВИ: дать учетной записи, от имени которой работает сервис регистрации событий (например, специальной учетной записи *LogService*) права на папку с установленным ПО Segment-V и Accord-V (на запись в файл EventDatabase.db, а также на чтение и создание файлов в папке);

5) на АРМ АБИ/АВИ: в утилите разграничения правил доступа (РПД) задать идентификатор и пароль для Главного администратора, создать группы администраторов БИ и ВИ, создать пользователей (из AD, указав адрес AD, указать имя домена), задать для них идентификаторы и пароли;

6) в утилите РПД группе АБИ запретить доступ к папке с vClient (выбрать папку –> сброс -> Сохранить), а группе АВИ – на папку «Сегмент-В.»;

7) в настройке комплекса «Аккорд» активировать защиту, заранее указав протоколы виртуального канала (Параметры –> Terminal Server) (если используется ПО ПАК «Аккорд-Win32 TSE»/ ПАК «Аккорд-Win64 TSE»);

Подробную информацию об использовании ПО ПАК «Аккорд-Win32»/ ПАК «Аккорд-Win64» и ШИПКА см. в соответствующей документации на указанные продукты.

3.11. Примеры настройки маршрутизации

Трафик из сети АРМ АБИ (внешняя сеть), направленный на защищаемые серверы (ESXi, vCenter), должен быть перенаправлен на прокси-сервер. Аналогично и для трафика из внутренней сети во внешнюю.

3.11.1. Добавление маршрутов в ОС

ВНИМАНИЕ! В случае выбора данного механизма необходимо проделывать аналогичные действия не только на АРМ АБИ/АВИ, но и для vCenter / ESXi / DNS / AD (и других участвующих во взаимодействии элементов).

Для Windows:

Рассмотрим пример для АРМ АБИ. Имеется сеть со следующими данными:

- IP-адрес внешнего (external) интерфейса прокси-сервера (default gateway) – 192.168.1.250;
- маска подсети (subnet mask) стандартная – 255.255.255.0;
- адрес vCenter сервера (для примера) – 10.1.1.253.

Тогда для добавления статического маршрута в командной строке (Пуск -> Выполнить, или <Ctrl>+<R>) следует набрать команду: *route ADD -p 10.1.1.253 MASK 255.255.255.255 192.168.1.250 METRIC 1*

и нажать <Ввод>.

Готово!

Пояснения:

route.exe – подпрограмма работы с маршрутами;

ADD – команда для добавления маршрута на указанный адрес. В данном случае на 10.1.1.253 (vCenter);

-p – данный ключ необходим для сохранения маршрута. Без его использования таблица маршрутов будет удален после перезагрузки ОС;

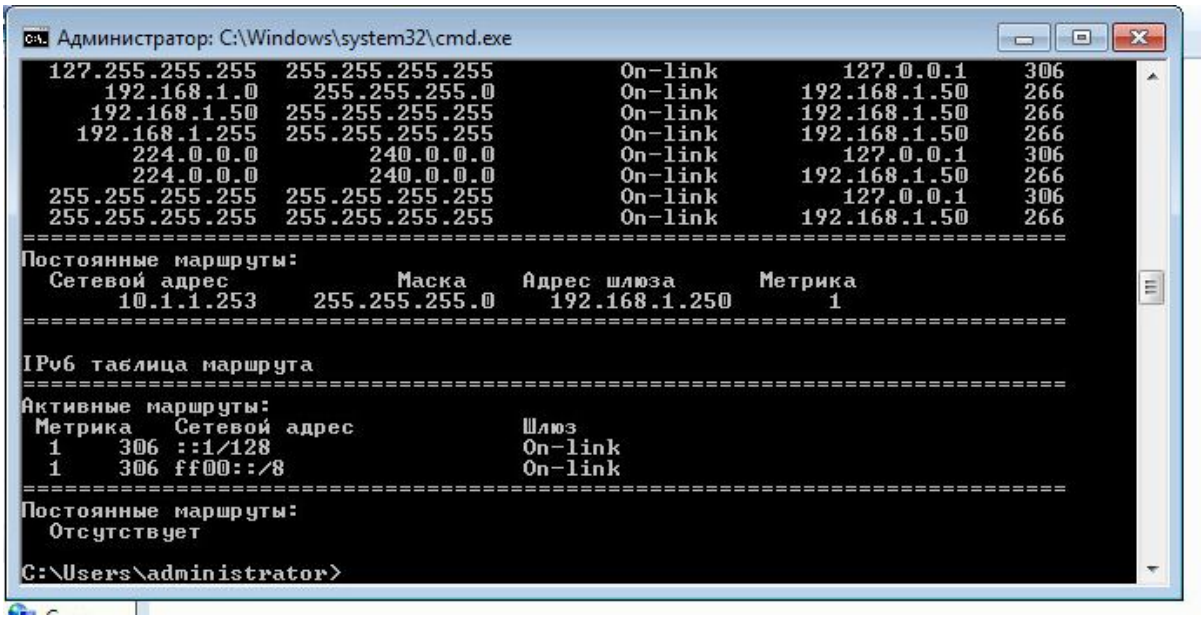
10.1.1.253 – адрес назначения (vCenter);

MASK – данный параметр следует установить перед прописыванием значения маски подсети;

192.168.1.250 – адрес основного шлюза. Чаще всего это IP-адрес внешнего интерфейса прокси-сервера;

METRIC 1 – параметр, определяющий приоритет указанного выше шлюза. 1- наивысший приоритет (цена).

Проверить прописанные маршруты можно командой route print. Для этого в командной строке (Пуск –> Выполнить –> cmd –> OK) следует набрать команду route print и нажать <Ввод>.



Для удаления всех существующих постоянных маршрутов служит команда *route -f*.

Для удаления какого-либо конкретного постоянного маршрута служит команда *route delete 10.1.1.253* (10.1.1.253 - указан в качестве примера).

3.11.2. Использование default gateway

ВНИМАНИЕ! В случае выбора данного механизма необходимо проделывать аналогичные действия не только на АРМ АБИ/АВИ, но и для vCenter / ESXi / DNS / AD (и других участвующих во взаимодействии элементов).

Необходимо указать в настройках сетевого соединения в качестве *default gateway* IP-адрес соответствующего интерфейса прокси-сервера «Сегмент-В.».

3.11.3. Настройка сетевого оборудования (на примере cisco 3725)

Пример стенда

ESXi-Y	10.1.1.24Y
vCenter	10.1.1.252
АРМ АБИ	192.168.1.50
Прокси-сервер (внешний интерфейс)	192.168.1.200
Прокси-сервер (внутренний интерфейс)	10.1.1.200
Порт cisco fa0/0	192.168.1.253
Порт cisco fa0/1	10.1.1.253

где Y – номер ESXi.

Настройка роутера

Проверка настройки интерфейсов.

```
Rack1R1#show ip interface brief
Interface          IP-Address        OK?   Method      Status              Protocol
FastEthernet0/0    192.168.1.253     YES   manual      up                      up
FastEthernet0/1    10.1.1.253        YES   manual      up                      up
FastEthernet1/0    unassigned        YES   unset       administratively down   down
FastEthernet2/0    unassigned        YES   unset       administratively down   down
Rack1R1#
```

1. ACL для фильтрации трафика.

Классифицируем трафик, идущий из внешней сети (192.168.1.0/24) к vCenter или ESXi (3шт):

```
Rack1R1#conf term
Rack1R1(config)#ip access-list extended to_vCenter
Rack1R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 host 10.1.1.252
Rack1R1(config-ext-nacl)#exit
Rack1R1(config)#ip access-list extended to_ESXi1
Rack1R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 host 10.1.1.241
Rack1R1(config-ext-nacl)#exit
Rack1R1(config)#ip access-list extended to_ESXi2
Rack1R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 host 10.1.1.242
Rack1R1(config-ext-nacl)#exit
Rack1R1(config)#ip access-list extended to_ESXi3
Rack1R1(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 host 10.1.1.243
Rack1R1(config-ext-nacl)#exit
```

2. Просмотр созданных ACL.

```
Rack1R1#show access-lists
Extended IP access list to_ESXi1
    10 permit ip 192.168.1.0 0.0.0.255 host 10.1.1.241
Extended IP access list to_ESXi2
    10 permit ip 192.168.1.0 0.0.0.255 host 10.1.1.242
Extended IP access list to_ESXi3
    10 permit ip 192.168.1.0 0.0.0.255 host 10.1.1.243
Extended IP access list to_vCenter
ermit ip 192.168.1.0 0.0.0.255 host 10.1.1.252
```

3. Перенаправление трафика, route-map.

Весь трафик из внешней сети, идущий на vCenter или ESXi, перенаправляем на внешний интерфейс FC:

```
Rack1R1(config)#route-map PBR
Rack1R1(config-route-map)#match ip address to_vCenter to_ESXi1 to_ESXi2 to_ESXi3
Rack1R1(config-route-map)#set ip next-hop 192.168.1.200
Rack1R1(config-route-map)#exit
Rack1R1(config)#exit
```

4. Просмотр route-map.

```
Rack1R1#show route
route-map PBR, permit, sequence 10
  Match clauses:
    ip address (access-lists): to_vCenter to_ESXi1 to_ESXi2 to_ESXi3
  Set clauses:
    ip next-hop 192.168.1.200
  Policy routing matches: 0 packets, 0 bytes
```

5. Применение route-map для интерфейса роутера.

```
Rack1R1(config)#int f0/0
Rack1R1(config-if)#ip policy route-map PBR
Rack1R1(config-if)#exit
Rack1R1(config)#exit
Rack1R1#
```

4. Удаление ПО ПАК «Сегмент-В.»

Для удаления (временного прекращения использования) комплекса достаточно восстановить первоначальную маршрутизацию и отключить при необходимости прокси-сервер.

В случае полноценного удаления на АРМ АБИ следует перейти во вкладку «Установка и удаление программ» и выполнить стандартную процедуру удаления ПО.

5. Лицензирование

Для работы с ПАК «Сегмент-В.» требуется лицензия. Она выдается производителем и поставляется на компакт-диске в составе комплекта поставки продукта или иным способом (файл license-v.lic).

Для формирования Поставщиком файла лицензии необходимы следующие параметры (они должны быть известны перед приобретением лицензии):

1) Срок действия лицензии (устанавливается в соответствии с потребностью Заказчика).

2) Уникальная идентификационная информация средства доверенной загрузки (СЗИ НСД «Аккорд-АМДЗ» или СЗИ НСД «Инаф»), установленного на автоматизированном рабочем месте администратора информационной безопасности инфраструктуры виртуализации. Определить данный параметр можно одним из следующих способов:

а) запустить утилиту «Segment-V.» из комплекта поставки комплекса.

Уникальная идентификационная информация средства доверенной загрузки содержится в поле «Серийный номер платы» отображаемого на экране информационного окна (рисунок 74). Данный параметр следует передать Поставщику для создания файла лицензии. В целях предотвращения возникновения ошибок при перепечатывании идентификационной информации, можно установить курсор в указанное поле и выполнить процедуру копирования с использованием стандартного сочетания клавиш (<Ctrl>+<C> и <Ctrl>+<V>).

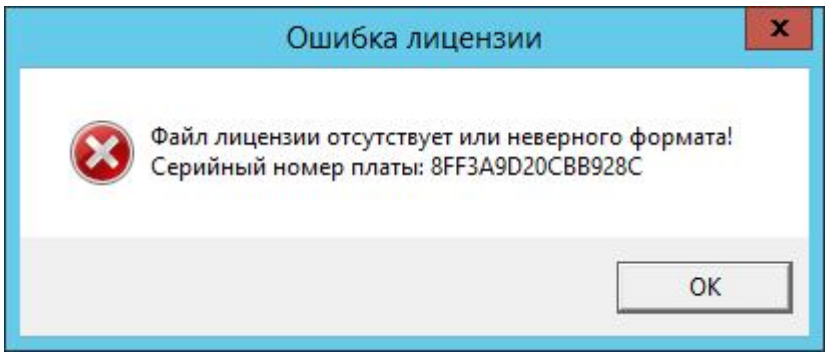


Рисунок 74 – Ошибка лицензии

б) запустить отдельно поставляемую утилиту Key-V-Info.exe. Уникальная идентификационная информация средства доверенной загрузки содержится в появившемся окне «Ключ лицензии». Данный параметр следует передать Поставщику для создания файла лицензии. В целях предотвращения возникновения ошибок при перепечатывании идентификационной информации, можно установить курсор в указанное поле и выполнить процедуру копирования с использованием стандартного сочетания клавиш (<Ctrl>+<C> и <Ctrl>+<V>).

3) Наименование продукта:

- «Accord-V.» – соответствует установке «Аккорд-В.» в качестве отдельного продукта;
- «Segment-V.» – соответствует установке «Сегмент-В.» в качестве отдельного продукта;
- «Accord-V. Enterprise» – соответствует совместному использованию «Аккорд-В.» и «Сегмент-В.».

4) Максимальное количество прокси-серверов (данный параметр учитывается только для ПАК «Сегмент-В.»; устанавливается в соответствии с потребностью Заказчика). Добавление в систему прокси-серверов в количестве, превышающем предусмотренное лицензией, невозможно.

5) Максимальное количество CPU в ESXi-серверах виртуальной инфраструктуры (устанавливается в соответствии с потребностью Заказчика). Подключение к виртуальной инфраструктуре, в которой суммарное число процессоров ESXi-серверов превышает заданное в лицензии, невозможно.

6) Максимальное количество виртуальных машин в виртуальной инфраструктуре (данный параметр учитывается только для ПАК «Аккорд-В.»; устанавливается в соответствии с потребностью Заказчика). Подключение к виртуальной инфраструктуре, в которой количество виртуальных машин превышает заданное в лицензии, невозможно.

Полученную от Поставщика лицензию (файл license-v.lic) необходимо скопировать в корень папки с установленным ПО управления комплексом:

C:\Program Files (x86)\OKB SAPR\Segment-V (по умолчанию) или

C:\Program Files (x86)\OKB SAPR\Accord-V (в случае совместной установки с ПАК «Аккорд-В.»).

Примечание: Лицензии на ПАК «Аккорд-В.» и ПАК «Сегмент-В.» аналогичны и отличаются наименованием продукта.

Проверка лицензии осуществляется только для утилиты **«Segment-V.» («Accord-V.»)**. Если проверка не была пройдена (отличается уникальная идентификационная информация средства доверенной загрузки, истек срок действия лицензии, неверна подпись лицензии, превышено допустимое лицензией количество прокси-серверов, ВМ, процессоров ESXi-серверов и т.п.), дальнейшая работа в утилите невозможна. Текущие же настройки будут сохранены, и прокси-серверы продолжат свою работу.

Продолжение работы станет возможным только после приведения параметров системы в соответствие с лицензией или после приобретения новой лицензии.

Статус лицензии, уникальная идентификационная информация средства доверенной загрузки и дата истечения срока действия лицензии отображаются на вкладке «Помощь» утилиты «Segment-V.» («Accord-V.») (рисунок 75).

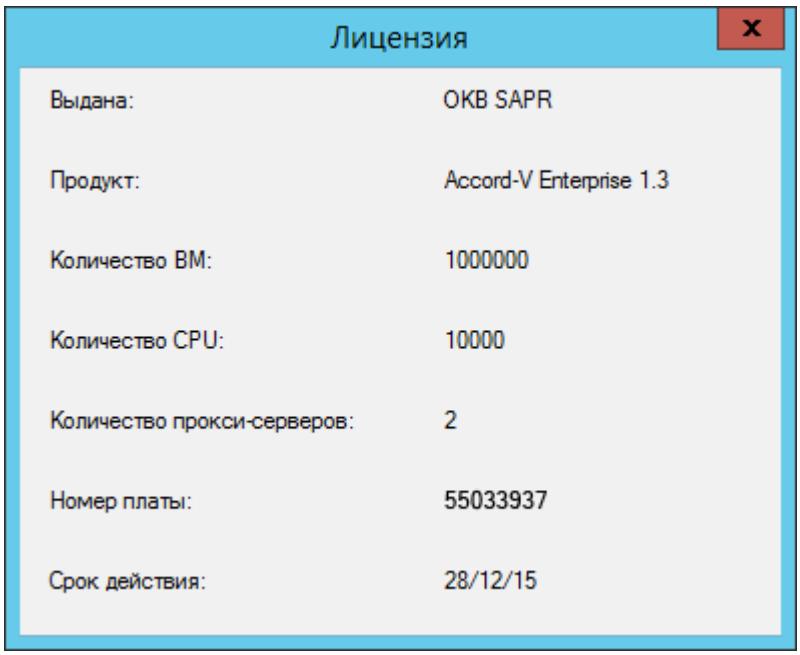


Рисунок 75 - Информация о лицензии

6. Техническая поддержка и информация о комплексе

Все вопросы, связанные с поддержкой ПАК «Сегмент-В.», Вы можете отправлять по адресу help@okbsapr.ru, либо обращаться по телефонам:

+7 (495) 994-49-96

+7 (495) 994-49-97

+7 (926) 235-89-17

+7 (926) 762-17-72

Мы будем рады узнать Ваши пожелания и предложения по поводу этой документации. Вы можете отправить их по адресу help@okbsapr.ru.

7. Возможные затруднения в работе с ПАК «Сегмент-В.» и методы их устранения

7.1. Принцип поиска проблемы

7.1.1. Прокси-сервер

Для проверки настроек прокси-сервера и сервисов, отвечающих за работу «Сегмент-В.», следует выполнить вход на прокси-сервер под учетной записью «accord» и выбрать третий пункт меню скрипта установки: *«3) Print current settings)»*.

На экран выводится следующая информация[1]:

- сетевые настройки сервера;
- IP-адрес защищаемого vCenter (только одного, если указывались еще vCenter или ESXi, не подключенные к гипервизору, данные о них не отобразятся);
- состояние сервисов;
- настройки безопасности (разрешен ли SSH, его fingerprint);
- статус High Availability (используется ли режим отказоустойчивости, реализованный средствами «Сегмент-В.»).

Необходимо проверить отобразившуюся информацию и изменить настройки, если текущие не соответствуют действительности. Для этого следует выбрать первый пункт меню скрипта установки: *«1) Reconfigure Segment-V. settings»* – после чего в открывшемся меню реконфигурирования указать, какие именно изменения требуется произвести. Процедура изменения параметров аналогична процедуре задания параметров в процессе первичной установки прокси-сервера.

7.1.2. Утилита управления «Segment-V.»

Решение проблемы с «зависшим» заданием в «Segment-V.» в момент закрытия vCenter:

1) подождать 120 секунд (таймаут выполнения операции). Если операция продолжает «висеть», перейти к следующим этапам;

2) закрыть утилиту «Segment-V»;

3) проверить список запущенных процессов, найти *AccordManager.exe* и завершить его принудительно;

4) повторно открыть «Segment-V.» и выяснить, соединение с какими прокси-серверами не было установлено;

[1)] в случае необходимости, воспользуйтесь сочетаниями клавиш <Shift>+<Page Up> для прокрутки экрана вверх, <Shift>+<Page Down> – для прокрутки экрана вниз

5) с помощью команды *ps aux | grep acc* проверить на каждом из таких прокси-серверов, запущен ли процесс *accordguard*;

6) если такой процесс запущен, завершить его (*kill -9 PID*);

7) вне зависимости от действий с *accordguard* перезапустить сервис *accordservice*:

/etc/init.d/accordservice.sh restart

(/etc/init.d/accordservice.sh start)

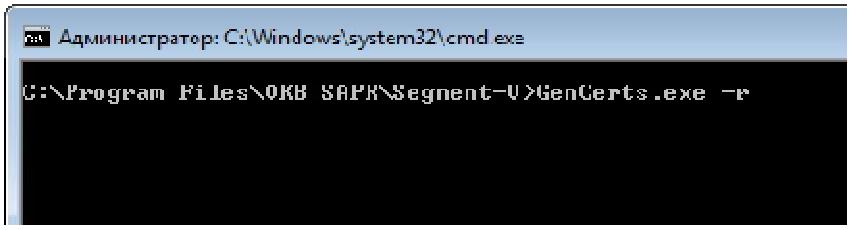
8) в утилите «Segment-V.» подключить прокси-серверы.

7.2. Сервисные команды

Перегенерирование сертификатов

Вызвать в папке с установленным ПО управления комплексом исполняемый файл GenCerts.exe:

- с параметром "-r" – для создания корневого сертификата;
- с параметром "-h" – для создания сертификата прокси-сервера.



Работа с базой данных

Вызвать в папке с установленным ПО управления комплексом исполняемый файл Repair.exe:

- с параметром "-log" – для создания базы данных сервиса регистрации событий (EventDatabase.db);
- с параметром "-db" – для создания базы данных утилиты управления (ManagedDatabase.bd).