ОКБ
ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

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

Quick Start

Руководство по быстрому старту

Листов 40

Москва
2016

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 над 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. Виртуальная машина работает полностью аналогично физическому компьютеру и обладает собственными центральным процессором, памятью, жестким диском и сетевым адаптером.

Доверенная загрузка – загрузка ОС только после проведения контрольных процедур идентификации/аутентификации пользователей, проверки целостности технических и программных средств ПЭВМ (РС) с использованием алгоритма пошагового контроля целостности.

КЦ - контроль целостности.

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.

1. Состав и схема развертывания комплекса

ПАК «Аккорд-В.» представляет собой комплекс программных и аппаратных средств, предназначенный для защиты инфраструктуры виртуализации, и включает в себя следующие компоненты:

1) **аппаратная часть – «Аккорд-АМДЗ»[1] -** предназначенная для защиты ESXi, vCenter (если он физический), АРМ АБИ/АВИ, а также, дополнительно, для защиты клиентских рабочих мест – в составе:

а) *контроллер («Аккорд-АМДЗ»)* - представляет собой карту расширения (expansion card), устанавливаемую в свободный слот материнской платы ПЭВМ (PC);

б) *съемник информации с контактным устройством,* обеспечивающий интерфейс между контроллером комплекса и персональным идентификатором пользователя;

в) *персональный идентификатор пользователя* – микропроцессорное устройство DS 199x («Touch memory»), USB-устройство Персональный идентификатор ШИПКА (ПИ ШИПКА).

2) **модули СПО «Аккорд-В.»:**

а) *ПО управления комплексом*, устанавливаемое на АРМ АБИ, включающее в себя следующие утилиты:

- «Installer-V.», предназначенную для развертывания агентов «Аккорд-В.» на ESXi;
- «Accord-V.», предназначенную для настройки доверенной загрузки виртуальных машин;
- «LogViewer-V.», предназначенную для 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);

3) **модули разграничения доступа** для ОС с vCenter (если он установлен на ОС Windows), гостевых ОС виртуальных машин, а также, дополнительно, для ОС АРМ АБИ/АВИ и клиентских рабочих мест (не являющихся виртуальными машинами):

а) *модуль «Аккорд-Win64 TSE»,* устанавливаемый в ОС с vCenter (если он установлен на ОС Windows), предназначенный для разграничения доступа к ресурсам ОС со стороны АБИ и АВИ;

[1)] В случае отсутствия на материнской плате ПЭВМ (для всех ESXi и для vCenter, если он физический) свободного слота PCI/PCI-X/PCI-Express вместо «Аккорд-АМДЗ» можно использовать СЗИ НСД «Инаф», подключаемый в свободный USB-порт ПЭВМ

б) *модуль «Аккорд-Win32 TSE» / «Аккорд-Win64 TSE» (СПО «Аккорд-ТС» и СПО «Аккорд-ТК»),* устанавливаемый в гостевую ОС ВМ, предназначенный для разграничения доступа пользователей к ресурсам ВМ и, в случае необходимости, обеспечивающий возможность удаленного подключения к ВМ с клиентских рабочих мест;

в) *модуль «Аккорд-X» («Аккорд-XL»),* устанавливаемый в ОС ВМ, предназначенный для разграничения доступа пользователей к ресурсам ВМ.

Для наглядности, схема развертывания комплекса представлена на рисунке 1.

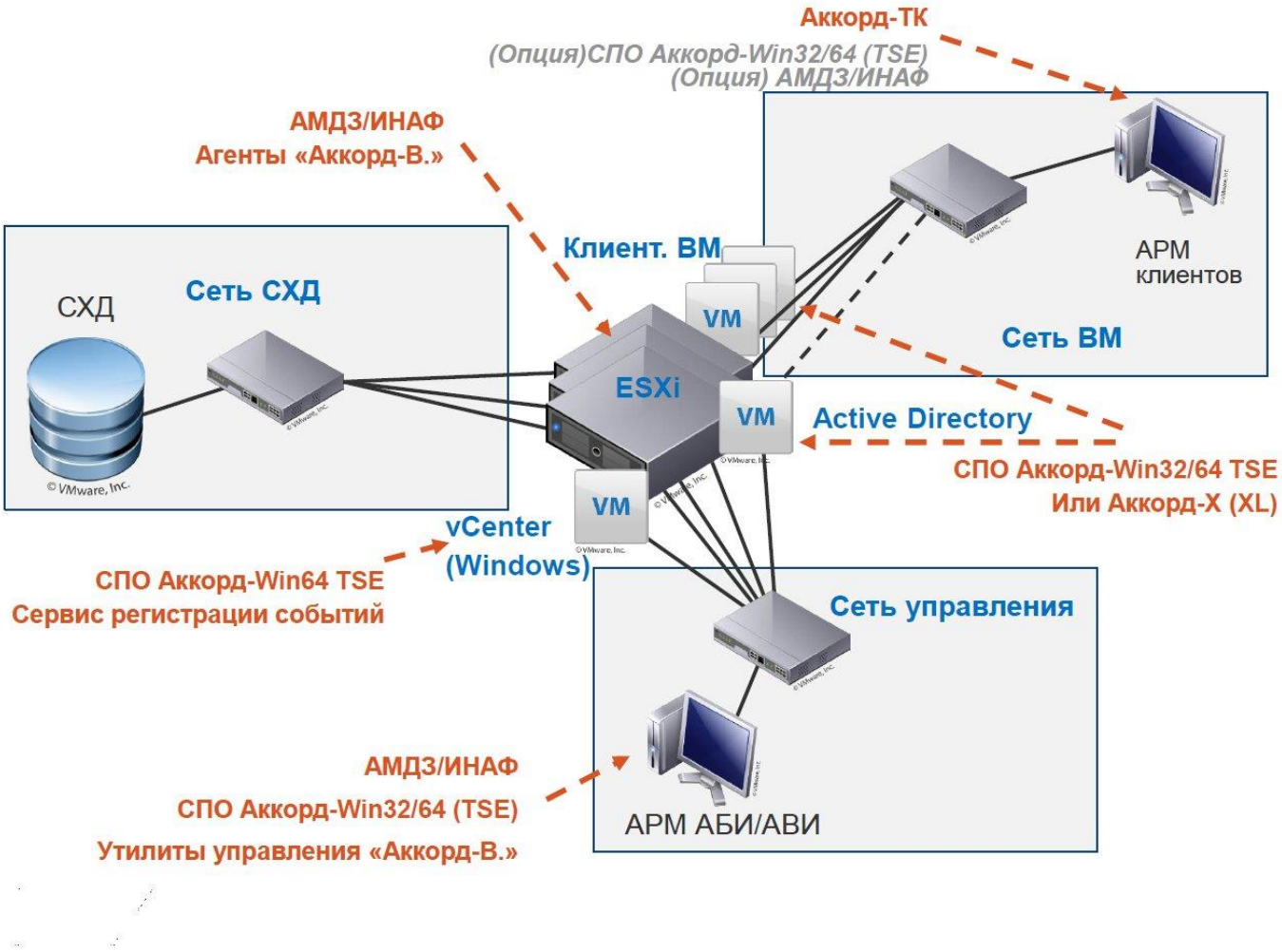


Рисунок 1 - Схема развертывания комплекса

2. Начало работы

Перед началом установки и настройки ПАК «Аккорд-В.» необходимо определиться с архитектурой развертываемой инфраструктуры виртуализации. Для этого следует ответить на следующие вопросы:

1) ESXi отдельные (без vCenter) или предполагается наличие vCenter; он физический или исполняется на виртуальной машине (на Windows или VMware vCenter Server Appliance (vCSA))?

2) АРМ АБИ совпадает с vCenter или отдельный?

3) где располагается сервис регистрации событий (на vCenter/ на отдельном АРМ (ВМ), например АРМ АБИ)?

2.1. Типовые варианты построения инфраструктуры виртуализации

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

1. vCenter совмещен с АРМ АВИ/АБИ и располагается на физическом СВТ, на нем установлен «Аккорд-АМДЗ», СПО «Аккорд-В.» и СПО разграничения доступа – «Аккорд-Win64 TSE».

При такой реализации возможны 2 варианта работы:

1) АВИ и АБИ работают локально на данном СВТ;
2) АВИ и АБИ работают удаленно, подключаясь к ОС с vCenter по RDP протоколу. В таком случае:
   - на АРМ, с которого будет происходить подключение, должен быть установлен терминальный клиент «Аккорд-ТК»;
   - на vCenter должно быть два сетевых интерфейса (один – для удаленных подключений, второй – для соединений с другими элементами инфраструктуры, такими как ESXi). На интерфейсе для удаленных подключений должен быть открыт только порт для RDP протокола (3389).

     Примечание: Если данное действие предполагается реализовывать встроенным firewall в Windows, то необходимо учитывать, что политики применяются не к отдельным сетевым картам, а только к сетевым профилям.

При этом в ОС с vCenter необходимо чтобы:

- доступ к ПО администрирования ПАК «Аккорд-Win64», ПО «Аккорд-В.» был только у АБИ;
- доступ к браузеру (в случае использования WebClient) и vClient был только у АВИ.

2. АРМ АБИ/АВИ не совмещен с vCenter. На нем установлено ПО «Аккорд-В.» и СПО разграничения доступа ПАК «Аккорд-Win64 TSE». В таком

случае **vCenter может быть любым (физическим/ ВМ с гостевой ОС Windows/ VCSA) или вообще отсутствовать.**

При такой реализации необходимо на каждом рабочем месте, имеющем связь с vCenter, установить СПО разграничения доступа («Аккорд-Win32 TSE»/ «Аккорд-Win64 TSE») и при помощи него ограничить доступ:

- к vClient и браузеру – для АБИ;
- к ПО администрирования «Аккорд-Win32 TSE»/ «Аккорд-Win64 TSE» и ПО «Аккорд-В.» – для АВИ.

Примечание:АРМ АБИ и АРМ АВИ могут быть совмещены.

Следует учитывать, что работа с vCenter в качестве ВМ (VCSA или Windows) требует подключения к ESXi для выполнения настройки контроля целостности и доверенной загрузки (подробнее см. «Руководство по установке»).

2.2. Расположение сервиса регистрации событий

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.

Возможные варианты расположения сервиса регистрации событий:

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

Примечание:

События 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.

2.3. Пример развертываемой инфраструктуры

Пример инфраструктуры представлен на рисунке 2.

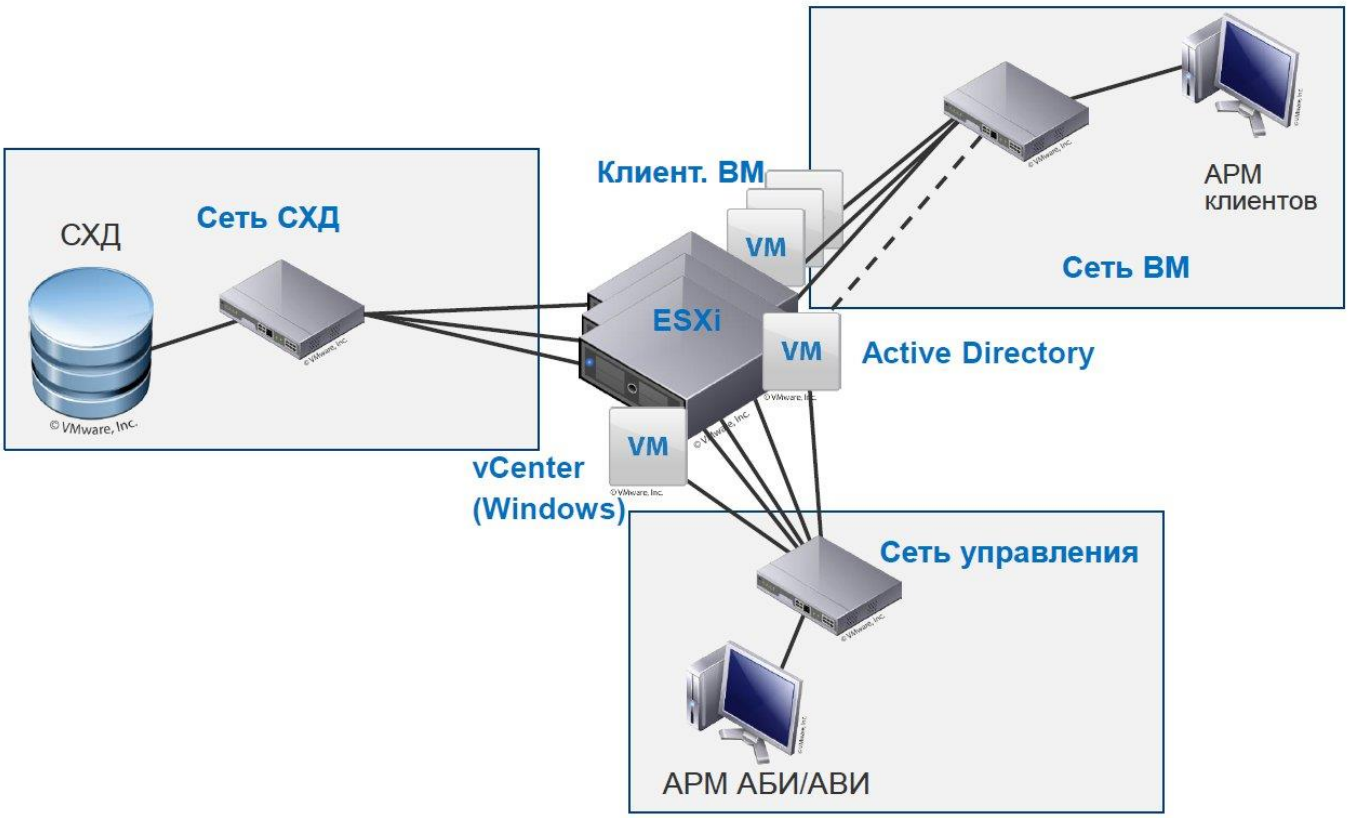


Рисунок 2 - Пример развертываемой инфраструктуры

3. Установка ESXi

ВНИМАНИЕ! При использовании контроллеров Аккорд-5.5/5.5.e (не Linux) установка ESXi должна обязательно выполняться с использованием MBR. Это необходимо для корректной работы «Аккорд-АМДЗ». Это **не накладывает** ограничение в размере 2ТБ для новых подключаемых дисков – только на тот, на котором установлен ESXi!

Для того чтобы выполнить установку с MBR при старте инсталлятора ESXi, после появления в правом нижнем углу экрана сообщения о возможности нажать <Shift>+<O>(буква) следует нажать данную комбинацию и через пробел добавить команду «formatwithmbr» (по умолчанию на экране уже имеется команда «runweasel», ее удалять не нужно).

ВНИМАНИЕ! В случае работы с большой инфраструктурой (обычно более 100 ВМ по 100 файлов) следует выполнить процедуру расширения места под БД агентов на ESXi.

Для этого в vClient следует выбрать нужный хост и Configuration -> System resource allocation -> Advanced -> Host (System -> Kernel -> kmanaged -> Visorfs -> etc).

Значения *limit* и *reservation* сменить с 28 до 50 Мб.

Выполнять данную процедуру можно "на живую", перезагрузка хоста не требуется. Проверка результата выполняется с помощью команды *vdf -h*.

Корректность установки можно проверить, подключившись к ESXi при помощи vClient и выбрав хост ->configuration -> storage и раздел, в который был установлен ESXi. Примеры ESXi с различными типами разметок представлены на рисунках 3, 4.

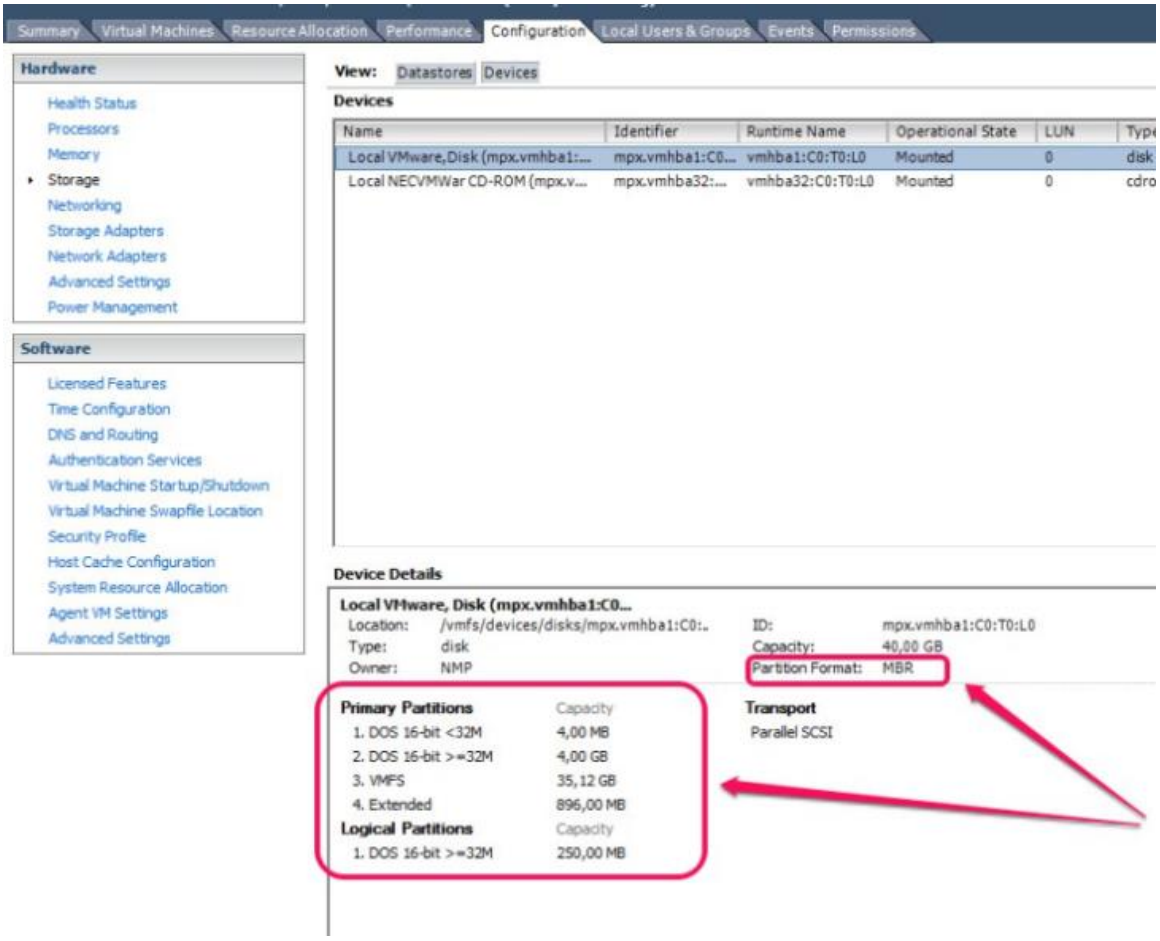


Рисунок 3 - ESXi с MBR разметкой

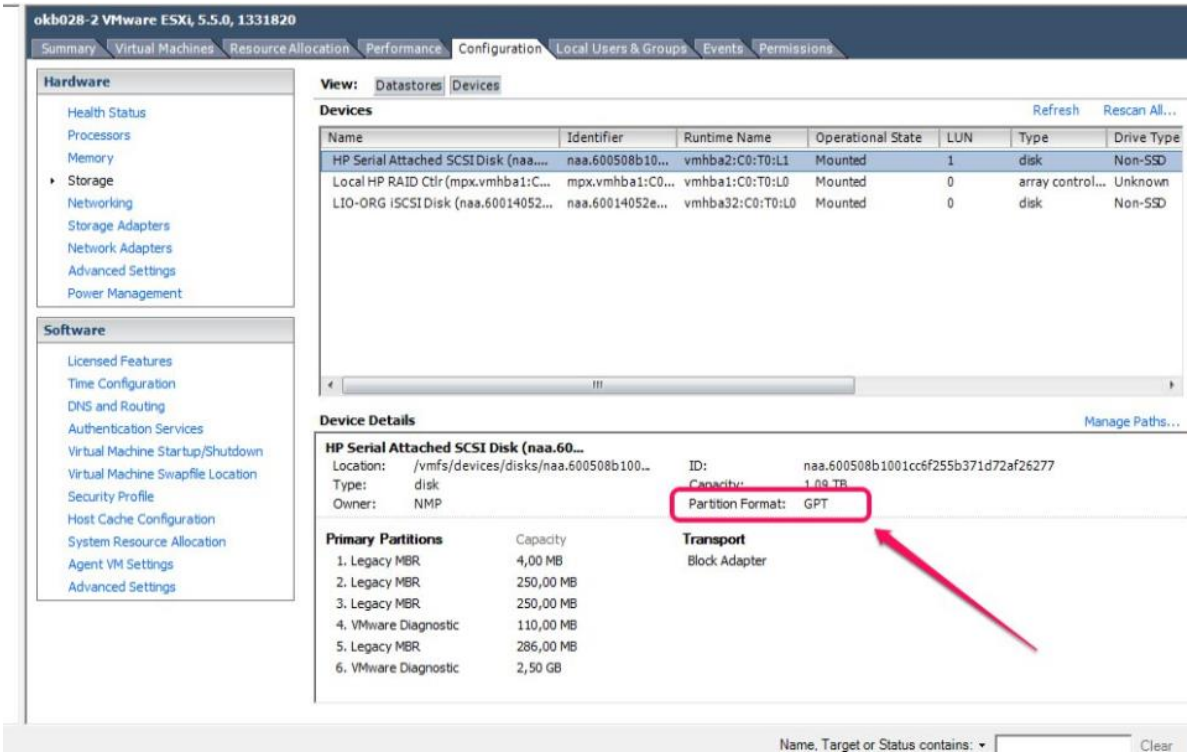


Рисунок 4 - ESXi с GPT разметкой

4. Установка и настройка аппаратной части комплекса

Следующий шаг – установка и настройка аппаратной части комплекса – «Аккорд-АМДЗ»[1]:

- на серверах ESXi;
- на vCenter, если он физический;
- на АРМ АБИ/АВИ (он может совпадать с vCenter).

Процедура установки и настройки «Аккорд-АМДЗ» описана в соответствующей документации на «Аккорд-АМДЗ» («Руководство по установке» (11443195.4012-038 98), «Руководство администратора» (11443195.4012-038 90)). Ниже приведены только особенности настройки «Аккорд-АМДЗ» на ESXi-серверах.

После установки «Аккорд-АМДЗ» следует выполнить процедуру настройки параметров учетной записи АБИ (пользователь «Главный администратор» в группе «Администраторы») и, если необходимо, пользователей (группа «Обычные»).

[1)] В случае отсутствия на материнской плате ПЭВМ (для всех ESXi и для vCenter, если он физический) свободного слота PCI/PCI-X/PCI-Express вместо «Аккорд-АМДЗ» можно использовать СЗИ НСД «Инаф», подключаемый в свободный USB-порт ПЭВМ

В процессе настройки «Аккорд-АМДЗ» следует установить на контроль и рассчитать контрольные суммы (КС) для следующих элементов:

1) содержимое каталога bootloader (в списке разделов «Аккорд-АМДЗ» каталог bootloader отобразится разделом с файлами ldlinux.sys, syslinux.cfg; данный раздел не доступен самому ESXi);

2) содержимое каталога bootbank (и altbootbank, если он не пуст), в частности:

- imgdb.tgz – содержит описание всех используемых драйверов и их зависимостях;
- файлы с расширениями v00/v01/v02 – драйверы;
- boot.cfg – конфигурационный файл загрузчика, содержащий указание на ядро и модули;
- tboot.b00 – ядро гипервизора;
- остальные файлы, расширение которых начинается на .b (модули гипервизора).

3) не относящиеся к специфике ESXi элементы:

- MBR;
- оборудование СВТ.

Примечание: файл state.tgz содержит настройки ESXi и постоянно обновляется, поэтому его не рекомендуется устанавливать на контроль (т.к. для него каждый раз придется пересчитывать КС).

Дополнительно рекомендуется устанавливать на контроль файлы с расширением .iso (vmwaretools) с раздела store (данная процедура не является обязательной, поскольку ESXi контролирует их самостоятельно).

ВНИМАНИЕ: в «Аккорд-АМДЗ» разделы могут отображаться дважды – достаточно установить на контроль только один экземпляр каждого раздела.

5. Создание в инфраструктуре необходимых ВМ

После успешного завершения процедуры установки и настройки «Аккорд-АМДЗ» необходимо выполнить процедуру создания в инфраструктуре необходимых виртуальных машин.

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

После выполнения данной процедуры следует перейти к установке и настройке СПО разграничения доступа.

6. Установка и настройка СПО разграничения доступа на физических АРМ (vCenter / АРМ АБИ) и ВМ

6.1. Общие сведения

Процедура установки и настройки СПО разграничения доступа «Аккорд-Win32 TSE» / «Аккорд-Win64 TSE» / «Аккорд-X» / «Аккорд-XL» описана в соответствующей документации, входящей в комплект поставки комплексов:

- «Аккорд-Win32»: «Руководство по установке» (11443195.4012-036 98), «Руководство администратора» (11443195.4012-036 90);
- «Аккорд-Win64»: «Руководство по установке» (11443195.4012-037 98), «Руководство администратора» (11443195.4012-037 90);
- «Аккорд-X»: «Руководство администратора» (11443195.4012-026 90).

ВНИМАНИЕ! СПО разграничения доступа **настраивается на АРМ АБИ/АВИ последним этапом** в связи с тем, что соответствующее ПО, к которому будет производиться разграничение доступа, появится только на следующем этапе.

Ниже описаны только особенности настройки «Аккорд-Win64 TSE» на сервере с vCenter.

6.2. Разделение ролей администраторов, создание и настройка их учетных записей на vCenter

В инфраструктуре виртуализации (в данном случае не рассматривается вариант без vCenter и Active Directory) необходимо выделить две роли: администратор безопасности информации (АБИ) и администратор инфраструктуры виртуализации (АВИ) (подробнее см. «Принятые термины, обозначения и сокращения»).

Для этого следует на АРМ управления комплексом vSphere в Active Directory завести учетные записи АБИ и АВИ. Дополнительно следует завести также учетную запись для сервиса регистрации событий.

Для учетной записи сервиса регистрации событий рекомендуется отключить возможность локального входа в систему (параметры групповой политики в Active Directory).

АБИ должен быть администратором в СПО разграничения доступа и пользователем в Windows. И наоборот, АВИ должен быть пользователем в СПО разграничения доступа и администратором в Windows. В таком случае администратор безопасности имеет возможность управлять распределением прав доступа (механизмами СПО разграничения доступа), но не имеет доступа к самим ресурсам (в силу соответствующих настроек Windows).

Для АБИ и сервиса регистрации событий следует назначить «Read Only» права на vCenter (корневому элементу) с галочкой propagate, отвечающей за наследование (рисунок 5).

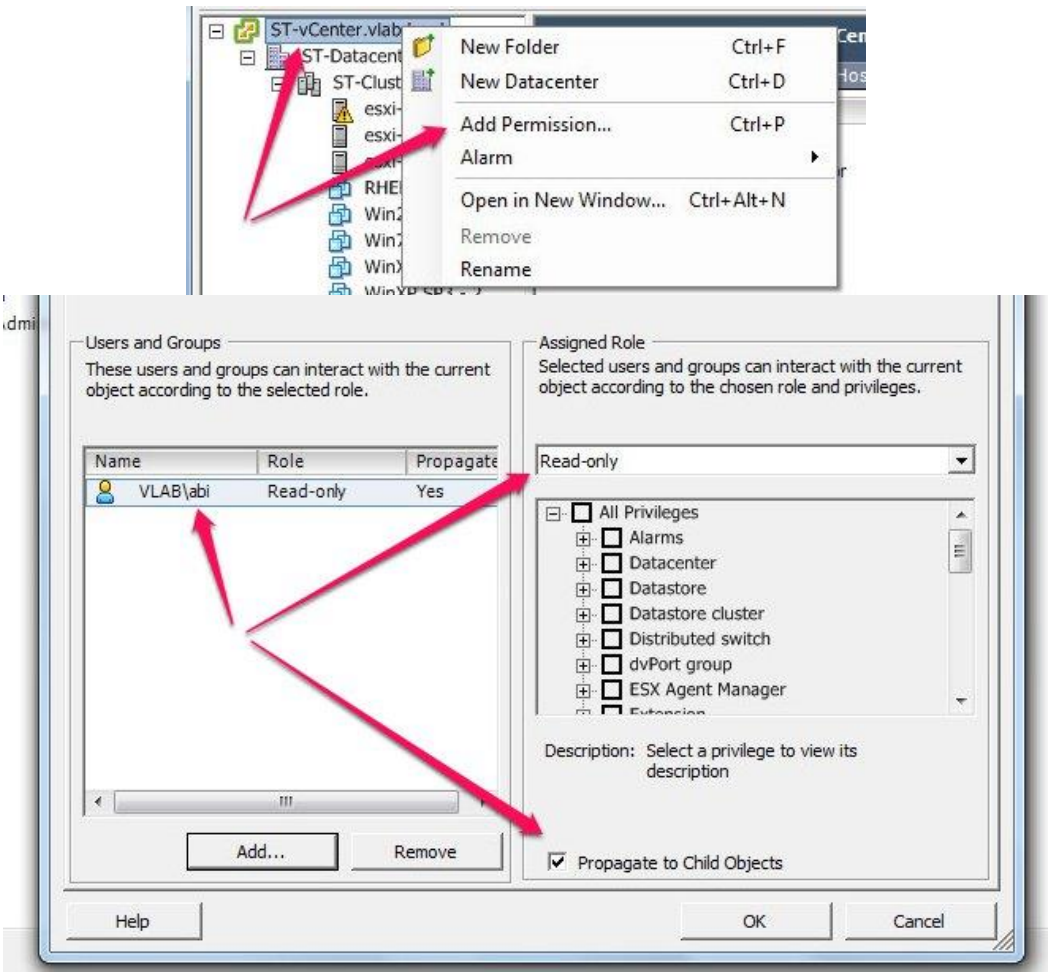


Рисунок 5 – Настройка учетных записей на vCenter

Учетная запись АБИ должна иметь полный доступ к папке с установленным ПО «Аккорд-В.»:

C:\Program Files (x86)\OKB SAPR\Accord-V

– данный пункт настраивается средствами ОС. Дополнительно необходимо с помощью СПО разграничения доступа «Аккорд-Win32 TSE» («Аккорд-Win64 TSE») оставить эту папку доступной только для АБИ.

Назначаемая роль АВИ на vCenter зависит от должностных обязанностей (примером такой роли может служить роль Virtual Machine user (sample), которая дает права на взаимодействие с уже существующими ВМ; подробнее см. саму роль на vCenter).

7. Синхронизация времени и открытие необходимых портов

Далее следует настроить одинаковое время на всех элементах системы (вручную или через ntp сервер).

ВНИМАНИЕ! ПО «Аккорд-В.» использует для соединения протокол SSL, поэтому, если время рассинхронизировано, компоненты комплекса не смогут установить соединение между собой!

Примечание. На ESXi время отображается в формате UTC, но если через vClient открыть закладку времени (Configuration ->TimeConfiguration), то в нем будет отображаться время с пересчетом относительно локального времени на элементе инфраструктуры, на котором запущен vClient.

Далее необходимо открыть следующие порты:

- в ОС с сервисом регистрации событий – 51179;
- в ОС АРМ АБИ – 51178/51179.

8. Установка ПО управления комплексом – модулей «Аккорд-В.»

8.1. Начало процедуры установки

Чтобы начать установку системы управления, необходимо запустить с правами администратора исполняемый файл **Accord-V.exe**, который находится на диске с дистрибутивом, и дать согласие на внесение программой изменений в компьютере. 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 <Install>, дождаться окончания процесса установки пакета и нажать кнопку <Finish>.

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

8.2. Установка модулей «Аккорд-В.»

В появившемся далее окне установки модулей «Аккорд-В.» необходимо указать путь к каталогу установки. По умолчанию установка всех программных компонентов 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. После выбора каталога установки следует ознакомиться с лицензионным соглашением, принять его посредством установки галочки в соответствующем поле и нажать кнопку <Далее> (рисунок 6).

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

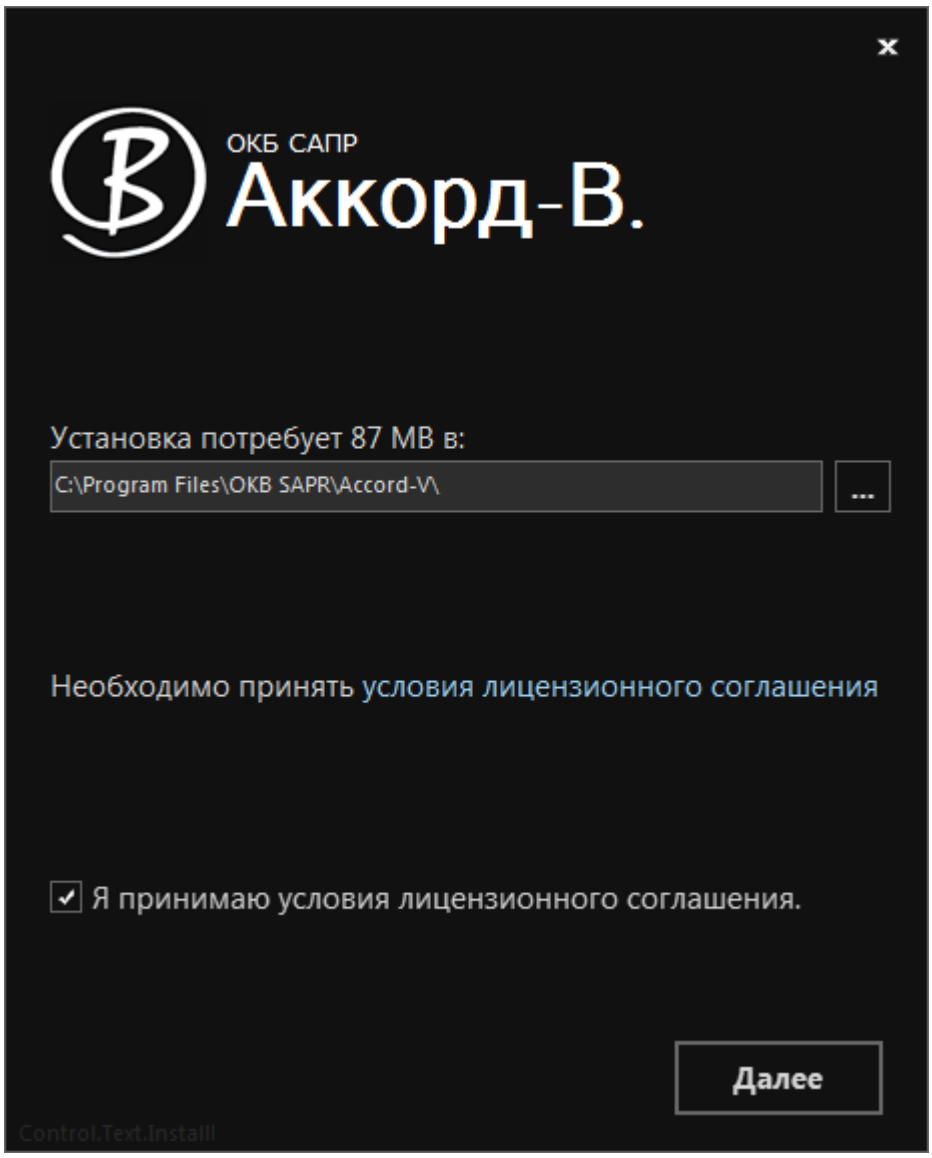


Рисунок 6 - Выбор пути установки

Далее необходимо выбрать компоненты устанавливаемого ПО и нажать кнопку <Установить> (рисунок 7).

Если выбран рекомендуемый вариант расположения сервиса регистрации событий (на отдельном АРМ), на данном этапе следует выполнить установку ПО без сервиса регистрации событий (данная процедура будет выполнена позже – см. 10).

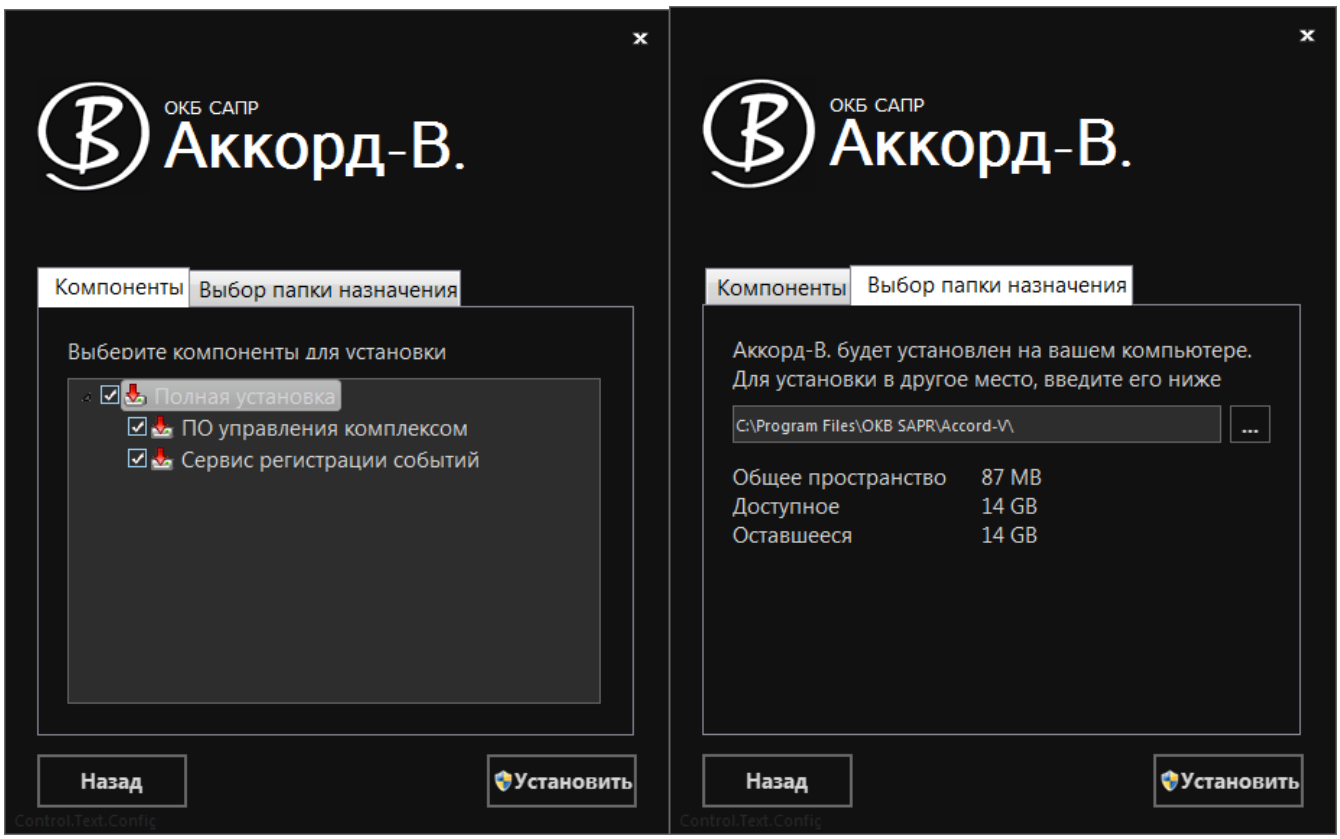


Рисунок 7 - Выбор компонентов установки

Начнется установка ПО, в процессе которой на рабочем столе ОС создаются ярлыки:

- «Installer-V.» – утилита для установки агентов «Аккорд-В.» на ESXi;
- «Accord-V.» – утилита управления комплексом «Аккорд-В.»;
- «LogViewer-V.» – утилита просмотра зарегистрированных событий.

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

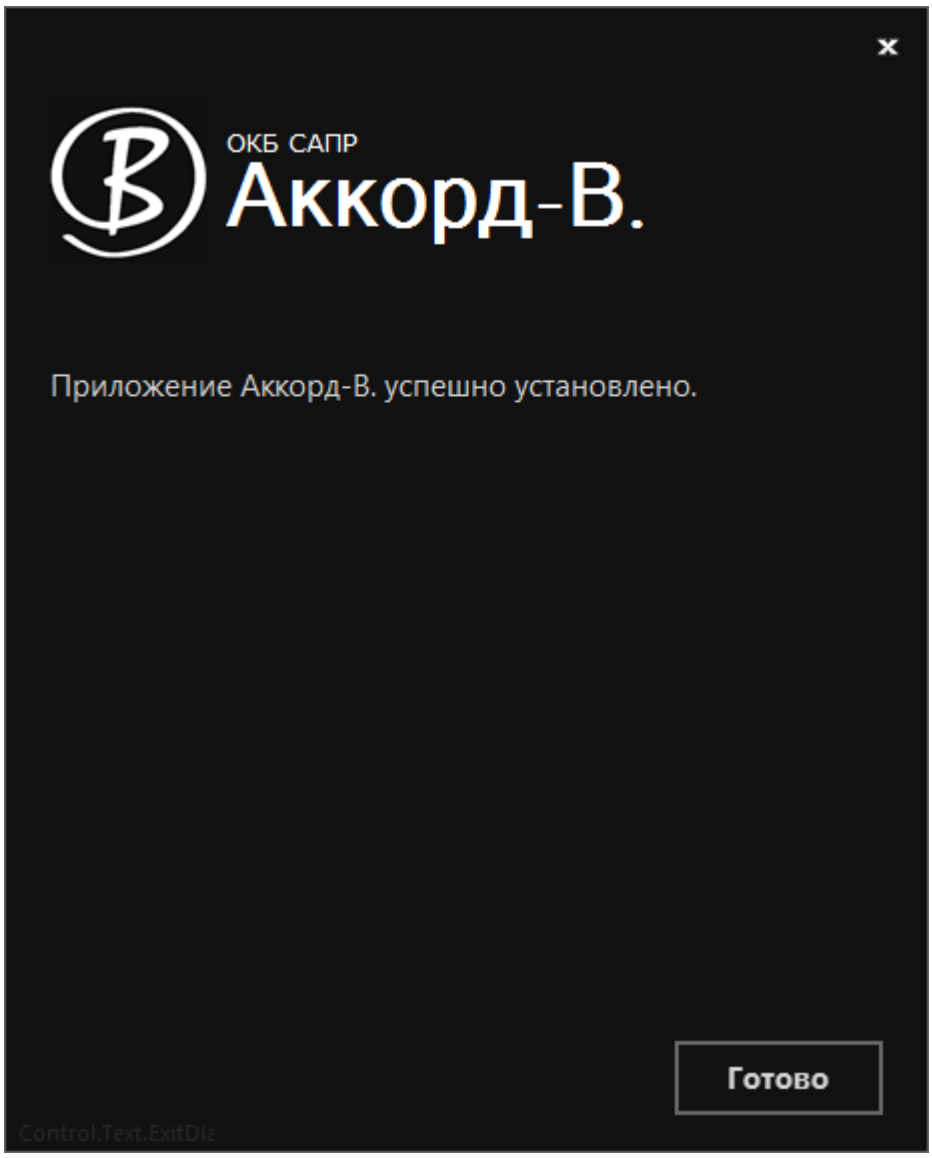


Рисунок 8 - Окончание процесса установки ПО «Аккорд-В.»

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

а) пользователь, запускающий «LogViewer-V.», должен иметь права на запись в файл LogConfig.xml и чтение/исполнение файлов в папке с установленным ПО «Аккорд-В.» (Accord-V). В данном случае указаны минимально требуемые права – данному пользователю можно также предоставлять права на всю папку Accord-V целиком;

б) для входа в утилиту «Accord-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»);

в) пользователь, запускающий «Accord-V.», должен иметь полный доступ к папке Accord-V;

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

д) пользователь, запускающий ««Installer-V.»», должен иметь права на запись в файл Config.xml, а также на чтение/исполнение файлов в каталоге с установленным ПО «Аккорд-В.» и в каталоге, в который будут сохраняться резервные копии (подробнее см. 15). В данном случае указаны минимально требуемые права – данному пользователю можно также предоставлять права на всю папку Accord-V целиком.

9. Установка агентов «Аккорд-В.» на ESXi

Установка агентов «Аккорд-В.» на ESXi производится централизованно с АРМ АБИ.

Для выполнения процедуры установки агентов «Аккорд-В.» на ESXi, необходимо запустить утилиту **Installer-V.exe** (ярлык на рабочем столе АРМ АБИ, созданный в процессе установки модулей «Аккорд-В.»).

ВНИМАНИЕ! АБИ, выполняющий установку агентов «Аккорд-В.», должен обладать достаточными правами на запись в папку с установленным ПО «Аккорд-В.» (см. 8.2).

Последовательность установки агентов зависит от используемой инфраструктуры.

1. Если в инфраструктуре используется vCenter, то в появившемся далее окне следует добавить vCenter, нажав на кнопку <Добавить vCenter>.

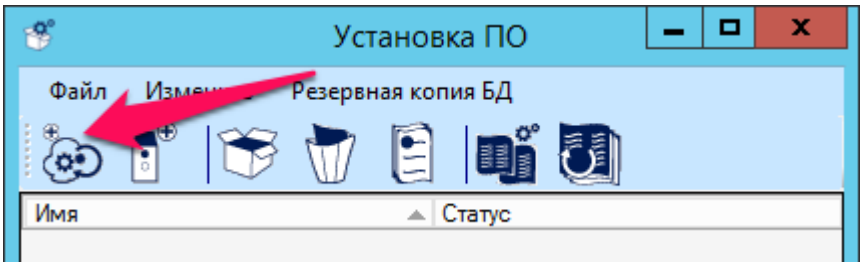


Рисунок 9 - Добавление vCenter

В появившемся окне следует ввести адрес добавляемого vCenter, а также имя и пароль учетной записи АБИ (поля «Имя пользователя» и «Пароль»), и нажать кнопку <Добавить>.

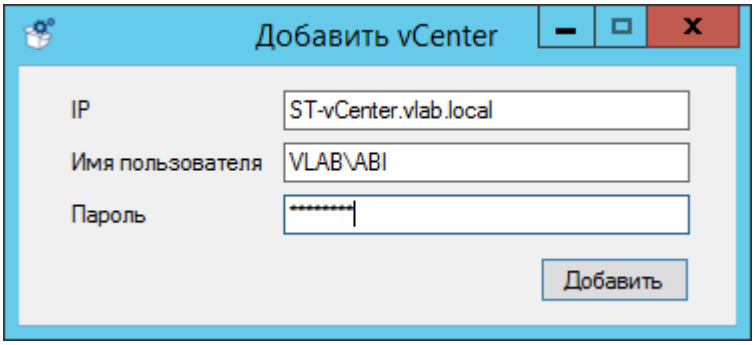


Рисунок 10 - Ввод параметров добавляемого vCenter

По завершении процедуры добавления vCenter на экран выводится соответствующее сообщение, а также появляется список ESXi, связанных с данным vCenter.

2. Если используются отдельные ESXi (без vCenter), то в окне установки ПО необходимо нажать кнопку <Добавить ESXi> (вторая слева) и ввести соответствующий IP-адрес (после этого данный хост также должен появиться в списке внизу).

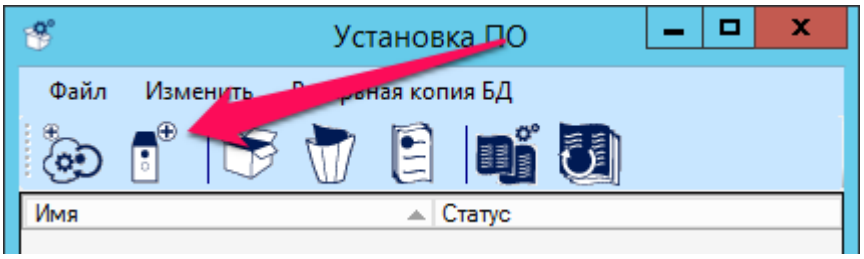


Рисунок 11 - Кнопка <Добавить ESXi>

После добавления ESXi одним из указанных выше способов, следует перейти к непосредственной процедуре установки агентов «Аккорд-В.» на ESXi.

Для этого в окне установки ПО следует выделить в списке нужный хост и нажать кнопку <Установить>.

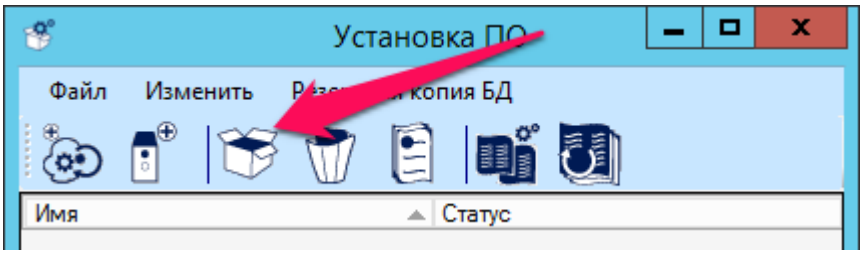


Рисунок 12 – Кнопка <Установить>

В появившемся окне (рисунок 13) необходимо ввести имя учетной записи на ESXi (root) и ее пароль для соответствующего хоста.

Для упрощения работы, в случае если на нескольких ESXi учетные записи root имеют одинаковые пароли, существует возможность выделить сразу несколько ESXi и в появившемся далее окне один раз ввести пароль учетной записи root, общий для всех выбранных ESXi.

ВНИМАНИЕ! Для всех выбранных хостов пароль от учетной записи root запрашивается **только один раз!** Таким образом, если пароли на хостах различны, следует выполнять установку на каждом ESXi отдельно, последовательно выделяя в списке нужный хост и нажимая кнопку <Установить>.

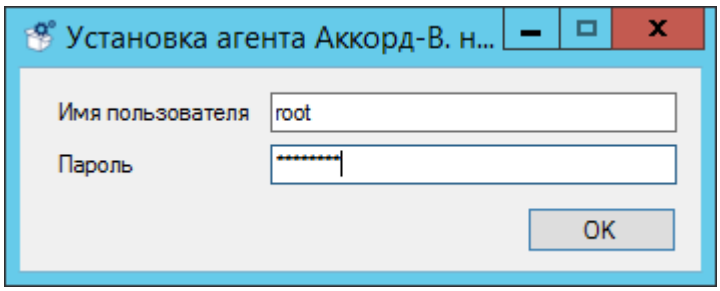


Рисунок 13 - Окно ввода пароля учетной записи root на ESXi

По нажатии кнопки <OK> в окне ввода пароля учетной записи root выполняется установка агентов «Аккорд-В.» на ESXi, в результате которой на экран выводится соответствующее сообщение.

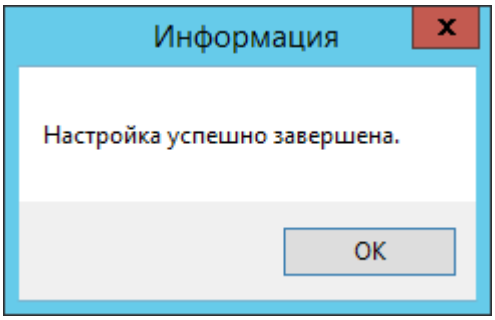


Рисунок 14 - Сообщение об успешном выполнении процедуры установки агентов «Аккорд-В.»

При этом статус для соответствующего хоста в окне установки ПО сменяется на «Установлен».

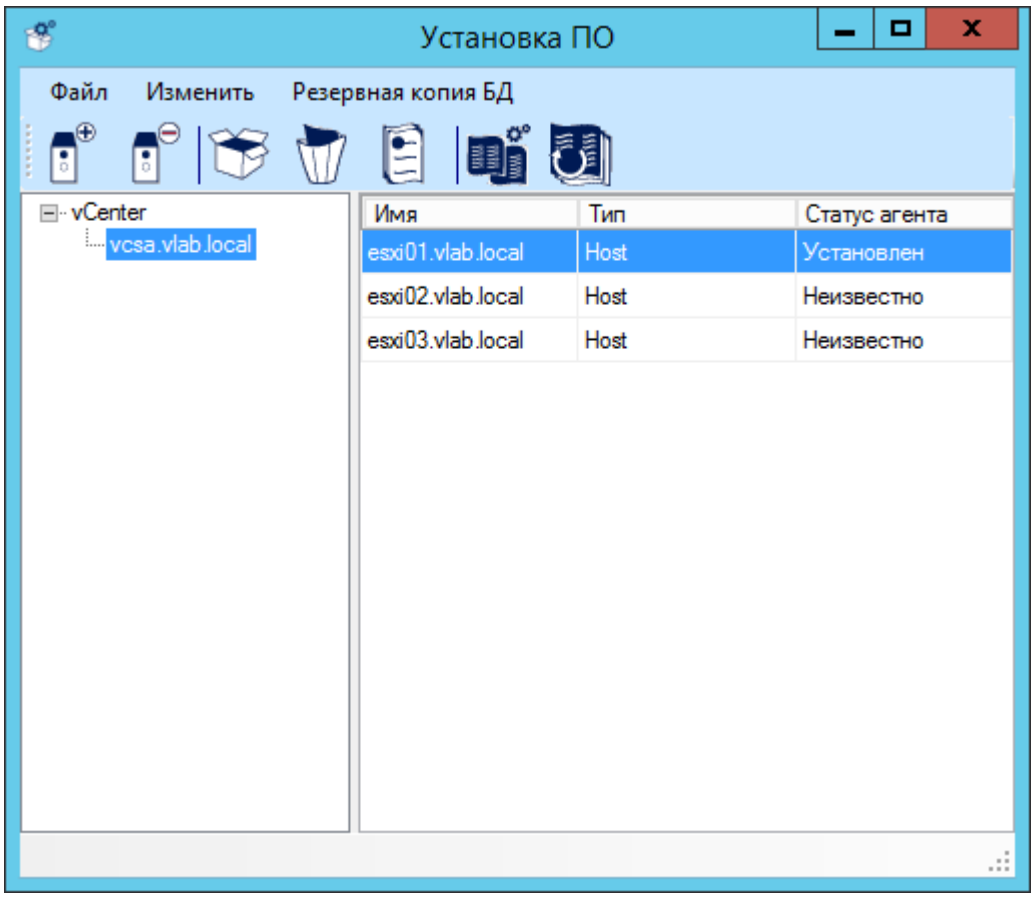


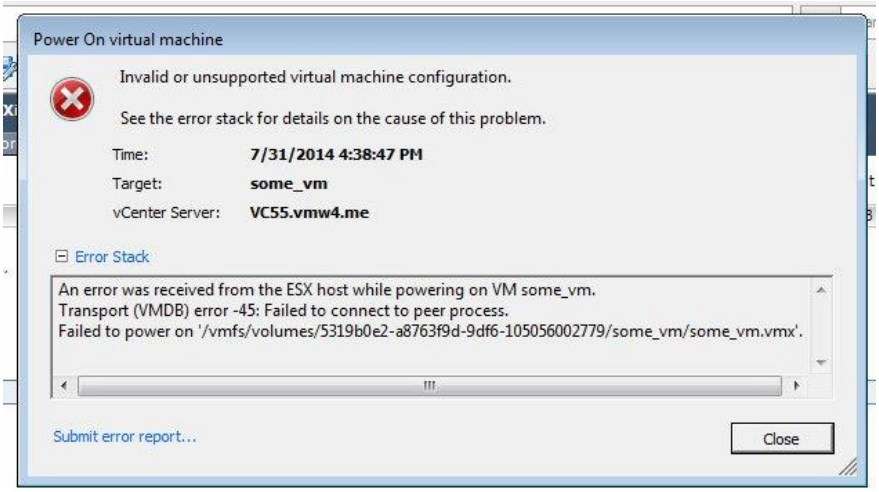
Рисунок 15 - Изменение статуса в окне установки ПО

ВНИМАНИЕ! Действия, связанные с установкой или удалением агентов на ESXi, следует выполнять только с помощью утилиты ««Installer-V.»».

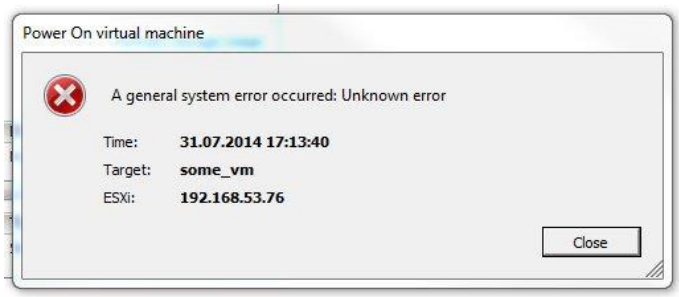
Следует учитывать, что статус установки агентов обновляется в окне утилиты ««Installer-V.»» только по факту установки или удаления агентов **с помощью данной утилиты**. Если агенты были удалены способом, отличным от указанного, статус их установки в утилите не изменится.

ВАЖНО! После установки агентов на ESXi включение ВМ на них будет заблокировано! При включении будут показываться следующие сообщения:

для vSphere 5.5 и 6.0:



для vSphere 5.0 и 5.1:



После установки ПО «Аккорд-В.» на межсетевом экране ESXi (firewall) автоматически откроются два порта (подробнее см. подраздел «Security Profile» вкладки «Configuration» для соответствующего хоста):

- порт 51178, предназначенный для взаимодействия с ПО управления доверенной загрузкой ВМ (сервис «accordservice»);
- порт 51179, предназначенный для взаимодействия с сервисом регистрации событий (сервис «accordlog»).

Также порт 51179 необходимо открыть вручную в брандмауэре Windows там, где установлен сервис регистрации событий (см. 10), а также на других промежуточных межсетевых экранах между серверами.

Если АРМ АБИ и АВИ являются различными СВТ, рекомендуется настроить firewall на ESXi так, чтобы подключения к сервисам «Аккорд-В.» могли выполняться только с АРМ АБИ. Пример подобной настройки показан на рисунке 16.

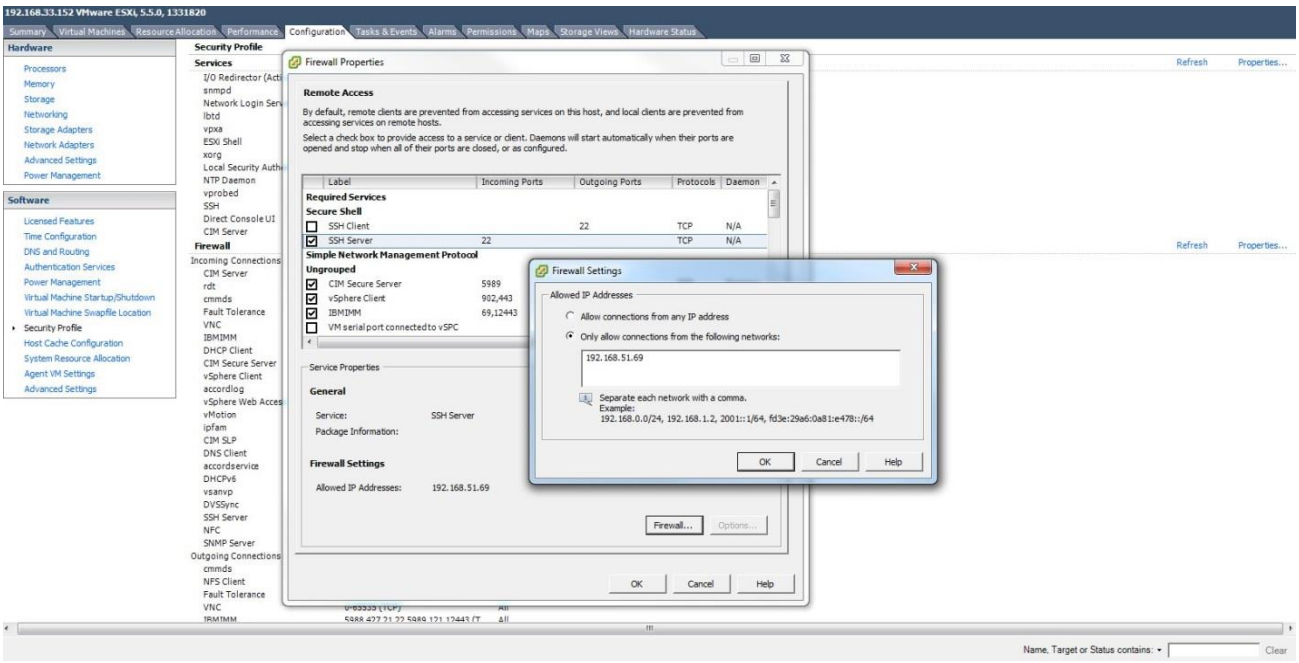


Рисунок 16 – Пример настройки firewall на ESXi

Следующим этапом необходимо выполнить установку сервиса регистрации событий.

10. Установка и настройка сервиса регистрации событий

Перед установкой сервиса регистрации событий необходимо создать для него отдельную учетную запись, от имени которой будет работать сервис (сервисная учетная запись – см. п. 6.2), обладающую следующими правами:

4) 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»;

5) на vCenter (в случае его использования) и на ESXi-хостах (в случае standalone) для данной учетной записи должны быть заданы ReadOnly Permissions (см. 6.2);

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

7) рекомендуется запретить (средствами домена) локальный и удаленный вход на ПК для сервисной учетной записи.

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, 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!

Примечание: агент «Аккорд-В.» записывает все события в /var/log/accordguard, а также дублирует их в syslog, если необходимо собирать события при помощи SIEM. Сервис регистрации событий постоянно забирает события с /var/log/accordguard (при этом удаляя их оттуда, но оставляя в syslog) и с vCenter.

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

Следует запустить утилиту **LogServiceInstall.exe** с правами администратора и начать установку сервиса регистрации событий, настроив при этом следующие параметры (рисунок 18):

- *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. Для нее должны быть назначены права «Read Only» в инфраструктуре VMware vSphere, отключен локальный вход в ОС (средствами домена) и даны права на запись в файл EventDatabase.db, а также на чтение и создание файлов в папке Accord-V.**

  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.») пользователю «LOCAL SERVICE» (рисунок 17).

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»).

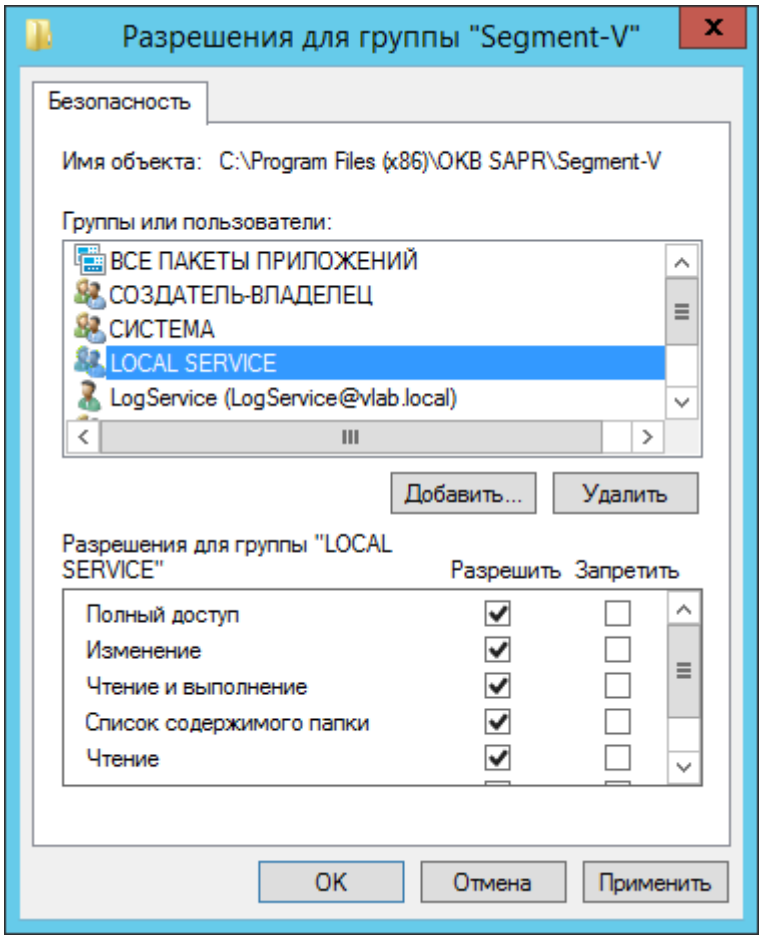


Рисунок 17 - Назначение прав сервисной учетной записи на папку с установленным ПО

- *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.

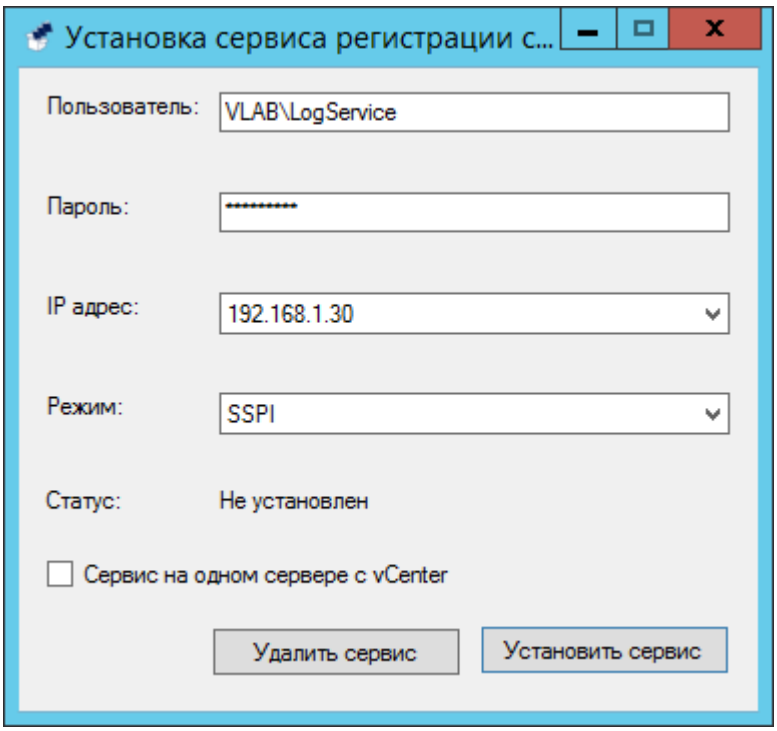


Рисунок 18 - Установка сервиса регистрации событий

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 19).

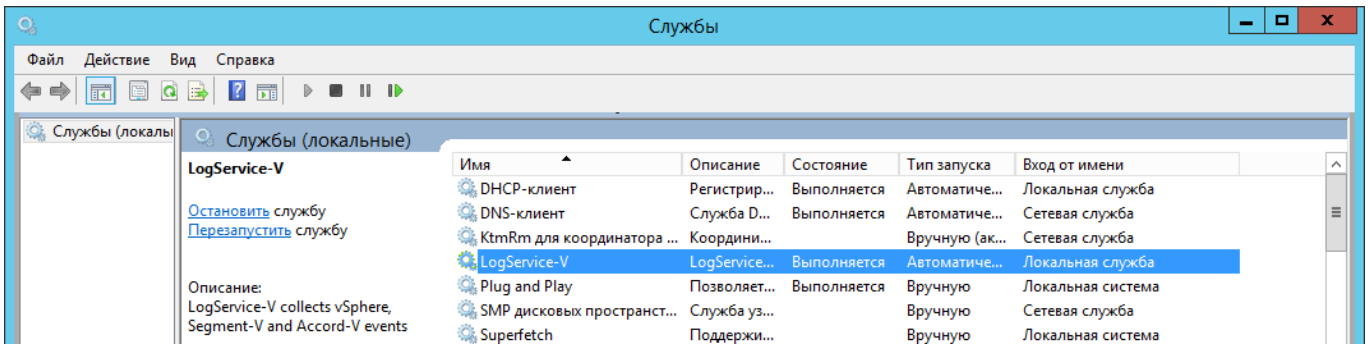


Рисунок 19 - Проверка запуска сервиса

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 20 – Кнопка <Настройки>

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

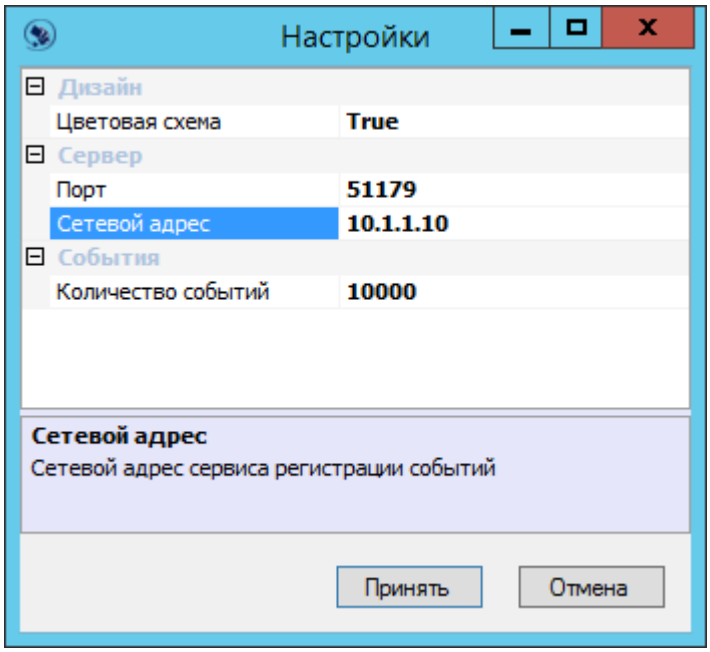


Рисунок 21 - Настройка IP-адреса сервиса регистрации событий

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).

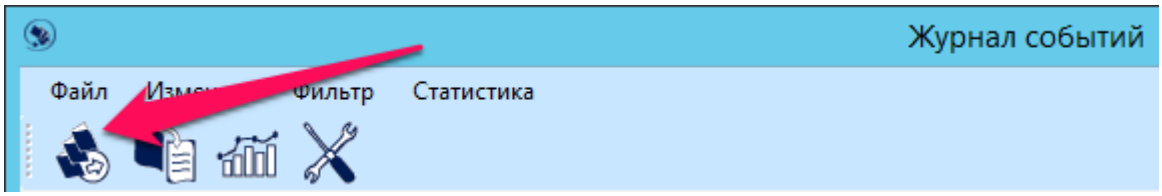


Рисунок 22 – Кнопка <Получить события>

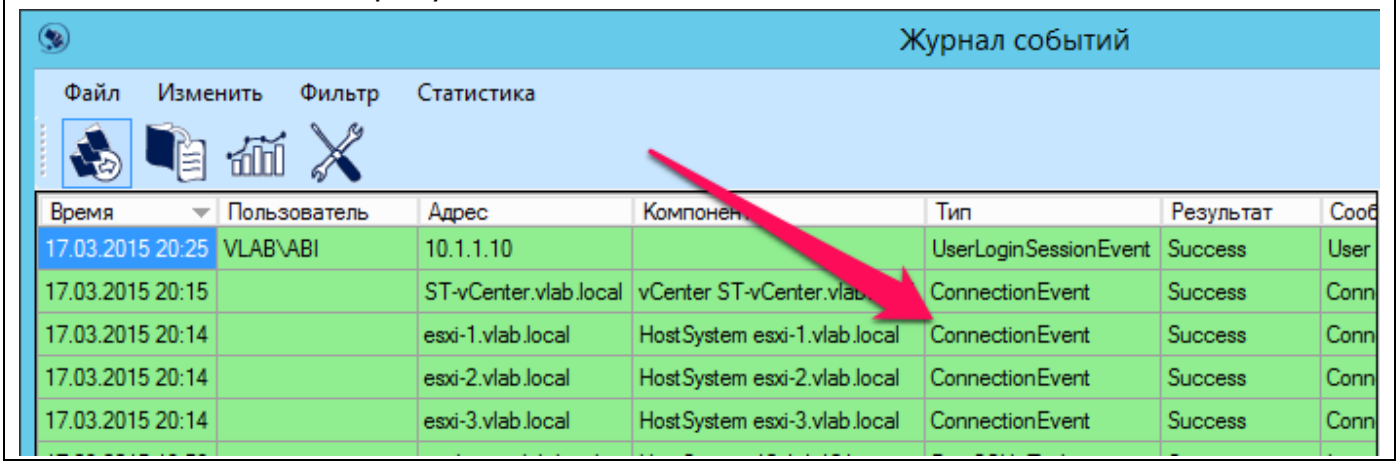
На экран выводится список всех выполненных событий.

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

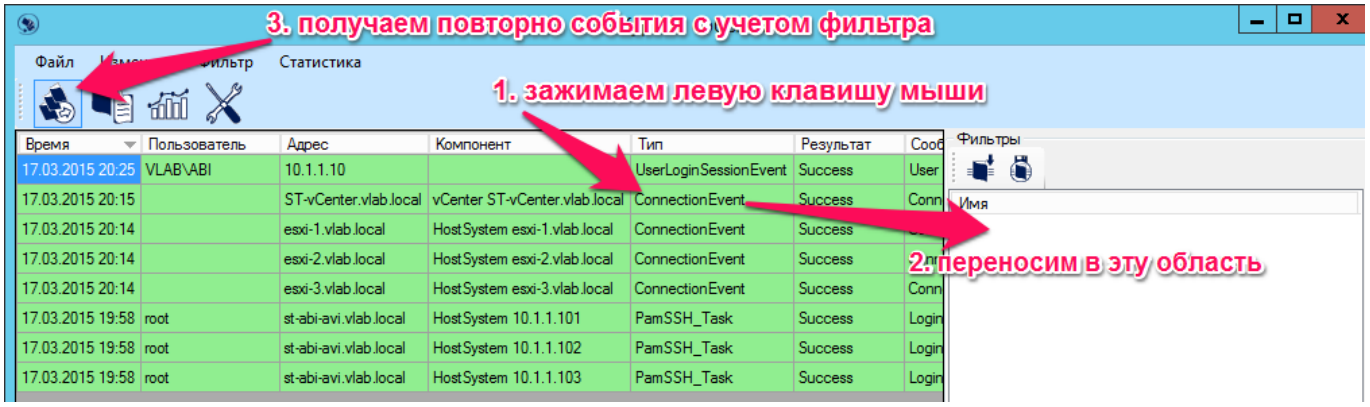
ВНИМАНИЕ! В списке полученных событий после первого старта сервиса отображаются события о подключении к vCenter и агентам «Аккорд-В.» на ESXi (тип «ConnectionEvent» – показывает, что соединение с указанными в файле конфигурации элементами прошло успешно). Необходимо удостовериться, что события подключения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

Возможной причиной, по которой соединение может быть не установлено, является рассинхронизированное время (подробнее см. 7).

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



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.



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

11. Предъявление лицензии

Для работы с утилитой настройки доверенной загрузки ВМ («Accord-V.») требуется лицензия. Она выдается производителем и поставляется на компакт-диске в составе комплекта поставки продукта или иным способом

(универсальный файл лицензии license-v.lic – для ПАК «Аккорд-В.» и ПАК «Сегмент-В.»).

Для предъявления лицензии потребуется скопировать с компакт-диска файл лицензии в корень папки с установленным ПО:

C:\Program Files (x86)\OKB SAPR\Accord-V

Подробнее о системе лицензирования см. соответствующий раздел «Руководства по установке» (11443195.4012.028 98) на комплекс.

12. Авторизация АБИ в системе

Далее следует на АРМ АБИ запустить с правами администратора утилиту **«Accord-V.»** и авторизоваться в системе – ввести учетные данные АБИ или воспользоваться функцией «использовать учетные данные текущей сессии».

Примечание: Следует помнить, что у учетной записи АБИ должны быть права на запись в базу данных ManagedDatabase.

Поле сервер, содержащее IP-адрес vCenter или ESXi, с которым будет происходить работа, заполняется автоматически из файла конфигурации. **Его изменение может привести к неправильной работе ПО!**

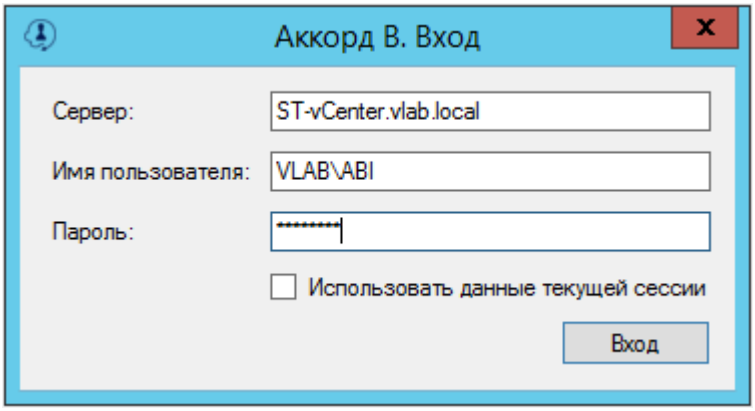


Рисунок 23 – Авторизация АБИ в системе

Если работа происходит с несколькими элементами (например, с несколькими ESXi), то запрос на авторизацию будет произведен для каждого из них.

После авторизации на экран выводится главное окно утилиты управления комплексом, в области задач которого появляются задачи на подключение к агентам «Аккорд-В.» на ESXi серверах.

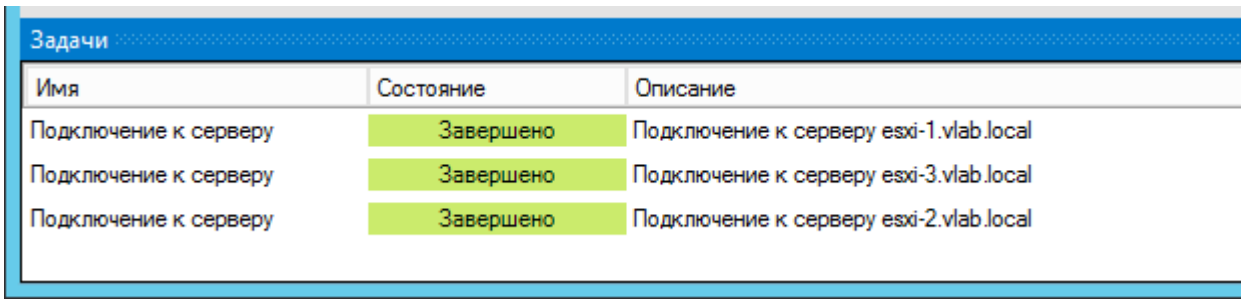


Рисунок 24 – Задачи на подключение к агентам

При этом состояния подключений могут быть выделены различными цветами:

- зеленый – соединение установлено;
- желтый – соединение установлено, но в настройках выбран небезопасный режим работы с ВМ;
- красный – соединение не удалось установить.

ВНИМАНИЕ! При потере соединения с агентом «Аккорд-В.» во время работы с утилитой «Accord-V.» (потеря соединения сопровождается сообщением «Ошибка соединения с хостом» при выполнении задач) статус соединения не обновится – необходимо перезапустить утилиту!

12.1. Настройка доверенной загрузки виртуальной машины с vCenter

Настройка доверенной загрузки виртуальной машины с vCenter (если vCenter реализован в качестве ВМ) имеет ряд существенных особенностей.

Поскольку контроль целостности и доверенную загрузку нельзя настроить для **включенной** виртуальной машины, необходимо ее выключить, однако после этого подключиться к данному vCenter в «Accord-V.» будет невозможно.

Поэтому *для vCenter на виртуальной машине* предлагается особый вариант настройки:

1) до выключения ВМ с vCenter зайти в утилиту «Accord-V.» и включить мягкий режим для тех хостов, на которые разрешена миграция виртуальному vCenter;

2) выйти из утилиты «Accord-V.» и выключить ВМ с vCenter;

3) отредактировать файл конфигурации Config.xml, заменив в строчке “InfoServer name” IP-адрес vCenter на IP-адрес ESXi;

4) включить утилиту «Accord-V.» и подключиться к ESXi, введя учетные данные ESXi пользователя;

5) выбрать виртуальную машину с vCenter и поставить ее на контроль, разрешив миграцию на данный хост и посчитав КС контролируемых компонентов;

6) выйти из утилиты «Accord-V.»;

7) если виртуальной машине с vCenter разрешено мигрировать на другие хосты, то после шага 6 для каждого из ESXi выполнить следующее:

- зайти через vClient на ESXi, на котором в данный момент находится vCenter, и разрегистрировать с него виртуальную машину с vCenter (Remove from Inventory);

8) подключиться к другому ESXi, на который разрешена миграция для ВМ с vCenter, и добавить виртуальную машину, открыв хранилище и выбрав соответствующий vmx файл (Add to Inventory);

9) повторить шаги 3-6 уже для этого ESXi.

10) вернуть в Config.xml текущий IP-адрес vCenter в поле "InfoServer name";

11) подключиться к ESXi и включить vCenter;

12) включить утилиту «Accord-V.» и отключить мягкий режим для хостов.

ВНИМАНИЕ! После такой настройки верная информация о текущих компонентах контроля виртуальной машины с vCenter будет отображаться **только при подключении к последнему ESXi, на котором выполнялась настройка vCenter**. Данная виртуальная машина будет отображаться как неконтролируемая, для остальных виртуальных машин информация будет корректной. Включение и проверка компонентов будет происходить в штатном режиме.

13. Настройка доверенной загрузки ВМ

Настройка доверенной загрузки ВМ осуществляется при помощи утилиты управления комплексом **«Accord-V.»** после авторизации АБИ в системе (подробнее см. 12).

ВНИМАНИЕ! В «Аккорд-В.» по умолчанию предусмотрена политика, когда неконтролируемые ВМ не включаются. Т.е. **после установки агента на ESXi никакие ВМ нельзя будет включить** (при этом работающие ВМ продолжат работу).

ВНИМАНИЕ! Процедура настройки доверенной загрузки ВМ выполняется только после предъявления лицензии (подробнее см. 11).

Для настройки доверенной загрузки ВМ необходимо выполнить следующие действия:

1. Настроить для необходимых ВМ параметры миграции (эта настройка отвечает за то, на каких ESXi ВМ смогут включиться; если вычислить КС для ВМ, но не разрешить миграцию никуда, то она не включится!). Для этого следует:

1) выбрать необходимую ВМ ***(должна быть в состоянии suspend или выключена)*** и нажать кнопку <Миграция> (или выбрать

соответствующий пункт контекстного меню, вызываемого посредством нажатия на ВМ правой клавишей мыши);

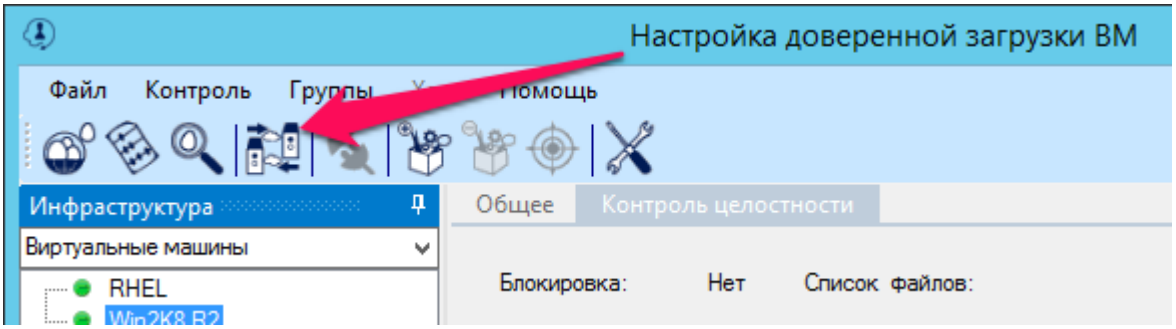


Рисунок 25 – Кнопка <Миграция>

2) в появившемся далее окне добавить ESXi серверы, на которые миграция будет разрешена. Для этого в левой области окна следует выбрать нужные хосты (в том числе при помощи клавиш <Shift> и <Ctrl>), нажать кнопку <+> для добавления в список разрешенных (правая часть окна), применить настройку, нажав кнопку <Применить> (рисунок 26), и дождаться завершения данной задачи.

ВНИМАНИЕ! В процессе выполнения процедуры настройки параметров миграции для ВМ применяются текущие настройки контроля целостности.

ВНИМАНИЕ! Если миграция не разрешена ни на один хост, то вне зависимости от настроек КЦ, ВМ нигде не включится!

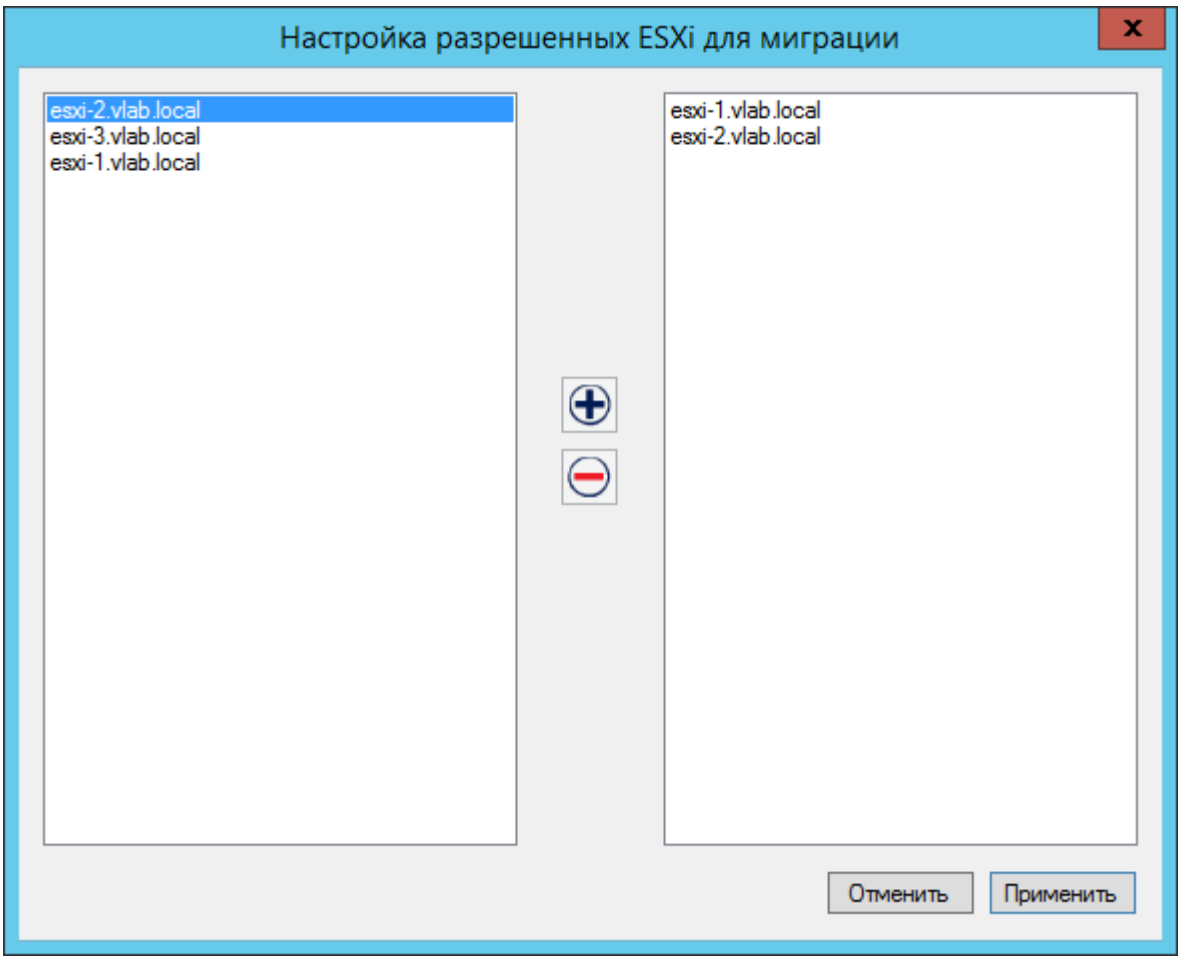


Рисунок 26 - Настройка списка ESXi серверов, на которые будет разрешена миграция ВМ

2. Вычислить КС необходимых элементов ВМ. Для этого следует:

1) выбрать ВМ и нажать кнопку <Установить> (рисунок 27) (или выбрать соответствующий пункт контекстного меню, вызываемого посредством нажатия на ВМ правой клавишей мыши);

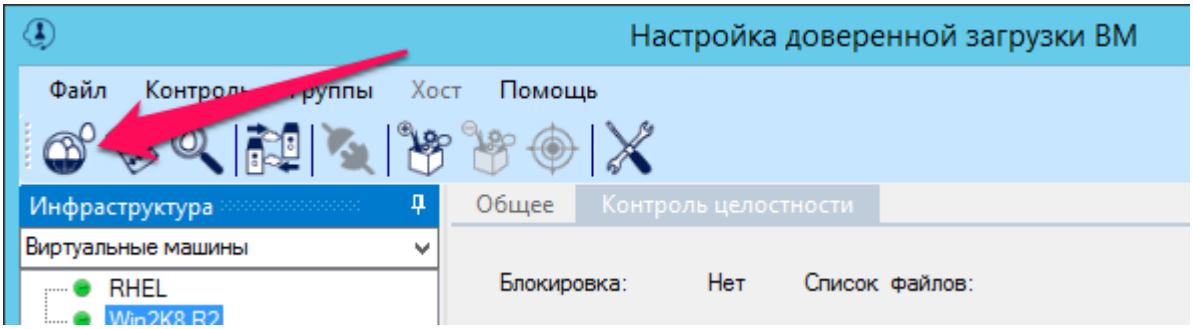


Рисунок 27 - Кнопка <Установить>

2) в появившемся далее окне (рисунок 28) выбрать для установки на контроль необходимые компоненты из следующего списка:

– «Оборудование» (vmx);

– «BIOS» – при каждом включении ВМ будет использоваться BIOS, поставленный на контроль;
– «MBR» – контролируется на каждом vmdk текущего состояния ВМ;
– «Файлы» – файлы, контролируемые при запуске (список отображается в колонке «Список файлов»).

Примечание: Для гостевых ОС существуют списки рекомендованных файлов для установки на контроль. Также существует возможность сохранять/загружать собственные списки файлов.

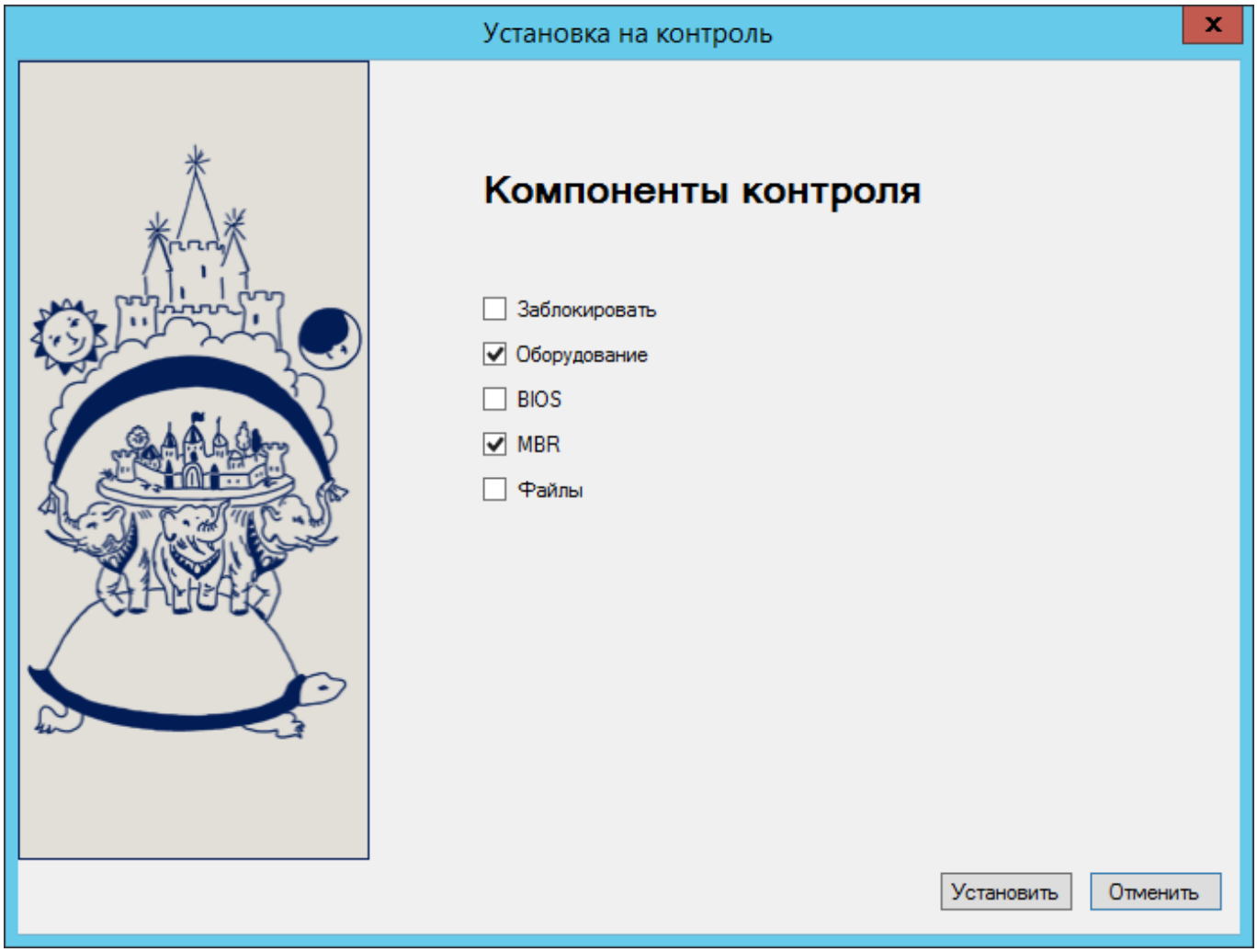


Рисунок 28 - Выбор компонентов контроля

3) в случае если на контроль не предполагается устанавливать файлы, нажать кнопку <Установить> (рисунок 28) и дождаться завершения процедуры расчета КС;

ВНИМАНИЕ! Нажимая кнопку <Установить>, Вы удаляете предыдущие настройки для ВМ!

4) в случае если на контроль устанавливаются файлы, следует нажать кнопку <Далее> (рисунок 29);

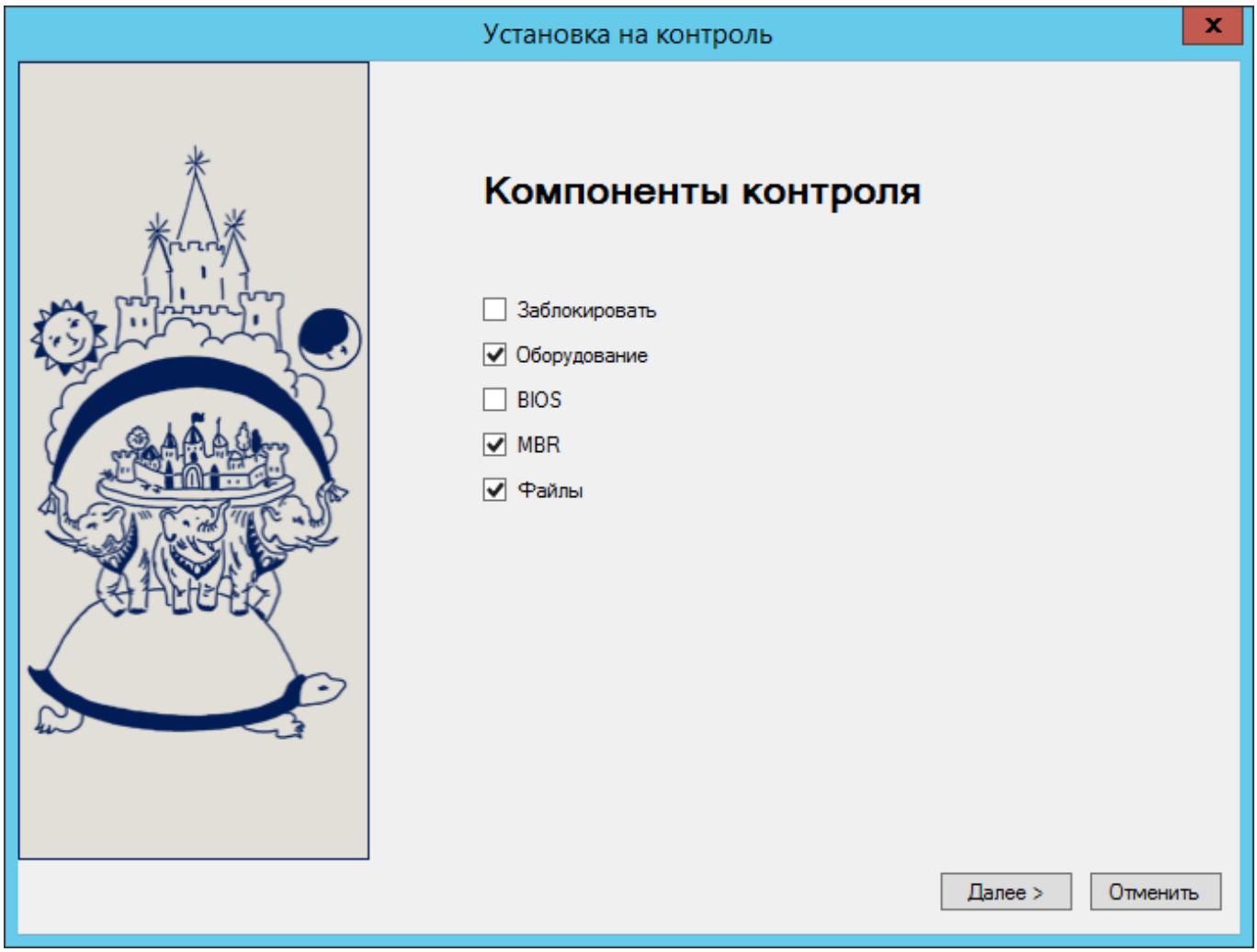


Рисунок 29 - Выбор компонентов контроля

5) в появившемся далее окне (рисунок 30) следует установить на контроль необходимые файлы. Для этого в левой области окна для соответствующих vmdk, принадлежащих данной ВМ, необходимо выбрать нужные файлы гостевой ОС (в том числе при помощи клавиш <Shift> и <Ctrl>) и нажать кнопку <+> для добавления в список контролируемых (правая часть окна);

ВНИМАНИЕ! Если для ВМ миграция не разрешена ни на один ESXi, список файлов получить будет невозможно.

Полученный список можно экспортировать в файл (кнопка <Экспорт>). Для импорта в дальнейшем необходимо выбрать vmdk, к которому будет применяться этот список, и нажать кнопку <Импорт>.

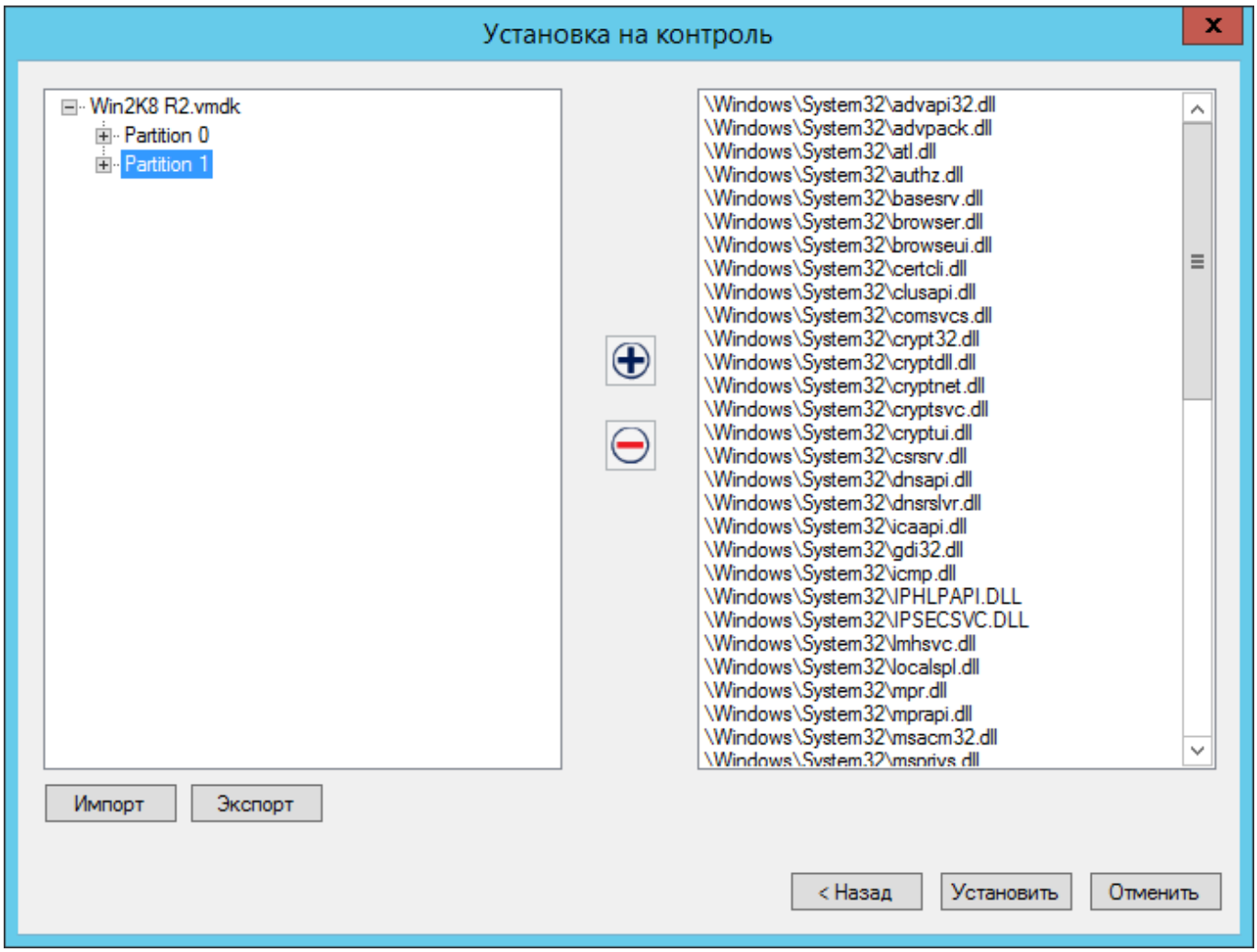


Рисунок 30 - Установка файлов на контроль

6) в завершение следует нажать кнопку <Установить> и дождаться окончания процедуры расчета КС (рисунок 31).

ВНИМАНИЕ! Нажимая кнопку <Установить>, Вы удаляете предыдущие настройки для ВМ!

ВНИМАНИЕ! В процессе расчета КС не включайте ВМ, иначе операция будет прервана!

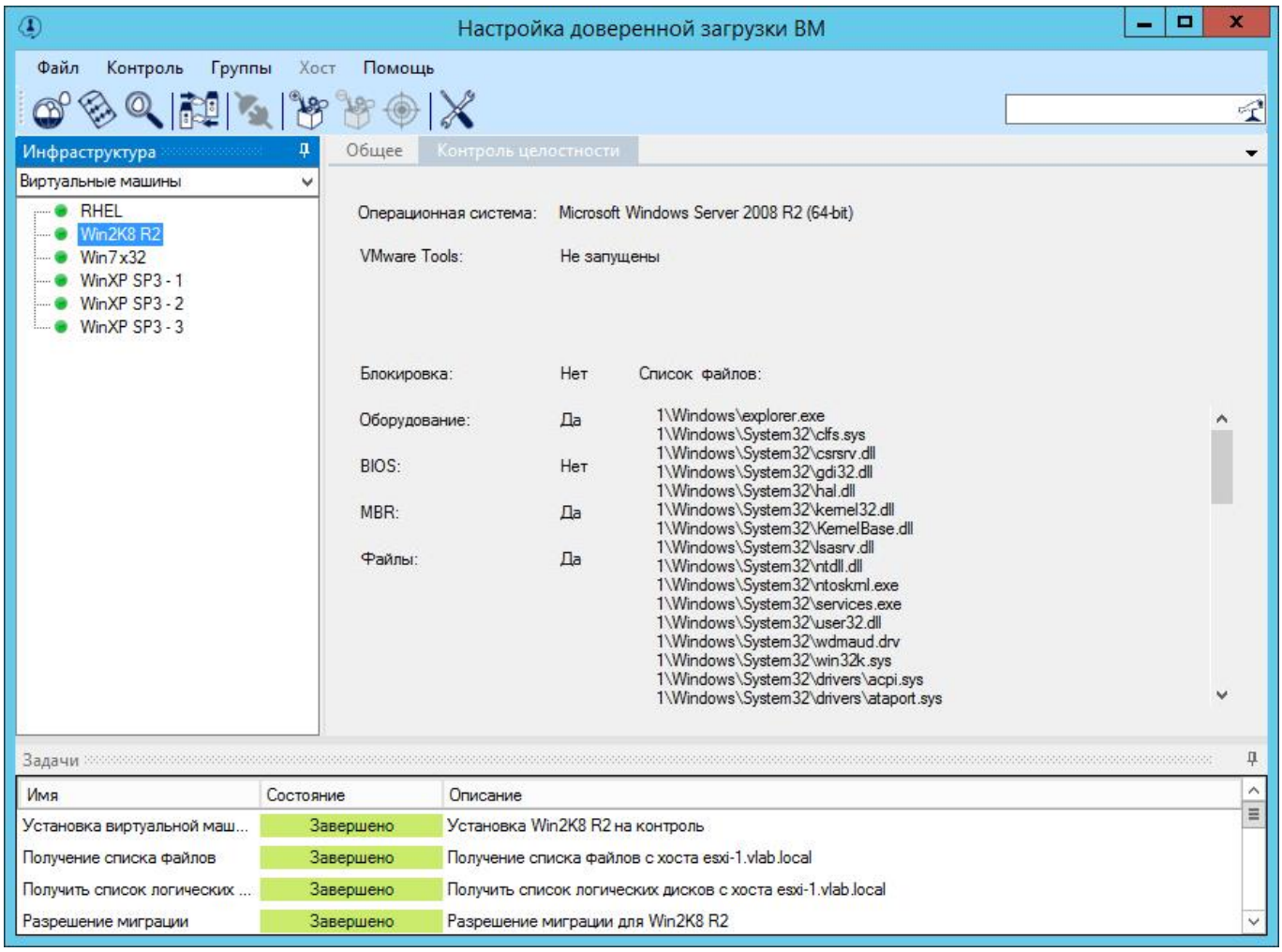


Рисунок 31 - Процесс установки на контроль

Работа с группами

В случае наличия множества однотипных ВМ (VDI) можно воспользоваться механизмом групп: вкладка «Группы» предназначена для объединения ВМ с едиными настройками.

ВНИМАНИЕ! При работе с группами следует учитывать, что ВМ должны соответствовать следующим требованиям:

1. если не предполагается устанавливать на контроль файлы, то BIOS должен существовать или отсутствовать на всех группируемых ВМ (BIOS создается при первом включении ВМ);

2. если предполагается установка файлов на контроль, то у группируемых ВМ должно совпадать количество vmdk, их порядок, порядок логических разделов внутри vmdk (соответственно, и устанавливаемые на контроль файлы должны существовать внутри vmdk).

Порядок работы с группами следующий:

1) создать группу, нажав кнопку <Добавить группу>;

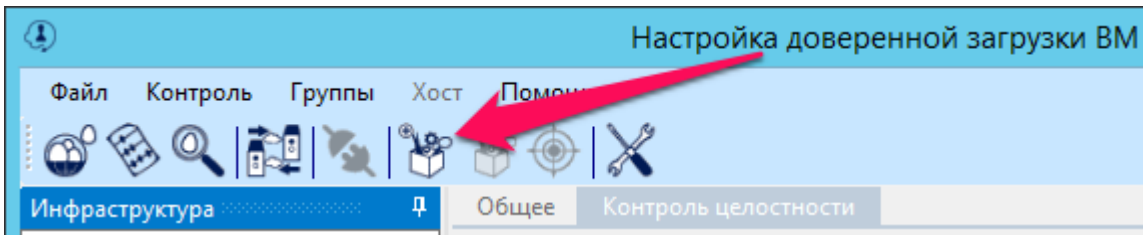


Рисунок 32 – Добавление группы

2) добавленную группу переименовать, нажав на нее правой клавишей мыши и выбрав пункт контекстного меню «Переименовать»;

ВНИМАНИЕ! При задании имени следует принимать во внимание ряд следующих ограничений на формат имени группы:

– имя группы не должно содержать символов кириллицы;

– имя группы не должно содержать менее трех символов;

– при задании имени группы возможно использование цифр, однако имя всегда должно начинаться с буквы.

3) добавить элементы (ВМ) в группу: нажать на кнопку <Добавить в группу> (рисунок 33), переместить нужные ВМ в правую часть появившегося окна (рисунок 34) и нажать кнопку <Применить>;

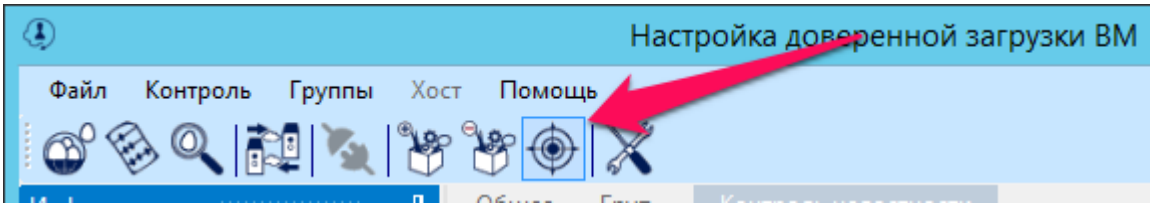


Рисунок 33 - Кнопка <Добавить в группу>

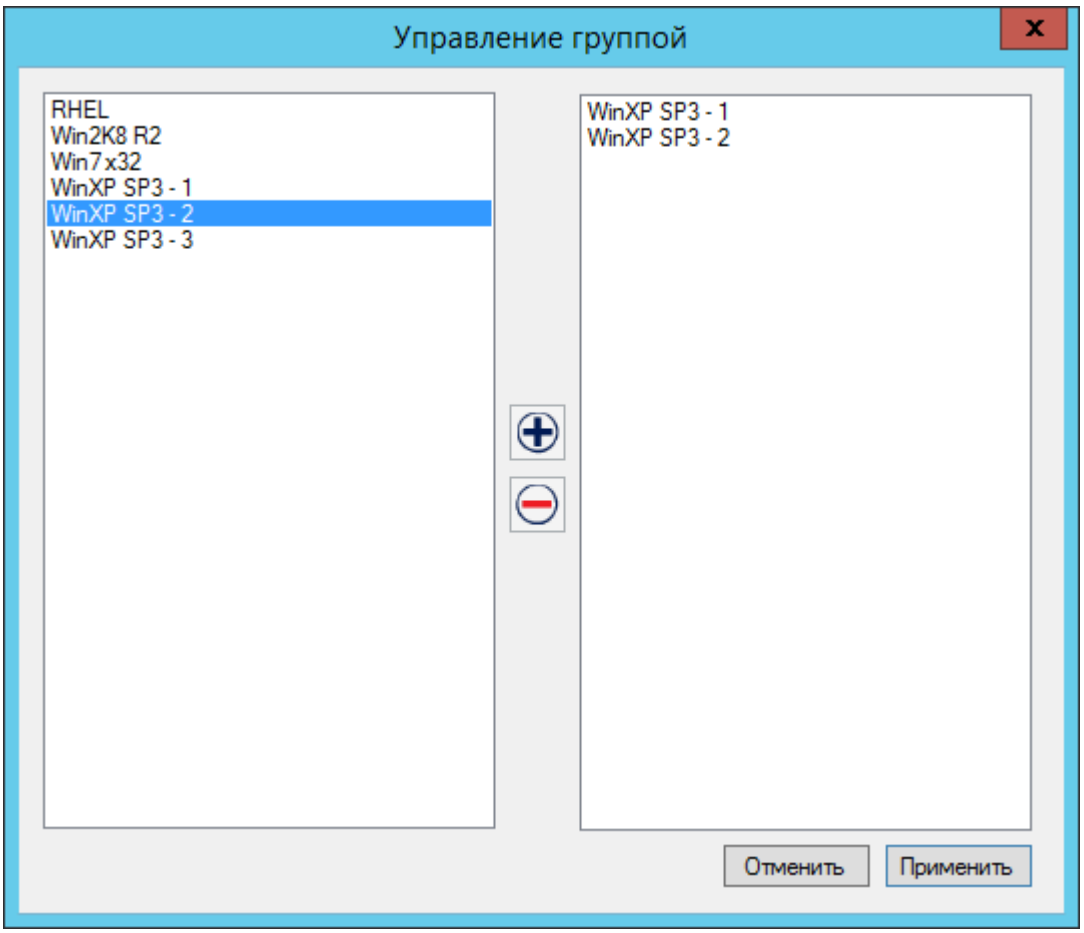


Рисунок 34 - Окно управления группой

4) выбрать группу в списке и настроить для нее параметры миграции – описание настройки параметров миграции см. выше;
5) вычислить КС необходимых элементов в сгруппированных ВМ, выбрав группу в списке и нажав кнопку <Установить>, – описание настройки параметров контроля см. выше.

В дальнейшем применяемые настройки миграции и параметры контроля для группы будут применяться для всех элементов в группе.

ВНИМАНИЕ! Если для ВМ отдельно выполнить установку на контроль, то она автоматически будет выведена из группы!

ВНИМАНИЕ! В процессе добавления в группу новой ВМ групповые настройки для нее наследуются автоматически.

Примечание. После добавления ВМ в группу при включении утилиты «Accord-V.» в инфраструктуре будут отображаться незагруженные ВМ (unloaded vm). Они пропадут из списка после получения инфраструктуры.

14. Настройка разграничения доступа на совмещенном АРМ АБИ/АВИ

В том случае если АРМ, на который устанавливается комплекс «Аккорд-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:

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

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

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

16) 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 Accord-V (на запись в файл EventDatabase.db, а также на чтение и создание файлов в папке);

17) 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;

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

19) 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»);

15. Создание резервных копий

На заключительном этапе настройки комплекса следует выполнить процедуру создания резервных копий:

1) баз данных (БД) с ESXi (с помощью утилиты «Installer-V.» – рисунок 35);

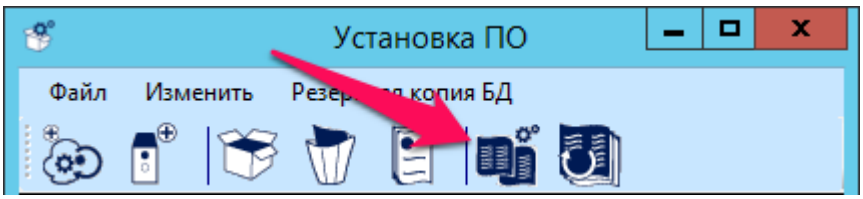


Рисунок 35 – Создание резервной копии БД

2) следующих элементов из каталога Accord-V (C:\Program Files (x86)\Accord-V):

- сертификаты: каталоги ./certs и cakey.pem;
- файл лицензии accord-v.lic;
- ManagedDatabase.db (БД настроек «Accord-V.»);
- EventDatabase.db (БД событий, зарегистрированных сервисом регистрации событий);
- файлы конфигурации Config.xml и LogConfig.xml;
- фильтры утилиты просмотра событий.

16. Включение режима ESXi Lockdown Mode

Далее следует включить режим ESXi Lockdown Mode.

Для этого на vCenter следует выбрать хост -> configuration -> security profile -> lockdown mode -> enabled.

Режим ESXi Lockdown Mode не позволит:

- установить/удалить агентов «Аккорд-В.»;
- перегенерировать сертификаты;
- сохранить/загрузить БД агентов «Аккорд-В.».

ВНИМАНИЕ! Все данные ESXi хранятся в ОЗУ. Если выполнять перезагрузку не стандартными способами, а путем отключения/включения питания, то возможна потеря данных в БД агентов «Аккорд-В.» (это также распространяется и на сами настройки ESXi). Поэтому после полноценной настройки комплекса рекомендуется перезагрузить все ESXi сервера.

На этом настройку «Аккорд-В.» можно считать завершенной!

Теперь ПАК «Аккорд-В.» готов к работе. Но мы настоятельно рекомендуем, прежде чем начинать использование той или иной функции ПАК «Аккорд-В.», внимательно ознакомиться с полным комплектом эксплуатационной документации на комплекс!