

Программный комплекс
«Система мониторинга и управления
событиями безопасности
Ankey SIEM Next Generation» v 5.2.3

Руководство по установке.
Часть 2

Установка ПК Ankey SIEM NG в
исполнении

Ankey SIEM NG VM

© ООО «Газинформсервис» с 2004 года

При инсталляции ПК Ankey SIEM NG VM необходимо ознакомиться с условиями лицензионного соглашения на использование конечным пользователем программы*, согласно которому весь функционал программного комплекса, в том числе отдельные его модули (составляющие)**, носители и документация, предоставляются на условиях «как есть»***.

Этот документ входит в комплект поставки программного обеспечения, и на него распространяются все условия лицензионного соглашения.

Ни одна из частей этого документа не может быть воспроизведена, опубликована, сохранена в электронной базе данных или передана в любой форме или любыми средствами, такими как электронные, механические, записывающие или иначе, для любой цели без предварительного письменного разрешения ООО «Газинформсервис».

Ankey SIEM NG VM® является зарегистрированным товарным знаком ООО «Газинформсервис».

Все названия компаний и продуктов, которые являются товарными знаками или зарегистрированными товарными знаками, принадлежат соответствующим владельцам.

За содержание, качество, актуальность и достоверность используемых в документе материалов, права на которые принадлежат другим правообладателям, а также за возможный ущерб, связанный с использованием этих материалов, ООО «Газинформсервис» ответственности не несет.

Дата редакции документа: 4 квартал 2024 года.

* Использование ПК Ankey SIEM NG VM означает согласие со всеми пунктами лицензионного соглашения.

** ПК Ankey SIEM NG VM включает в свой состав компоненты платформы, коннекторы (модули сбора и обработки данных) и контент (модули выявления нарушений ИБ (корреляционной обработки данных)).

*** Выполнение основных функций программы (функциональные возможности), предусмотренных (-е) действующей релизной версией. Комплектность, предусмотренная действующей релизной версией изделия. Документация, предусмотренная действующей релизной версией изделия.

Содержание

1 Об этом документе	5
2 О ПК Ankey SIEM NG VM	9
2.1 Архитектура ПК Ankey SIEM NG VM.....	10
2.1.1 Компонент Ankey SIEM Next Generation Core	10
2.1.2 Компонент Ankey SIEM Next Generation Collector	10
2.1.3 Компонент Ankey SIEM Next Generation Management and Configuration	10
2.2 Схема взаимодействия компонентов.....	11
3 Развертывание Ankey SIEM NG VM.....	13
3.1 Требования к программному обеспечению	13
3.2 Требования к аппаратному обеспечению	14
3.2.1 Требования к аппаратному обеспечению Ankey SIEM NG VM.....	14
3.2.2 Требования к аппаратному обеспечению мобильного Ankey SIEM NG VM	15
3.3 Рекомендации по развертыванию ПК Ankey SIEM NG VM в виртуальной среде	15
3.4 Рекомендации к установке ПК Ankey SIEM NG VM на ОС Astra Linux SE.....	17
3.5 Сценарий развертывания Ankey SIEM NG VM	19
3.6 Об установке компонентов на Linux с помощью ролей	20
3.7 Установка роли Deployer.....	21
3.8 Установка компонента Ankey SIEM NG MC	23
3.8.1 Установка роли SqlStorage	23
3.8.2 Установка роли JatobaStorage и онлайн активация лицензии.....	24
3.8.3 Установка роли JatobaStorage и офлайн активация лицензии.....	26
3.8.4 Установка роли Management and Configuration.....	28
3.9 Установка компонента Ankey SIEM NG Core на Linux	30
3.9.1 Установка роли RMQ Message Bus на сервер Ankey SIEM NG Core ...	30
3.9.2 Установка роли Core	31
3.10 Установка компонента Ankey SIEM NG Collector.....	34
3.10.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Collector ...	34
3.10.2 Установка роли Collector	35
3.10.3 Дополнительная настройка компонента Ankey SIEM NG Collector для мобильного Ankey SIEM NG VM.....	37
3.10.4 Установка компонента Ankey SIEM NG Collector на Microsoft Windows	37
3.11 Активация лицензии ПК Ankey SIEM NG VM	38
3.11.1 Активация лицензии на Linux при наличии доступа к интернету.....	39
3.11.2 Активация лицензии на Linux при отсутствии доступа к интернету ...	39
3.12 Удаление лицензионного ключа.....	40
3.13 Установка доверенного сертификата для сайта ПК Ankey SIEM NG VM	40
3.14 Установка пользовательского сертификата для RMQ Message Bus и компонентов Ankey SIEM NG Core и Ankey SIEM NG Collector	41
3.15 Настройка обновления экспертных данных.....	43

3.15.1 Схемы получения обновлений экспертных данных, поддерживаемые Ankey SIEM NG VM	43
3.15.2 Удаление компонента UCS	47
3.15.3 Изменение параметров обновления экспертных данных для роли Management and Configuration.....	47
3.15.4 Аппаратные и программные требования к локальному серверу обновлений.....	49
3.15.5 Установка локального сервера обновлений	49
3.15.6 Активация лицензии локального сервера обновлений	50
3.15.7 Настройка подключения локального сервера обновлений к прокси-серверу	50
3.15.8 Настройка автоматического переноса обновлений в закрытый сегмент сети	52
3.15.9 Ручной перенос обновлений Ankey SIEM NG VM в закрытый сегмент сети	53
3.15.10 Проверка и изменение параметров локального сервера обновлений	54
3.16 Настройка ПК Ankey SIEM NG VM для обеспечения его безопасной работы Ankey SIEM NG Core установлен на Linux.....	55
4 Обновление ПК Ankey SIEM NG VM с помощью дистрибутивов	59
4.1 Обновление роли Deployer	59
4.2 Обновление компонента Ankey SIEM NG MC на Linux	60
4.2.1 Обновление роли SqlStorage	60
4.2.2 Обновление роли JatobaStorage.....	61
4.2.3 Обновление роли Management and Configuration	62
4.3 Обновление компонента Ankey SIEM NG Core на Linux.....	64
4.3.1 Обновление роли RMQ Message Bus на сервере Ankey SIEM NG Core	64
4.3.2 Обновление роли Core	65
4.4 Обновление компонента Ankey SIEM NG Collector на Linux	66
4.5 Обновление компонента Ankey SIEM NG Collector на Microsoft Windows	67
5 Просмотр и изменение параметров конфигурации ПК Ankey SIEM NG VM	68
5.1 Просмотр и изменение конфигурации компонентов ПК Ankey SIEM NG VM на Linux.....	68
5.1.1 Просмотр конфигурации роли.....	68
5.1.2 Изменение конфигурации роли.....	68
5.1.3 Настройка SMTP-сервера для отправки уведомлений по электронной почте	69
6 Диагностика и решение проблем	71
Перечень сокращений.....	72
Приложение А Порядок установки ПК Ankey SIEM NG VM	75
Приложение Б Параметры конфигурации компонентов ПК Ankey SIEM NG VM на Linux.....	76
Приложение В Применение патчей в ПК Ankey SIEM NG (5.2.3).....	89

1 Об этом документе

Руководство по установке содержит информацию для планирования и выполнения развертывания программного комплекса Ankey SIEM Next Generation в варианте исполнения «Ankey SIEM NG VM» (далее также – Ankey SIEM NG VM) в инфраструктуре организации.

Примечание. Описание вариантов исполнения ПК Ankey SIEM NG и их функций приведено в документе «Руководство администратора Ankey SIEM NG 5.2.3».

В руководстве вы найдете типовые схемы развертывания ПК Ankey SIEM NG VM, а также инструкции по установке, первоначальной настройке, обновлению и удалению продукта.

Руководство адресовано руководителям и специалистам ИТ-подразделения организации, которые планируют и выполняют развертывание ПК Ankey SIEM NG VM.

Комплект документации ПК Ankey SIEM NG VM включает в себя документы, представленные в таблице 1.1.

Таблица 1.1 – Комплект документации ПК Ankey SIEM NG

Каталог	Наименование документа	Описание
Сведения о релизе	Обзор новых возможностей Ankey SIEM NG	Содержит описание изменений между выпускаемой и предыдущей версиями ПК Ankey SIEM NG
	Актуальные версии прикладных модулей ПК Ankey SIEM NG	Содержит список актуальных версий сборок всех поддерживаемых ресурсов к ПК Ankey SIEM NG, разработанных ООО "Газинформсервис"
Основное	Руководство администратора Ankey SIEM NG	Содержит справочную информацию о ПК Ankey SIEM NG и вариантах его исполнения, а также инструкции по настройке и администрированию продукта
	Руководство оператора Ankey SIEM NG	Содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности
	Руководство по настройке Ankey SIEM NG Event Broker	Содержит справочную информацию и инструкции по настройке и администрированию компонента Event Broker

Каталог	Наименование документа	Описание
Инсталляция	Руководство по установке Часть 1. Установка ПК Ankey SIEM NG в исполнениях Ankey SIEM NG и Ankey SIEM NG с дополнительным компонентом VM	Содержит информацию для внедрения вариантов исполнения Ankey SIEM NG и Ankey SIEM NG с дополнительным компонентом VM в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта
	Руководство по установке Часть 2. Установка ПК Ankey SIEM NG в исполнении Ankey SIEM NG VM	Содержит информацию для внедрения варианта исполнения Ankey SIEM NG VM в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта
Подключение инфраструктуры	Руководство по настройке аудита активов Ankey SIEM NG (AM+VM+HCC)	Содержит рекомендации по интеграции элементов ИТ-инфраструктуры организации с ПК Ankey SIEM NG для аудита активов
	Руководство по интеграции с источниками событий Ankey SIEM NG.	Содержит рекомендации по интеграции элементов ИТ-инфраструктуры организации с ПК Ankey SIEM NG для сбора событий с источников
	Руководство по интеграции с источниками событий Ankey SIEM NG. Приложение А	Содержит перечни регистрируемых событий, маппинг событий и результаты обработки для поддерживаемых источников пакета стандартных коннекторов ПК Ankey SIEM NG
	Руководство по интеграции с источниками событий Ankey SIEM NG. Список изменений	Содержит список изменений пакета стандартных коннекторов ПК Ankey SIEM NG
Настройка корреляции	Пакет общих ресурсов контента. Описание пакета экспертизы <Номер версии пакета>.	Содержит справочную информацию и инструкции по установке и настройке пакета общих ресурсов контента ПК Ankey SIEM NG
	Пакет общих ресурсов контента Приложение А <Номер версии пакета>.	Содержит списки применимых правил корреляции из состава пакета общих ресурсов контента ПК Ankey SIEM NG для поддерживаемых источников
	Пакет общих ресурсов контента Список изменений <Номер версии пакета>	Содержит список изменений пакета общих ресурсов контента ПК Ankey SIEM NG

Каталог	Наименование документа	Описание
	Пакет мониторинга SIEM Описание пакета экспертизы <Номер версии пакета>	Содержит списки применимых правил корреляции из состава пакета мониторинга SIEM для ПК Ankey SIEM NG
	Пакет мониторинга SIEM Список изменений <Номер версии пакета>	Содержит список изменений пакета мониторинга SIEM к ПК Ankey SIEM NG
Инструкции к разработке	Руководство разработчика Ankey SIEM NG	Содержит рекомендации по созданию правил нормализации, корреляции, агрегации и обогащения событий, описание утилит Ankey SIEM NG SDK для их отладки, а также информацию о доступных в ПК Ankey SIEM NG функциях сервиса REST API
	Синтаксис языка запроса PDQL	Содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с ПК Ankey SIEM NG
	PDQL-запросы для анализа активов	Содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в ПК Ankey SIEM NG
Дополнительно	Инструкция по обновлению Ankey SIEM NG с версии 4.x на версию 5.x	Содержит шаги, необходимые для обновления ПК Ankey SIEM NG с версии 4.1 до версии 5.2
	Инструкция по установке и настройке Ankey Update Mirror	Содержит информацию об установке и настройке локального сервера обновлений для получения обновлений экспертных данных компонента Ankey SIEM NG VM
	Инструкция по обновлению пакетов ресурсов с версии 3.x.x на версию 4.x.x	Содержит информацию, необходимую для обновления пакетов ресурсов ПК Ankey SIEM NG с версии 3.x.x на версию 4.x.x

В документе приняты условные обозначения.

Таблица 1.2 – Условные обозначения

Пример текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
❖ Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите кнопку ОК	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду <code>Stop-Service</code>	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
<code>Ctrl+Alt+Delete</code>	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

2 О ПК Ankey SIEM NG VM

Ankey SIEM Next Generation в варианте исполнения Ankey SIEM NG VM – это система управления событиями и информацией о безопасности, которая предназначена для сбора, хранения и анализа данных о событиях, которые генерируют различные источники в ИТ-инфраструктуре организаций. ПК Ankey SIEM NG VM позволяет обеспечивать мониторинг информационной безопасности как всей инфраструктуры, так и отдельных подразделений, узлов и приложений.

ПК Ankey SIEM NG VM предоставляет следующие основные возможности:

- **Инвентаризация активов.** Система регулярно собирает данные о сетевых узлах и связях между ними.
- **Визуализация данных.** Сводная информация об активах, событиях и инцидентах отображается в веб-интерфейсе системы в виде диаграмм и таблиц.
- **Сбор и анализ данных об уязвимостях на активах.** Система предоставляет информацию об ИТ-инфраструктуре, полученную путем активного и пассивного сбора данных;
- **Предоставление информации об уязвимостях на активах.** На основе постоянно обновляемой базы знаний Ankey SIEM NG VM предоставляет пользователю и другим системам актуальную информацию об уязвимостях, обнаруженных на активах. Ankey SIEM NG VM определяет способы устранения уязвимостей и позволяет настраивать политики контроля.
- **Оценка уязвимостей на активах.** Система выбирает среди уязвимостей те, которые необходимо устранять в первую очередь, и отображает степень защищенности активов.
- **Отправка уведомлений.** Оповещение ответственных об изменениях в ИТ-инфраструктурах организаций, о работе задач сбора данных Ankey SIEM NG VM, собираемых событиях, а также о выявляемых инцидентах ИБ.

При активации дополнительного модуля Host Compliance Control с помощью лицензии обеспечивается выполнение следующих функций:

- **Сбор информации о параметрах безопасности.** Дополнительный модуль Host Compliance Control (НСС) получает полную информацию о составе ИТ-инфраструктуры и собирает сведения о параметрах безопасности.
- **Оценка соответствия стандартам безопасности.** Дополнительный модуль Host Compliance Control (НСС) отслеживает соответствие ИТ-инфраструктуры готовым стандартам, отдельным требованиям и может приоритезировать обнаруженные риски;

2.1 Архитектура ПК Ankey SIEM NG VM

2.1.1 Компонент Ankey SIEM Next Generation Core

Компонент Ankey SIEM Next Generation Core (далее также – Ankey SIEM NG Core) является основным компонентом системы, ее управляющим сервером. Ankey SIEM NG Core устанавливается в центральном офисе компании или в крупных территориальных и функциональных подразделениях и выполняет следующие функции:

- централизованное хранение конфигурации активов;
- централизованное управление всеми компонентами системы;
- автоматизацию процесса управления уязвимостями;
- поддержку веб-интерфейса системы.

2.1.2 Компонент Ankey SIEM Next Generation Collector

Компонент Ankey SIEM Next Generation Collector (далее также — Ankey SIEM NG Collector) имеет модульную структуру и сканирует активы системы в режимах черного и белого ящика. Модули сканирования позволяют обнаруживать узлы и их открытые сетевые сервисы и проводить специализированные проверки в режиме теста на проникновение.

Ankey SIEM NG Collector в режиме активного и пассивного сканирования собирает следующую информацию об активах:

- название;
- версию и производителя операционной системы;
- установленные обновления ОС;
- список установленного ПО;
- параметры ОС и ПО;
- учетные записи пользователей и их привилегии;
- данные об аппаратном обеспечении, запущенных сетевых сервисах и службах ОС;
- параметрах сети и средств защиты.

Компонент Ankey SIEM NG Collector управляет перечисленными модулями и обеспечивает мониторинг их состояния, а также передачу данных между модулями и компонентом Ankey SIEM NG Core. Собранные данные используются компонентом Ankey SIEM NG Core для расчета уязвимости активов.

К одному компоненту Ankey SIEM NG Core можно подключать несколько компонентов Ankey SIEM NG Collector. Это позволяет увеличивать производительность, учитывать при сканировании топологию сети и типы каналов связи (например, наличие межсетевых экранов или других средств защиты).

2.1.3 Компонент Ankey SIEM Next Generation Management and Configuration

Компонент Ankey SIEM NG VM Management and Configuration (далее – Ankey SIEM NG Management and Configuration или Ankey SIEM NG MC) обеспечивает:

- сервис единого входа в продукты ПК Ankey SIEM NG VM, развернутые в инфраструктуре организации;

- управление пользователями системы, включая создание учетных записей, назначение прав, блокирование и активацию учетных записей;
- интеграцию с Microsoft Active Directory, включая аутентификацию пользователей и синхронизацию прав доступа;
- управление иерархией продуктов «Газинформсервис»;
- журналирование действий пользователей;

2.2 Схема взаимодействия компонентов

Взаимодействие компонентов ПК Ankey SIEM NG VM отражено на рисунке 2.1.

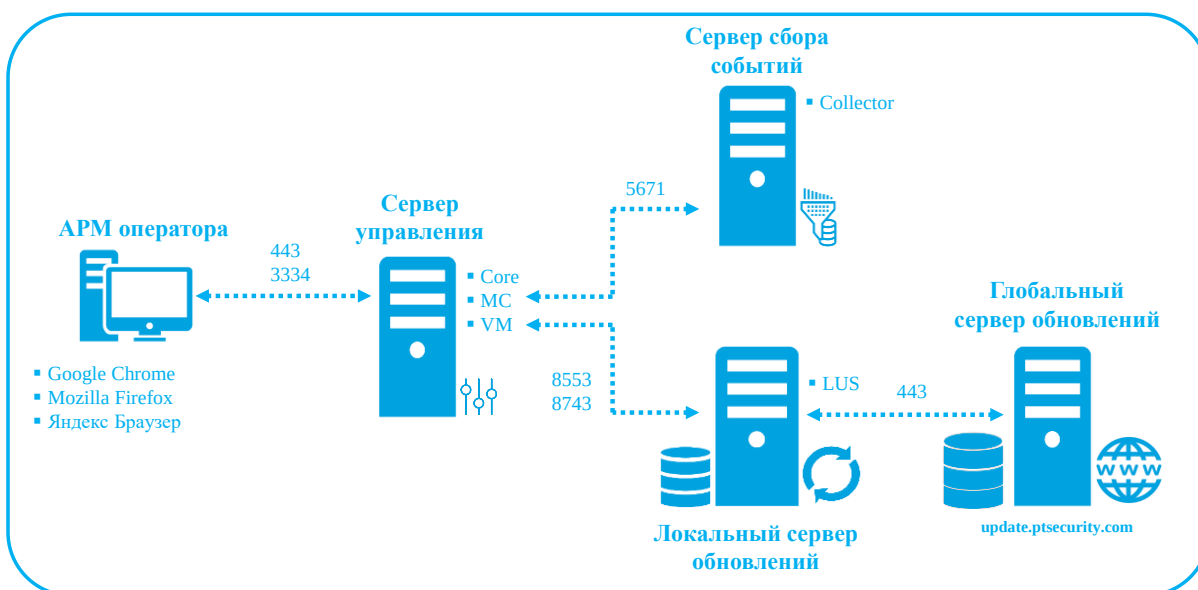


Рисунок 2.1 – Схема взаимодействия компонентов ПК Ankey SIEM NG VM

Алгоритм взаимодействия:

1. Модули компонента Ankey SIEM NG Collector сканируют ИТ-инфраструктуру предприятия, собирают сведения о сетевых узлах и события с источников. Собранные данные коллекторы передают в Ankey SIEM NG Core.
2. Компонент Ankey SIEM NG Core обрабатывает и хранит результаты сканирования с подробной информацией об обнаруженных ОС, ПО, службах, портах и прочими сведениями об узлах и связях между ними. Также компонент хранит параметры задач на сбор данных, профилей сканирования и транспортов, данные и сценарии справочников и осуществляет контроль доступа к этим данным, связываясь с остальными компонентами системы для выполнения пользовательских запросов.
3. Используя данные базы уязвимостей Ankey SIEM NG VM, компонент Ankey SIEM NG Core рассчитывает уязвимости на активах.

4. Компонент Ankey SIEM NG MC обеспечивает доступ к системе через сервис единого входа и журналирует действия пользователей.
5. Для управления системой, просмотра данных, построения отчетов и мониторинга пользователь подключается к компоненту Ankey SIEM NG Core через веб-интерфейс в соответствии с правами, которые назначены в Ankey SIEM NG MC.

Для обеспечения сетевого взаимодействия компонентов ПК Ankey SIEM NG VM должны быть доступны для входящих соединений порты, которые представлены в таблице 2.1 .

Таблица 2.1 – Компоненты и порты взаимодействия

Источник	Получатель	TCP-порт
Рабочая станция пользователя	Ankey SIEM NG Core	443
Ankey SIEM NG Collector	Ankey SIEM NG Core	5671
Рабочая станция пользователя	Ankey SIEM NG MC	3334

Внимание! На сервере, на который необходимо установить роль Deployer, порты 4505/TCP, 4506/TCP, 5000/TCP должны быть доступны для входящих соединений.

Для исходящих соединений не требуется создавать правила межсетевого экрана. Для удаленного доступа к серверам компонентов рекомендуется разрешить соединения от рабочих станций администратора через порт 3389/TCP к серверам на Microsoft Windows, через порт 22/TCP – к серверам на Linux.

3 Развертывание Ankey SIEM NG VM

Для развертывания Ankey SIEM NG VM вам потребуется один сервер. На него необходимо установить компоненты Ankey SIEM NG Core, Ankey SIEM NG MC и Ankey SIEM NG Collector.

Компоненты системы могут быть установлены в виртуальной среде (см. раздел 3.3).

В зависимости от физической или логической топологии ИТ-инфраструктуры организации может потребоваться сканировать узлы, расположенные в отдельных сетевых сегментах. В этом случае на каждый сегмент рекомендуется устанавливать отдельный коллектор. Количество серверов, требуемых для такой схемы развертывания, увеличивается на число дополнительных коллекторов.

Если вы планируете развертывать Ankey SIEM NG VM на базе уже развернутого ПК Ankey SIEM NG, вам не требуется устанавливать компоненты и выделять дополнительные аппаратные ресурсы. Для работы Ankey SIEM NG VM необходимо активировать лицензию (см. раздел 3.11), перезапустить службы компонента Ankey SIEM NG Core, а затем выйти из системы и заново войти в нее.

3.1 Требования к программному обеспечению

Все компоненты Ankey SIEM NG VM поддерживают установку на 64-разрядные ОС семейства Linux – Astra Linux Special Edition 1.7.5¹ (на базе ядра Linux версии 5.15) или Debian 10.3–10.13 (на базе ядра Linux версии 5.10). Кроме того, вы можете установить компонент Ankey SIEM NG Collector на Microsoft Windows Server 2012, 2012 R2, 2016, 2019 и 2022.

В случае развертывания мобильного Ankey SIEM NG VM необходимо также использовать операционные системы не ниже Debian 10.13 и Astra Linux 1.7.5.

Если ПК Ankey SIEM NG устанавливается на Debian, и в Debian 10.3–10.13 используется версия ядра ниже требуемой, перед установкой или обновлением Ankey SIEM NG необходимо обновить версию ядра ОС, установив метапакет `linux-image-5.10-amd64`. При обновлении версии ядра не требуется обновление ОС. Для установки или обновления Debian необходимо использовать полный установочный образ. Он содержит необходимый набор пакетов и не требует подключения к интернету (подробнее см. на сайте debian.org).

Если ПК Ankey SIEM NG устанавливается на Astra Linux, ознакомьтесь с рекомендациями по установке ОС в разделе 3.4.

При установке или обновлении операционной системы необходимо указать в качестве используемого формата размещения таблиц разделов на физическом жестком диске стандарт GPT.

¹ Рекомендации по настройке ОС Astra Linux приведены в разделе 3.4.

Примечание. При развертывании компонента Ankey SIEM NG Collector устанавливается драйвер WinPcap 4.1.3. Не рекомендуется дополнительно устанавливать другие версии драйвера WinPcap, поскольку работа другой версии драйвера может привести к некорректной работе модуля hostdiscovery.

Для работы в интерфейсе Ankey SIEM NG VM рекомендуется использовать последние версии браузеров Google Chrome, Mozilla Firefox, Microsoft Chromium Edge или Яндекс.Браузер.

3.2 Требования к аппаратному обеспечению

3.2.1 Требования к аппаратному обеспечению Ankey SIEM NG VM

Компоненты Ankey SIEM NG VM необходимо устанавливать на серверы, удовлетворяющие приведенным ниже аппаратным требованиям.

Примечание. При развертывании Ankey SIEM NG VM на базе существующего ПК Ankey SIEM NG дополнительные аппаратные ресурсы не требуются.

Таблица 3.1 – Аппаратные требования к серверу Ankey SIEM NG Core, Ankey SIEM NG MC и Ankey SIEM NG Collector

Компонент сервера	Минимальное требование
Центральный процессор	Тактовая частота 2,2 ГГц, суммарно 32 логических ядра. Поддержка инструкций SSE4.2 и AVX
Память (ОЗУ)	64 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски	4 диска ² емкостью 1200 ГБ и скоростью вращения 10 000 об./мин. каждый

Таблица 3.2 – Аппаратные требования к серверу компонента Ankey SIEM NG Collector, размещенному в отдельном сегменте сети

Компонент сервера	Минимальное требование
Центральный процессор	Тактовая частота 2,2 ГГц, суммарно 8 логических ядер
ОЗУ	32 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски	2 диска ³ емкостью 1200 ГБ и скоростью вращения 7200 об./мин. каждый

² Для Linux рекомендуется объединить диски в массив RAID 10 и преобразовать файловую систему в ext4 (размер блока 4096 байт). Дисковое пространство рекомендуется распределить между двумя разделами – объемом 200 ГБ для работы ОС (корневым каталогом /) и объемом 2200 ГБ для работы компонентов и баз данных (каталогом /var).

³ Рекомендуется объединить диски в массив RAID 1 и преобразовать файловую систему в NTFS (для Microsoft Windows) или ext4 (для Linux, размер блока 4096 байт).

3.2.2 Требования к аппаратному обеспечению мобильного Ankey SIEM NG VM

Ankey SIEM NG возможно установить в обычной комплектации с меньшими требованиями к аппаратным ресурсам и меньшей производительностью.

Компоненты мобильного ПК Ankey SIEM NG VM необходимо устанавливать на сервер, удовлетворяющий приведенным ниже аппаратным требованиям.

Таблица 3.3 – Аппаратные требования к серверу Ankey SIEM NG Core, Ankey SIEM NG MC и Ankey SIEM NG Collector

Компонент сервера	Минимальное требование
Центральный процессор	Тактовая частота 2,2 ГГц, суммарно 6 логических ядер. Рекомендуется использовать процессор с поддержкой технологии многопоточности.
Память (ОЗУ)	32 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Свободное дисковое пространство, SSD	500 ГБ

3.3 Рекомендации по развертыванию ПК Ankey SIEM NG VM в виртуальной среде

Внимание! Не используйте динамическую миграцию виртуальных машин для сервера Ankey SIEM NG Core, например VMware vSphere vMotion, так как после каждой миграции необходимо повторно активировать лицензию на Ankey SIEM NG VM.

Рекомендуется использовать версию 11 виртуальной машины VMware vSphere и версию 6.0 гипервизора VMware ESXi с приведенными ниже параметрами распределения ресурсов.

Настройка гипервизора

Рекомендуется использовать технологию Storage I/O Control при обмене данными между гипервизором и хранилищами, содержащими виртуальные машины, на которых будут развернуты компоненты системы.

Для закрепления за виртуальной машиной выделенных для нее аппаратных ресурсов (например, логических ядер) рекомендуется в параметрах виртуальной машины **VM Options** → **Advanced** в раскрывающемся списке **Latency Sensitivity** выбрать **High**. Для каждой такой виртуальной машины нужно дополнительно оставлять два свободных логических ядра.

Настройка центрального процессора

В аппаратных требованиях к центральному процессору указано минимальное количество логических ядер. Если сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить вдвое меньше физических ядер. Если технология Hyperthreading не используется,

количество выделенных физических ядер должно быть равно количеству логических. Например, если виртуальной машине требуется 56 логических ядер и сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить два процессора по 14 ядер каждый.

Для повышения производительности виртуальной машины рекомендуется в блоке параметров **Hyperthreaded Core Sharing** выбрать режим **None**, в блоке параметров **Resource Allocation** передвинуть максимально вправо ползунок **Reservation** и установить флажок **Unlimited**.

Настройка BIOS

Для исключения задержек при выходе ядер процессора из спящего режима рекомендуется выбрать в параметрах BIOS производительный режим работы системы (профиль Performance в серверах компании Dell или аналогичные профили в серверах других производителей).

Для повышения производительности ядер процессоров, поддерживающих технологию Intel Turbo Boost, рекомендуется включить в системных параметрах BIOS использование этой технологии.

Настройка оперативной памяти

Объем оперативной памяти, выделяемой каждой виртуальной машине, не должен быть меньше значения, указанного в аппаратных требованиях. Также необходимо учитывать, что часть оперативной памяти сервера (до 8% от общего объема) должна быть зарезервирована для работы гипервизора.

Для работы виртуальной машины рекомендуется зарезервировать постоянный объем оперативной памяти, установив в блоке параметров **Resources Allocation** флажок **Reserve all guest memory (All locked)**.

Настройка виртуальных жестких дисков

Объем и производительность виртуальных жестких дисков не должны быть меньше значений, указанных в аппаратных требованиях.

При создании виртуального жесткого диска на шаге **Create a Disk** в блоке параметров **Disk Provisioning** рекомендуется выбрать вариант **Thick Provision Eager Zeroed**, на шаге **Advanced Options** в блоке параметров **Mode** рекомендуется установить флажок **Independent**, а затем выбрать вариант **Persistent**.

3.4 Рекомендации к установке ПК Ankey SIEM NG VM на ОС Astra Linux SE

Установку и администрирование ОС Astra Linux SE версий необходимо осуществлять согласно официальной документации производителя⁴.

Перед разворачиванием ПК Ankey SIEM NG VM на Astra Linux Special Edition 1.7 необходимо на серверах компонентов выполнить действия, указанные в бюллетенях производителя (последний актуальный бюллетень [№ 2024-0212SE17MD](#), подробнее см. [в справочном центре Astra Linux](#)).

Рекомендации к установке базовой системы и выбору ядра

При установке ОС Astra Linux необходимо выбрать тип ядра **generic** версии 5.15. Тип ядра **hardened** не поддерживается ПК Ankey SIEM NG.

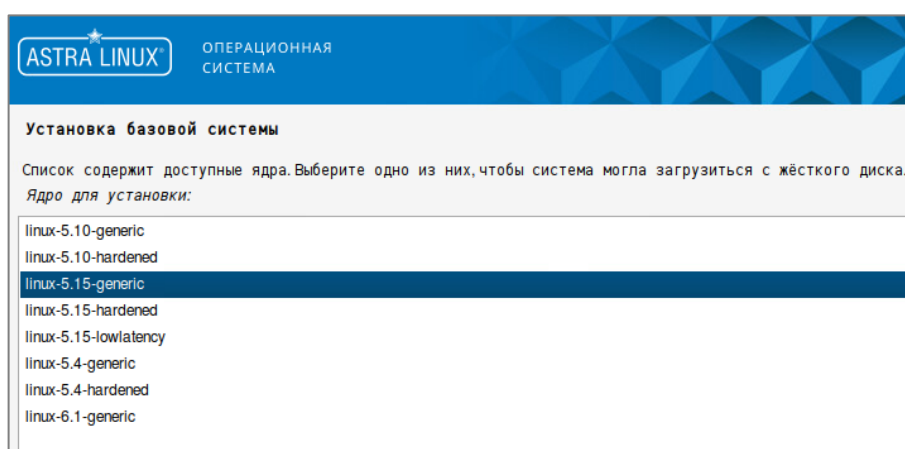


Рисунок 3.1 –Выбор типа ядра при установке ОС

Рекомендации к выбору дополнительных настроек ОС

Уровень защищенности ОС влияет на перечень дополнительных настроек, доступных для выбора. Рекомендуется использовать максимальный уровень защищенности «Смоленск» для более гибкой настройки ОС.

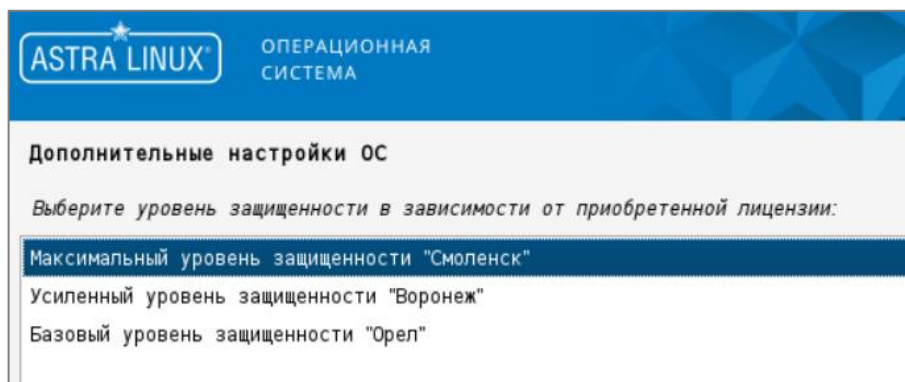


Рисунок 3.2 –Выбор уровня защищенности

⁴ Официальная документация для Astra Linux SE версий 1.7.x представлена в [справочном центре Astra Linux](#).

Вы можете настроить параметры безопасности ОС с учетом особенностей проекта или сохранить настройки, заданные по умолчанию для выбранного уровня безопасности.

Внимание! Параметр **Запрос пароля для команды sudo** должен быть отключен, как показано на рисунке 3.3.

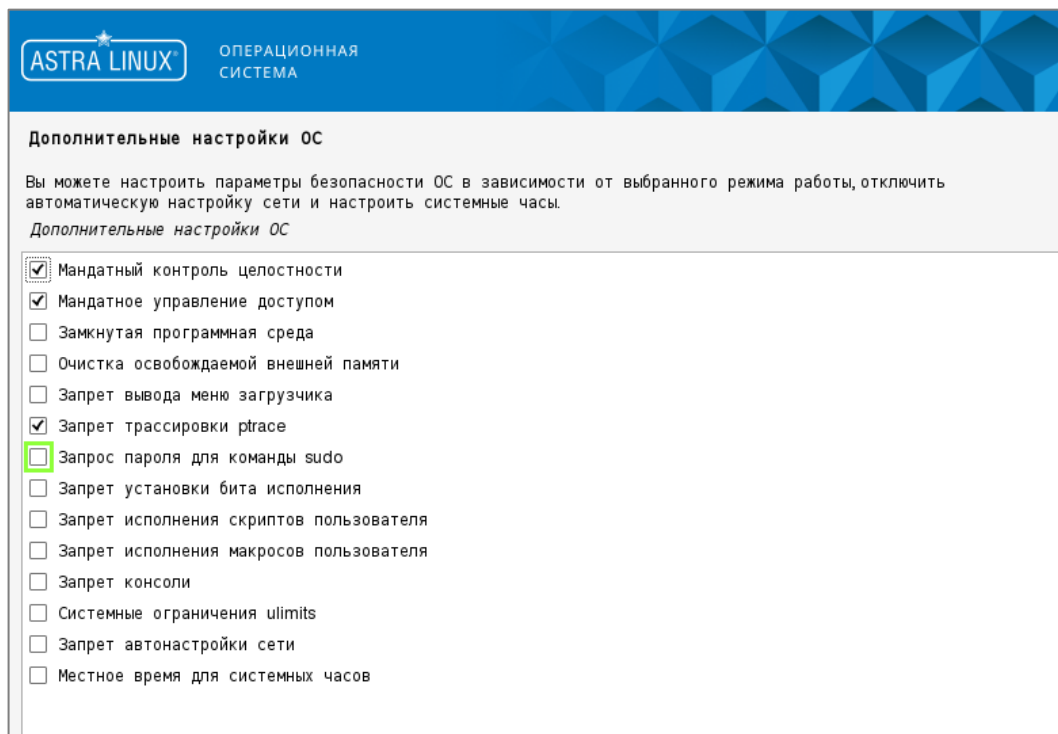


Рисунок 3.3 – Дополнительные настройки ОС Astra Linux

Если операционная система Astra Linux была установлена с активированным параметром **Запрос пароля для команды sudo**, то его можно отключить с помощью команды `sudo astra-sudo-control disable` в интерфейсе командной строки операционной системы.

После установки всех компонентов ПК, в случае необходимости, запрос пароля для команды `sudo` возможно включить в уже установленной операционной системе с помощью команды `sudo astra-sudo-control enable`, которую следует выполнить в интерфейсе командной строки с правами суперпользователя.

Если при установке ОС Astra Linux был включен параметр **Мандатный контроль целостности**, то для учетной записи, которая используется при установке компонентов системы, необходимо выбрать максимальный уровень целостности.

Рекомендации к установке ролей ПК Ankey SIEM NG VM на ОС Linux

Перед началом установки ролей ПК необходимо корректно настроить репозитории для ОС Linux. Полная информация о настройке репозитория в Astra Linux приведена [в справочном центре Astra Linux](#).

В случае наличия доступа к глобальной сети Интернет в файле `sources.list` следует проверить наличие или добавить адреса [Интернет-репозитория для ОС Astra Linux SE](#):

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-main/ 1.7_x86-64  
main contrib non-free
```

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-update/ 1.7_x86-64  
main contrib non-free
```

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-base/ 1.7_x86-64  
main contrib non-free
```

```
deb https://download.astralinux.ru/astra/stable/1.7_x86-64/repository-extended/ 1.7_x86-  
64 main contrib non-free
```

Все остальные ссылки следует закомментировать или удалить.

На время процесса установки ПК Ankey SIEM NG рекомендуется отключить обновление ОС Astra Linux SE из интернет-репозитория.

В случае отсутствия доступа к глобальной сети Интернет необходимо настроить локальный репозиторий ОС Astra Linux SE. Для этого необходимо создать каталог и распаковать в него архив с пакетами локального репозитория. Далее в файл `/etc/apt/sources.list` следует добавить ссылку на каталог, в котором содержатся пакеты локального репозитория. Например, `deb [trusted=yes] file:<Полный путь до каталога с локальным репозиторием> main non-free`.

Все остальные ссылки следует закомментировать или удалить.

3.5 Сценарий развертывания Ankey SIEM NG VM

Компоненты Ankey SIEM NG Core и Ankey SIEM NG MC устанавливаются на Linux. При такой установке базовыми единицами развертывания являются роли (см. раздел 3.5).

При развертывании необходимо придерживаться следующего порядка действий:

1. Установка роли Deployer.
2. Установка компонента Ankey SIEM NG MC.
3. Установка компонента Ankey SIEM NG Core.
4. Установка компонента Ankey SIEM NG Collector.
5. Активация лицензии.
6. Настройка Ankey SIEM NG VM для обеспечения его безопасной работы.

Если на сервере компонента установлен Kaspersky Endpoint Security, необходимо приостановить его работу на время развертывания Ankey SIEM NG VM. Во время развертывания операционная система сервера может быть перезагружена. После перезагрузки необходимо повторно приостановить работу Kaspersky Endpoint Security.

3.6 Об установке компонентов на Linux с помощью ролей

Роль является базовой единицей развертывания на Linux и представляет собой совокупность служб, утилит и сценариев, обеспечивающих работу определенного набора функций системы. Каждая роль поставляется в виде отдельного архива, который может содержать Docker-образы или deb-пакеты.

При развертывании системы создаются экземпляры ролей, которые распределяются по приложениям определенного типа (Management and Configuration или Ankey SIEM NG VM). Такая архитектура позволяет гибко и удобно развертывать систему, а также обновлять и настраивать ее в дальнейшем. Тип приложения определяется составом входящих в него экземпляров ролей:

- приложение Management and Configuration содержит только роли SqlStorage/JatobaStorage и Management and Configuration;
- приложение Ankey SIEM NG VM – только роли Core, RMQ Message Bus и Collector.

Примечание. При развертывании системы можно создать несколько приложений одного типа (например, несколько приложений Management and Configuration), однако такие конфигурации не поддерживаются производителем.

Управление развертыванием обеспечивается ролью Deployer, которая построена на базе системы управления конфигурациями SaltStack. Ее модуль Salt Master обеспечивает общее управление установкой (созданием экземпляров) ролей, модули Salt Minion – установку ролей на каждый сервер системы.

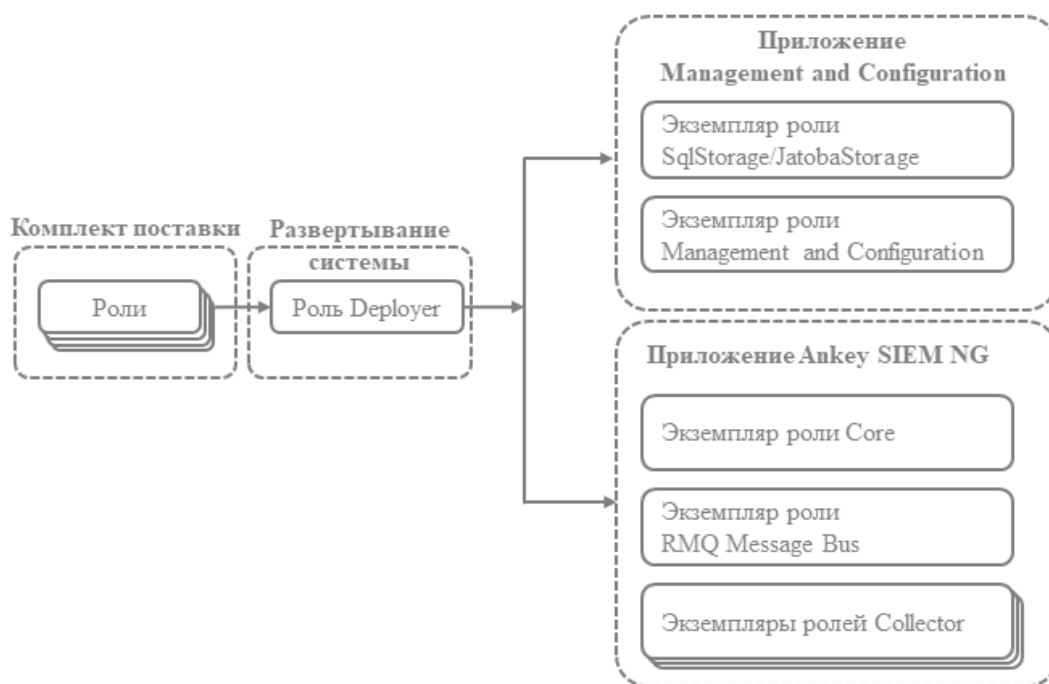


Рисунок 3.4 – Развертывание системы с помощью ролей

Для установки компонента может потребоваться установка как одной, так и нескольких ролей. В общем случае установка роли делится на следующие этапы:

1. Распаковка архива и запуск сценария установки.
2. Выбор приложения для установки роли. Вам потребуется или выбрать ранее созданное приложение необходимого типа, или создать новое, если приложение необходимого типа отсутствует. При создании приложения нужно ввести его идентификатор, который среди прочего будет использоваться в качестве имени каталога для размещения файлов всех экземпляров ролей, входящих в состав данного приложения.

Примечание. Вы можете использовать идентификаторы, предлагаемые системой по умолчанию. Например, если для приложения Management and Configuration использовать предлагаемый по умолчанию идентификатор mc-application, файлы всех экземпляров ролей этого приложения будут размещены в каталоге /var/lib/deployed-roles/mc-application.

3. Ввод названия экземпляра роли и выбор сервера для ее установки. Введенное название среди прочего будет использоваться в качестве имени каталога для размещения файлов создаваемого экземпляра роли (например, файлов журналов и файлов конфигурации).

Примечание. Вы можете использовать названия, предлагаемые системой по умолчанию. Например, если для роли Collector использовать предлагаемое по умолчанию название agent, файлы этого экземпляра ролей будут размещены в каталоге /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли %Компонент%>. Например: /var/lib/deployed-roles/mc-application/agent.

4. Проверка и изменение параметров конфигурации.
5. Запуск установки.

3.7 Установка роли Deployer

Для установки роли вам потребуется архив `deployer_<Номер версии>.tar.gz` из комплекта поставки.

Роль устанавливается на сервер с любым из компонентов Ankey SIEM NG VM, либо на отдельный сервер..

Внимание! Для любой конфигурации Ankey SIEM NG VM необходимо установить только один экземпляр роли Deployer. Установка второго экземпляра роли Deployer на сервер любого компонента сделает работу Ankey SIEM NG VM невозможной и потребует переустановки всей системы.

Внимание! Для корректной работы Ankey SIEM NG VM необходимо, чтобы подсеть его Docker-контейнеров не совпадала с подсетями, используемыми в вашей организации. По умолчанию система виртуализации Docker использует подсеть 172.17.0.0/12. Если эта подсеть уже используется вашим оборудованием, вы можете изменить подсеть во время развертывания Ankey SIEM NG VM при установке роли Deployer. Для этого в наборе конфигурационных параметров **Advanced configuration** необходимо указать в качестве значения параметра **CustomDockerAddressPool** подсеть, отличную от используемых в вашей организации, а в качестве значения параметра **CustomDockerNetworkSize** – размер этой подсети. Вы также можете изменить подсеть Docker-контейнера уже установленного Ankey SIEM NG VM по инструкции из раздела «Подсеть Docker-контейнера Ankey SIEM NG VM совпадает с одной из подсетей предприятия» Руководства администратора Ankey SIEM NG.

Внимание! На сервере, на который необходимо установить роль Deployer, порты 4505/TCP, 4506/TCP, 5000/TCP должны быть доступны для входящих соединений.

Для установки роли вам потребуется архив `deployer_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. Если роль устанавливается на сервере с Astra Linux, отключите на этом сервере обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
2. Если на сервере, на который устанавливается роль Deployer, есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
3. Распакуйте архив `deployer_<Номер версии>.tar.gz`:
`tar -xf deployer_<Номер версии>.tar.gz`
4. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
5. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов. По завершении подготовки откроется окно с текстом лицензионного соглашения.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
8. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера, на который устанавливается роль Deployer.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

9. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **ОК**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.
Роль установлена.

3.8 Установка компонента Ankey SIEM NG MC

Компонент Ankey SIEM NG Management and Configuration необходимо установить на одну операционную систему с компонентом Ankey SIEM NG Core.

Установка компонента Ankey SIEM NG Management and Configuration делится на следующие этапы:

1. Установка роли `SqlStorage/JatobaStorage`.
2. Установка роли `Management and Configuration`.

Перед установкой компонента Ankey SIEM NG MC необходимо принять решение, какая именно роль будет установлена `SqlStorage` (СУБД PostgreSQL) или `JatobaStorage` (СУБД Jatoba).

Для установки роли `JatobaStorage` потребуется:

- доступ к глобальной сети Интернет (для получения лицензии в режиме онлайн или офлайн);
- действующий ключ активации для СУБД Jatoba.

3.8.1 Установка роли `SqlStorage`

Для установки роли вам потребуется архив `sqlstorage_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `sqlstorage_<Номер версии>.tar.gz`:
`tar -xf sqlstorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения `Management and Configuration` и нажмите кнопку **ОК**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).
--

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

8. В открывшемся окне выберите вариант с доменным именем или IPv4-адресом сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли SqlStorage и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
11. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.

Внимание! Если в параметре HostAddress указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
13. Нажмите кнопку **OK**.

Роль установлена.

3.8.2 Установка роли JatobaStorage и онлайн активация лицензии

Для установки роли вам потребуется архив jatobastorage_<Номер версии>.tar.gz из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив jatobastorage_<Номер версии>.tar.gz:
`tar -xf jatobastorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли ./install.sh.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Management and Configuration и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем или IPv4-адресом сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли JatobaStorage и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.

10. Для выполнения онлайн активации СУБД Jatoba следует выбрать вариант **Basic configuration**.
Откроется список основных параметров для настройки установки СУБД.
11. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) сервера Ankey SIEM NG Core или его IPv4-адрес.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. В поле **JatobaLicenseActivationType** выберите значение `online`.
13. В поле **LicenceKey** удалите значение по умолчанию `XXXXXX-XXXXXX-XXXXXX-XXXX` и вручную введите ключ для активации СУБД Jatoba.
14. Если устанавливается роль `JatobaStorage` с лицензией, для которой необходимо подтверждение по электронной почте, в качестве значения параметра **LicenseEmail** укажите адрес электронной почты, указанный при получении лицензии.
15. В поле **LicenseServerUri** по умолчанию должно содержаться значение `https://licence.gaz-is.ru`.
16. Значения в других полях следует оставить по умолчанию.
17. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
18. Выберите **ОК** и нажмите на клавиатуре клавишу **Enter**.
Роль установлена.

Внимание! Перед установкой других ролей ПК Ankey SIEM NG VM необходимо проверить работоспособность docker-контейнера с СУБД Jatoba. После установки роли `JatobaStorage` выполнить команду `docker ps -a`.
В результате вывода команды должны содержаться данные обо всех установленных docker-контейнерах и их состоянии. Название docker-контейнера с СУБД Jatoba будет зависеть от названия роли (например: `storage-jatoba`). В колонке `STATUS` должно быть значение `UP` «количество времени», в течение которого docker-контейнер с СУБД Jatoba активен. Docker-контейнер с СУБД Jatoba должен быть активен не менее, чем 3 минуты и не перезапускаться с интервалом до 30 секунд.
Чтобы проверить статус активации лицензии СУБД Jatoba в логах, следует выполнить команду `docker ps -a` и определить `CONTAINER ID` для docker-контейнера.
Для вывода логов docker-контейнера с СУБД Jatoba следует выполнить команду `docker logs <идентификатор docker-контейнера, например 20d228ccd15f>`. В логах docker-контейнера СУБД Jatoba не должно содержаться сообщений типа: `[license info]: license file name: /license/jatoba.cer (not found)`

3.8.3 Установка роли JatobaStorage и офлайн активация лицензии

Для установки роли вам потребуется архив `jatobastorage_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `jatobastorage_<Номер версии>.tar.gz`:
`tar -xvf jatobastorage_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения **Management and Configuration** и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем или IPv4-адресом сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли **JatobaStorage** и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Для выполнения онлайн активации СУБД Jatoba следует выбрать вариант **Basic configuration**.
Откроется список основных параметров для настройки установки СУБД.
11. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) сервера Ankey SIEM NG Core или его IPv4-адрес.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. В поле **JatobaLicenseActivationType** выберите значение `offline`.
13. В поле **LicenceKey** удалите значение по умолчанию `XXXXX-XXXXX-XXXXX-XXX` и вручную введите ключ для активации СУБД Jatoba.
14. Если устанавливается роль **JatobaStorage** с лицензией, для которой необходимо подтверждение по электронной почте, в качестве значения параметра **LicenseEmail** укажите адрес электронной почты, указанный при получении лицензии.
15. В поле **LicenseServerUri** по умолчанию должно содержаться значение `https://licence.gaz-is.ru`.
16. Значения в других полях следует оставить по умолчанию.

17. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
18. Выберите **ОК** и нажмите на клавиатуре клавишу **Enter**.
Роль установлена.

❖ Для офлайн активации лицензии:

1. После установки роли `JatobaStorage` перейдите в каталог `/var/lib/deployed-roles/<Название приложения Ankey SIEM NG MC, например: mc-application-ankey>/<Название роли СУБД Jatoba, например: jatobastorage>/config/license/` и проверьте наличие файла `request.dat`.
2. Перенесите файл `request.dat` на хост с доступом к глобальной сети Интернет.
3. В веб-браузере хоста с доступом к глобальной сети интернет необходимо перейти на сайт <https://license.gaz-is.ru/offlineActivate/>. В веб-браузере должна отобразиться страница **Офлайн-активация**.
4. Для формирования запроса на офлайн активацию лицензии СУБД `Jatoba` скопируйте в окно ввода активационный запрос для получения файла лицензии или скопируйте и вставьте запрос из файла `request.dat`.
В ответ на запрос из файла `request.dat` будет предоставлен файл лицензии `license.bin`.
5. Сохраните на хосте файл `license.bin` и переименуйте с соблюдением регистра в `jatoba.cer`.
6. Скопируйте файл `jatoba.cer` в каталог `/var/lib/deployedroles/<название приложения Management and Configuration, например: mc-applicationankey>/<название роли СУБД Jatoba, например: jatobastorage>/config/license/`.

Внимание! Для того, чтобы скопировать файл `jatoba.cer` в каталог `license`, может потребоваться временно изменить уровень прав доступа с **755** на **777**.

7. Для изменения уровня доступа к каталогу `license` выполните команду `chmod 777 /var/lib/deployed-roles/mc-application/jatobastorage-<уникальный идентификатор>/config/license` с правами суперпользователя.
8. После успешного копирования файла `jatoba.cer` в каталог `license` восстановите уровень доступа по умолчанию, выполнив команду `chmod 755 /var/lib/deployed-roles/mc-application/jatobastorage-<уникальный идентификатор>/config/license` с правами суперпользователя.

Внимание! Если не восстановить уровень доступа каталога `license` по умолчанию, то `docker`-контейнер с СУБД `Jatoba` будет постоянно перезапускаться и работоспособность `Ankey SIEM NG VM` будет нарушена.

9. Лицензия для СУБД `Jatoba` активирована.

Примечание. Подробнее о получении лицензии с активацией офлайн вы можете прочитать в Руководстве по установке СУБД `Jatoba` [на сайте производителя](#).

Внимание! Перед установкой других ролей ПК `Ankey SIEM NG VM` необходимо проверить работоспособность `docker`-контейнера с СУБД `Jatoba`. После установки роли `JatobaStorage` выполнить команду `docker ps -a`.

В результате вывода команды должны содержаться данные обо всех установленных `docker`-контейнерах и их состоянии. Название `docker`-контейнера с СУБД `Jatoba` будет зависеть от названия роли (например: `storage-jatoba`). В колонке `STATUS` должно быть значение `UP` «количество времени», в течение которого `docker`-контейнер с СУБД `Jatoba` активен. `Docker`-контейнер с СУБД `Jatoba` должен быть активен не менее чем 3 минуты и не перезапускаться с интервалом до 30 секунд.

Чтобы проверить статус активации лицензии СУБД `Jatoba` в логах следует выполнить команду `docker ps -a` и определить `CONTAINER ID` для `docker`-контейнера.

Для вывода логов `docker`-контейнера с СУБД `Jatoba` следует выполнить команду `docker logs <идентификатор docker-контейнера, например 20d228ccd15f>`. В логах `docker`-контейнера СУБД `Jatoba` не должно содержаться сообщений типа `[license info]: license file name: /license/request.dat (not found)`

3.8.4 Установка роли **Management and Configuration**

Внимание! Если вы устанавливаете `Ankey SIEM NG VM` в изолированном сегменте сети без прямого подключения к интернету, необходимо предварительно установить и настроить локальный сервер обновлений в соответствии с инструкциями в разделе «Настройка обновления экспертных данных» (см. раздел 3.22)

Для установки роли вам потребуется архив `managementandconfiguration_<Номер версии>.tar.gz` из комплекта поставки и токен аутентификации, который хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта `Base64`. Этот набор символов необходимо будет указать в качестве значения конфигурационного параметра `PackagesSourceCredentialToken` на одном из шагов инструкции.

Примечание. Новые пользователи `Ankey SIEM NG VM` получают файл `instance-access-token.key` вместе с лицензией на продукт, а существующие пользователи, обновляющиеся с версии 5.0 или ниже – вместе с дистрибутивом или через службу технической поддержки.

❖ Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `managementandconfiguration_<Номер версии>.tar.gz`:
`tar -xf managementandconfiguration_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения **Management and Configuration**.
5. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
8. В открывшемся окне введите название экземпляра роли **Management and Configuration** и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
10. В качестве значения параметра `DefaultLocale` выберите язык веб-интерфейса приложения **Management and Configuration**.
11. Убедитесь, что в качестве значения параметров `HostAddress` и `PostgreHost` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.

Внимание! Если в параметрах указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. в качестве значения параметра `ExpertDataUpdateMethod` выберите:
 - если обновление экспертных данных будет осуществляться напрямую с сервера обновлений «Газинформсервис» или с помощью локального сервера обновлений – **Online.**;
 - если вручную – **Offline.**
13. В качестве значения параметра `PackagesSourceUri` укажите:
 - если вы устанавливаете Ankey SIEM NG VM в сегменте сети с прямым подключением к интернету – адрес глобального сервера обновлений `https://update.ptsecurity.com/packman/v1/`;

- если в изолированном сегменте сети без прямого подключения к интернету – адрес локального сервера обновлений в формате `http://<Адрес сервера>:<Порт>/packman/v1/`.

Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.

В качестве значения параметра `PackagesSourceCredentialToken` укажите содержимое файла `instance-access-token.key`.

14. Нажмите кнопку **ОК**.
15. Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
16. Нажмите кнопку **ОК**.
17. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.9 Установка компонента Ankey SIEM NG Core на Linux

Компонент Ankey SIEM NG Core устанавливается с помощью ролей RMQ Message Bus и Core в следующем порядке: сначала устанавливается роль RMQ Message Bus, затем роль Core.

Внимание! Для установки компонента Ankey SIEM NG Core необходимо, чтобы TCP-порт 80 был свободен. Если этот порт занят каким-либо веб-сервером, выключите этот веб-сервер, удалите его или перенесите на другой порт.

3.9.1 Установка роли RMQ Message Bus на сервер Ankey SIEM NG Core

Для установки роли вам потребуется архив `rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `rmqmessagebus_<Номер версии>.tar.gz`:
`tar -xvf rmqmessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**. Начнутся распаковка и подготовка пакетов, необходимых для установки.

- По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант **Create New Application**.
 5. В открывшемся окне введите идентификатор приложения Ankey SIEM NG VM и нажмите кнопку **OK**.
 6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
 7. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
9. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
11. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Core.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **OK**.
14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.9.2 Установка роли Core

Для установки роли вам потребуется архив `core_<Номер версии>.tar.gz` из комплекта поставки.

Чтобы установить роль:

1. На сервере Ankey SIEM NG Core распакуйте архив `core_<Номер версии>.tar.gz`:
`tar -xf core_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки.

- По завершении подготовки откроется окно для выбора приложения **Application selection**.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG VM.
 5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
 6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.

Внимание! Можно создать только один экземпляр (Instance).

7. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Core.
8. В открывшемся окне введите название экземпляра роли Core и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
10. В качестве значения параметра **DefaultLocale** выберите желаемый язык интерфейса приложения Ankey SIEM NG VM.

Внимание! Укажите корректные значения основных параметров:
 HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
 MCAAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334
 KBAddress: https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091
 PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
 RMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>

Внимание! Если в параметрах указать значение localhost, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

11. Если требуется настройка отправки уведомлений из компонента Ankey SIEM NG Core по электронной почте, то выберите вариант **Advanced configuration**.
Откроется страница со списком основных и дополнительных параметров для настройки роли Core.
12. В качестве значения параметра **DefaultLocale** выберите желаемый язык веб-интерфейса приложения Ankey SIEM NG VM.
13. Укажите значения дополнительных параметров для настройки отправки уведомлений из компонента Ankey SIEM NG Core по электронной почте на почтовый сервер:
 - EmailNotificationRetryPeriodSeconds: <указать значение в секундах, по умолчанию 60>;
 - Smtphost: <IP-адрес или FQDN SMTP-сервера, по умолчанию localhost>;

- Smtppassword: <Пароль служебной учетной записи для подключения Ankey SIEM NG VM CORE к SMTP-серверу>;
- Smtpport: <Порт SMTP-сервера для входящих подключений от Ankey SIEM NG VM CORE, по умолчанию 25>;
- Smtpsender: <Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте от компонента Ankey SIEM NG Core, по умолчанию Notification System<NoReply@SiemNotifications.com>>;
- Smtpsseenabled: <Для подключения к SMTP-серверу службы Ankey SIEM NG VM CORE используют защищенное (True) или незащищенное (False) соединение, по умолчанию False>;
- Smtppuser: <Логин служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу. Служебная учетная запись для Core должна быть создана и настроена на почтовом сервере заранее, до установки роли Core >;
- Smtppusedefaultcredentials: <Режим аутентификации SMTP-сервера:
True - для аутентификации используются логин и пароль служебной учетной записи Network Service (необходимо очистить значения параметров Smtppuser и Smtppassword);
False - для аутентификации используются логин и пароль, указанные в параметрах Smtppuser и Smtppassword, по умолчанию True>.

14. Нажмите кнопку **ОК**.

Начнется установка пакетов. По завершении установки появится сообщение **Deployment configuration successfully applied**.

15. Если требуется включение генерации внутренних событий Ankey SIEM NG VM в активном канале веб-интерфейса, то выберите вариант **Advanced configuration** аналогично п.11 и затем включите параметр **SendAlertsToSiem**.

16. Нажмите кнопку **ОК**.

17. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.10 Установка компонента Ankey SIEM NG Collector

В этом подразделе приведены инструкции по установке компонента Ankey SIEM NG Collector на Linux и Microsoft Windows. Установка компонента на Linux выполняется с помощью роли Collector.

Внимание! Если Ankey SIEM NG Collector установлен на Linux, Ankey SIEM NG VM не сможет собирать события с профилем CheckpointOpsecLog, собирать данные по протоколам SMB, DCE и RPC в режиме пентеста, а также использовать протокол Kerberos. Производительность работы Ankey SIEM NG Collector, установленного на Linux, в режиме пентеста на 15–40% ниже, чем на Microsoft Windows.

Если Ankey SIEM NG Collector устанавливается на Linux и на этом сервере уже установлен Kaspersky Endpoint Security, необходимо обновить антивирусные базы Kaspersky Endpoint Security и включить компонент Kaspersky Security Network (KSN).

Если в процессе установки ОС Astra Linux 1.7.x было установлено ПО **Средства работы в сети**, то перед установкой Ankey SIEM NG Collector необходимо установить пакет `libsasl2-modules-gssapi-mit` с помощью команды `apt install libsasl2-modules-gssapi-mit`. Если не установить пакет `libsasl2-modules-gssapi-mit`, то установка Ankey SIEM NG Collector не будет успешно выполнена.

3.10.1 Установка модуля Salt Minion на сервер Ankey SIEM NG Collector

Если Ankey SIEM NG Collector устанавливается на отдельный сервер, перед установкой роли необходимо установить на этот сервер модуль Salt Minion.

Внимание! Если на сервере, на котором разворачивается компонент, уже установлена роль Deployer, установка модуля Salt Minion не требуется.

- ❖ Чтобы установить модуль Salt Minion:
 1. Если на сервере Ankey SIEM NG Collector есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
`rm /etc/salt/pki/minion/minion_master.pub`
 2. Если Ankey SIEM NG Collector устанавливается на Astra Linux, на сервере Ankey SIEM NG Collector отключите обязательный ввод пароля для выполнения команды `sudo`:
`sudo astra-sudo-control disable`
 3. Если Ankey SIEM NG Collector устанавливается на Debian, на сервере компонента установите утилиту `sudo`, выполнив в интерфейсе терминала команду от имени суперпользователя (`root`):
`apt-get install sudo`

4. Если Ankey SIEM NG Collector устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `etc/sudoers` строку:
<Логин учетной записи, от имени которой устанавливается компонент>
`ALL=(ALL:ALL) NOPASSWD: ALL`
5. На сервере с установленной ролью `Deployer` запустите сценарий:
`/var/lib/deployer/role_packages/deployer_<Номер версии>/deploy_minion.sh`
6. В открывшемся окне введите полное доменное имя (FQDN) или IPv4-адрес сервера Ankey SIEM NG Collector и нажмите кнопку **ОК**.

Внимание! Если в окне указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

7. В открывшемся окне введите логин учетной записи, от имени которой устанавливается компонент, на сервере Ankey SIEM NG Collector и нажмите кнопку **ОК**.
8. В открывшемся окне **Info** нажмите кнопку **ОК**.
9. Введите пароль учетной записи с правами суперпользователя на сервере Ankey SIEM NG Collector.
10. Если требуется, в открывшемся окне введите FQDN или IPv4-адрес сервера и нажмите кнопку **ОК**.
По завершении установки появится сообщение `Minion on '<FQDN или IPv4-адрес сервера>' successfully installed.`

Модуль Salt Minion установлен.

3.10.2 Установка роли Collector

Для установки роли вам потребуется архив `agent-linux_<Номер версии>` из комплекта поставки.

❖ Чтобы установить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `agent-linux_<Номер версии>`:
`tar -xf agent-linux_<Номер версии>`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для установки.
По завершении подготовки откроется окно для выбора приложения.
4. Выполните одно из следующих действий:
 - если в открывшемся окне для выбора доступен вариант с идентификатором установленного ранее приложения Ankey SIEM NG VM – выберите этот вариант;
 - если вариант с идентификатором установленного ранее приложения Ankey SIEM NG VM отсутствует – выберите вариант **Create New Application**.

5. Если вы выбрали вариант **Create New Application**, в открывшемся окне введите идентификатор приложения Ankey SIEM NG VM и нажмите кнопку **OK**.
6. В открывшемся окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера Ankey SIEM NG Collector.
9. В открывшемся окне введите название экземпляра роли Collector и нажмите кнопку **OK**.
Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров.
11. В качестве значения параметра `AgentName` введите название коллектора, которое будет отображаться в веб-интерфейсе приложения **Ankey SIEM NG VM**.
12. Убедитесь, что в качестве значения параметра `AgentRMQHost` указано полное доменное имя (FQDN) или IPv4-адрес Ankey SIEM NG Core.

Внимание! Если в параметре `AgentRMQHost` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать FQDN или IPv4-адрес сервера.

13. В качестве значения параметра `AgentRMQVirtualHost` выберите **Core**.
14. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
15. Нажмите кнопку **OK**.
16. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

Примечание. Для корректной работы Ankey SIEM NG Collector в ОС Linux требуется отдельно скачать и установить ODBC-драйвер (версия для 64-разрядной архитектуры) для требуемых источников, которые будут подключаться к ПК Ankey SIEM NG VM. Драйвер вы можете скачать с официальных сайтов производителей источников.

3.10.3 Дополнительная настройка компонента Ankey SIEM NG Collector для мобильного Ankey SIEM NG VM

Сканирование в режиме **Аудит** по умолчанию выполняется в четыре потока. Если вы используете мобильный Ankey SIEM NG VM, для сокращения времени сканирования рекомендуется увеличение количества потоков.

Примечание. Количество потоков для мобильного Ankey SIEM NG VM приведены исходя из тестирований на ноутбуке, соответствующем минимальным требованиям. Значение можно увеличить на усмотрение заказчика с учетом ограничений сети.

- ❖ Чтобы изменить количество потоков сканирования:
 1. На сервере, где установлен Ankey SIEM NG Collector, откройте папку `/opt/core-agent/modules/`.
 2. Откройте файл `scanner-audit.json`.
 3. В параметре **capacity** измените значение с 4 на 15.
 4. Сохраните изменения и закройте файл.
 5. Перезапустите службу командой `service core-agent restart` для применения изменений.

Количество потоков сканирования изменено.

3.10.4 Установка компонента Ankey SIEM NG Collector на Microsoft Windows

Для установки компонента Ankey SIEM NG Collector на Microsoft Windows вам потребуется архив `agent-windows_<Номер версии>.tar.gz` из комплекта поставки.

- ❖ Чтобы установить компонент Ankey SIEM NG Collector:
 1. Запустите файл `AnkeyAgentSetup_<Номер версии>.exe`. Откроется окно мастера установки.
 2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
 3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Продолжить**.
 4. Укажите пути для установки.

Примечание. Если вы хотите установить компоненты в папки по умолчанию, не изменяйте значения полей.

5. Нажмите кнопку **Продолжить**.
6. В поле **Имя коллектора** введите имя коллектора, которое будет отображаться в интерфейсе Ankey SIEM NG VM.
7. В блоке параметров **Адрес обработчика данных** в раскрывающемся списке выберите значение **Core** и укажите в поле IP-адрес или полное доменное имя (FQDN) сервера Ankey SIEM NG Core.

Внимание! Если в поле указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.

8. Нажмите кнопку **Продолжить**.
9. Мастер установки выполнит проверку указанных вами параметров и отобразит их после проверки.

Примечание. По результатам проверки мастер может отображать сообщения о некорректных значениях указанных параметров. В этом случае вам необходимо вернуться, нажимая кнопку **Назад**, и указать корректные значения параметров.

10. Нажмите кнопку **Установить**.
11. По завершении установки нажмите кнопку **Заккрыть**.
12. Если устанавливается первый компонент Ankey SIEM NG Collector на Windows и компонент Ankey SIEM NG Core установлен на Linux, на сервере с установленной ролью Deployer выполните команды:

```
cp /opt/deployer/pki/legacy_ca/windows-selfsigned-default.pem  
/opt/deployer/pki/trusted_ca/  
dpkg-reconfigure deployer  
/opt/deployer/bin/Restart-Configuration.ps1 -RoleTypeId RmqMessageBus
```
13. Если устанавливается первый компонент Ankey SIEM NG Collector на Windows и компонент Ankey SIEM NG Core установлен на Linux, перезапустите службу Core Collector.
14. Для подключения модуля Salt Minion к модулю Salt Master выполните команду:

```
saltcfg set -p SaltMasterHost <IP-адрес или FQDN сервера с модулем Salt  
Master>
```

Компонент Ankey SIEM NG Collector установлен.

3.11 Активация лицензии ПК Ankey SIEM NG VM

Для активации лицензии вам потребуются следующие файлы из комплекта поставки:

- шаблон ключа <Номер лицензии>.grdvd;
- текстовый файл с серийным номером Ankey SIEM NG VM <Идентификатор ключа>.txt;
- мастер активации лицензий GuardantActivationWizard.exe (только для офлайн-активации на серверах под управлением Microsoft Windows).

Активация лицензии выполняется на сервере компонента Ankey SIEM NG Core.

Если активировать несколько лицензий, система будет использовать только одну из них – имеющую самую раннюю дату окончания. В случае приобретения продукта, который может быть развернут на базе уже установленного Ankey SIEM NG (например, приобретения лицензии на дополнительный компонент Ankey SIEM NG VM) необходимо активировать объединенную лицензию на оба продукта (ее можно запросить в службе технической поддержки «Газинформсервис»). В противном случае после активации отдельной лицензии на второй продукт в системе будет доступен набор функций только одного продукта.

После изменения аппаратной конфигурации сервера Ankey SIEM NG Core (например, по причине замены центрального процессора) необходимо повторно активировать лицензию. Количество таких повторных активаций ограничено – не более пяти раз. Дальнейшие попытки активации приведут к ошибке мастера активации «Количество активаций для введенного серийного номера исчерпано». Для получения нового шаблона ключа и нового серийного номера необходимо обратиться в службу технической поддержки (см. раздел 6).

Если вы повторно активировали лицензию (например, после переустановки ОС или компонента Ankey SIEM NG Core) и при этом не изменяли аппаратную конфигурацию сервера, счетчик активаций не уменьшается (количество таких повторных активаций не ограничено).

Информация о лицензии доступна на странице **Система → Управление системой**.

3.11.1 Активация лицензии на Linux при наличии доступа к интернету

❖ Чтобы активировать лицензию:

1. На сервер Ankey SIEM NG Core в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` скопируйте шаблон ключа `<Номер лицензии>.grdvd` и текстовый файл с серийным номером `<Идентификатор ключа>.txt`.
2. Запустите активацию лицензии от имени суперпользователя (root):

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')  
/usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер  
лицензии>.grdvd /serialfile=/var/lib/microservice/<Идентификатор  
ключа>.txt
```

По завершении активации появится сообщение `License activation Succeeded`.

Лицензия активирована.

3.11.2 Активация лицензии на Linux при отсутствии доступа к интернету

Для активации лицензии вам потребуется рабочая станция с доступом в интернет и файл `GuardantActivationWizard.exe` из комплекта поставки.

❖ Чтобы активировать лицензию:

1. На сервер Ankey SIEM NG Core в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` скопируйте шаблон ключа `<Номер лицензии>.grdvd` и текстовый файл с серийным номером `<Идентификатор ключа>.txt`.
2. Выполните команду от имени суперпользователя (root):

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')  
/usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер  
лицензии>.grdvd /serialfile=/var/lib/microservice/<Идентификатор  
ключа>.txt /offline
```

- Мастер активации лицензий создаст в каталоге `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` файл `<Номер лицензии>.grdvd.toserver`.
3. На рабочей станции с доступом в интернет разместите в одной папке файлы `GuardantActivationWizard.exe` и `<Номер лицензии>.grdvd.toserver`.
 4. Запустите файл `GuardantActivationWizard.exe`.
Откроется окно мастера активации лицензий.
 5. Нажмите кнопку **Указать файл лицензии**.
 6. В открывшемся окне выберите файл `<Номер лицензии>.grdvd.toserver` и нажмите кнопку **Открыть**.
 7. Нажмите кнопку **Далее**.
Мастер активации лицензий создаст файл `<Номер лицензии>.grdvd.fromserver`. Папка с файлом откроется автоматически.
 8. Нажмите кнопку **Готово**.
 9. Скопируйте файл `<Номер лицензии>.grdvd.fromserver` на сервер **Ankey SIEM NG Core** в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing`.
 10. Выполните команду:

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')  
/usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер  
лицензии>.grdvd.fromserver
```


По завершении активации появится сообщение `License activation Succeeded`.

Лицензия активирована.

3.12 Удаление лицензионного ключа

❖ Чтобы удалить ключ на Linux, выполните команду:

```
docker exec -it $(docker ps | awk '/licensing/ {print $NF}')  
/usr/local/bin/guardantutils/grdspactivation /delete=<Идентификатор ключа>
```

Ключ удален.

3.13 Установка доверенного сертификата для сайта ПК Ankey SIEM NG VM

При развертывании ПК Ankey SIEM NG VM для его сайта автоматически устанавливается самоподписанный сертификат, поставляемый в составе дистрибутива. Поэтому при попытке подключения к сайту вы получите предупреждение о том, что создаваемое подключение не защищено.

Вы можете установить собственный доверенный сертификат, который должен отвечать следующим требованиям:

- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- иметь заголовок `BEGIN CERTIFICATE` без дополнительных заголовков;

- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит с заголовком BEGIN RSA PRIVATE KEY без дополнительных заголовков;

Примечание. Чтобы расшифровать зашифрованный с помощью алгоритма RSA ключ, необходимо выполнить команду `openssl rsa -in encrypted.key -out decrypted.key`.

- включать область применения сертификата Digital Signature или Key Encipherment;
 - в расширении Extended Key Usage (EKU) содержать записи serverAuth и clientAuth;
 - в расширении Subject Alternative Name (SAN) содержать запись об FQDN сервера компонента или его IP-адресе в зависимости от значения параметра HostAddress (оно может быть равно как FQDN, так и IP-адресу).
- ❖ Чтобы установить доверенный сертификат на Linux:
1. На сервере с установленной ролью Deployer разместите файлы сертификатов центров сертификации всей цепочки в каталоге `/opt/deployer/pki/trusted_ca/`.
 2. Выполните команду:
`dpkg-reconfigure deployer`
SSLCertificatePemFileName: <Имя файла сертификата>
SSLKeyFileName: <Имя файла закрытого ключа>
Например:
SSLCertificatePemFileName: website.crt
SSLKeyFileName: website.key

Сертификат установлен.

Внимание! Имена файлов сертификата и ключа не должны совпадать с именами файлов, которые уже находятся в папке сертификатов: замена содержимого стандартных файлов приведет к некорректной работе системы.

3.14 Установка пользовательского сертификата для RMQ Message Bus и компонентов Ankey SIEM NG Core и Ankey SIEM NG Collector

Для RMQ Message Bus и компонентов Ankey SIEM NG Core и Ankey SIEM NG Collector вы можете установить пользовательский сертификат безопасности, который должен отвечать следующим требованиям:

- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- использовать отдельные файлы для хранения сертификата центра сертификации (ЦС), пользовательского сертификата и закрытого ключа;

- иметь заголовок BEGIN CERTIFICATE без дополнительных заголовков;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит с заголовком BEGIN RSA PRIVATE KEY без дополнительных заголовков;

Примечание. Чтобы расшифровать зашифрованный с помощью алгоритма RSA ключ, необходимо выполнить команду `openssl rsa -in encrypted.key -out decrypted.key`.

- включать область применения сертификата Digital Signature или Key Encipherment;
- содержать в расширении Extended Key Usage (EKU) записи аутентификации сервера `serverAuth` и аутентификации клиента `clientAuth`;
- содержать в поле Common Name значения `core` или `agent` для компонентов Ankey SIEM NG Core и Ankey SIEM NG Collector соответственно.

❖ Чтобы установить пользовательский сертификат RMQ Message Bus и компонентов Ankey SIEM NG Core и Ankey SIEM NG Collector на Linux:

1. Разместите файлы сертификата ЦС, пользовательского сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей RMQ Message Bus, Core, и Collector.
2. **Измените конфигурацию роли RMQ Message Bus:**
`CACertFile: <Имя файла сертификата ЦС>`
`CertFile: <Имя файла пользовательского сертификата>`
`KeyFile: <Имя файла закрытого ключа>`
3. **Измените конфигурацию роли Core:**
`CACertificateFileName: <Имя файла сертификата ЦС>`
`RMQsslCertificateFileName: <Имя файла пользовательского сертификата>`
`RMQsslKeyFileName: <Имя файла закрытого ключа>`
4. **Измените конфигурацию роли Collector:**
`Agent_RMQ_SSL_CA_Certificate: <Полный путь к файлу сертификата ЦС>`
`Agent_RMQ_SSL_Certificate: <Полный путь к файлу пользовательского сертификата>`
`Agent_RMQ_SSL_Key: <Полный путь к файлу закрытого ключа>`

Сертификат установлен.

3.15 Настройка обновления экспертных данных

Автоматическое обновление экспертных данных в Ankey SIEM NG VM осуществляется с помощью сервиса Package Management, который входит в состав компонента AK SIEM NG MC. Сервис получает пакеты обновлений с глобального сервера обновлений напрямую или через локальный сервер обновлений Ankey Update Mirror и устанавливает их в продукты с соответствующими лицензиями. Такой способ обновления стал возможен благодаря переходу на новую модель хранения экспертных данных.

Внимание! Процесс миграции на новую модель хранения экспертных данных является обязательным при обновлении ПК Ankey SIEM NG 5.2.3 с версии 4.x на версию 5.x и необходим для корректной работы системы и получения обновлений экспертных данных. Миграция запускается после обновления Ankey SIEM NG.

Для миграции на новую модель хранения экспертных данных после обновления роли Management and Configuration необходимо из комплекта поставки скопировать файл миграционного пакета данных с названием вида migration.vm.s.1.0.v.<Версия пакета данных>.pkg и разместить его на сервере с ролью Management and Configuration в каталоге /var/lib/deployed-roles/mc-application-ankey/managementandconfiguration/data/resources/local-packages/.

Внимание! Файл миграционного пакета необходимо разместить в каталоге в течение 24 часов с момента начала обновления системы.

3.15.1 Схемы получения обновлений экспертных данных, поддерживаемые Ankey SIEM NG VM

Порядок настройки подключения к серверу обновлений зависит от размещения Ankey SIEM NG в инфраструктуре компании.

1. Получение обновлений напрямую с глобального сервера обновлений

Схема получения обновлений напрямую доступна в случае, если ПК Ankey SIEM NG доступно прямое подключение к интернету (рисунок 1.1). Для получения обновлений необходимо при установке (см. подраздел 3.8.4) или обновлении роли Management and Configuration (см. подраздел 4.2.3) указать значения параметров ExpertDataUpdateMethod, PackagesSourceUri и PackagesSourceCredentialToken. Если роль Management and Configuration уже установлена, укажите значения параметров в соответствии с инструкцией (см. раздел 3.15.3).

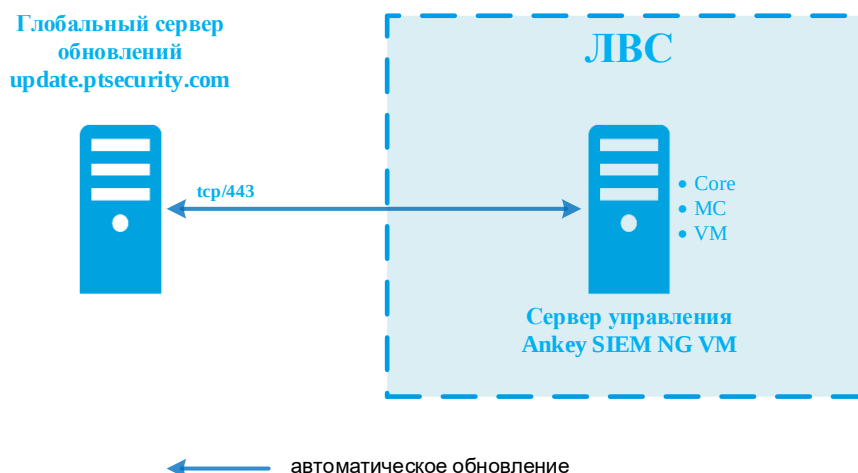


Рисунок 1.1 – Схема получения обновлений напрямую с глобального сервера обновлений

2. Получение обновлений через локальный сервер обновлений, который установлен в изолированном сегменте локальной сети

В случае, если ПК Ankey SIEM NG установлен в изолированном сегменте локальной сети организации и доступ в демилитаризованную зону (далее также – DMZ) отсутствует, вы можете развернуть и настроить в изолированном сегменте локальной сети организации локальный сервер обновлений Ankey Update Mirror, который будет подключаться к глобальному серверу обновлений через прокси-сервер (рисунок 1.2). Он будет загружать обновления с глобального сервера обновлений и передавать их в изолированный сегмент сети.

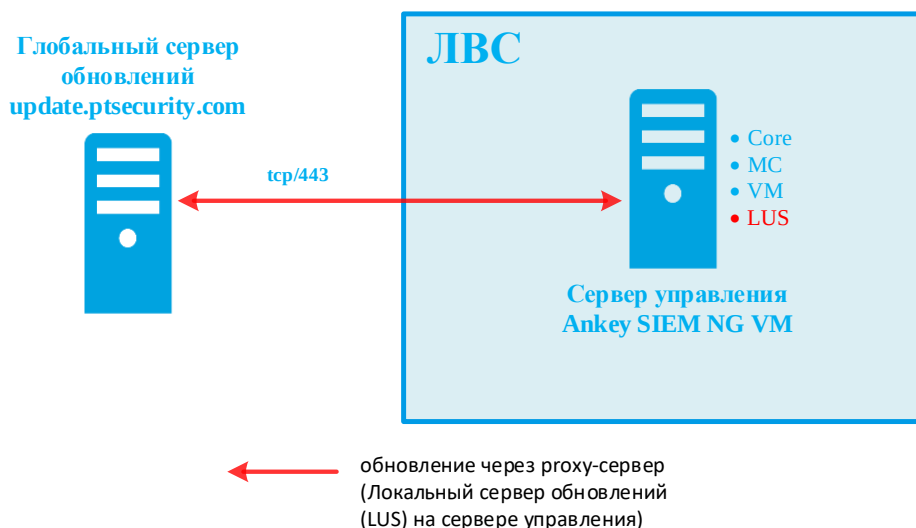


Рисунок 1.2 – Схема получения обновлений через локальный сервер обновлений

3. Получение обновлений через локальный сервер обновлений Ankey Update Mirror, установленный в демилитаризованной зоне.

В случае, если ПК Ankey SIEM NG установлен в изолированном сегменте сети организации и имеет доступ в демилитаризованную зону, вы можете развернуть и настроить в демилитаризованной зоне локальный сервер обновлений Ankey Update Mirror, который будет подключаться к глобальному серверу обновлений напрямую или через прокси-сервер (рисунок 1.3). Он будет загружать обновления с глобального сервера обновлений и передавать их в изолированный сегмент сети.

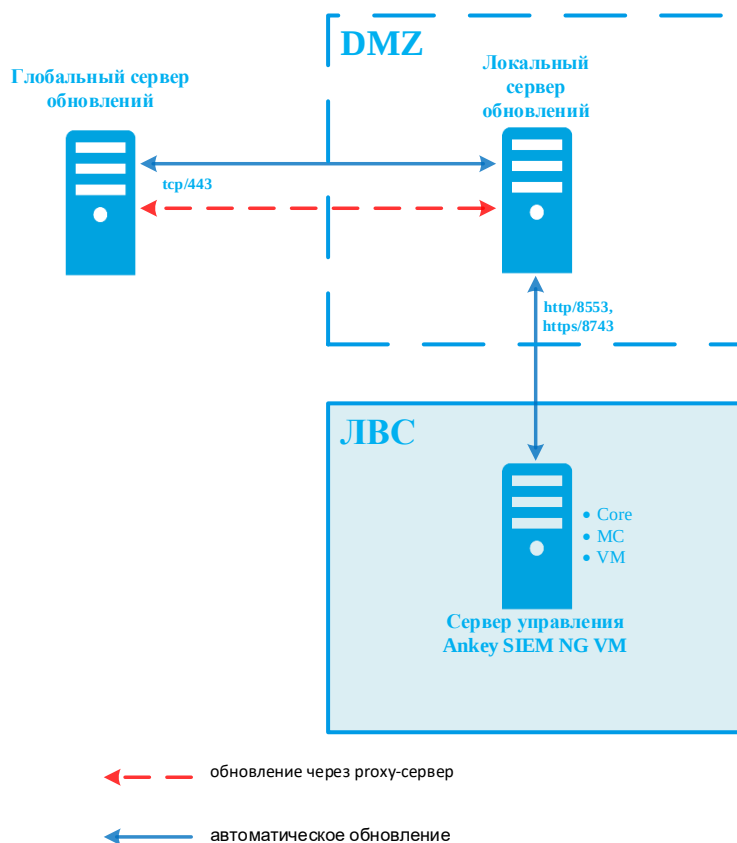


Рисунок 1.3 – Схема получения обновлений с одним Ankey Update Mirror, установленным в демилитаризованной зоне

4. Получение обновлений через два локальных сервера обновлений Ankey Update Mirror, установленных в закрытом сегменте сети и демилитаризованной зоне.

В случае, если ПК Ankey SIEM NG установлен в изолированном от интернета сегменте сети и не должен иметь выход в демилитаризованную зону, вы можете использовать схему обновления с двумя локальными серверами обновлений:

- первый локальный сервер обновлений Ankey Update Mirror установлен в изолированном сегменте сети, где находится ПК Ankey SIEM NG. Установка этого локального сервера Ankey Update Mirror возможна в двух вариантах:
 - вариант 1 – Ankey Update Mirror установлен на сервере управления (рисунок 1.4);
 - вариант 2 – Ankey Update Mirror установлен на отдельном сервере (рисунок 1.5).

- второй локальный сервер обновлений Ankey Update Mirror находится в демилитаризованной зоне. Локальный сервер обновлений в демилитаризованной зоне будет загружать обновления с глобального сервера обновлений.

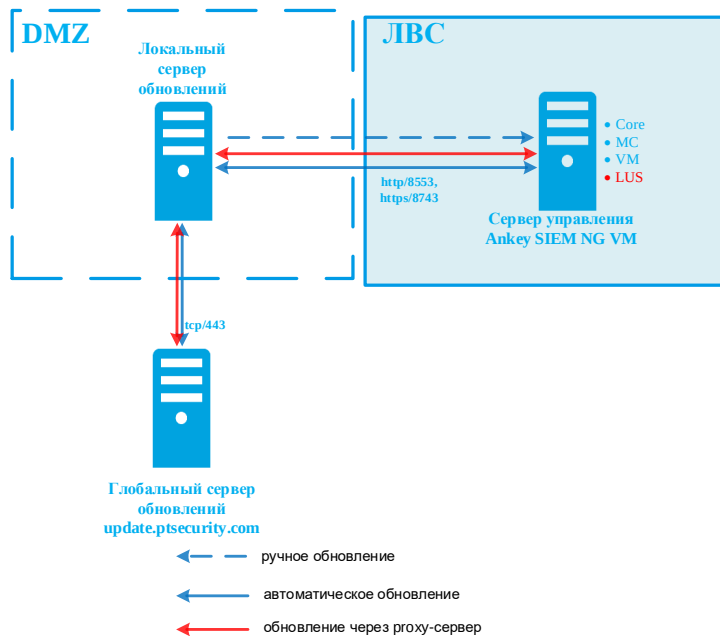


Рисунок 1.4 – Схема получения обновлений с двумя Ankey Update Mirror, установленными в закрытом сегменте сети и в демилитаризованной зоне (вариант 1)

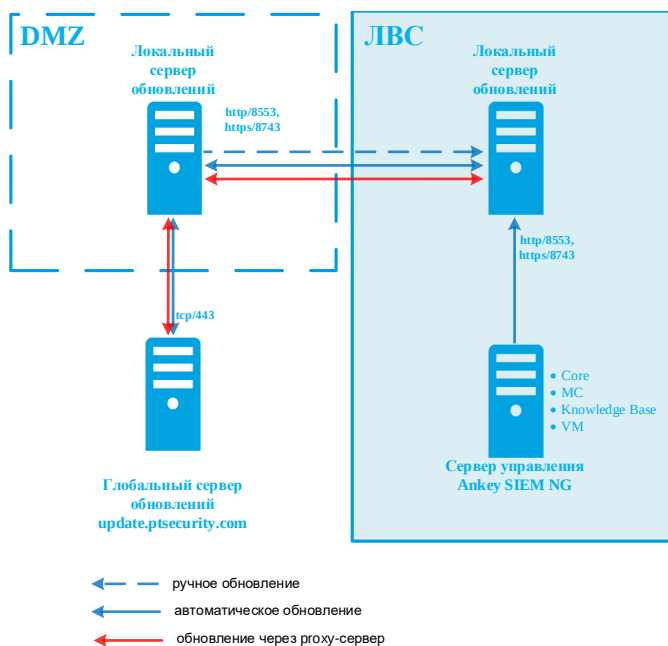


Рисунок 1.5 – Схема получения обновлений с двумя Ankey Update Mirror, установленными в закрытом сегменте сети и в демилитаризованной зоне (вариант 2).

3.15.2 Удаление компонента UCS

Начиная с версии Ankey SIEM NG 5.2.3 функцию доставки экспертных данных выполняет локальный сервер обновлений Ankey Update Mirror.

Если до обновления ПК Ankey SIEM NG с версии 4.x на 5.x для выполнения этой функции был установлен компонент UCS, вы можете удалить его с целью освобождения дискового пространства, поскольку после установки Ankey Update Mirror этот компонент более не требуется.

Примечание. Удаление компонента UCS требуется только при его наличии.

1. Для удаления пакетов компонента UCS выполните команду:
`apt-get --purge autoremove ucs-ankey ucs-branding`
После выполнения команды отобразятся предупреждения, свидетельствующие о неполном удалении:
`dpkg: предупреждение: при удалении ucs-ankey каталог «/srv/updater/products» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-ankey каталог «/srv/updater/fus» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-ankey каталог «/srv/salt» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-ankey каталог «/opt/ucs/ucs-ankey/salt» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-ankey каталог «/etc/opt/ucs/ucs-ankey» не пуст, поэтому не удалён`
`dpkg: предупреждение: при удалении ucs-branding каталог «/opt/siem/ucs-branding/salt» не пуст, поэтому не удалён`
2. Для полной очистки необходимо удалить каталоги UCS:
`rm -R /srv/updater/`
`rm -R /srv/salt/`
`rm -R /opt/ucs/`
`rm -R /opt/siem/ucs-branding/`
`rm -R /etc/opt/ucs/`

3.15.3 Изменение параметров обновления экспертных данных для роли Management and Configuration

Перед настройкой подключения к серверу обновлений нужно получить токен для аутентификации и настроить параметры обновления экспертных данных для роли Management and Configuration. Новые пользователи Ankey SIEM NG VM получают токен вместе с лицензией на продукт. Токен хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64. Этот набор символов необходимо будет указать в качестве значения конфигурационного параметра `PackagesSourceCredentialToken` на одном из шагов инструкции.

Примечание. Чтобы получить новый токен аутентификации, необходимо обратиться в техническую поддержку ООО «Газинформсервис».

- ❖ Чтобы изменить параметры роли:
 1. На сервере с установленной ролью **Deployer** распакуйте архив `managementandconfiguration_<Номер версии>.tar.gz` из комплекта поставки:
`tar -xvf managementandconfiguration_<Номер версии>.tar.gz`
 2. Запустите сценарий:
`managementandconfiguration_<Номер версии>/install.sh`
 3. В открывшемся окне нажмите кнопку **Yes**.
 4. В открывшемся окне выберите вариант с идентификатором приложения роли.
 5. В открывшемся окне выберите вариант с названием экземпляра роли.
Откроется окно для выбора набора параметров.
 6. Выберите вариант **Advanced configuration**.
 7. Откроется страница со списком параметров (см. приложение Б).
 8. В качестве значения параметра `ExpertDataUpdateMethod` выберите:
 - если обновление экспертных данных будет осуществляться напрямую с сервера обновлений «Газинформсервис» или с помощью локального сервера обновлений – **Online**;
 - если вручную – **Offline**.
 9. В качестве значения параметра `PackagesSourceUri` укажите:
 - если Ankey SIEM NG установлен в сегменте сети с прямым подключением к интернету – адрес глобального сервера обновлений `https://update.ptsecurity.com/packman/v1/`.
 - если в изолированном сегменте сети без прямого подключения к интернету – адрес локального сервера обновлений в формате `http://<Адрес сервера>:<Порт>/packman/v1/`.
- Примечание.** Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.
10. В качестве значения параметра `PackagesSourceCredentialToken` укажите содержимое файла `instance-access-token.key`.
 11. Нажмите кнопку **ОК**.
Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
 12. Нажмите кнопку **ОК**.
- Параметры роли изменены.

3.15.4 Аппаратные и программные требования к локальному серверу обновлений

Локальный сервер обновлений может быть установлен как на физическом сервере, так или в виртуальной среде.

Примечание. Вы можете установить локальный сервер обновлений на один сервер с ролью Deployer.

Аппаратные требования

Для работы сервера требуются следующие минимальные аппаратные ресурсы:

- 1 ядро процессора;
- 2 ГБ оперативной памяти;
- 100 ГБ свободного места на диске.

Программные требования

Локальный сервер обновлений поддерживает установку на операционные системы семейства Linux – Astra Linux Special Edition 1.7, Debian 10, Debian 11, Ubuntu 18.04 или Ubuntu 22.04.

3.15.5 Установка локального сервера обновлений

В разделе приводится инструкция по установке локального сервера обновлений в закрытом сегменте сети или в демилитаризованной зоне.

Примечание. По умолчанию локальный сервер обновлений использует для подключения по протоколам HTTP и HTTPS порты 8553 и 8743 соответственно. Вы можете изменить (см. раздел 3.15.10) эти значения в параметрах сервиса получения обновлений.

Перед выполнением инструкции нужно убедиться, что физический сервер или виртуальная машина, на которые вы планируете устанавливать локальный сервер обновлений, удовлетворяет аппаратным и программным требованиям (см. раздел 3.15.4).

❖ Чтобы установить локальный сервер обновлений:

1. Скопируйте архив с дистрибутивом локального сервера обновлений в любой каталог на сервере или виртуальной машине, на которые планируете устанавливать локальный сервер обновлений.

Примечание. Архив имеет название `pt-update-mirror-<Версия локального сервера обновлений>.tar.gz` и содержит установочный пакет `pt-update-mirror-<Версия локального сервера обновлений>.deb`, исполняемый файл `pt-update-mirror`, конфигурационный файл `config.json` и информационный файл `README.md`.

2. Перейдите в каталог со скопированным архивом:
`cd <Путь к каталогу с архивом>`
3. Распакуйте скопированный архив:

- tar -xvf pt-update-mirror-`<Версия локального сервера обновлений>`.tar.gz
4. Запустите установку локального сервера обновлений:
`dpkg -i pt-update-mirror-<Версия локального сервера обновлений>.deb`
Локальный сервер обновлений установлен.
При установке локального сервера обновлений создается пользователь `pt-update-mirror`, который используется при выполнении сервером различных операций.

Если локальный сервер обновлений установлен в демилитаризованной зоне, необходимо активировать на нем лицензию в соответствии с инструкцией (см. раздел 3.15.6).

Если локальный сервер обновлений установлен в закрытом сегменте сети, активировать на нем лицензию необходимо только в случае, когда планируется автоматический перенос обновлений (см. раздел 3.22.6) между локальными серверами в закрытом сегменте сети и демилитаризованной зоне.

3.15.6 Активация лицензии локального сервера обновлений

После установки локального сервера обновлений нужно активировать его лицензию. Это необходимо для аутентификации локального сервера на глобальном сервере обновлений «Газинформсервис».

Примечание. Если перенос обновлений на локальный сервер будет осуществляться вручную, активировать его лицензию не нужно.

Вы можете активировать лицензию с помощью токена лицензии, который хранится в файле `license-access-token.key`, полученном на физическом носителе или в электронном письме на адрес, указанный при покупке.

Примечание. При наличии нескольких лицензий вы можете активировать их по очереди.

Если локальный сервер обновлений должен подключаться к интернету через прокси-сервер, перед активацией лицензии нужно настроить подключение к этому прокси-серверу.

- ❖ Чтобы активировать лицензию с помощью токена лицензии:
 1. Выполните команду:
`sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --license-token <Путь к файлу license-access-token.key>`
 2. Запустите процесс скачивания обновлений с помощью команды обновления репозитория:
`sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository update`

Лицензия активирована.

3.15.7 Настройка подключения локального сервера обновлений к прокси-серверу

Для подключения локального сервера обновлений к интернету через прокси-сервер необходимо указать параметры этого подключения в конфигурационном файле локального сервера.

Локальный сервер обновлений поддерживает подключение к прокси-серверу по протоколам HTTP и HTTPS.

Подключение к прокси-серверу по протоколу HTTP

❖ Чтобы настроить подключение локального сервера обновлений к прокси-серверу:

1. На локальном сервере обновлений откройте конфигурационный файл `config.json`:
`sudo nano /etc/pt-update-mirror/config.json`
2. В качестве значения параметра `proxy` укажите IP-адрес (и при необходимости порт) используемого прокси-сервера:
`"proxy": "http://<IP-адрес прокси-сервера>:<Порт>"`
3. Если прокси-сервер требует аутентификации, укажите логин и пароль для подключения:
`"proxy-user": "<Логин>",`
`"proxy-password": "<Пароль>"`
4. Сохраните изменения в файле `config.json`.
5. Перезапустите локальный сервер обновлений:
`sudo systemctl restart pt-update-mirror.service`

Подключение настроено.

Подключение к прокси-серверу по протоколу HTTPS

Для проверки подлинности при передаче данных по протоколу HTTPS необходимо выпустить сертификат SSL, который должен:

- соответствовать формату PEM;
- использовать подпись с применением алгоритма шифрования SHA-256;
- использовать алгоритм шифрования ключей RSA;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит;
- включать в себя область применения сертификата Digital Signature или Key Encipherment;
- содержать в расширении Subject Alternative Name (SAN) запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом продукта;
- если в цепочке между корневым сертификатом и сертификатами компонентов и систем есть промежуточные сертификаты – включать в себя всю цепочку сертификатов.

Для корректной работы необходимо добавить выпущенный сертификат в список доверенных.

❖ Чтобы добавить сертификат в список доверенных:

1. Скопируйте файлы сертификата в каталог `/usr/local/share/ca-certificates/` на узле, на который установлен локальный сервер обновлений.
2. Обновите список доверенных сертификатов:
`sudo update-ca-certificates`

Сертификат добавлен в список доверенных.

❖ Чтобы настроить подключение локального сервера обновлений к прокси-серверу:

1. На локальном сервере обновлений откройте конфигурационный файл `config.json`:
`sudo nano /etc/pt-update-mirror/config.json`

2. В качестве значения параметра `proxy` укажите IP-адрес (и при необходимости порт) используемого прокси-сервера:
`"proxy": "https://<IP-адрес прокси-сервера>:<Порт>"`
3. Если прокси-сервер требует аутентификации, укажите логин и пароль для подключения:
`"proxy-user": "<Логин>",`
`"proxy-password": "<Пароль>"`
4. Сохраните изменения в файле `config.json`.
5. Перезапустите локальный сервер обновлений:
`sudo systemctl restart pt-update-mirror.service`

Подключение настроено.

3.15.8 Настройка автоматического переноса обновлений в закрытый сегмент сети

Если между локальными серверами обновлений есть сетевое взаимодействие, вы можете настроить их подключение друг к другу. Это позволит автоматически переносить обновления с глобального сервера обновлений «Газинформсервис» в Ankey SIEM NG VM в закрытом сегменте сети через цепочку локальных серверов обновлений.

Вы можете настроить автоматический перенос обновлений как по протоколу HTTP, так и по протоколу HTTPS.

Подключение по протоколу HTTP

Для подключения по протоколу HTTP вместо порта по умолчанию 80 используется порт 8553. Если требуется, вы можете изменить порт (см. раздел 3.15.10) для подключения.

❖ Чтобы настроить автоматический перенос обновлений:

1. На локальном сервере обновлений в изолированном сегменте откройте конфигурационный файл `config.json`:
`sudo nano /etc/pt-update-mirror/config.json`
2. В качестве значения параметра `update-server` укажите адрес локального сервера обновлений в демилитаризованной зоне:
`"update-server": "http://<Адрес локального сервера обновлений>:<Порт>"`

Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений.

3. В качестве значения параметра `verify_ssl` укажите `false`.
4. Если подключение к локальному серверу в демилитаризованной зоне выполняется через прокси-сервер, настройте параметры подключения к прокси-серверу (см. раздел 3.15.7).
5. Сохраните изменения в файле `config.json`.
6. Перезапустите сервис обновлений в закрытом сегменте сети:
`sudo systemctl restart pt-update-mirror.service`

Перенос обновлений настроен.

Подключение по протоколу HTTPS

Для подключения по протоколу HTTPS вместо порта по умолчанию 443 используется порт 8743. Если требуется, вы можете изменить порт

(см. раздел 3.15.10) для подключения.

Для проверки подлинности при передаче данных по протоколу HTTPS необходимо выпустить сертификат SSL, который должен:

- соответствовать формату PEM;
- использовать подпись с применением алгоритма шифрования SHA-256;
- использовать алгоритм шифрования ключей RSA;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит;
- включать в себя область применения сертификата Digital Signature или Key Encipherment;
- содержать в расширении Subject Alternative Name (SAN) запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом продукта;
- если в цепочке между корневым сертификатом и сертификатами компонентов и систем есть промежуточные сертификаты – включать в себя всю цепочку сертификатов.

Для корректной работы необходимо назвать файлы сертификата и его ключа `cert.crt` и `cert.key` соответственно и поместить их в каталог `/etc/pt-update-mirror/https_certs/` на локальном сервере обновлений.

❖ Чтобы настроить автоматический перенос обновлений:

1. На локальном сервере обновлений в изолированном сегменте откройте конфигурационный файл `config.json`:
`sudo nano /etc/pt-update-mirror/config.json`
2. В качестве значения параметра `update-server` укажите адрес локального сервера обновлений в демилитаризованной зоне:
`"update-server": "https://<Адрес локального сервера обновлений>:<Порт>"`

Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений.

3. Если подключение к локальному серверу в демилитаризованной зоне выполняется через прокси-сервер, настройте параметры подключения к прокси-серверу (см. раздел 3.15.7).
4. Сохраните изменения в файле `config.json`.
5. Перезапустите сервис обновлений в закрытом сегменте сети:
`sudo systemctl restart pt-update-mirror.service`

Перенос обновлений настроен.

3.15.9 Ручной перенос обновлений Ankey SIEM NG VM в закрытый сегмент сети

Если между локальными серверами обновлений отсутствует сетевое взаимодействие, вам нужно вручную перенести обновления в закрытый сегмент сети для последующего обновления Ankey SIEM NG VM.

❖ Чтобы вручную перенести обновления в закрытый сегмент сети:

1. На локальном сервере обновлений в демилитаризованной зоне запустите получение обновлений с глобального сервера обновлений «Газинформсервис»:

- sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository update
2. Запустите экспорт репозитория с обновлениями в файл:
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository export --
repo vm-expertise <Название файла>.tgz

Примечание. Выполнение команды экспорта без ключа --repo <Название репозитория> позволяет экспортировать все репозитории базы обновлений в указанный архив. Вы можете просмотреть список репозитория в базе обновлений локального сервера с помощью команды sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository view.

3. Скопируйте с помощью внешнего носителя полученный файл архива в каталог, принадлежащий пользователю pt-update-mirror, на локальном сервере обновлений в закрытом сегменте сети.
4. На локальном сервере обновлений в закрытом сегменте сети импортируйте обновления из скопированного файла архива:
sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository import
<Путь к архиву>/<Название архива>.tgz

Обновления Ankey SIEM NG VM перенесены.

3.15.10 Проверка и изменение параметров локального сервера обновлений

Проверка состояния сервера

- ❖ Чтобы проверить состояние локального сервера обновлений, на локальном сервере выполните команду:

```
sudo systemctl status pt-update-mirror
```

На экране отобразится информация о параметрах загрузки и состоянии локального сервера.

Проверка состояния таймера получения обновлений

- ❖ Чтобы проверить состояние таймера получения обновлений, на локальном сервере выполните команду:

```
sudo systemctl status pt-update-mirror-update.timer
```

На экране отобразится информация о параметрах загрузки и состоянии таймера получения обновлений.

Проверка состояния сервиса получения обновлений

- ❖ Чтобы проверить состояние сервиса получения обновлений, на локальном сервере выполните команду:

```
sudo systemctl status pt-update-mirror-update
```

На экране отобразится информация о параметрах загрузки и состоянии сервиса получения обновлений.

Просмотр журналов событий сервиса получения обновлений

- ❖ Чтобы просмотреть журнал событий сервиса получения обновлений,

на локальном сервере выполните команду:

```
journalctl -u pt-update-mirror.service
```

На экране отобразится список событий сервиса получения обновлений.

Изменение времени получения обновлений

По умолчанию обновление запускается в 13, 27, 42 и 58 минут каждого часа. Вы можете изменить эти значения в параметрах таймера получения обновлений.

❖ Чтобы изменить время получения обновлений:

1. Откройте файл `pt-update-mirror-update.timer`:
`sudo nano etc/systemd/system/pt-update-mirror-update.timer`
2. В блоке параметров `Timer` в качестве значения параметра `OnCalendar` укажите нужное время получения обновлений (в формате `systemd.timer`).
3. Сохраните изменения в файле `pt-update-mirror-update.timer`.
4. Примените изменения таймера:
`sudo systemctl daemon-reload`
5. Перезапустите таймер получения обновлений:
`sudo systemctl restart pt-update-mirror-update.timer`

Время получения обновлений изменено.

Изменение порта подключения по протоколам HTTP и HTTPS

По умолчанию локальный сервер обновлений использует для подключения по протоколам HTTP и HTTPS порты 8553 и 8743 соответственно. Вы можете изменить эти значения в параметрах сервиса получения обновлений.

❖ Чтобы изменить порт подключения:

1. Откройте файл `pt-update-mirror.service`:
`sudo nano etc/systemd/system/pt-update-mirror.service`
2. Выполните одно из следующих действий:
 - если для подключения локального сервера используется протокол HTTP, в блок параметров `Service` в конец строки с параметром `ExecStart` добавьте ключ `--http-port <Порт>`.
 - если для подключения локального сервера используется протокол HTTPS, в блок параметров `Service` в конец строки с параметром `ExecStart` добавьте ключ `--https-port <Порт>`.
3. Сохраните изменения в файле `pt-update-mirror.service`.
4. Примените изменения таймера:
`sudo systemctl daemon-reload`
5. Перезапустите локальный сервер обновлений:
`sudo systemctl restart pt-update-mirror`

Порт подключения изменен.

3.16 Настройка ПК Ankey SIEM NG VM для обеспечения его безопасной работы Ankey SIEM NG Core установлен на Linux

В этом подразделе приводятся инструкции по настройке развернутой конфигурации ПК Ankey SIEM NG VM для обеспечения его безопасной работы.

Компоненты системы рекомендуется разместить в доверенном сегменте сети. Доступ к ним из других сегментов рекомендуется ограничить с помощью межсетевого экрана.

❖ Чтобы настроить ПК Ankey SIEM NG VM:

1. На серверах под управлением Linux разрешите удаленный доступ по протоколу SSH только с рабочих станций администраторов:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -m comment --comment "SSH admin access" -j ACCEPT
```

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, -s 198.51.100.0,198.51.100.1,192.0.2.0/24.

2. На сервере Ankey SIEM NG Core разрешите доступ к веб-интерфейсу системы с рабочих станций пользователей:

```
iptables -F DOCKER-USER
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций пользователей> -p tcp -m multiport --dports 443,3334,8091,8190 -m conntrack --ctstate NEW -m comment --comment "Web user access" -j ACCEPT
```
3. В файл custom.env, расположенный в каталоге /var/lib/deployed roles/<Идентификатор приложения Ankey SIEM NG VM>/<Название экземпляра роли SqlStorage/JatobaStorage>/images/storage-pgadmin/config/, добавьте параметры:

```
PGADMIN_CONFIG_MASTER_PASSWORD_REQUIRED=True
PGADMIN_DEFAULT_PASSWORD=<Пароль PGAdmin>
```
4. Перезапустите службы компонентов Ankey SIEM NG Core:

```
docker restart $(docker ps | awk '/core-{kb-/{print $NF}')
```
5. Пересоберите службу pgAdmin:

```
cd /var/lib/deployed-roles/<Идентификатор приложения Management and Configuration>/<Название экземпляра роли SqlStorage/JatobaStorage>/images/storage-pgadmin
docker-compose down
docker-compose up -d
```
6. Разрешите входящие соединения от коллекторов:

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера Ankey SIEM NG Collector> -p tcp -m tcp --dport 5671 -m conntrack --ctstate NEW -m comment --comment "From Ankey SIEM NG Collector to Ankey SIEM NG Core" -j ACCEPT
```
7. На серверах под управлением Linux заблокируйте все входящие соединения, кроме разрешенных:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -j DROP
```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -j REJECT
```

8. Для сохранения созданных правил на серверах под управлением Debian установите пакет iptables-persistent:
`apt-get install iptables-persistent`

Примечание. Порядок сохранения правил на серверах под управлением Astra Linux описан в справочном центре производителя операционной системы.

9. Сохраните правила межсетевого экрана:
`netfilter-persistent save`
10. На серверах коллекторов под управлением Microsoft Windows удалите все правила удаленного доступа по протоколу RDP:
`netsh advfirewall firewall delete rule name=all protocol=tcp localport=3389`
`netsh advfirewall firewall delete rule name=all protocol=udp localport=3389`
11. Разрешите удаленный доступ по протоколу RDP только с рабочих станций администраторов:
`netsh advfirewall firewall add rule name="Allow RDP TCP in" dir=in action=allow protocol=tcp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>`
`netsh advfirewall firewall add rule name="Allow RDP UDP in" dir=in action=allow protocol=udp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>`

Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, `remoteip=198.51.100.0,198.51.100.1,192.0.2.0/24`.

12. Если для сбора событий по стандарту syslog и протоколу Netflow коллекторы на Microsoft Windows не используют порты по умолчанию, на серверах коллекторов удалите правила для входящих соединений с этих портов:
`for %P IN (514,1468) DO (netsh advfirewall firewall delete rule name=all protocol=tcp localport=%P)`
`for %P IN (514,2055) DO (netsh advfirewall firewall delete rule name=all protocol=udp localport=%P)`
13. Разрешите входящие соединения для сбора событий по стандарту syslog и протоколу Netflow на серверах коллекторов на Linux для портов, указанных при создании задачи на сбор событий:
`iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p tcp -m tcp --dport 1468 -m conntrack --ctstate NEW -m comment --comment "Agent SysLog (TCP)" -j ACCEPT`

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p udp -
m udp --dport 514 -m conntrack --ctstate NEW -m comment --comment
"Agent SysLog (UDP)" -j ACCEPT
```

14. Смените пароли служебных учетных записей в Ankey SIEM NG VM (подробнее см. «Руководство администратора Ankey SIEM NG VM»).
15. На серверах под управлением Microsoft Windows убедитесь, что пароли для входа в операционную систему соответствуют требованиям к сложности, установленным в организации.
16. На серверах под управлением Linux для каждого администратора Ankey SIEM NG VM создайте отдельную учетную запись:
adduser <Логин администратора>
17. На рабочих станциях администраторов Ankey SIEM NG VM сгенерируйте ключевую пару.

Примечание. Для генерации ключевой пары на Linux вы можете использовать утилиту ssh-keygen, на Microsoft Windows – PuTTYgen.

18. На серверах под управлением Linux добавьте открытый ключ в файл /home/<Логин администратора>/.ssh/authorized_keys.
 19. В файле /etc/ssh/sshd_config раскомментируйте и измените значения параметров (разрешите вход только с помощью SSH-ключей):
PubkeyAuthentication yes
RhostsRSAAuthentication no
HostbasedAuthentication no
PermitEmptyPasswords no
PasswordAuthentication no
 20. В файле /etc/sudoers измените значение параметра:
<Логин администратора> ALL=(ALL) ALL
 21. Для каждого пользователя Ankey SIEM NG VM создайте отдельную учетную запись.
 22. Смените пароль учетной записи **Administrator**.
- Ankey SIEM NG VM настроен

4 Обновление ПК Ankey SIEM NG VM с помощью дистрибутивов

Вы можете обновлять компоненты ПК Ankey SIEM NG VM с помощью дистрибутивов.

Внимание! Перед началом обновления создайте резервную копию данных компонентов.

Прежде чем приступить к обновлению ПК Ankey SIEM NG VM, рекомендуется остановить все задачи по сбору данных, а также убедиться, что на период обновления не запланирован запуск задач по расписанию. Это позволит избежать накопления очередей во время обновления, а также ошибок при выполнении задач после обновления.

Перед началом обновления необходимо убедиться в отсутствии ошибок в работе системы (индикатор состояния системы не красный).

В версии 3.0 обновлены SSL-сертификаты, поставляемые в составе ПК Ankey SIEM NG VM. Во время обновления системы с версии 2.1 (после обновления Ankey SIEM NG Core и до обновления коллекторов) будут недоступны как сами коллекторы, так и работа с задачами на сбор данных.

Для обновления Ankey SIEM NG VM необходимо обратиться в техническую поддержку «Газинформсервис» и получить дистрибутивы с новыми версиями компонентов. Перед началом обновления рекомендуется создать резервную копию данных.

Начиная с версии 4.0 базовыми единицами установки и обновления компонентов Linux являются роли (см. раздел 3.5). Обновление компонентов на Linux необходимо выполнять в следующем порядке: роль Deployer → Ankey SIEM NG MC → Ankey SIEM NG Core → Ankey SIEM NG Collector.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.1 Обновление роли Deployer

Внимание! Для корректной работы Ankey SIEM NG VM необходимо, чтобы подсеть его Docker-контейнеров не совпадала с подсетями, используемыми в вашей организации. По умолчанию система виртуализации Docker использует подсеть 172.17.0.0/12. Вы можете изменить подсеть по инструкции из раздела «Подсеть Docker-контейнера Ankey SIEM NG VM совпадает с одной из подсетей предприятия» Руководства администратора.

Для обновления роли вам потребуется архив `deployer_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. Распакуйте архив `deployer_<Номер версии>.tar.gz`:

- tar -xf deployer_<Номер версии>.tar.gz
2. Запустите сценарий:
ankey_deployer_<Номер версии>/install.sh
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов. По завершении подготовки откроется окно с текстом лицензионного соглашения.
4. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
5. Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**.
7. Откроется страница со списком основных параметров.
8. Убедитесь, что в качестве значения параметра **HostAddress** указан IP-адрес или FQDN сервера, на который установлена роль Deployer.
9. Нажмите кнопку **OK**.
10. Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
11. Нажмите кнопку **OK**.
12. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

4.2 Обновление компонента Ankey SIEM NG MC на Linux

Компонент Ankey SIEM NG MC необходимо обновлять в следующем порядке: сначала обновить роль `SqlStorage` или `JatobaStorage`, затем – роль `Management and Configuration`.

4.2.1 Обновление роли `SqlStorage`

Для обновления роли `SqlStorage` потребуется архив `SqlStorage_<Номер новой версии>.tar.gz`, который содержится в дистрибутиве ПК Ankey SIEM NG VM.

- ❖ Чтобы обновить роль `SqlStorage`:
 1. На сервер с компонентом Ankey SIEM NG Core скопируйте архив `sqlstorage_<Номер версии>.tar.gz` в каталог `/opt`.
 2. Перейдите в каталог с архивом `sqlstorage_<Номер версии>.tar.gz` и распакуйте его, выполнив команду `tar -xf sqlstorage_<Номер версии>.tar.gz`.
 3. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
 4. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
 5. Выберите вариант с идентификатором `<идентификатор приложения, например, managementandconfiguration>` или с тем названием, которое выбрал пользователь при создании приложения.

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с названием экземпляра роли <название роли, например SqlStorage>.
Откроется окно для проверки и изменения параметров установки.
8. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
9. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера с компонентом Ankey SIEM NG Core.
10. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение *Deployment configuration successfully applied*.
11. Нажмите кнопку **OK**.
12. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль SqlStorage обновлена.

4.2.2 Обновление роли JatobaStorage

СУБД Jatoba функционирует в docker-контейнере. Перед началом обновления СУБД Jatoba может потребоваться новый лицензионный ключ. Вы можете получить актуальный ключ активации для новой лицензии СУБД Jatoba, отправив запрос на электронную почту jatoba-support@gaz-is.ru.

Активация новой лицензии для СУБД Jatoba необходима в том случае, если при обновлении СУБД Jatoba обновляется версия docker-контейнера.

В процессе обновления роли JatobaStorage может потребоваться повторная активация лицензии для СУБД Jatoba, так как в процессе обновления СУБД Jatoba дополнительно обновляется и docker-контейнер, что приводит к нарушению условий лицензирования, из-за чего СУБД Jatoba внутри docker-контейнера перестает корректно функционировать.

Для обновления роли JatobaStorage потребуется архив JatobaStorage_<Номер новой версии>.tar.gz, который содержится в дистрибутиве ПК Ankey SIEM NG VM.

❖ Чтобы обновить роль JatobaStorage:

1. На сервер с компонентом Ankey SIEM NG Core скопируйте архив `jatobastorage_<Номер версии>.tar.gz` в каталог `/opt`.
2. Перейдите в каталог с архивом `jatobastorage_<Номер версии>.tar.gz` и распакуйте его, выполнив команду `tar -xvf jatobastorage_<Номер версии>.tar.gz`.
3. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
4. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
5. Выберите вариант с идентификатором <идентификатор приложения, например, `managementandconfiguration`> или с тем названием, которое выбрал пользователь при создании приложения.

6. В открывшемся окне выберите вариант с названием экземпляра роли <название роли, например JatobaStorage>.
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров установки.
8. Убедитесь, что в качестве значения параметра HostAddress указано полное доменное имя (FQDN) или IPv4-адрес сервера с компонентом Ankey SIEM NG Core.
9. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
10. В поле **JatobaLicenseActivationType**, с помощью клавиши «Space/Пробел» выберите режим активации лицензии (**Online** или **Offline**).
11. В поле **LicenseKey** введите актуальный лицензионный ключ.
12. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение Deployment configuration successfully applied.
13. Если не требуется корректировка дополнительных параметров, то с помощью стрелок на клавиатуре выполните переход на графическую кнопку **OK** и нажмите клавишу «Ввод/Enter».
14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль JatobaStorage обновлена.

Для повторной активации лицензии СУБД Jatoba следует выполнить инструкции, которые приведены в подразделе 3.8.2 или 3.8.3 в зависимости от типа активации, которая была выбрана при установке СУБД Jatoba.

Внимание! При активации лицензии в режиме офлайн файлы с расширением .bak в каталоге /var/lib/deployedroles/<название приложения MC, например: mc-applicationankey>/<название роли СУБД Jatoba, например: jatobastorage>/config/license/ следует игнорировать.

4.2.3 Обновление роли Management and Configuration

Внимание! Для получения обновлений экспертных данных Ankey SIEM NG VM в изолированном сегменте сети без прямого подключения к интернету необходим локальный сервер обновлений, установленный и настроенный в соответствии с инструкциями в разделе «Настройка обновления экспертных данных» (см. раздел 3.15).

Для обновления роли вам потребуется архив managementandconfiguration_<Номер версии>.tar.gz из комплекта поставки и токен аутентификации, который хранится в файле instance-access-token.key и представляет собой набор символов, закодированных с использованием стандарта Base64. Этот набор символов необходимо будет указать в качестве значения конфигурационного параметра PackagesSourceCredentialToken на одном из шагов инструкции.

Примечание. Новые пользователи Ankey SIEM NG VM получают файл `instance-access-token.key` вместе с лицензией на продукт, а существующие пользователи, обновляющиеся с версии 5.0 или ниже – вместе с дистрибутивом или через службу технической поддержки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `managementandconfiguration_<Номер версии>.tar.gz` :
`tar -xf managementandconfiguration_<Номер версии>.tar.gz`
2. **Запустите сценарий:**
`managementandconfiguration_<Номер версии>/install.sh`
3. В открывшемся окне нажмите кнопку **Yes**.
Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения `Management and Configuration`.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите вариант с названием экземпляра роли `Management and Configuration`.
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
8. В качестве значения параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера Ankey SIEM NG Core.
9. В качестве значения параметра `ExpertDataUpdateMethod` выберите:
 - Если обновление экспертных данных будет осуществляться напрямую с сервера обновлений «Газинформсервис» или с помощью локального сервера обновлений – **Online**.
 - Если вручную – **Offline**.
10. В качестве значения параметра `PackagesSourceUri` укажите:
 - Если вы обновляете Ankey SIEM NG VM в сегменте сети с прямым подключением к интернету – адрес глобального сервера обновлений
`https://update.ptsecurity.com/packman/v1/`.
 - Если в изолированном сегменте сети без прямого подключения к интернету – адрес локального сервера обновлений в формате
`http://<Адрес сервера>:<Порт>/packman/v1/`.

Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.

11. В качестве значения параметра `PackagesSourceCredentialToken` укажите содержимое файла `instance-access-token.key`.
12. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **ОК**.
14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

4.3 Обновление компонента Ankey SIEM NG Core на Linux

Компонент необходимо обновлять в следующем порядке: сначала обновить роль `RMQ Message Bus`, затем – роль `Core`.

4.3.1 Обновление роли `RMQ Message Bus` на сервере Ankey SIEM NG Core

Для обновления роли вам потребуется архив `rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью `Deployer` распакуйте архив `rmqmessagebus_<Номер версии>.tar.gz`:
`tar -xf rmqmessagebus_<Номер версии>.tar.gz`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения `Ankey SIEM NG VM`.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите вариант с названием экземпляра роли `RMQ Message Bus`, который установлен на сервер `Ankey SIEM NG Core`.
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
8. Убедитесь, что в качестве значения параметра `HostAddress` указано полное доменное имя (FQDN) или IPv4-адрес сервера `Ankey SIEM NG Core`.
9. Нажмите кнопку **ОК**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **ОК**.

11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

4.3.2 Обновление роли Core

Для обновления роли вам потребуется архив `core_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить роль:

1. Выполните команду:
`/opt/deployer/bin/Restart-Configuration.ps1 -roletypeid core`
2. На сервере Ankey SIEM NG Core распакуйте архив `core_<Номер версии>.tar.gz`:
`tar -xf core_<Номер версии>.tar.gz`
3. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
4. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
5. Выберите вариант с идентификатором приложения Ankey SIEM NG VM.
6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с названием экземпляра роли Core.
Откроется окно для проверки и изменения параметров установки.
8. Выберите вариант **Basic configuration**.
Откроется страница со списком основных параметров.
9. Проверьте значения параметров:
HostAddress: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
MCAddress: `https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:3334`
KBAddress: `https://<FQDN или IPv4-адрес сервера Ankey SIEM NG Core>:8091`
PostgreHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
RMQHost: <FQDN или IPv4-адрес сервера Ankey SIEM NG Core>
10. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
11. Нажмите кнопку **OK**.
12. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

4.4 Обновление компонента Ankey SIEM NG Collector на Linux

Внимание! Для обновления версий 2.1 и 3.0 компонента до версии 4.0 или выше необходимо удалить существующую роль Collector и установить роль Collector из комплекта поставки в соответствии с инструкцией (см. пункт 3.10.2).

Для обновления компонента необходимо обновить роль Collector. Для обновления роли вам потребуется архив `agent-linux_<Номер версии>` из комплекта поставки.

❖ Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `agent-linux_<Номер версии>`:
`tar -xf agent-linux_<Номер версии>`
2. Перейдите в каталог, куда был распакован архив, и запустите сценарий установки роли `./install.sh`.
3. В открывшемся окне нажмите кнопку **Yes**.
Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Ankey SIEM NG VM.
5. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
6. В открывшемся окне выберите вариант с названием экземпляра роли Collector.
Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров.
8. Убедитесь, что в качестве значения параметра `AgentRMQHost` указан IP-адрес или FQDN сервера Ankey SIEM NG Core. В качестве значения параметра `AgentRMQVirtualHost` выберите **Core**.
9. Нажмите кнопку **OK**.
Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

4.5 Обновление компонента Ankey SIEM NG Collector на Microsoft Windows

Внимание! В результате обновления компонентов установленные ранее пользовательские сертификаты безопасности будут заменены сертификатами из комплекта поставки. Если для работы компонентов использовались сертификаты безопасности, отличные от стандартных, необходимо снова настроить их после обновления.

Для обновления вам потребуется архив `agent-windows_<Номер версии>.tar.gz` из комплекта поставки.

❖ Чтобы обновить компонент Ankey SIEM NG Collector:

1. Запустите файл `AnkeyAgentSetup_<Номер версии>.exe`.
Откроется окно мастера обновления.
2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Обновить**.
4. По завершении обновления нажмите кнопку **Заккрыть**.
5. В командной строке Microsoft Windows выполните команду от имени администратора:

```
coreagentcfg set -p AgentRMQVirtualHost mpx.
```

Компонент Ankey SIEM NG Collector обновлен.

5 Просмотр и изменение параметров конфигурации ПК Ankey SIEM NG VM

В этом разделе приведены инструкции по просмотру и изменению параметров конфигурации компонентов ПК Ankey SIEM NG VM. Описания параметров приведены в приложении Б.

5.1 Просмотр и изменение конфигурации компонентов ПК Ankey SIEM NG VM на Linux

Конфигурация компонента включает в себя параметры конфигураций ролей, с помощью которых компонент был установлен. Для изменения конфигурации компонента необходимо изменить конфигурацию той или иной роли.

В результате просмотра или изменения конфигурации роли в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы изменений. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

5.1.1 Просмотр конфигурации роли

- ❖ Чтобы просмотреть конфигурацию роли:
 1. На сервере с установленной ролью Deployer запустите сценарий:
`<Название роли>/install.sh`
 2. В открывшемся окне нажмите кнопку **Yes**.
 3. В открывшемся окне выберите вариант с идентификатором приложения роли.
 4. В открывшемся окне выберите вариант с названием экземпляра роли.
Откроется окно для выбора набора параметров.
 5. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров (см. приложение Б).
 6. По завершении просмотра нажмите кнопку **Cancel**.
 7. В окне для выбора набора параметров нажмите кнопку **Cancel**.

5.1.2 Изменение конфигурации роли

- ❖ Чтобы изменить конфигурацию роли:
 1. На сервере с установленной ролью Deployer запустите сценарий:
`<Название роли>/install.sh`
 2. В открывшемся окне нажмите кнопку **Yes**.
 3. В открывшемся окне выберите вариант с идентификатором приложения роли.
 4. В открывшемся окне выберите вариант с названием экземпляра роли.
Откроется окно для выбора набора параметров.
 5. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров (см. приложение Б).
 6. Измените значения параметров.

7. Нажмите кнопку **OK**.
8. В открывшемся окне нажмите кнопку **Submit**. Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
9. Нажмите кнопку **OK**.
10. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Конфигурация роли изменена.

5.1.3 Настройка SMTP-сервера для отправки уведомлений по электронной почте

Уведомления Ankey SIEM NG VM содержат информацию об изменениях в ИТ-инфраструктуре предприятия, о работе задач сбора данных и состоянии системы. Вы можете настроить отправку уведомлений по электронной почте, указав при создании задачи адреса получателей уведомления. Подробнее о создании задач для отправки уведомлений см. Руководство оператора. Перед созданием задачи необходимо настроить SMTP-сервер.

❖ Чтобы настроить SMTP-сервер для отправки уведомлений по электронной почте:

1. На сервере с установленной ролью `Deployer` распакуйте архив `ankey_core_<Номер версии>.tar.gz`:
`tar -xf ankey_core_<Номер версии>.tar.gz`
2. Запустите сценарий:
`ankey_core_<Номер версии>/install.sh`
3. В открывшемся окне нажмите кнопку **Yes**.
4. В открывшемся окне выберите вариант с идентификатором приложения роли.
5. В открывшемся окне выберите вариант с названием экземпляра роли.
Откроется окно для выбора набора параметров.
6. Выберите вариант **Advanced configuration**.
Откроется страница со списком параметров (см. приложение Б).
7. Укажите значения параметров:
`Smtphost`: <IP-адрес или FQDN SMTP-сервера>
`Smtppassword`: <Пароль служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу>
`Smtpport`: <Порт SMTP-сервера для входящих подключений от Ankey SIEM NG Core>
`Smtpsender`: <Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте>
`Smtuser`: <Логин служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу>

Примечание. Для публичных почтовых сервисов значения параметров `Smtpsender` и `Smtuser` должны совпадать.

8. Чтобы отключить проверку валидности сертификата при подключении к SMTP-серверу, в качестве значения параметра `SmtplgnoreCertificateValidation` выберите **True**.
9. В качестве значения параметра `SmtptSecureSocketOptions` выберите вариант шифрования при подключении к SMTP-серверу.
10. Нажмите кнопку **OK**.
11. В открывшемся окне нажмите кнопку **Submit**.
12. Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **OK**.
14. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

SMTP-сервер настроен

6 Диагностика и решение проблем

Инструкции по диагностике и решению проблем, возникающих при работе с ПК Ankey SIEM NG VM, представлены в документе «Руководство администратора Ankey SIEM NG VM 5.2.3».

Если выполнение указанных в документе шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки ООО «Газинформсервис».

Примечание. Порядок обращения в службу технической поддержки, а также особенности и ограничения услуг технической поддержки представлены в документе «Руководство администратора Ankey SIEM NG VM 5.2.3».

Перечень сокращений

AIO	–	All in One – конфигурация ПК Ankey SIEM NG VM для низконагруженных систем. Все компоненты устанавливаются на одном сервере
API	–	Application Programming Interface – протокол для взаимодействия компьютерных программ, который позволяет использовать функции одного приложения внутри другого
AVX	–	Advanced Vector Extensions (AVX) – расширение системы команд x86 для микропроцессоров Intel и AMD
CIDR	–	Classless Inter-Domain Routing – бесклассовая адресация
CSV	–	Comma-Separated Values – текстовый формат, предназначенный для представления табличных данных
DNS	–	Domain Name System – компьютерная распределённая система для получения информации о доменах
EB	–	Модуль Ankey SIEM Next Generation Event Broker
EPS	–	Events Per Second – количество событий в секунду
ES	–	Компонент Ankey SIEM Next Generation Events Storage
FQDN	–	Fully Qualified Domain Name – имя домена, не имеющее неоднозначностей в определении
HDD	–	Hard disk drive – запоминающее устройство
HTTP	–	HyperText Transfer Protocol – протокол передачи гипертекста
HTTPS	–	HyperText Transfer Protocol Secure – расширение протокола HTTP в целях повышения уровня безопасности
ILM	–	Information Lifecycle Management – перемещение информации различного рода и ценности в системе хранения данных (СХД) на основании модифицирующихся требований бизнеса к критериям защищенности и доступности информации с учетом ее ценности, актуальности и оптимизации расходов на ее хранение
IOPS	–	Input/output operations per second – количество операций ввода-вывода в секунду

IP	–	Internet Protocol – маршрутизируемый протокол сетевого уровня стека TCP/IP
LDAP	–	Lightweight Directory Access Protocol – протокол прикладного уровня для доступа к службе каталогов X.500, разработанный IETF как облегчённый вариант разработанного ИТУ-T протокола DAP
MC	–	Компонент Ankey SIEM NG VM Management and Configuration
PDQL	–	Язык, разработанный для написания запросов в процессе обработки событий, инцидентов, динамических групп активов и табличных списков в ПК Ankey SIEM NG VM
PEM	–	Privacy Enhanced Mail Certificate – сертификат, зашифрованный в Base64, широко применяемый как формат категории интернет-файлов
RC	–	Компонент Ankey SIEM NG VM Retro Correlator
RDP	–	Remote Desktop Protocol – протокол удалённого рабочего стола
RSA	–	Rivest, Shamir и Adleman – криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел
RTO	–	Recovery Time Objective – допустимое время восстановления данных
SAN	–	Subject Alternative Name – расширение X.509, позволяющее связать различные значения с сертификатом безопасности с помощью поля subjectAltName
SAS	–	Serial Attached SCSI – последовательный компьютерный интерфейс, разработанный для подключения различных устройств хранения данных
SATA	–	Serial ATA – последовательный интерфейс обмена данными с накопителями информации
SCADA	–	Supervisory Control And Data Acquisition – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления

SHA	–	Secure Hash Algorithm – семейство криптографических хеш-функций
SIEM	–	Security information and event management – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности
SMTP	–	Simple Mail Transfer Protocol – сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP
SOC	–	Security operations center – центр управления безопасностью отвечает за защиту организации от киберугроз
SSD	–	Solid-State Driv – компьютерное энергонезависимое немеханическое запоминающее устройство на основе микросхем памяти
SSH	–	Secure Shell – сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений
SSL	–	Secure Sockets Layer – криптографический протокол, который подразумевает более безопасную связь
TCP	–	Transmission Control Protocol – протоколов передачи данных интернета
UDP	–	User Datagram Protocol – протокол транспортного уровня
АСУ ТП	–	Автоматизированная система управления технологическим процессом
БД	–	База данных
ИБ	–	Информационная безопасность
ИТ	–	Информационные технологии
ОЗУ	–	Оперативное запоминающее устройство
ОС	–	Операционная система
ПК	–	Программный комплекс
СУБД	–	Система управления базами данных
ЦС	–	Центр сертификации

Приложение А

Порядок установки ПК Ankey SIEM NG VM

Пример распределения ролей и алгоритма инсталляции по серверам ПК Ankey SIEM NG VM представлен на рисунке А.1.

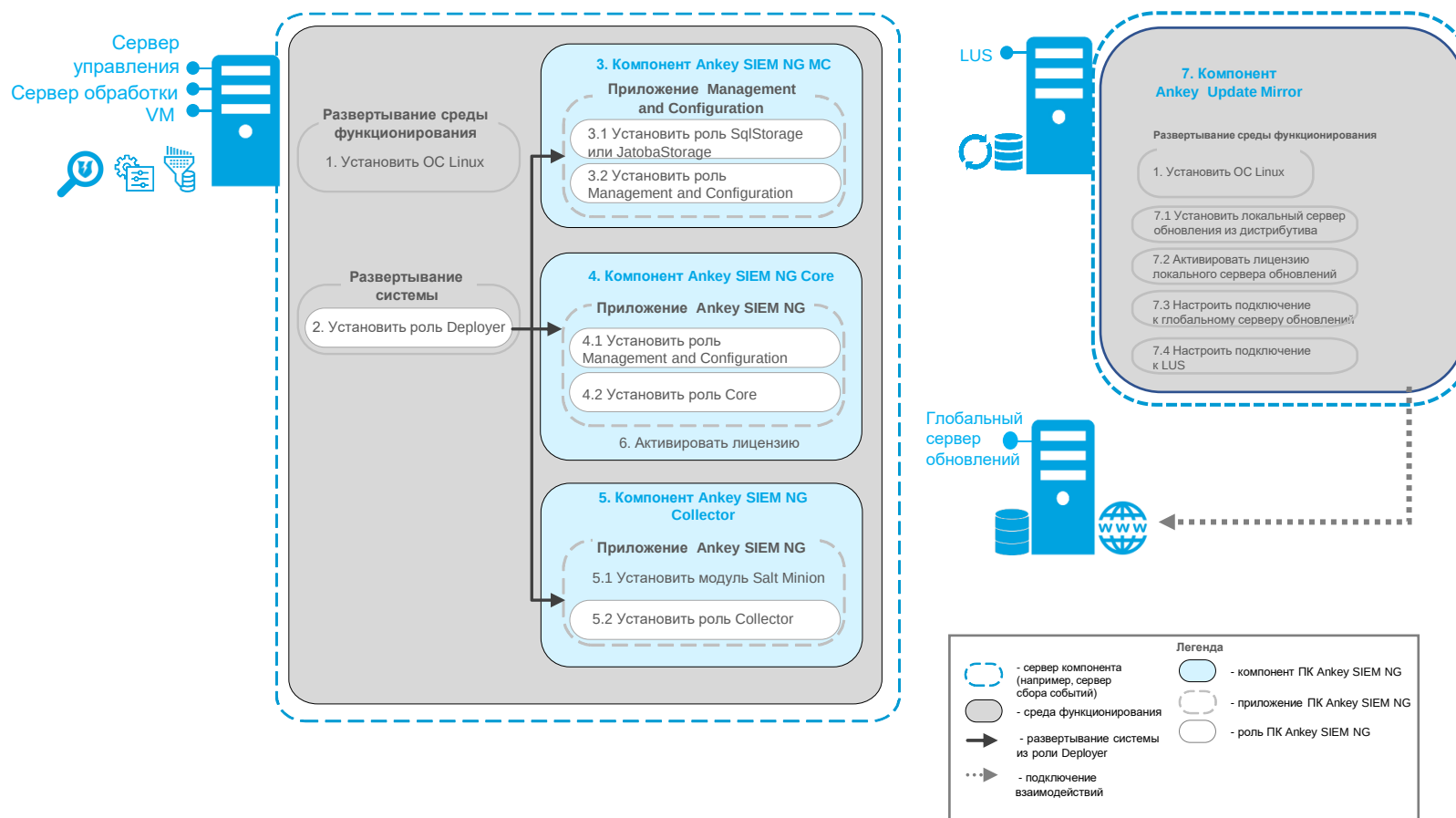


Рисунок А.1 – Алгоритм инсталляции ПК Ankey SIEM NG VM

Приложение Б

Параметры конфигурации компонентов ПК Ankey SIEM NG VM на Linux

В этом приложении приведены описания параметров и их значения по умолчанию.

Таблица Б.1 – Параметры конфигурации роли Deployer

Параметр	Описание	Значение по умолчанию
CustomDockerAddressPool	Подсеть Docker, которую необходимо использовать для Docker-контейнеров вместо подсети по умолчанию	–
CustomDockerNetworkSize	Размер подсети, указанной пользователем в параметре CustomDockerAddressPool	–
HostAddress	IP-адрес или FQDN сервера с установленной ролью Deployer	–
RegistryBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	–
RegistryPort	Номер порта для доступа к локальному реестру Docker-образов	5000

Таблица Б.2 – Параметры конфигурации роли SqlStorage и JatobaStorage

Параметр	Описание	Значение по умолчанию
Параметры конфигурации роли SqlStorage		
CACertificateFileName	Имя файла корневого сертификата	rootCA.crt
CollectorAgentSyslogUdpPort	Порт для прослушивания журналов syslog по протоколу UDP	54528
DockerRegistry	Порт для доступа к реестру Docker-образов	Адрес сервера компонента Ankey SIEM NG Core
EnableFilesLogCollection	Запись журналов в файл вместо их централизованного сбора включена (True) или выключена (False)	False
HostAddress	IP-адрес или FQDN сервера с установленной ролью SqlStorage/JatobaStorage	–
Network	Сетевое имя реестра Docker-образов	storage-network.sqlstorage
NetworkDriver	Драйвер Docker-образов	bridge
PgAdminPort	Порт для доступа к PgAdmin	9001
PgAnalyzeScaleFactor	Доля от числа кортежей в таблице, которая прибавляется к значению параметра PgAnalyzeThreshold при расчете порога срабатывания команды ANALYZE. Например, если значение	0.0

Параметр	Описание	Значение по умолчанию
	PgAnalyzeThreshold равно 200 000, а значение параметра PgAnalyzeScaleFactor равно 0,1, то для таблицы в 1 000 000 кортежей порог срабатывания команды будет $200\,000 + 100\,000 = 300\,000$ кортежей	
PgAnalyzeThreshold	Минимальное число добавленных, измененных или удаленных кортежей, при котором будет выполняться команда ANALYZE для отдельно взятой таблицы	200000
PgEffectiveCacheSize	Эффективный размер дискового кэша, доступный для одного запроса	6GB
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgHardDiskType	Тип используемого оборудования для хранилища (возможные значения – HDD или SSD)	HDD
PgLogLevel	Уровень журналирования работы СУБД PostgreSQL (возможные значения – panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5)	warning
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@sswordP@ssword
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgSharedBufferSize	Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти	4GB
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
PgVacuumNapTime	Минимальная задержка между двумя запусками автоочистки для отдельной базы данных	20min
PgWorkMem	Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске	200MB
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key
Параметры конфигурации роли JatobaStorage		
CACertificateFileName	Имя файла корневого сертификата	rootCA.crt

Параметр	Описание	Значение по умолчанию
CollectorAgentSyslogUdpPort	Порт для прослушивания журналов syslog по протоколу UDP	54528
DockerRegistry	Порт для доступа к реестру Docker-образов	Адрес сервера компонента Ankey SIEM NG Core
EnableFilesLogCollection	Запись журналов в файл вместо их централизованного сбора включена (True) или выключена (False)	False
HostAddress	IP-адрес или FQDN сервера с установленной ролью SqlStorage/JatobaStorage	–
Network	Сетевое имя реестра Docker-образов	storage-network.sqlstorage
NetworkDriver	Драйвер Docker-образов	bridge
PgAdminPort	Порт для доступа к PgAdmin	9001
PgEffectiveCacheSize	Эффективный размер дискового кэша, доступный для одного запроса	6GB
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgHardDiskType	Тип используемого оборудования для хранилища (возможные значения – HDD или SSD)	HDD
PgLogLevel	Уровень журналирования работы СУБД PostgreSQL (возможные значения – panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5)	warning
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@sswordP@ssword
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgSharedBufferSize	Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти	4GB
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
PgWorkMem	Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске	200MB
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key

Таблица Б.3 – Параметры конфигурации роли Management and Configuration

Параметр	Описание	Значение по умолчанию
ActionLogBatchSize	Количество записей о действиях пользователей, которые служба MC Identity and Access Management Service одновременно отправляет службе MC User Action Logging Service	100
ActionLogMillisecondsDelay	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	1000
DefaultLocale	Интерфейс Ankey SIEM NG MC отображается на русском (ru-RU) или английском (en-US) языке	ru-RU
ExpertDataUpdateMethod	Метод получения обновлений экспертных данных. Возможные значения: Online или Offline	—
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG MC	—
IamCookieLifetime	Время жизни неактивной сессии в ПК Ankey SIEM NG VM (в часах)	168
LdapTimeout	Тайм-аут подключения к LDAP-серверу (в миллисекундах)	60000
LogCleanLimit	Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены	1000000
MasterRedirectEnabled	В случае иерархической установки аутентификация пользователя выполняется на главной (флажок установлен) или на локальной (флажок снят) площадке	Флажок снят
PackageManagementPort	Номер порта сервиса управления пакетами Package Management	8585
PackagesSourceCredentialToken	Токен для авторизации на сервере обновлений. Хранится в файле instance-access-token.key и представляет собой набор символов, закодированных с использованием стандарта Base64	—
PackagesSourceUri	Адрес сервера обновлений	—
PostgreHost	IP-адрес или FQDN сервера с установленной ролью SqlStorage или JatobaStorage	—
PostgrePassword	Пароль служебной учетной записи для доступа Ankey SIEM NG MC к СУБД PostgreSQL	P@sswordP@ssword
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Ankey SIEM NG MC	5432

Параметр	Описание	Значение по умолчанию
PostgreUserName	Логин служебной учетной записи для доступа Ankey SIEM NG MC к СУБД PostgreSQL	pt_system
TmSiteAlias	Псевдоним площадки	SITE
TmSiteId	Идентификатор площадки	–
TmTenantManagerId	Идентификатор службы MC Tenant Manager Service	–

Таблица Б.4 – Параметры конфигурации роли Core

Параметр	Описание	Значение по умолчанию
ConsiderEventsImportance	В случае изменения IP-адреса актива система обновляет его конфигурацию сразу (флажок установлен) или по расписанию (флажок снят)	Флажок установлен
ContentDeployerPort	Номер порта сервиса установки обновлений экспертизы Content Deployer	8586
DefaultAssetTtl	Время устаревания активов (<Дни>.<Часы>:<Минуты>:<Секунды>)	90.00:00:00
DefaultLocale	Интерфейс Ankey SIEM NG VM отображается на русском (ru-RU) или английском (en-US) языке	ru-RU
EmailNotificationRetryCount	Максимальное количество попыток отправки сообщения на SMTP-сервер	10
EmailNotificationRetryPeriodSeconds	Период между попытками отправки сообщения на SMTP-сервер (в секундах)	60
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
MCAddress	IP-адрес или FQDN сервера Ankey SIEM NG Management and Configuration	–
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL	P@sswordP@ssword
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Ankey SIEM NG Core	–
PostgreUserName	Логин служебной учетной записи для подключения Ankey SIEM NG Core к СУБД PostgreSQL	pt_system
PtkbDbName	Имя базы знаний, из которой импортируются данные об уязвимостях	–

Параметр	Описание	Значение по умолчанию
PtkbUpdateCheckPeriod	Период проверки наличия обновления для базы знаний, используемой в Ankey SIEM NG Core (<Часы>:<Минуты>:<Секунды>)	00:05:00
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
RMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к RabbitMQ	P@ssword
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Core к RabbitMQ	mpx_core
SendAlertsToSiem	При нарушении и восстановлении контролируемых параметров источников регистрируются соответствующие события (флажок установлен). Если флажок не установлен, события не регистрируются	Флажок не установлен
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpIgnoreCertificateValidation	Ankey SIEM NG Core проверяет (False) или не проверяет (True) валидность сертификата при подключении к SMTP-серверу	True
SmtpPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу	–
SmtpPort	Порт SMTP-сервера для входящих подключений от Ankey SIEM NG Core	25
SmtpSecureSocketOptions	Варианты шифрования при подключении к SMTP-серверу: None – шифрование не используется; Auto – почтовый сервер определяет, использовать ли протокол SSL или протокол TLS. Если сервер не поддерживает протоколы SSL и TLS, то шифрование не используется; SslOnConnect – протоколы SSL или TLS используются при соединении; StartTls – протокол TLS используется после приветствия сервера. Если сервер не поддерживает расширение STARTTLS, соединение прерывается; StartTlsWhenAvailable – протокол TLS используется после приветствия сервера, если сервер поддерживает расширение STARTTLS	Auto

Параметр	Описание	Значение по умолчанию
SmtпSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.com>
SmtпUser	Логин служебной учетной записи для подключения Ankey SIEM NG Core к SMTP-серверу	–
TtlCheckPeriod	Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)	01.00:00:00
UsageMonitoringCheckingPeriod	Период запуска проверок по чек-листу (<Часы>:<Минуты>:<Секунды>)	00:15:00
VulnerStateCheckInterval	Период проверки статусов экземпляров уязвимостей (<Дни>.<Часы>:<Минуты>:<Секунды>)	01.00:00:00
VulnerStateCheckPeriodEnabled	Ankey SIEM NG Core проверяет (флажок установлен) или не проверяет (флажок снят) статусы экземпляров уязвимостей	Флажок установлен
VulnerStateCheckPeriodEnd	Время окончания суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)	01:00:00
VulnerStateCheckPeriodOfRetry	Продолжительность паузы (<Часы>:<Минуты>:<Секунды>) перед повторным запуском проверки, если предыдущий запуск завершился с ошибкой	00:01:00
VulnerStateCheckPeriodStart	Время начала суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)	00:00:00

Таблица Б.5 – Параметры конфигурации роли Collector

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	–
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	–

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	32768M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	—
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentName	Имя коллектора в веб-интерфейсе ПК Ankey SIEM NG VM	FQDN сервера Ankey SIEM NG Collector
AgentRMQHost	IP-адрес или FQDN сервера RabbitMQ.	localhost

Параметр	Описание	Значение по умолчанию
	Примечание. Брокер RabbitMQ устанавливается на сервер Ankey SIEM NG Core и обеспечивает обмен сообщениями между компонентами ПК Ankey SIEM NG VM	
AgentRMQPassword	Пароль служебной учетной записи для подключения Ankey SIEM NG Collector к RabbitMQ	P@ssword
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Collector	5671
AgentRMQUser	Логин служебной учетной записи для подключения Ankey SIEM NG Collector к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_Certificate	Путь к файлу корневого SSL-сертификата	RMQ_Server.crt
Agent_RMQ_SSL_Certificate	Путь к файлу публичного SSL-сертификата	RMQ_Agent_Client.crt
Agent_RMQ_SSL_Enabled	Ankey SIEM NG Collector подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен
Agent_RMQ_SSL_Key	Путь к файлу закрытого ключа SSL-сертификата	RMQ_Agent_Client.key

Таблица Б.6 – Параметры конфигурации роли RMQ Message Bus

Параметр	Описание	Значение по умолчанию
CACertFile	Имя файла корневого сертификата	rootCA.crt
CertFile	Имя файла публичного сертификата	RMQ_Server.crt
HostAddress	IP-адрес или FQDN сервера с установленной ролью RMQ Message Bus	–
KeyFile	Имя файла закрытого ключа сертификата	RMQ_Server.pem
MEMORY_HIGH_WATERMARK_GB	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах). Примечание. Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений	10
RMQAdminPassword	Пароль служебной учетной записи администратора RabbitMQ	P@ssword
RMQAdminUser	Логин служебной учетной записи администратора RabbitMQ	Administrator

Параметр	Описание	Значение по умолчанию
RMQAgentPassword	Пароль служебной учетной записи для доступа коллекторов к RabbitMQ	P@ssword
RMQAgentUser	Логин служебной учетной записи для доступа коллекторов к RabbitMQ	agent
RMQHttpPort	Порт для доступа к RabbitMQ по протоколу HTTP	5672
RMQHttpsPort	Порт для доступа к RabbitMQ по протоколу HTTPS	5671
RMQLogRotateSize	Максимальный размер сохраняемых файлов журналов (G для гигабайтов, M для мегабайтов, K для килобайтов)	50M
RMQPassword	Пароль служебной учетной записи для доступа Ankey SIEM NG Core к RabbitMQ	P@ssword
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для доступа Ankey SIEM NG Core к RabbitMQ	core
RMQ_DISK_FREE_LIMIT	Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах). Примечание. Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений	20
WATERMARK_PAGING_RATIO	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK). Примечание. Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск	0.5

Таблица Б.7 – Параметры конфигурации роли Retro Correlator

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	32768M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	—
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При	—

Параметр	Описание	Значение по умолчанию
	достижении порогового значения коллектор переходит в режим SafeMode2	
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	–
AgentName	Имя коллектора в веб-интерфейсе ПК Ankey SIEM NG VM	FQDN сервера Ankey SIEM NG RC
AgentRMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
AgentRMQPassword	Пароль служебной учетной записи для доступа Ankey SIEM NG RC к RabbitMQ	P@ssword
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от Ankey SIEM NG Collector	5671
AgentRMQUser	Логин служебной учетной записи для доступа Ankey SIEM NG RC к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_Certificate	Путь к файлу корневого SSL-сертификата	rootCA.crt
Agent_RMQ_SSL_Certificate	Путь к файлу публичного SSL-сертификата	RMQ_Agent_Client.crt
Agent_RMQ_SSL_Enabled	Ankey SIEM NG Collector подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен
Agent_RMQ_SSL_Key	Путь к файлу закрытого ключа SSL-сертификата	RMQ_Agent_Client.key
CoreAddress	IP-адрес или FQDN сервера Ankey SIEM NG Core	localhost
CsvSeparator	Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков	;
DefaultLogLevel	Уровень журналирования для служб Ankey SIEM NG RC (возможные значения – fatal, error, warn, info, debug или trace)	info
HostAddress	IP-адрес или FQDN сервера Ankey SIEM NG RC	localhost
InternalRMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
InternalRMQPassword	Пароль служебной учетной записи для доступа к RabbitMQ	P@ssword

Параметр	Описание	Значение по умолчанию
InternalRMQPort	Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG RC при аутентификации с помощью логина и пароля (plain)	5672
InternalRMQPortSSL	Порт сервера RabbitMQ для входящих соединений от Ankey SIEM NG RC при аутентификации с помощью сертификатов безопасности (ssl)	5671
InternalRMQUser	Логин служебной учетной для доступа к RabbitMQ	siem
InternalRMQVirtualHost	Имя виртуального узла RabbitMQ	/
LogCount	Максимальное количество файлов журналов Ankey SIEM NG RC (архивированных и неархивированных)	10
LogPlain	Максимальное количество неархивированных файлов журналов Ankey SIEM NG RC	2
LogSize	Максимальный размер файла журнала Ankey SIEM NG RC (в байтах)	104857600
MaxTableListsSize	Максимальный объем оперативной памяти, выделяемый для хранения табличных списков (в мегабайтах)	8192
RetroControllerHost	IP-адрес для входящих подключений от коллектора на Debian	0.0.0.0

Приложение В

Применение патчей в ПК Ankey SIEM NG (5.2.3)

После установки основных компонентов ПК Ankey SIEM NG VM необходимо ознакомиться с данным разделом и проверить наличие пакетов исправлений (патчей) в текущей версии Системы. Пакеты исправлений включены в дистрибутив ПК Ankey SIEM NG и предназначены для исправления некритичных ошибок текущей версии Системы.

В случае наличия пакетов исправлений, необходимо перейти в папку, содержащую пакет исправлений и выполнить шаги, приведенные в инструкции в формате TXT, которая находится в папке с пакетом исправления.

Пакеты исправлений находятся по пути

<Ankey SIEM NG 5.x.x SR (26.x.xxxxx) >/<Дополнительно> в составе дистрибутива ПК Ankey SIEM NG.

В версии ПК Ankey SIEM NG 5.2.3 (26.2.13166) были добавлены следующие исправления:

1. **Патч для устранения уязвимости обхода аутентификации в Ankey SIEM NG MC**
Данный патч устраняет уязвимость, при использовании которой возможно обойти аутентификацию в Ankey SIEM NG версии 5.2.3 SR (26.2.13166). В случае успешной эксплуатации уязвимости возможно имперсонировать любую учетную запись Ankey SIEM NG MC и получить все возможные привилегии.
2. **Патч для исправления бесконечной перезагрузки службы Topology**
Данный патч исправляет бесконечную перезагрузку службы Topology после обновления Ankey SIEM NG с версии 4.1 SR (25.1.5988) до версии 5.2.3 SR (26.2.13166).
3. **Патч для исправления ошибки при аудите ОС Windows**
Данный патч устраняет ошибку при использовании доменной учетной записи для аудита операционных систем семейства Windows в Ankey SIEM NG 5.2.3 SR (26.2.13166) с помощью компонента Ankey SIEM NG Collector для ОС Linux.