Программный комплекс «Solar Dozor»

Версия 7.12

Руководство по установке и настройке

МОСКВА, 2024

Содержание

Список иллюстраций

Список таблиц

Перечень терминов и сокращений

АРМ	Автоматизированное рабочее место
БД	База данных
ИБ	Информационная безопасность
ИТ	Исключаемый текст
КА	Контентный анализ
ОЕ	Организационная единица
ОС	Операционная система
ПО	Программное обеспечение
ПК	Программный комплекс
СХД	Система хранения данных
Solar webProxy	Модуль контроля веб-трафика
СУБД	Система управления базами данных
УЗ	Учетная запись (пользователя)
УЦ	Удостоверяющий центр
ФХ	Файловое хранилище
ЦП	Центральный процессор – электронный блок либо интегральная схема, исполняющая машинные инструкции, главная часть аппаратного обеспечения компьютера или программируемого логического контроллера
ЭЦП	Электронная цифровая подпись
AD	Active Directory – служба каталогов для операционных систем семейства Windows. В каталоге хранятся сведения о различных объектах сетей, например, о компьютерах и учетных записях их пользователей. С помощью AD можно использовать групповые политики для единообразия настройки пользовательской рабочей среды и развертывания программного обеспечения на множестве компьютеров
CEF	Common Event Format – общий формат события
CLI	Command Line Interface – интерфейс командной строки
CRL	Certificate Revocation List – список отозванных сертификатов
DC	Domain controller — контроллер домена
DHCP	Dynamic Host Configuration Protocol – протокол динамической настройки узла
FQDN	Fully Qualified Domain Name – полное имя домена (имя домена, не имеющее неоднозначностей в определении)
GUI	Graphical User Interface – графический интерфейс пользователя
MD	Обозначение используется на рисунках и помечает элемент управления, отображаемый при наличии в системе модуля Мультидозор
MIME	Multipurpose Internet Mail Extension – многоцелевое расширение Интернет-почты
PID	Product Identifier – Идентификатор модели устройства

RFC	Request for Comments – спецификации и стандарты, применяемые в Интернет
SMB	Server Message Block – сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SMTP	Simple Mail Transfer Protocol – простой протокол передачи почты
TNEF	Transport Neutral Encapsulation Format – собственный формат вложений электронной почты, используемый Microsoft Outlook и Microsoft Exchange Server
TTS	Transportable Tablespaces – транспортируемые (перемещаемые) табличные пространства
VID	Vendor Identifier – Идентификатор производителя
Кластер	Совокупность серверов Solar Dozor, соединённых между собой управляющими связями.
master-узел	Управляющий (главный) сервер кластера Solar Dozor, непосредственно связанный с каждым из остальных.
slave-узел	Любой узел кластера Solar Dozor, не являющийся управляющим.

Использование стилей

Шрифт без форматирования	Основной текст
Моноширинный шрифт	Пользовательский ввод
Рамка	Программный вывод на экран
Курсивный шрифт	Наименования документов
Полужирный подчёркнутый фиолетовый шрифт	Внутренняя ссылка
Полужирный шрифт	Наименование элементов интерфейса

1. Введение

1.1. Назначение документа

В настоящем руководстве описаны задачи, возникающие при развёртывании ПК «Solar Dozor» (далее – Solar Dozor), а также способы и примеры их решения в ряде стандартных сценариев.

1.2. Аудитория

Документ предназначен для системных и сетевых администраторов, а также для сотрудников службы информационной безопасности компаний, внедряющих Solar Dozor.

2. О системе Solar Dozor

Программный комплекс «Solar Dozor» – это система контроля корпоративных коммуникаций класса Data Leak Prevention (DLP), с помощью которой можно выявлять и блокировать несанкционированную передачу данных с компьютеров, а также определять признаки корпоративного мошенничества.

К основным функциональным возможностям Solar Dozor относятся:

- контроль каналов утечки данных (электронной почты, социальных сетей, мессенджеров и т. п.);
- контроль использования сетевых ресурсов сотрудниками;
- отслеживание и ограничение движения потоков информации;
- отслеживание и блокирование сетевых коммуникаций сотрудников;
- сбор, анализ и хранение сообщений о фактах передачи информации (при этом обеспечивается анализ содержимого сообщений и документов); выявление документов определённой структуры и содержания; сравнение текстовых, графических и табличных документов с заранее заданными эталонными документами; распознавание в текстах сообщений определенных последовательностей – ИНН, номеров паспортов и т. д.;
- сбор, систематизация и хранение данных о сотрудниках (ведение досье на каждого сотрудника);
- сбор, систематизация и хранение данных о местонахождении материалов, содержащих конфиденциальную информацию, и о сотрудниках, имеющих к доступ к ним;
- поддержка процессов работы сотрудников службы безопасности (создание и настройка правил передачи и хранения информации; мониторинг событий и инцидентов; отслеживание действий сотрудников; назначение сотрудников, ответственных за разбор инцидентов; получение статистических отчетов);
- учет и контроль рабочего времени сотрудников;
- поддержка проведения расследований инцидентов информационной и экономической безопасности (поиск данных, выявление рабочих и личных контактов сотрудников; автоматический анализ сетевой активности каждого сотрудника; подсказка следующих шагов в процессе расследования).

3. Условия эксплуатации

3.1. Требования к квалификации персонала

Квалификация системного администратора Solar Dozor должна быть достаточной для выполнения задач по обслуживанию системы, обеспечивающих бесперебойное функционирование всех её компонентов.

К задачам системного администратора Solar Dozor относятся:

- настройка компонентов Solar Dozor;
- мониторинг процессов системы;
- управление подсистемой архивирования;
- реагирование на служебные уведомления системы.

Требования к квалификации системного администратора Solar Dozor:

- знания и навыки администрирования ОС Linux и СУБД PostgreSQL;
- понимание особенностей работы Solar Dozor;
- понимание работы сетевых протоколов;
- базовые знания языка PL/SQL;
- знания в области безопасности ОС класса UNIX.

В своей работе системные администраторы Solar Dozor должны использовать документацию по обслуживанию Solar Dozor и документацию по ОС Linux и СУБД PostgreSQL.

3.2. Требования к АРМ администратора

3.2.1. Аппаратное обеспечение

АРМ системного администратора Solar Dozor должно быть оборудовано персональным компьютером с подключением к интернету. Минимально рекомендованные характеристики оборудования:

- Объем свободной оперативной памяти – не менее 4 ГБ после загрузки браузера.
- Разрешение экрана при работе с GUI от 1600x900.

АРМ системного администратора Solar Dozor должно иметь терминальный доступ к master-узлу Solar Dozor.

3.2.2. Программное обеспечение

В состав ПО компьютера для АРМ системного администратора Solar Dozor должен входить браузер. Гарантируется корректная работа GUI Solar Dozor в браузерах Google Chrome, Mozilla Firefox, Yandex, Edge и Atom актуальных версий. В других браузерах работа GUI Solar Dozor невозможна.

Для корректной работы GUI Solar Dozor необходимо в настройках браузера разрешить выполнение **javascript** и сохранение файлов **cookies**. Кроме того, рекомендуется отключить сторонние расширения браузера, поскольку некоторые расширения могут негативно влиять на работу Solar Dozor.

Внимание!

Рекомендуется использовать настройки размера шрифта и масштаба экрана по умолчанию, поскольку изменение этих настроек может привести к искажению дизайна и некорректной работе GUI Solar Dozor.

4. Планирование установки Solar Dozor

4.1. Варианты установки

Solar Dozor имеет три варианта установки:

- **Одномашинная конфигурация** – все функции Solar Dozor выполняются одним физическим сервером.
- **Распределённая конфигурация** – функции Solar Dozor выполняются несколькими серверами. Такая конфигурация позволяет равномерно распределять нагрузку между серверами и достигать таким образом большей производительности. Количество серверов может быть увеличено в любой момент эксплуатации Solar Dozor без его остановки. Распределённая конфигурация (кластер) Solar Dozor имеет топологию «звезда», то есть один из узлов (главный) непосредственно связан с каждым из остальных (подчинённые узлы).
- **Территориально-распределённая конфигурация** (модуль **Мультидозор**) – функции Solar Dozor выполняются несколькими серверами в территориально-распределенной организации. Такая конфигурация используется, когда функции Solar Dozor выполняются серверами в подкластерах. Количество серверов может быть увеличено в любой момент эксплуатации модуля **Мультидозор** без его остановки. Территориально-распределённая конфигурация (кластер и подкластеры) Solar Dozor имеет топологию «звезда», то есть один из узлов (главный узел кластера) непосредственно связан с каждым из остальных (подчинённые узлы кластера и подкластеров).

В одномашинной конфигурации сервер Solar Dozor является главным узлом. Здесь и далее главный узел будет называться master-узлом, а подчинённые – slave-узлами.

4.2. Режимы перехвата почтового потока

Перехват почтовых сообщений в Solar Dozor осуществляется в одном из трех режимов:

- Пассивный режим – серверы Solar Dozor не препятствуют ни передаче почтовых сообщений внутри корпоративной сети, ни почтовому потоку между корпоративной сетью и внешним миром. В этом режиме на почтовых серверах организации настраивается ответвление почтового потока на сервер (серверы) Solar Dozor для дальнейшего анализа и хранения. Процедура настройки ответвления почтового потока подробно описана в разделе **Приложение В, *Ответвление сообщений с почтовых серверов***.

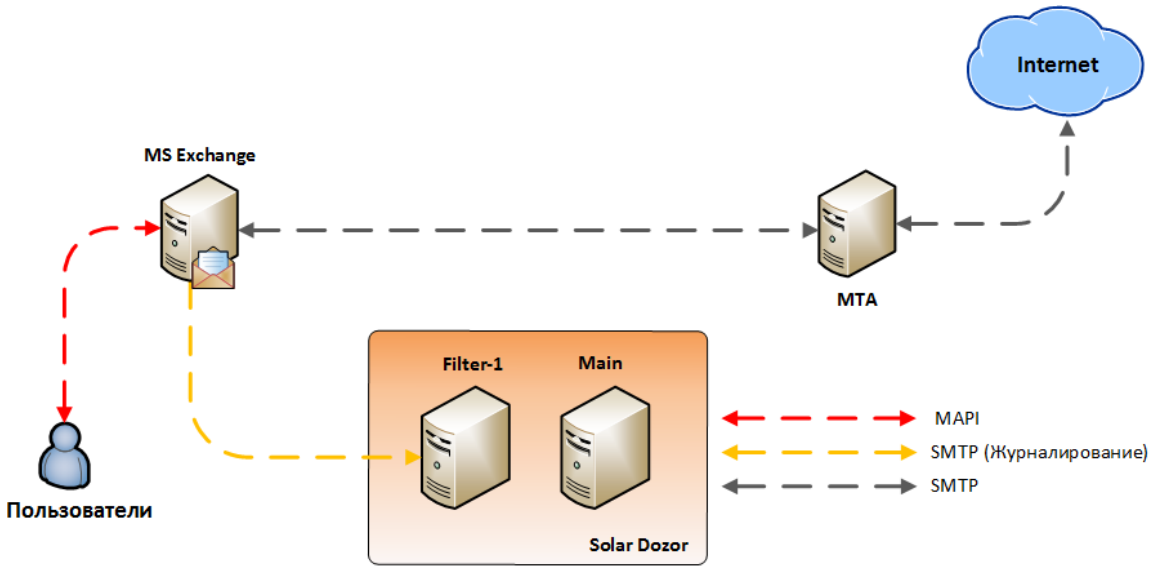


Рис. 4.1. Схема подключения Solar Dozor в пассивном режиме

- Активный режим – серверы Solar Dozor не препятствуют передаче почтовых сообщений внутри корпоративной сети, но создают барьер на пути почтового потока между корпоративной сетью и внешним миром. В этом режиме становится возможным активный контроль передачи почтовых сообщений в соответствии с заданными критериями вплоть до полной их блокировки. Активный режим требует включения сервера (серверов) Solar Dozor в разрыв между почтовым сервером организации и почтовым шлюзом.

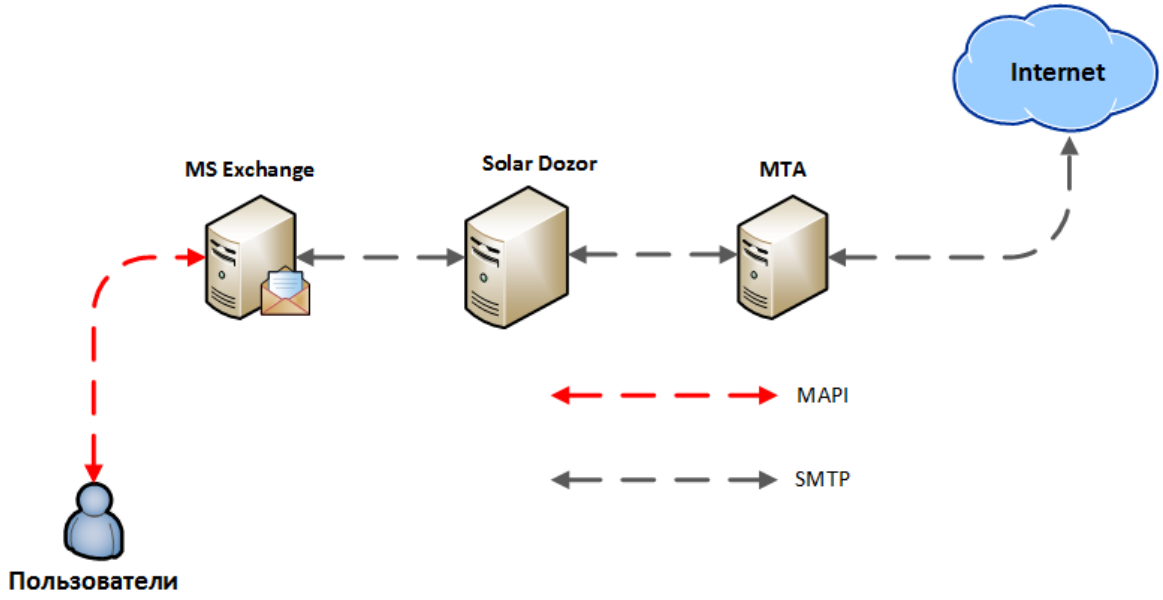


Рис. 4.2. Схема подключения одномашинной конфигурации Solar Dozor в активном режиме

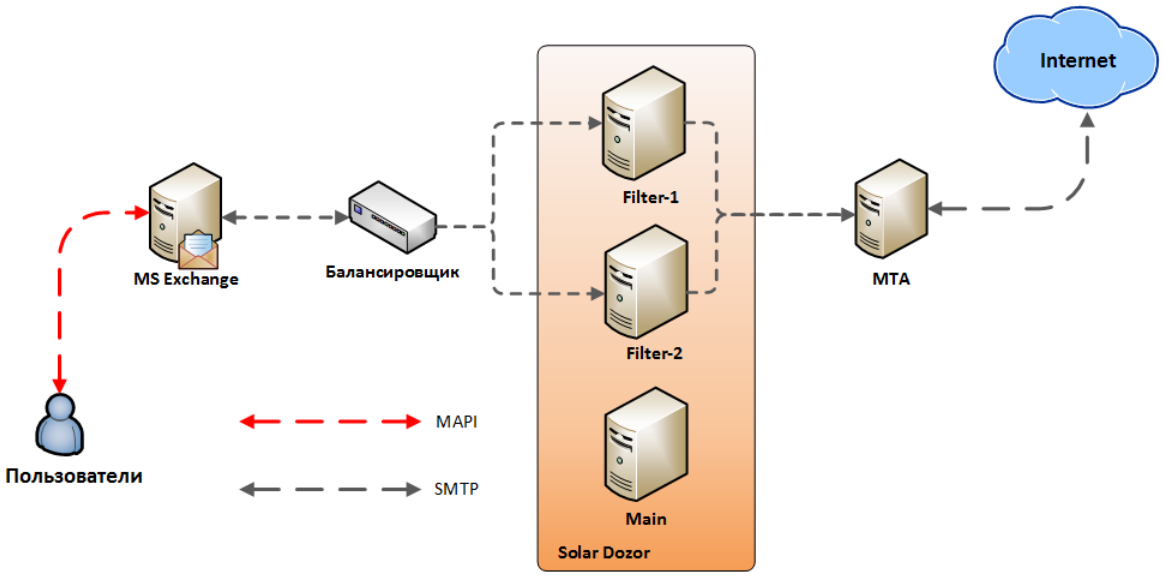


Рис. 4.3. Схема подключения распределённой конфигурации Solar Dozor в активном режиме

Для работы распределённой конфигурации в активном режиме требуется наличие балансировщика нагрузки на серверы фильтрации. Функции балансировщика могут быть реализованы как с помощью специального аппаратного обеспечения, так и с помощью программных настроек почтового сервера организации.

- Гибридный режим – на пути почтового потока между корпоративной сетью и внешним миром создаётся барьер лишь для одного направления (например, исходящая почта), а другое направление контролируется в пассивном режиме. В гибридном режиме наличие балансировщика требуется только в случае, когда барьер на активно контролируемом направлении создан двумя или более серверами.

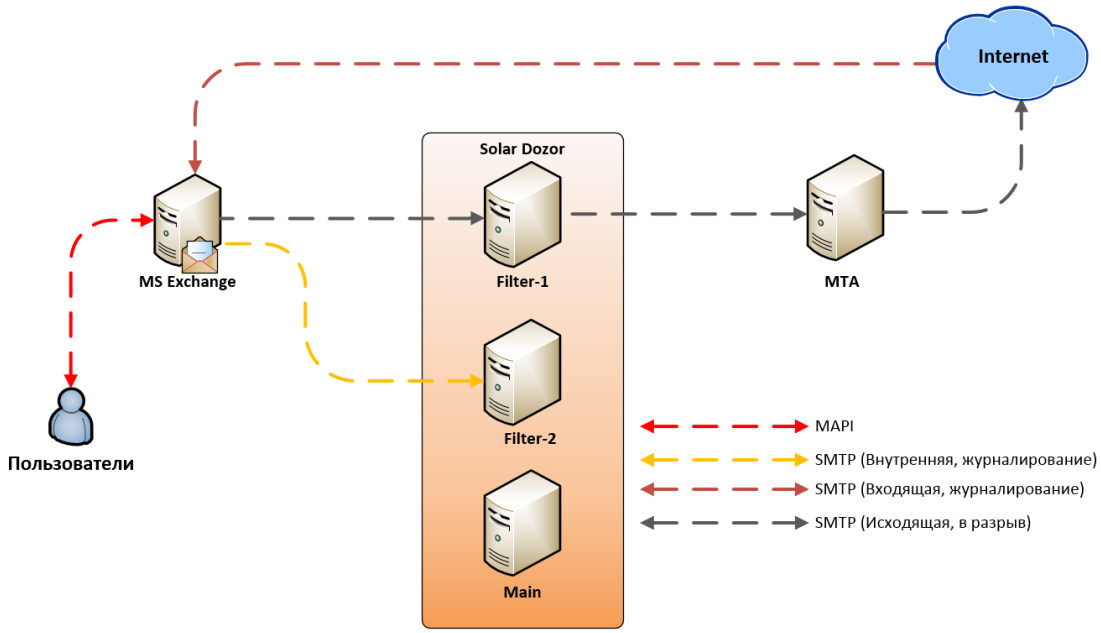


Рис. 4.4. Схема подключения Solar Dozor в гибридном режиме

4.3. Выбор схемы развертывания

Не рекомендуется использовать одномашинную конфигурацию при большом объёме почтового трафика (более 10 ГБ в сутки), так как при этом возрастает риск аварийной остановки Solar Dozor в случае сбоев при фильтрации почтовых сообщений. Следует использовать распределённую конфигурацию, в которой задачи фильтрации ложатся на slave-узлы, а master-узел освобождён от них. Если в организации существуют требования к отказоустойчивости, предполагающие безостановочную работу Solar Dozor, рекомендуется использование двух или более slave-узлов в качестве почтовых фильтров, так как в этом случае аварийная остановка одного из них не приводит к прекращению фильтрации в целом.

Активный (гибридный) режим используется если существует необходимость контролировать передаваемые данные в реальном времени, например, если внутри корпоративной сети имеются высокочувствительные к разглашению сведения.

В любой конфигурации Solar Dozor существует возможность горизонтального масштабирования. Кластер Solar Dozor в любой момент может быть дополнен любым количеством серверов, при этом нет необходимости в остановке работающих узлов кластера.

4.4. Рекомендации по размещению в сетевой инфраструктуре

Настоятельно рекомендуется размещать кластер Solar Dozor в отдельной подсети, в которую нет доступа из других корпоративных подсетей. Системные администраторы и администраторы безопасности должны иметь доступ к веб-интерфейсу master-узла по протоколу HTTPS, системные администраторы должны дополнительно иметь доступ к master-узлу по протоколу SSH.

Схема верхнего уровня взаимодействия Solar Dozor с внешними системами представлена на Рис.4.5. Синим цветом обозначены сервисы Solar Dozor, белым – внешние сервисы корпоративной сети, зелёным – ресурсы сети Интернет.

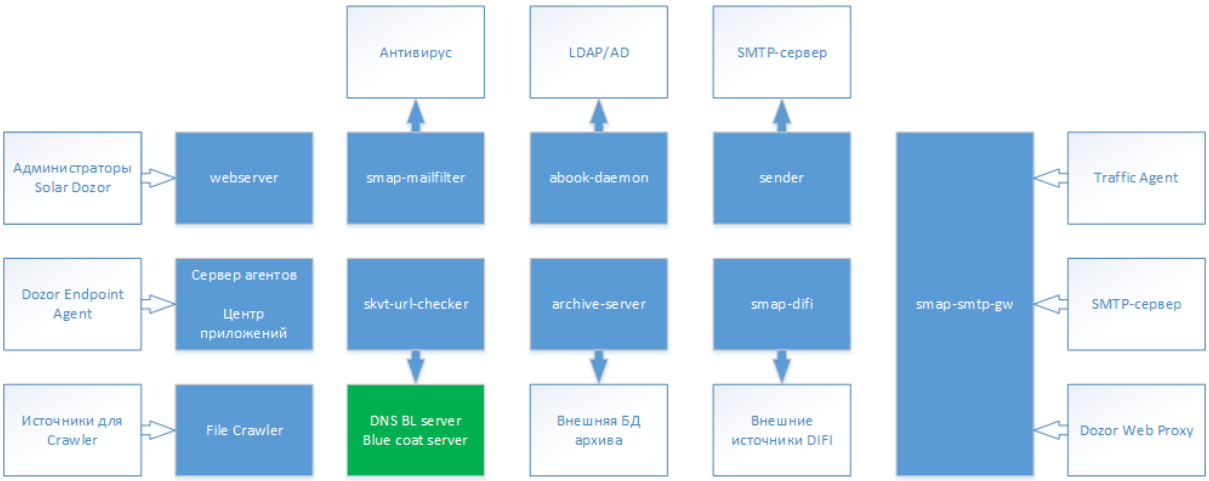


Рис. 4.5. Взаимодействие Solar Dozor с внешними системами

Пример взаимодействия сервисов и утилит Solar Dozor по обеспечению функционирования модуля Dozor Endpoint Agent представлен на Рис.4.6.

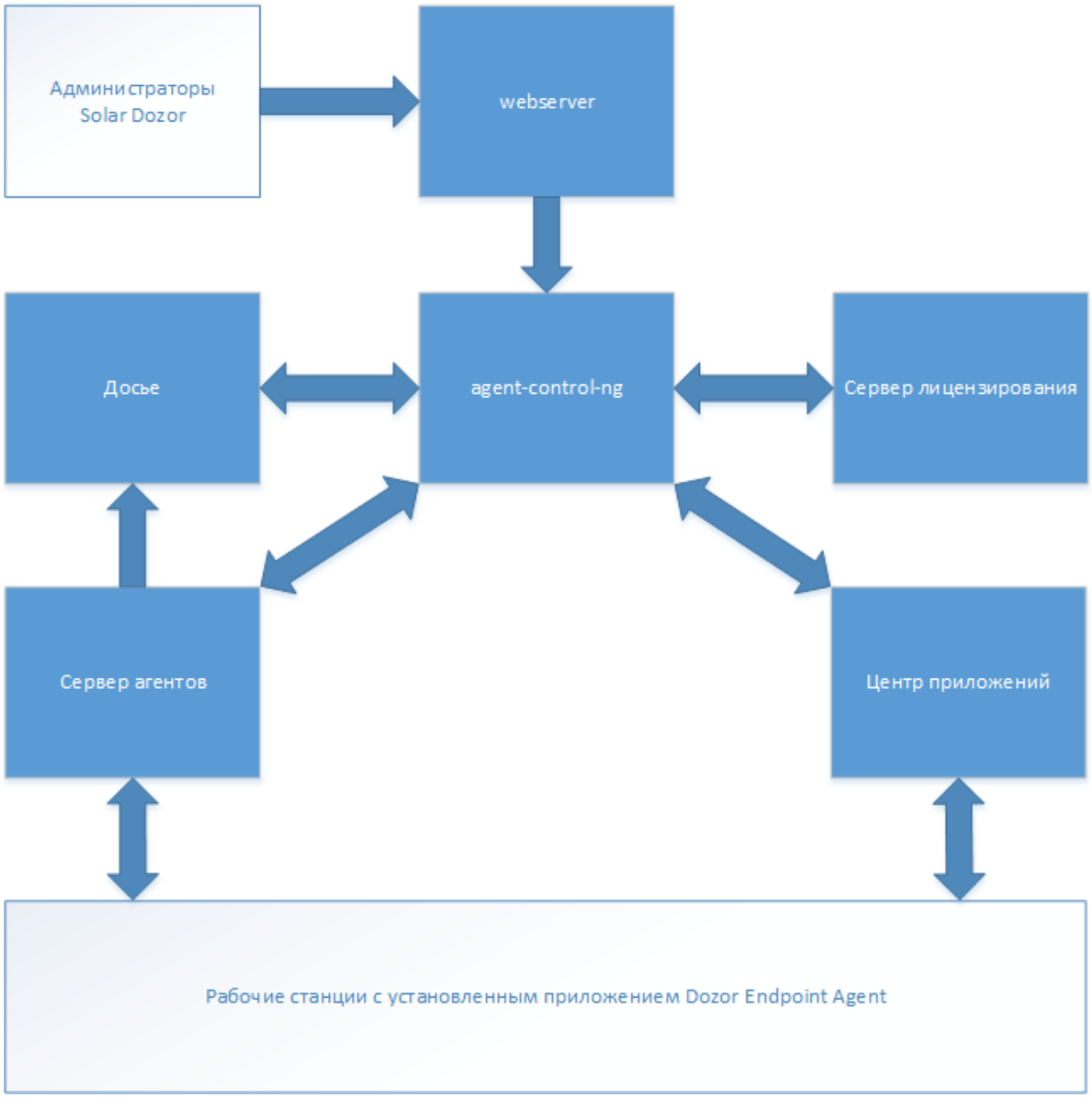


Рис. 4.6. Взаимодействие Dozor Endpoint Agent с Solar Dozor

В Табл.4.1 приведено описание взаимодействия сервисов и утилит Solar Dozor с указанием портов, назначенных по умолчанию. Все сервисы используют протокол TCP.

Внимание!

При обновлении с предыдущих версий используемые порты автоматически не меняются, даже если был установлен порт по умолчанию, и в новой версии он отличается от порта в старой. В этом случае следует обратиться к документации на изначально установленную версию.

Табл. 4.1. Описание портов, используемых по умолчанию

Порт	Сервисы		Описание
	откуда	куда	
22	АРМ администратора	Узлы Solar Dozor	Удалённое администрирование
22	Узлы Solar Dozor	Узлы Solar Dozor	Взаимодействие узлов Solar Dozor между собой
80	monitor-httpd	monitor-httpd	Веб-сервер подсистемы мониторинга
389	abook-sync abook-daemon agent-control-ng monitor-ng	Контроллеры домена, серверы LDAP	Отображение данных пользователей и рабочих станций из домена Active Directory в системе Solar Dozor
443	АРМ администратора	webserver	Организация точки входа в веб-интерфейс администратора
1010	mailfilter	HAProxy	Взаимодействие с внешним балансировщиком
1025	sender Почтовый сервер	smap-smtp-gw	Ответвление почтового трафика в Solar Dozor
1344	mailfilter Прокси-серверы	Антивирус tragent	Прием запросов на поиск вирусов по протоколу ICAP от узла с ролью **Фильтр почтового потока** Прием запросов по протоколу ICAP от ICAP-прокси
2214	ds-bus-rc	Узлы Solar Dozor	Распределенное управление кластером Solar Dozor
2266	archive-server	filestorage-ng	Извлечение сообщений из файлового хранилища
2266	abook-daemon	filestorage-ng	Прикрепление сохранённых файлов к карточке персоны
2266	filestorage-ng	filestorage-ng	Перенос сообщений из локального файлового хранилища в центральное файловое хранилище
2269	webserver	abook-daemon	Работа с Досье (просмотр и редактирование)
2269	agent-control-ng	abook-daemon	Получение информации о пользователях для привязки к АРМ
2269	agent-server	abook-daemon	Получение информации об активности персон (контроль рабочего времени)
2269	mailfilter archive-server crawler-ccc report-server abook-daemon (slave)	abook-daemon	Получение информации о персонах для использования в политике фильтрации. Перенос информации о персонах и группах в архив для использования в поиске и для индексации.
2272	webserver	incident-daemon	Работа с инцидентами (просмотр и редактирование)
2344	mailfilter	Антивирус	Прием запросов на поиск вирусов по протоколу ICAP от узла с ролью **Фильтр почтового потока**
3000	archiver	archive-server	Помещение сообщений в архив

Порт	Сервисы		Описание
	откуда	куда	
3000	webserver	archive-server	Получение сообщений из архива
3001	webserver	action-server	Выполнение действий над сообщениями
3002	webserver mailfilter	category-server	Проверка принадлежности текстов категориям (антиспам)
3003	agent-server webserver	agent-media-server	Помещение медиаинформации в хранилище
3004	webserver mailfilter ocr-server crawler-ccc agent-control-ng	license-server	Получение информации о лицензии
3006 (master)	agent-server	agent-control-ng	Передача данных об агентах серверу управления endpoint-серверами
3010	tragent	mailfilter	Прием сообщений от узла с ролью **Сервис перехвата и анализа сетевого трафика**
3012	agent-server	media-processor-action-server	Прием запросов от сервера агентов на создание задач по распознаванию текста медиаданных и выдача их результатов
3023	mailfilter	ocr-server	Проверка актуальности лицензии движка ContentReader Engine
3030	webserver	uba-server	Подключение к сервису **uba-server** из веб-интерфейса
3268	abook-sync abook-daemon agent-control-ng monitor-ng	Контроллеры домена, серверы LDAP	Отображение данных пользователей и рабочих станций из домена Active Directory в системе Solar Dozor
3900	webserver	grafana	Прием соединений от сервера веб-интерфейса
4444	agent	agent-server	Сервис обслуживания Endpoint Agent
5434	abook-sync action-server abook-daemon webserver report-server agent-control-ng software-center	database	Доступ сервисов к БД политики
5439	crawler-ccc crawler-pccc crawler-snapshot	crawler-database	Доступ Crawler (Краулера) к БД PostgreSQL
5440	action-server	action-server-database	Доступ сервера действий к БД PostgreSQL

Порт	Сервисы		Описание
	откуда	куда	
5441	software-center	БД PostgreSQL	Доступ центра приложений к своей БД
5442	media-processor-action-server	media-processor-action-server-database	Доступ сервера действий по обработке медиаданных к своей БД PostgreSQL
5445	archive-server	Узел, на котором была создана схема БД архива	Доступ сервера архива к БД PostgreSQL
5558	webserver	monitor-ng	Проверка соединений, заданных в конфигурации
7001	skvt-cassandra Все узлы кластера	skvt-cassandra	Поиск информации на серверах Cassandra различных узлов системы. Для корректной работы Cassandra в кластере необходимо, чтобы этот порт был открыт в firewall
7199	skvt-cassandra Все узлы кластера	skvt-cassandra	Внутренний мониторинг при запуске диагностических утилит
7837	archive-server	indexer-ng	Уведомления о новых и изменённых сообщениях в БД архива
7837	webserver	indexer-ng	Получение информации о сообщениях в БД архива
8008	webserver	smap-request-handler	Обработка запросов администратора безопасности
8080	crawler-processor crawler-scanner	crawler-ccc	Получение экземпляров задач от CCC сервиса
8090	crawler-ccc	crawler-pccc	Обмен информацией между CCC и PCCC
8090	webserver	crawler-pccc	Подключение к сервису PCCC из веб-интерфейса
8123	webserver	clickhouse	Прием запросов сервисом clickhouse из веб-интерфейса
8445	webserver-local	webserver	Подключение локальных веб-серверов к основному
9000	webserver	report-server	Получение информации об отчётах
9001	Узлы Solar Dozor	clickhouse	Выборка данных из БД Clickhouse
9042	filestorage-ng	skvt-cassandra	Доступ к индексу ФХ
9042	ocr-server	skvt-cassandra	Кэширование результатов распознавания
9090	Сервер Cisco Webex	imcrawler	Передача сообщений Webex на анализ в Solar Dozor
9160	filestorage-ng ocr-server	skvt-cassandra	Обмен информацией с узлами, входящими в кластер Cassandra
9200	webserver	smap-elasticsearch	Внешний поисковый индексатор elasticsearch. Принимает запросы от веб-интерфейса на поиск слов в базе данных поисковой машины Elasticsearch (внешний индекс)
9200	action-server archive-server	smap-elasticsearch	Закладка новых индексов сообщений в Elasticsearch
9201	indexer-ng	smap-elasticsearch	Управление кластером поисковой машины elasticsearch (внешний индекс)
9201	incident-daemon webserver	smap-elasticsearch	Закладка новых индексов инцидентов в Elasticsearch

Порт	Сервисы		Описание
	откуда	куда	
	report-server		
9301	mailfilter webserver	difi	Взаимодействие с сервером проверки по алгоритму цифровых отпечатков в распределённой среде (при наличия соответствующего модуля)
9302	mailfilter webserver	idid	Взаимодействие с сервером проверки по алгоритму цифровых идентификаторов (IDID) в распределённой среде (при наличия соответствующего модуля)
9303	mailfilter webserver	god-server	Взаимодействие с сервером распознавания графических объектов (god-server) в распределённой среде (при наличия соответствующего модуля)
9400	Агенты	Центр приложений	Передача статуса агента
9400	agent-control-ng	Центр приложений	Управление задачами развертывания агентов
9401	Сервер управления Dozor Endpoint Agent	Центр приложений	Получение состояния Агентов от узла с ролью **Центр приложений**
9666	crawler-scanner	crawler-snapshot	Взаимодействие с сервисом отпечатков для получения и отправки информации
9998	mailfilter webserver	smap-tikaserver	Извлечение текстов, распаковка офисных документов, определение кодировок в распределенной среде
10000	mailfilter	ocr-server	Обращения за распознаванием текста изображений
10050	monitor-agent	monitor-server	Прием сервером мониторинга информации о статистических показателях
10051	monitor-agent	monitor-server	Прием сервером мониторинга информации о статистических показателях
11000	media-processor-action-server	media-processor-ocr-server	Обращения за распознаванием текста медиаданных (например, снимков демонстрации экрана)
11344	Прокси-серверы	tragent	Прием запросов по протоколу ICAPS от ICAP-прокси
16379	mailfilter archive-server filestorage-ng indexer-ng ocr-server smap-smtp-gw	smap-redis	Хранение счетчиков
33033	Внешний клиент	api-gateway	Передача запросов от внешнего клиента к сервису интеграции
61616	crawler-processor crawler-scanner	activemq	Обмен данными между сканером и обработчиком Хранение очередей

Примечание

Если в конфигурации Solar Dozor меняется какой-либо порт, необходимо поменять и разрешающее правило.

Внимание!

- *Порт 22 должен быть открыт на всех узлах Solar Dozor – используется для доступа к CLI по протоколу SSH, а также для синхронизации конфигурации между узлами с использованием учетной записи **dozor**.*
- *Порт 443 должен быть открыт на master-узле, и на всех узлах, где предполагается использование локального веб-сервера – используется для доступа к GUI с помощью браузера.*
- *Порт 80 должен быть открыт на master-узле – используется для службы мониторинга.*

Внимание!

Ни один сторонний сервис на узлах кластера Solar Dozor не должен использовать порт 8443 (зарезервирован для веб-сервера).

4.5. Требования к серверам Solar Dozor

Ниже описаны требования, предъявляемые к оборудованию серверов Solar Dozor в зависимости от выбранной схемы развёртывания и статистики трафика внутри организации. Предполагается, что система хранения данных (СХД), содержащая БД архива почтовых сообщений, примонтирована к файловой системе master-узла. Под процессором понимается виртуальный процессор (технология Hyper-treading) при тактовой частоте физического процессора не ниже 2.1 ГГц. Срок хранения данных в архиве считается равным одному году. Требования к СХД прямо и линейно пропорциональны сроку хранения данных в архиве, остальные требования не зависят от него.

Рекомендуемые характеристики аппаратного обеспечения СХД:

- Количество операций ввода-вывода в секунду (IOPS) – не менее 2000. IOPS может быть увеличен за счёт использования большего количества жёстких дисков меньшей ёмкости при сохранении общего объёма СХД.
- Технология виртуализации данных – RAID 10 или RAID 6.
- Интерфейс подключения жёстких дисков – SAS. Скорость вращения шпинделя – 10k или выше.
- Для хранения индексов Elasticsearch по возможности выделить диски SSD.

Внимание!

Приведённые ниже значения рассчитаны на обеспечение работоспособности Solar Dozor без использования модулей Traffic Analyzer, Dozor File Crawler, OCR, Endpoint Agent, UBA и модуля распознавания графических объектов. Для получения значений, достаточных для использования одного или нескольких из этих модулей, следует обратиться в службу технической поддержки поставщика ПО Solar Dozor.

4.5.1. Требования к одномашинной конфигурации

Табл. 4.2. Требования к серверу Solar Dozor

СХД, ТБ/год	Оперативная память, ГБ	Число процессоров (vCPU)	СУБД архива
1 ГБ в сутки			
1	32	8	PostgreSQL
5 ГБ в сутки			
4	72	20	PostgreSQL
10 ГБ в сутки			
7	80	28	PostgreSQL

4.5.2. Требования к распределённой конфигурации

Требования, предъявляемые к master-узлу в распределённой конфигурации, не зависят от выбранного режима (активного или пассивного), то есть предполагается, что задачи фильтрации почтовых сообщений решаются исключительно slave-узлами. Требования к СХД являются суммарными по всему кластеру Solar Dozor, а не отдельными для каждого узла. Требования с использованием символа **+** означают, что для фильтрации указанного объёма суточного трафика настоятельно рекомендуется использование двух или более slave-узлов.

Табл. 4.3. Требования к оборудованию master-узла кластера Solar Dozor

СХД, ТБ/год	Оперативная память, ГБ	Число процессоров (vCPU)	Дисковое пространство, ГБ
1 ГБ в сутки			
1	32	8	300
5 ГБ в сутки			
4	40	8	300
10 ГБ в сутки			
7	40	8	300
20 ГБ в сутки			
14	64	10	300
40 ГБ в сутки			
30	96	10	300

Табл. 4.4. Требования к оборудованию slave-узлов кластера Solar Dozor

Оперативная память, ГБ	Число процессоров (vCPU)	СУБД архива	Дисковое пространство, ГБ
1 ГБ в сутки			

Оперативная память, ГБ	Число процессоров (vCPU)	СУБД архива	Дисковое пространство, ГБ
32	8	PostgreSQL	300
5 ГБ в сутки			
32	8	PostgreSQL	300
10 ГБ в сутки			
40	20	PostgreSQL	300
20 ГБ в сутки			
40 + 40	16 + 16	PostgreSQL	300
40 ГБ в сутки			
48 + 48	24 + 24	Oracle	300

4.6. Требования к инфраструктуре

Для поддержания нормальной работоспособности Solar Dozor, инфраструктура корпоративной сети должна соответствовать следующим требованиям:

- Наличие DNS-сервера и сервера точного времени.
- Сеть должна пропускать трафик между компонентами Solar Dozor в соответствии с матрицей доступа (подробнее см. раздел 4.4).
- Пропускная способность сетевых интерфейсов серверов системы не менее 100 Мбит/с.

4.7. Необходимое ПО для установки

Для установки Solar Dozor необходимо наличие следующего ПО:

- дистрибутив ОС Alt Linux версии 10.1 или 10.2;
- SSH-клиент;
- лицензия на Solar Dozor.

Также необходимо наличие локальной копии дистрибутива ОС или наличие доступа к официальному репозиторию ОС.

5. Установка ОС

Для установки ОС Alt Linux 10.1 необходимо запустить сервер с использованием установочного диска или USB-носителя и выполнить следующие действия:

1. Выбрать язык инсталлятора по усмотрению. Далее предполагается, что выбран русский язык.

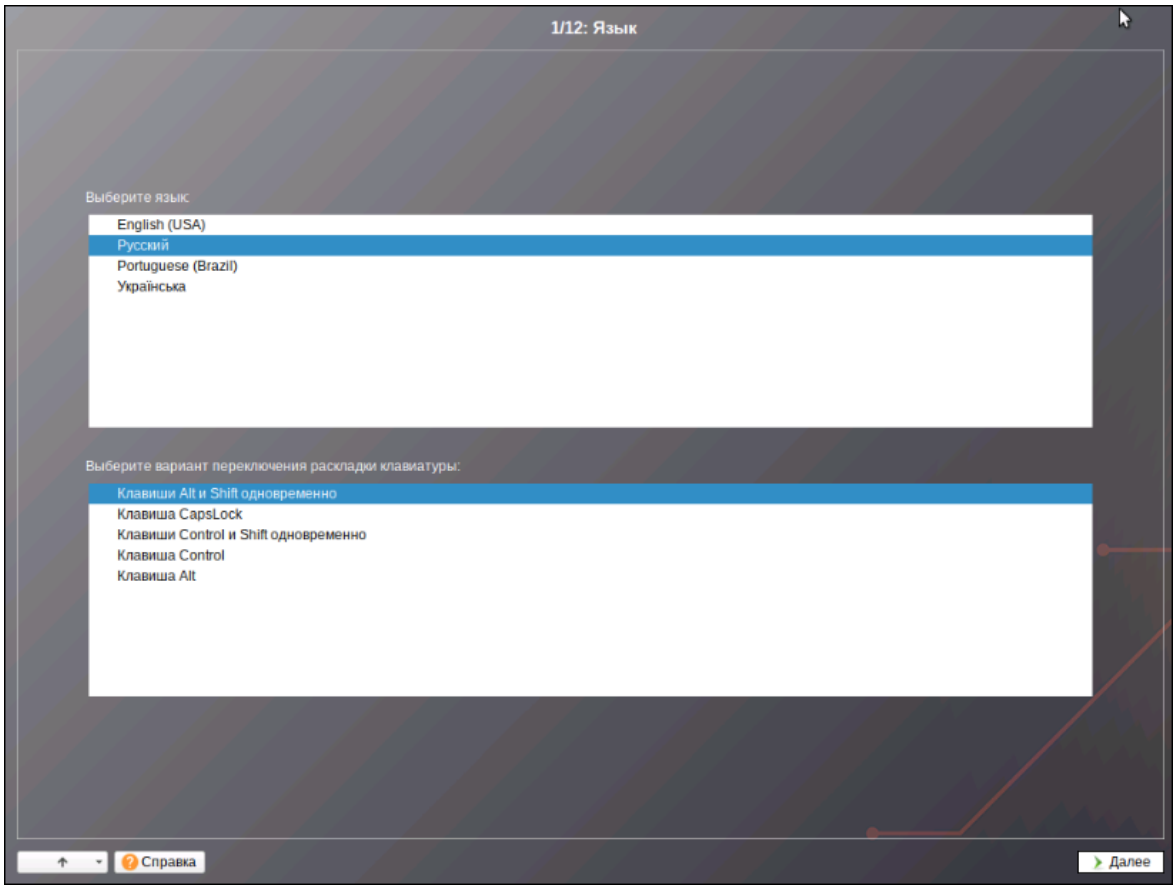


Рис. 5.1. Выбор языка инсталлятора

2. В окне **Лицензионный договор** нажать **Далее**.

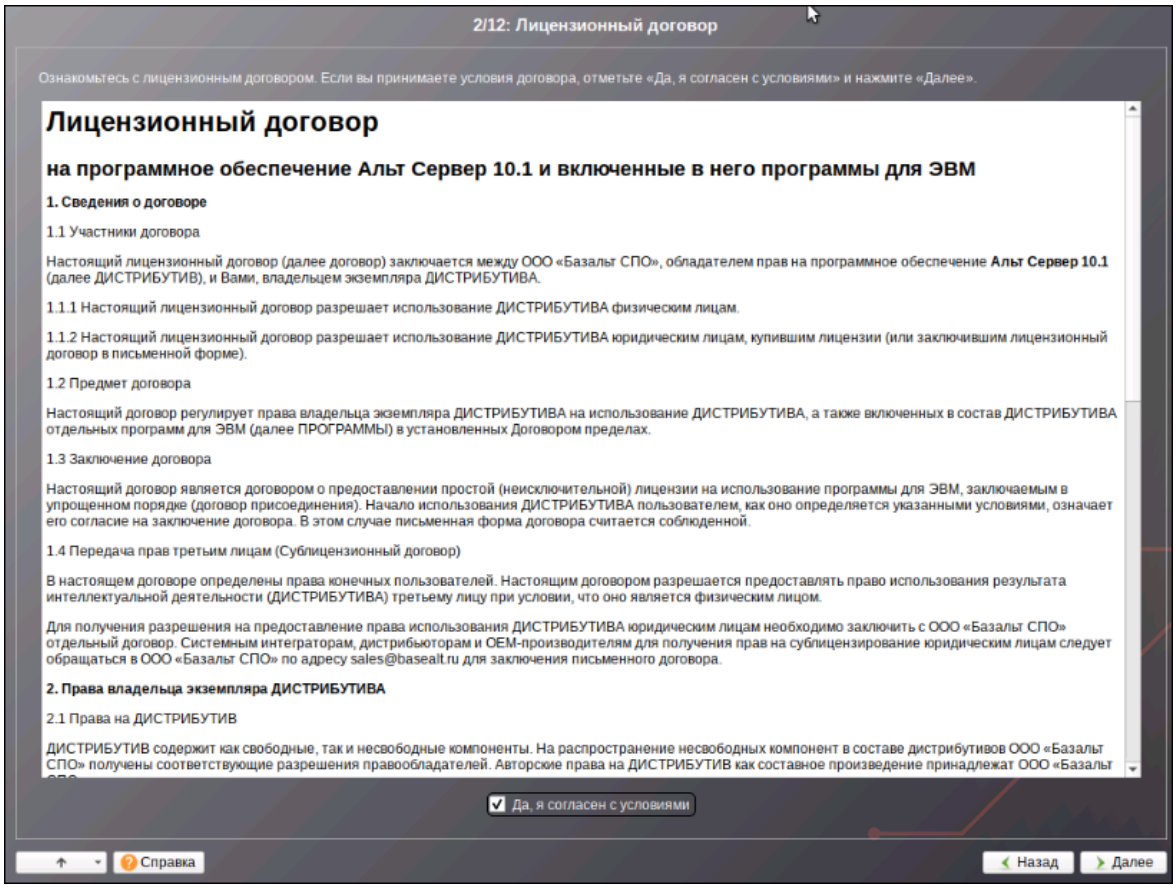


Рис. 5.2. Настройка сетевого интерфейса

3. В окне **Дата и время** установить актуальный часовой пояс и нажать **Далее**.

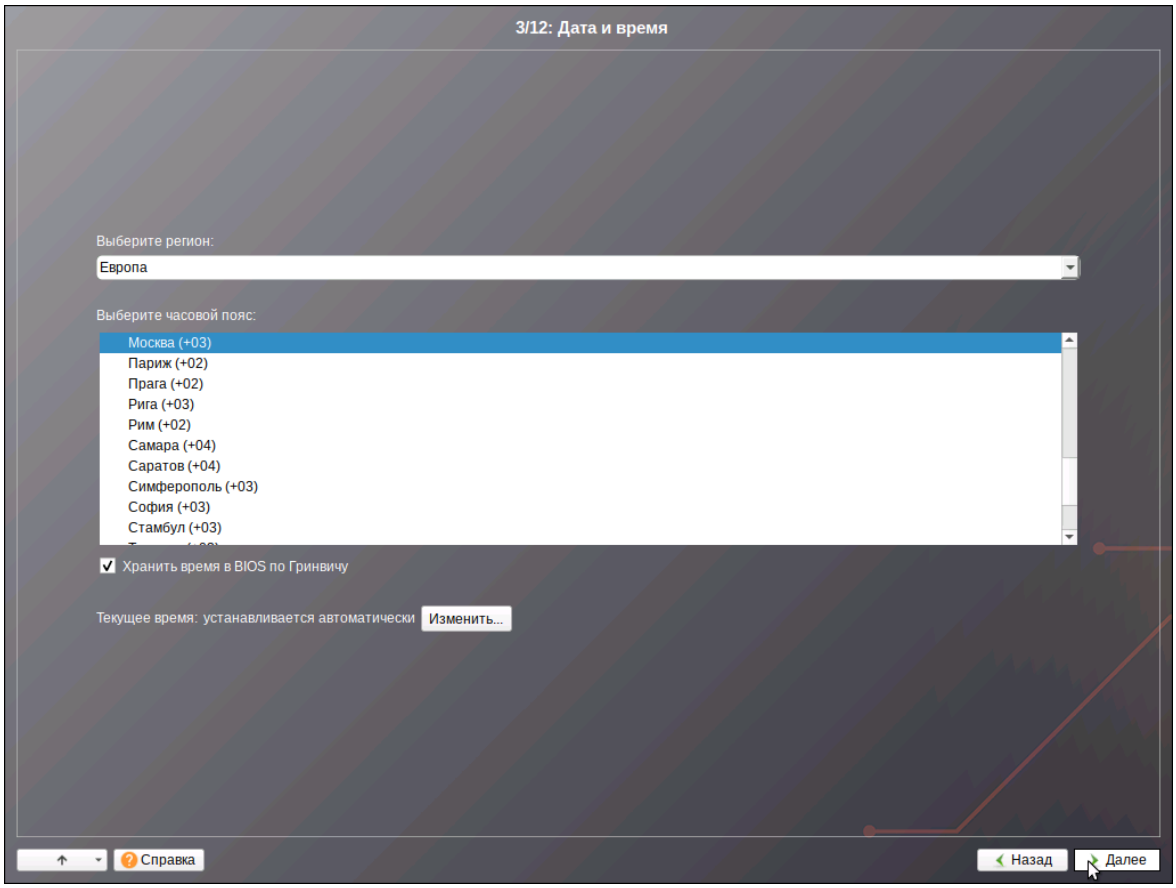


Рис. 5.3. Настройка часового пояса

4. В окне **Подготовка диска** выбрать профиль **Вручную** и нажать **Далее**.

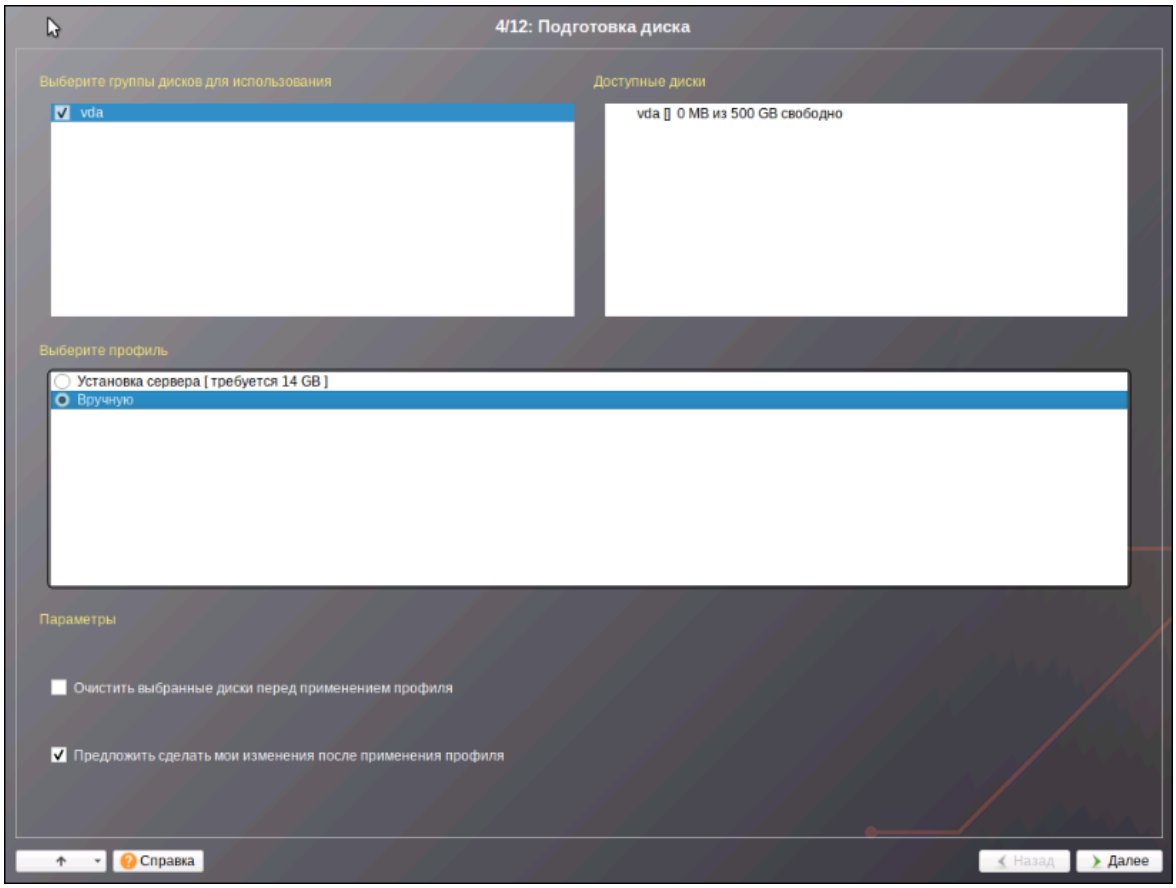


Рис. 5.4. Выбор профиля разбиения диска

5. Выбрать неразмеченный диск и нажать **Удалить**.

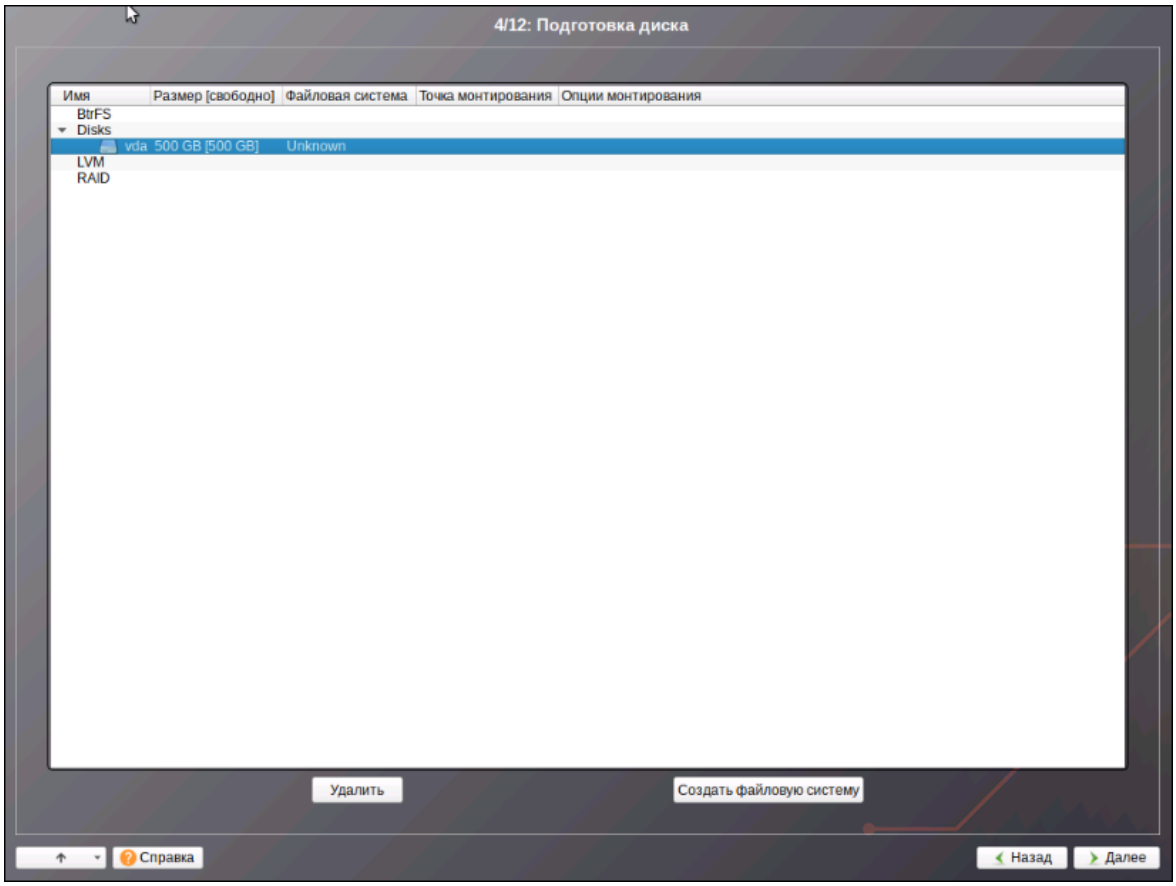


Рис. 5.5. Выбор профиля разбиения диска

6. Нажать кнопку **Создать раздел**.

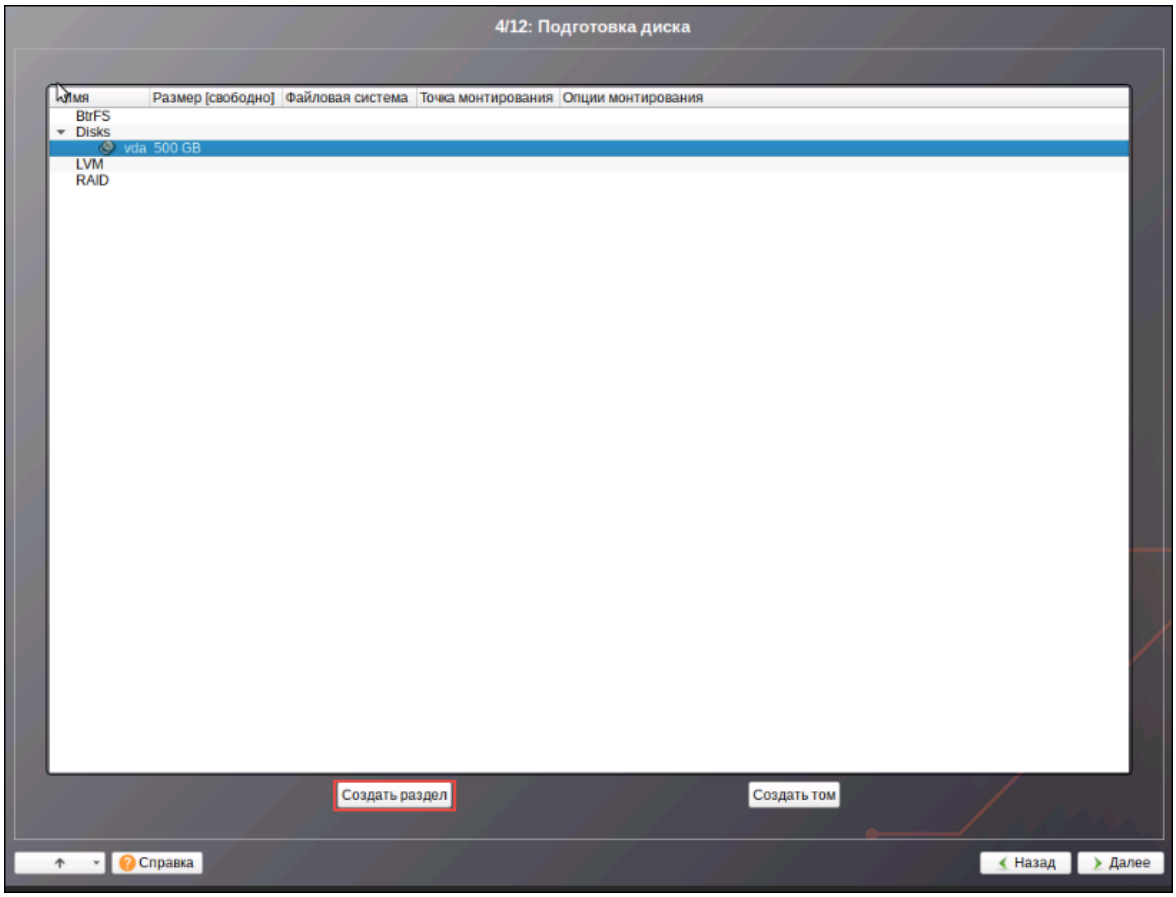


Рис. 5.6. Выбор профиля разбиения диска

7. Выделить 1 ГБ дискового пространства, указать тип раздела равным **Linux** и нажать **OK**.

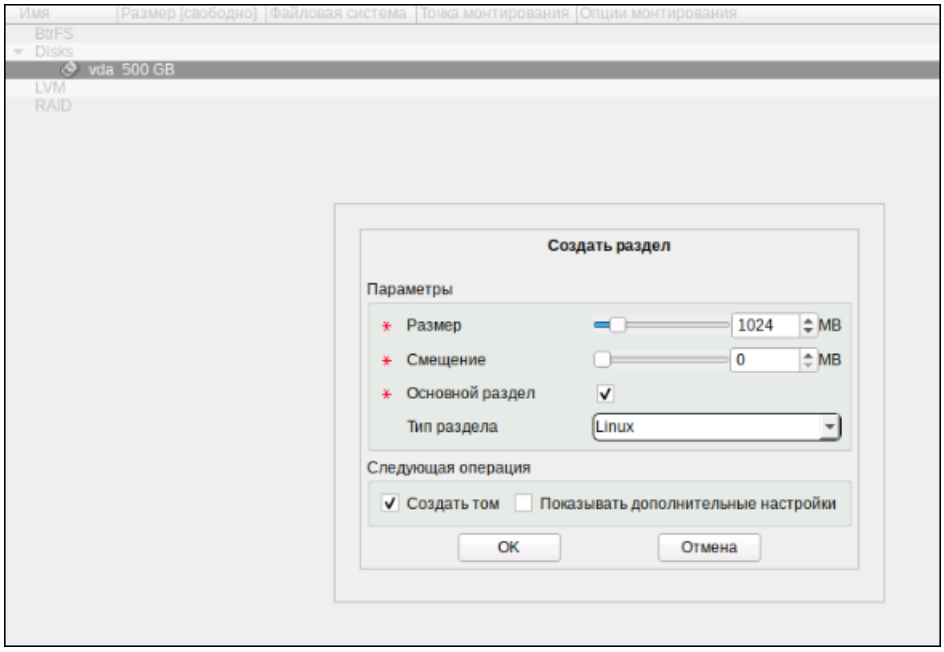


Рис. 5.7. Создание раздела /boot

8. В появившемся диалоговом окне выбрать файловую систему **Ext2/3/4** и нажать **ОК**.

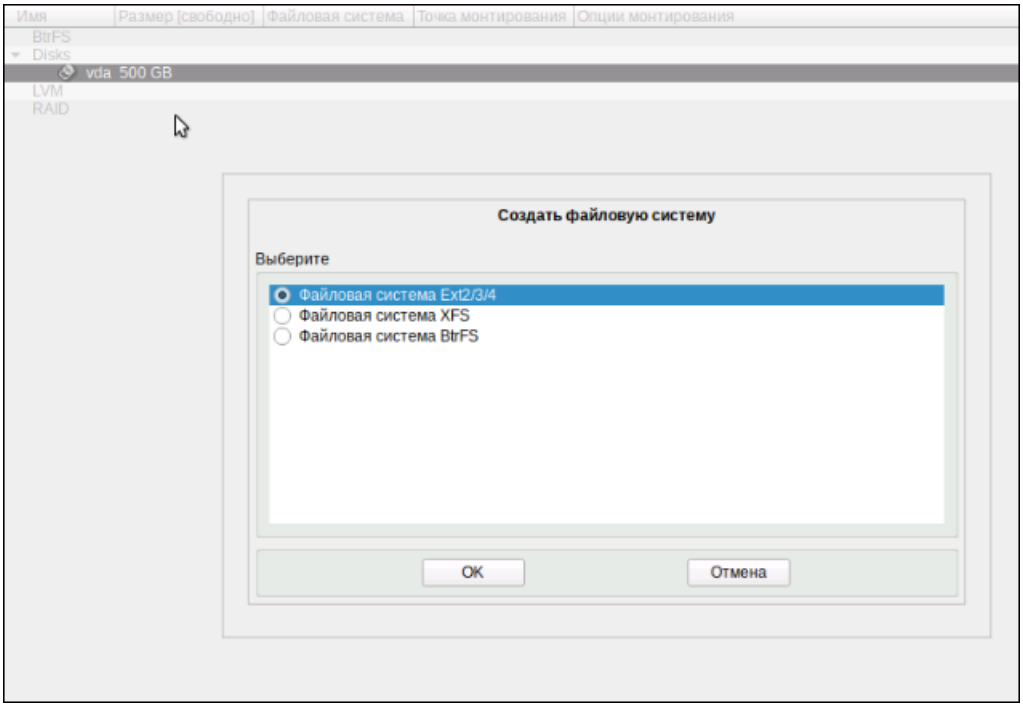


Рис. 5.8. Выбор файловой системы для раздела /boot

9. Задать точку монтирования **/boot** и нажать **ОК**.

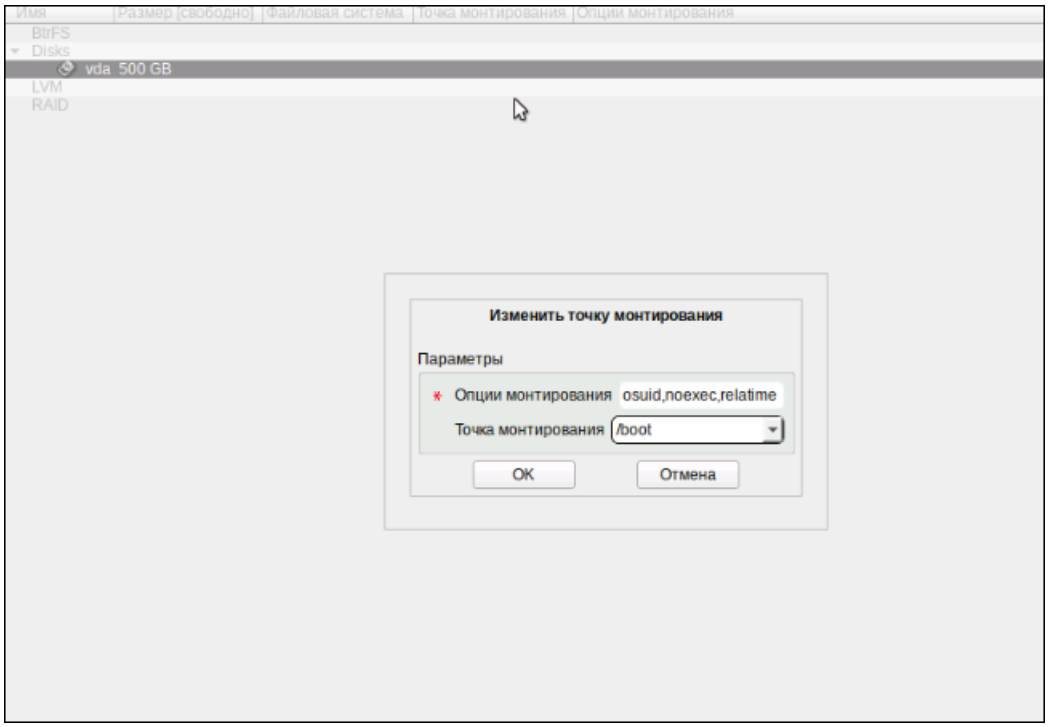


Рис. 5.9. Выбор точки монтирования для раздела /boot

10. Нажать кнопку **Создать раздел**. Выделить 4 ГБ дискового пространства, указать тип раздела равным **Linux Swap** и нажать **ОК**.

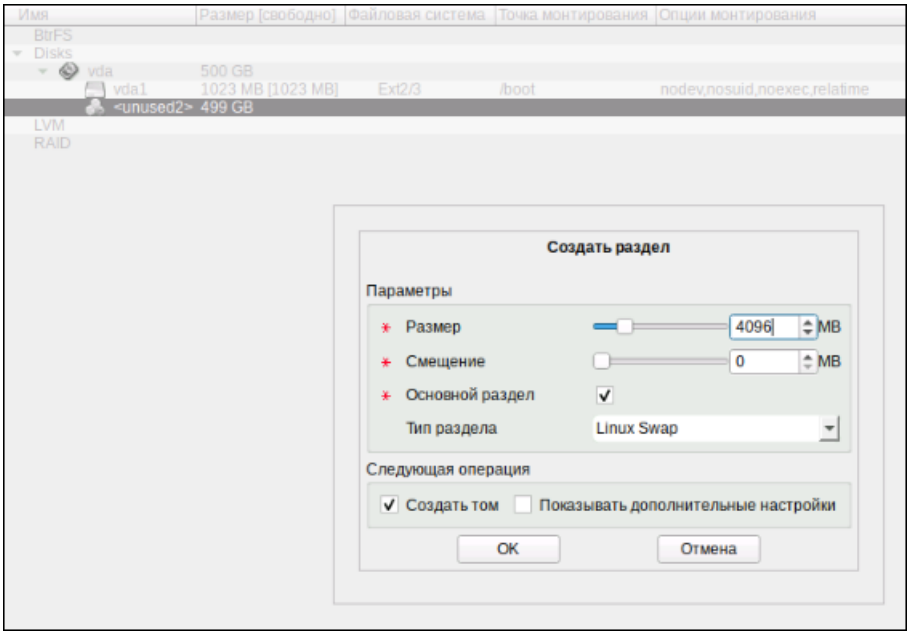


Рис. 5.10. Создание SWAP-раздела

11. Нажать кнопку **Создать раздел**. Выделить оставшуюся дискового пространства, указать тип раздела равным **Linux LVM** и нажать **ОК**.

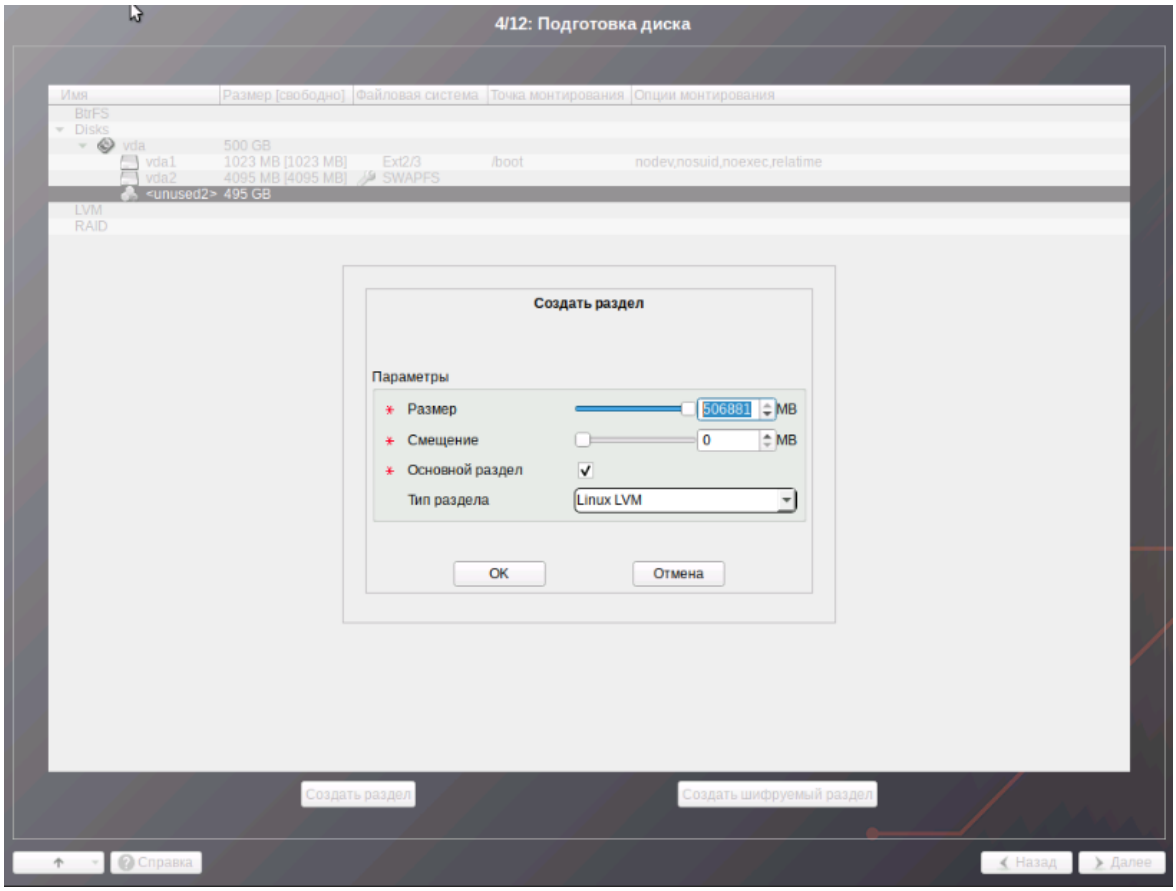


Рис. 5.11. Создание раздела Linux LVM

12 В списке выбрать **LVM** и нажать кнопку **Создать группу томов**.

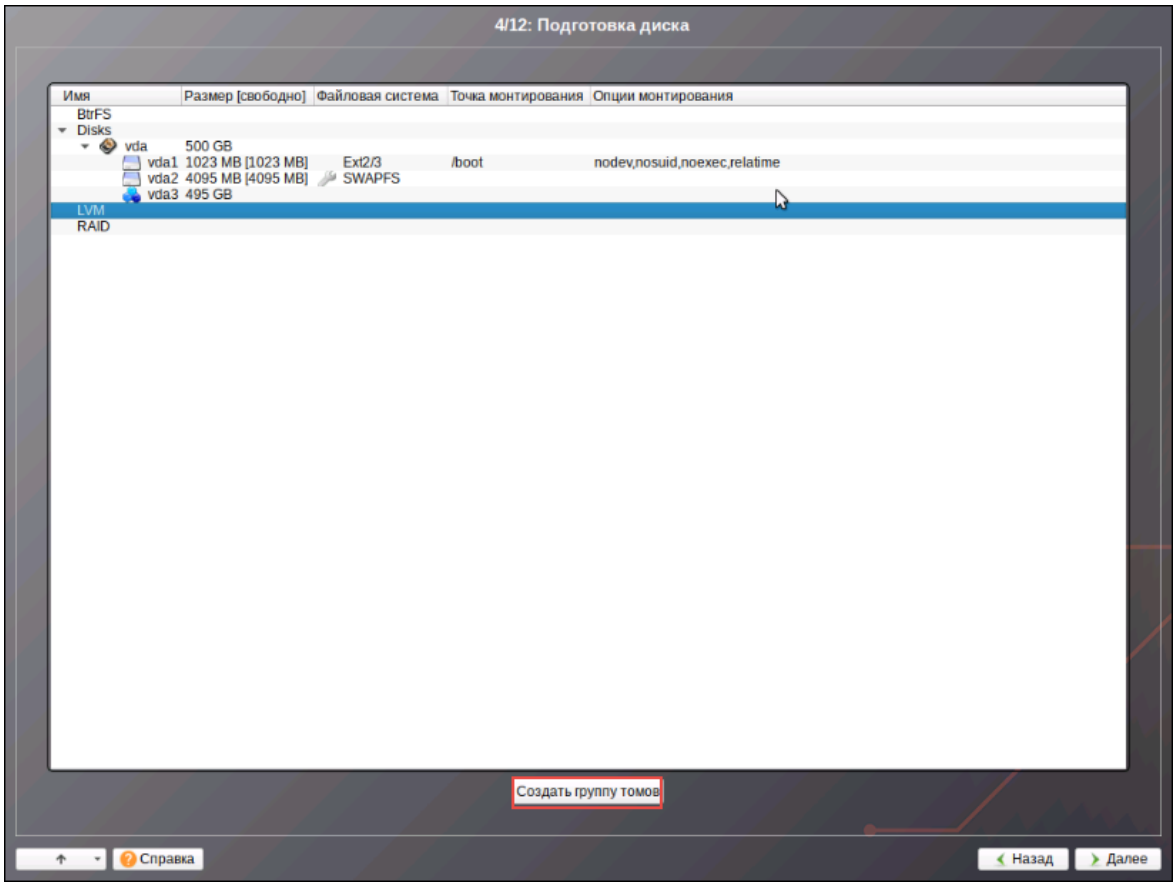


Рис. 5.12. Создание LVM-томов

13. Ввести имя группы томов и нажать **ОК**.

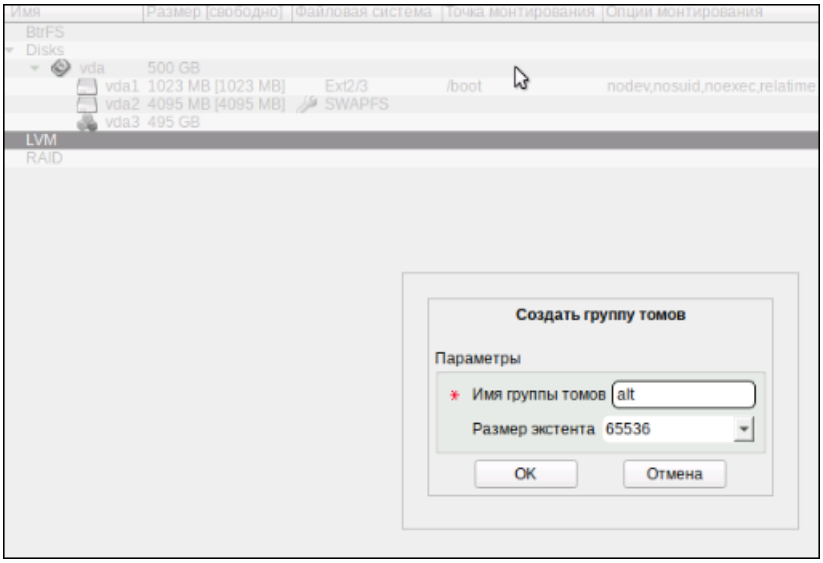


Рис. 5.13. Ввод имени группы томов

14. В списке выбрать неиспользуемое пространство и нажать кнопку **Создать том**. Ввести имя **root**, выделить не менее 50 ГБ дискового пространства и нажать **ОК**.

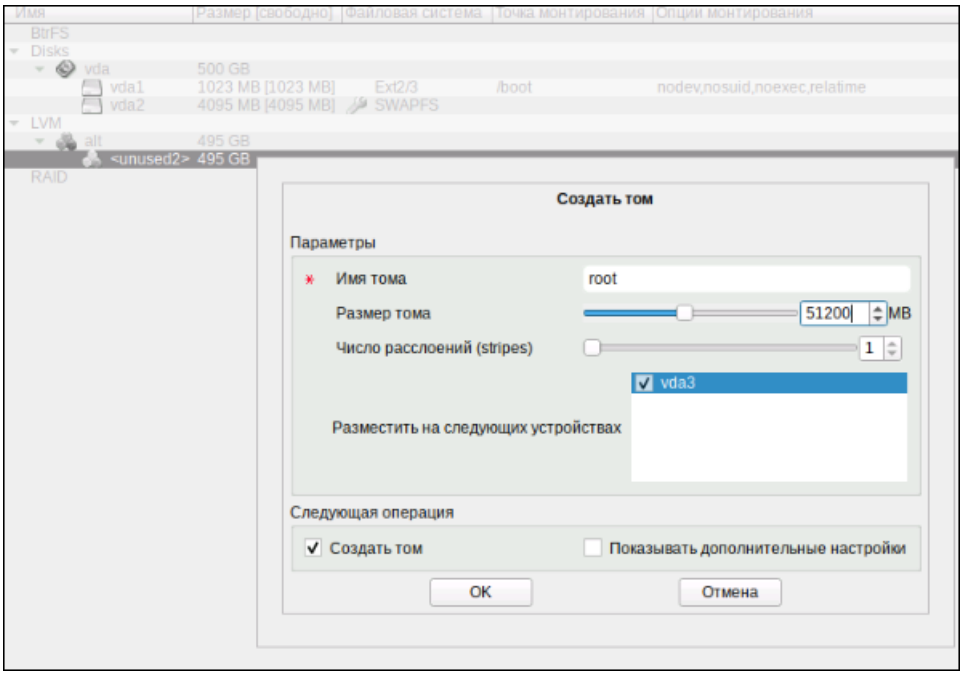


Рис. 5.14. Создание тома /root

15. В появившемся диалоговом окне выбрать файловую систему **Ext2/3/4** и нажать **OK**.

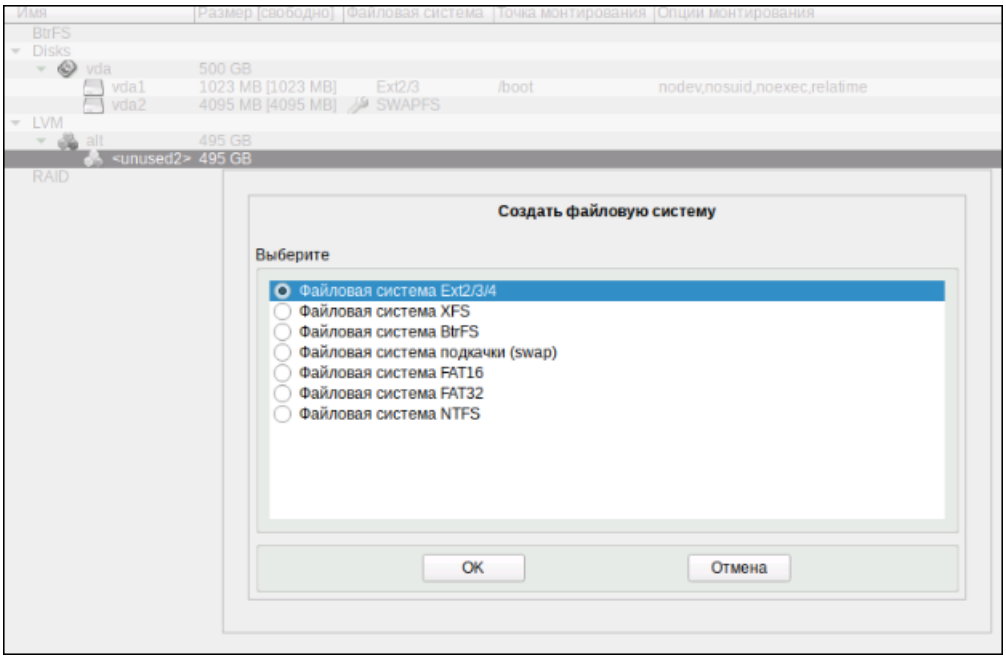


Рис. 5.15. Выбор файловой системы для тома /root

16. Задать точку монтирования **/** и нажать **OK**.

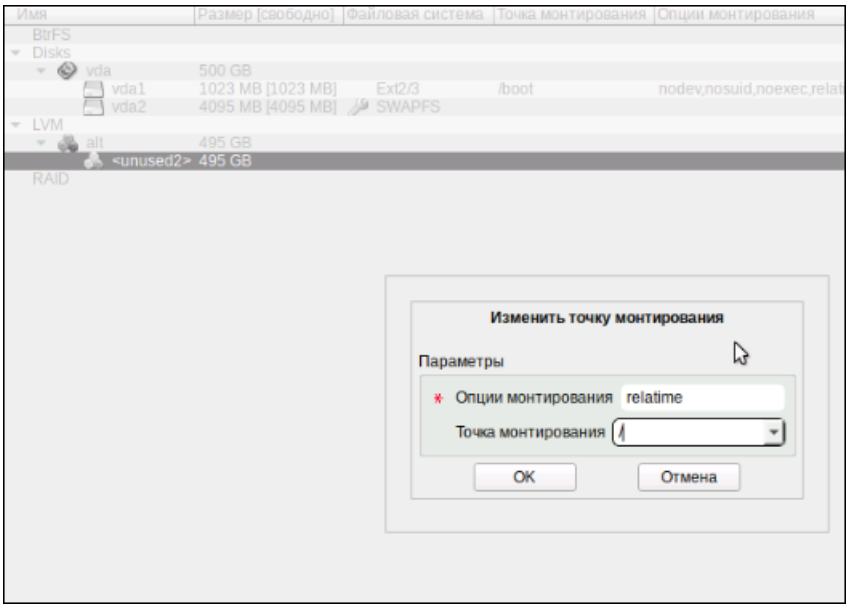


Рис. 5.16. Выбор точки монтирования для раздела /root

17. Выполнить аналогичные действия для разделов **/data**, **/opt** и **/var**, задавая для них одноимённые точки монтирования и указывая следующие значения:

    - **/data** – не менее 100 ГБ дискового пространства, файловая система **XFS**.
    - **/var** – 50 ГБ дискового пространства, файловая система **Ext2/3/4**.
    - **/opt** – всё оставшееся дисковое пространство, файловая система **Ext2/3/4**.

    Внимание!

    Крайне желательно, чтобы объем пространства, выделенного для раздела opt, составлял не менее 130 ГБ. Этот раздел в процессе эксплуатации Solar Dozor активно наполняется данными, и исчерпание свободного места на нем приведет к аварийной остановке Solar Dozor.

18. Нажать **Далее**.

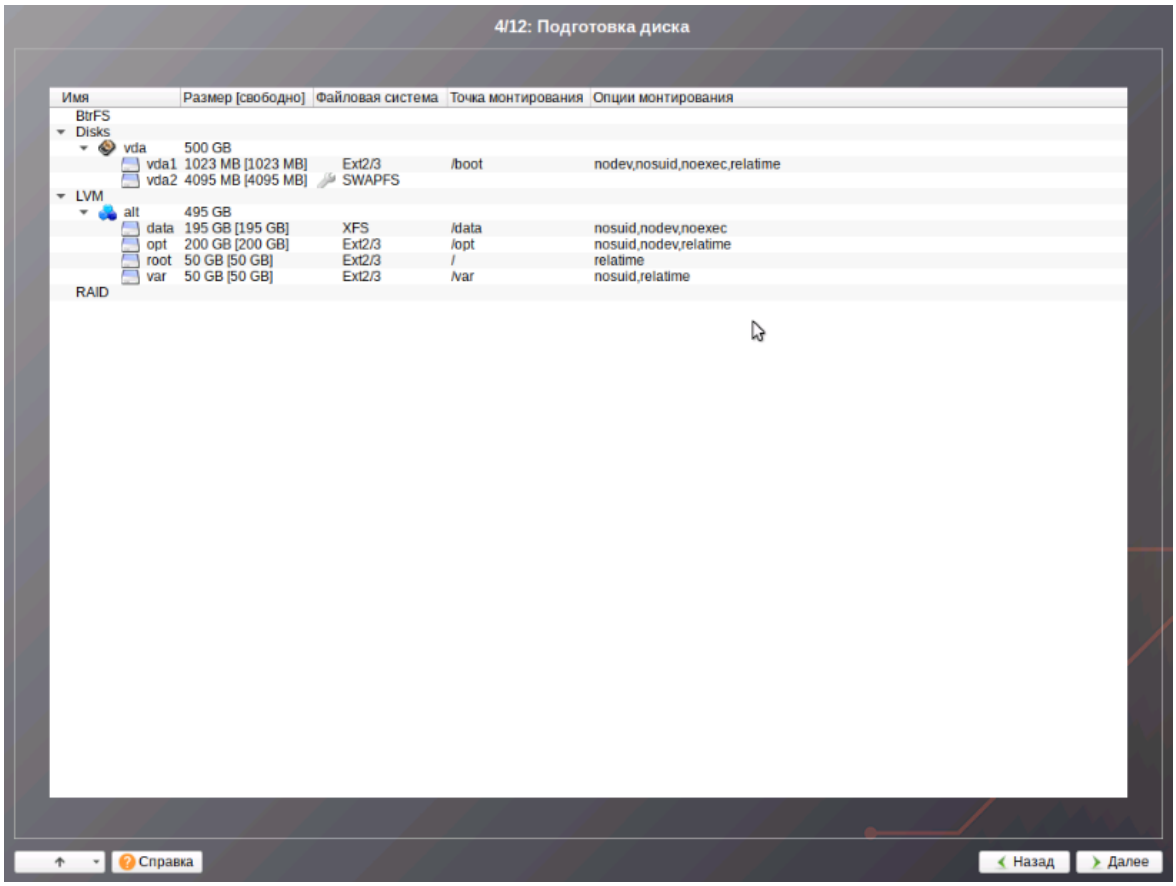


Рис. 5.17. Подготовка диска: продолжение установки

19. Подтвердить операцию, нажав **ОК**.

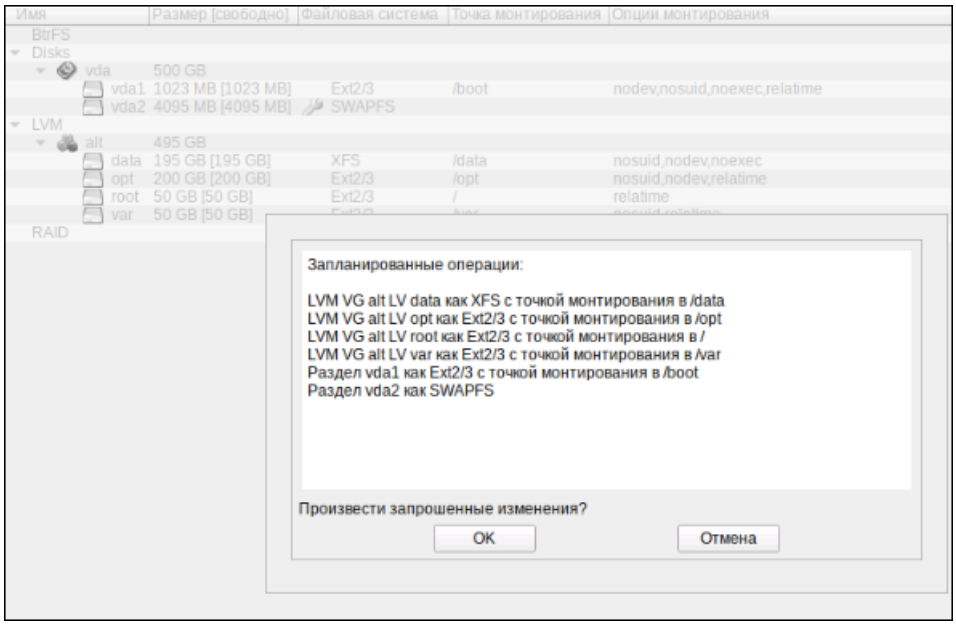


Рис. 5.18. Список действий по созданию разделов

20. Выбрать профиль **Минимальная установка** и компонент **Система управления NetworkManager** (опционально).

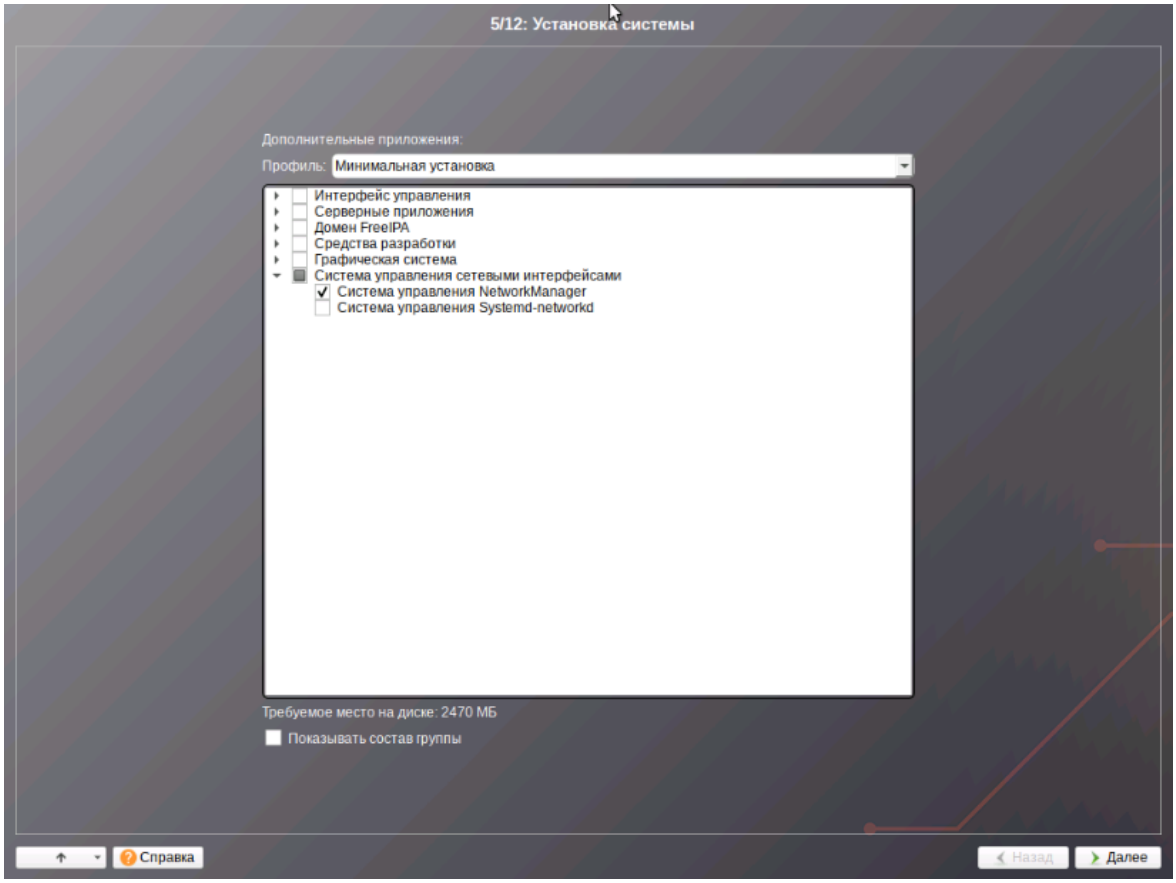


Рис. 5.19. Список действий по созданию разделов

21. Нажать **Далее**. Начнётся установка ОС, на экране отобразится индикатор выполнения.

22. После завершения установки базовой системы следует шаг сохранения настроек, не требующий вмешательства пользователя, на экране отображается индикатор выполнения. Далее будет выполнен переход к шагу установки загрузчика.

23. Нажать **Далее**.

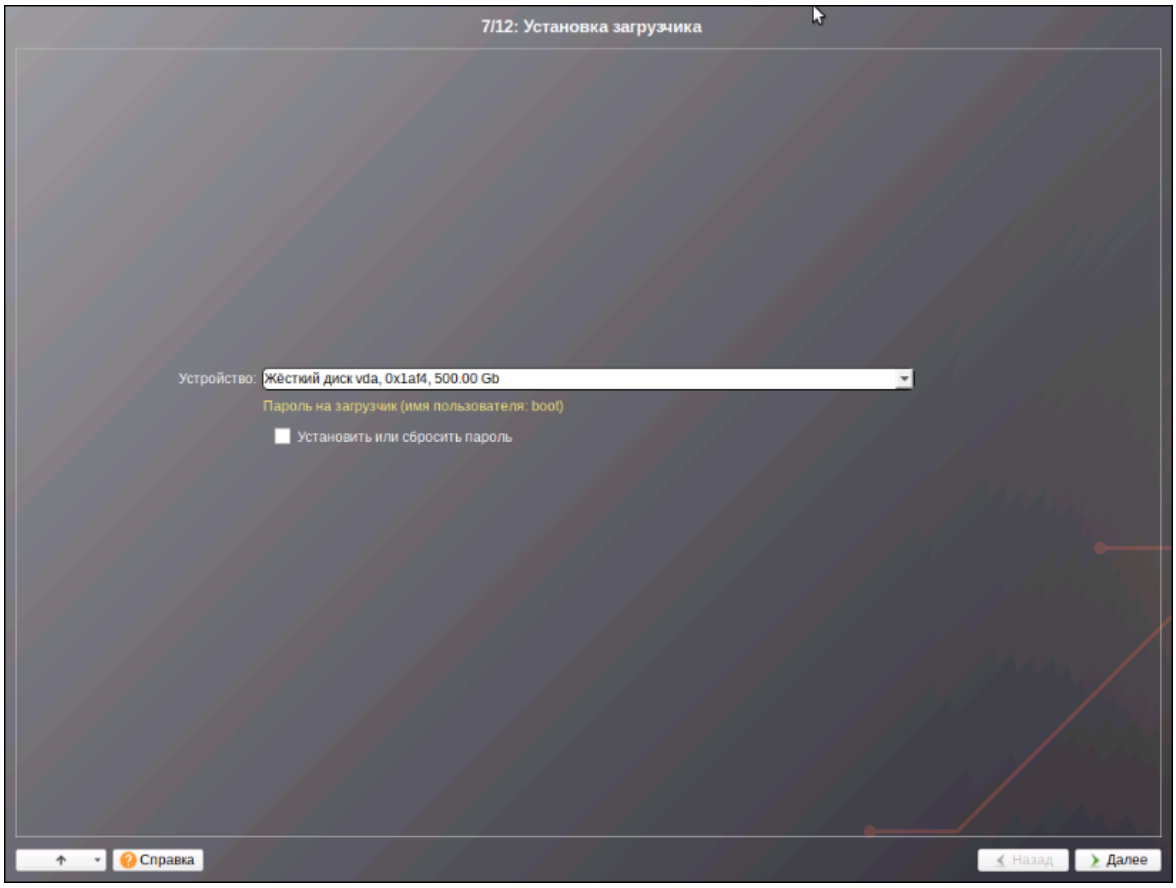


Рис. 5.20. Окно установки загрузчика

24. В поле **Имя компьютера** указать сетевое сервера и нажать **Далее**.

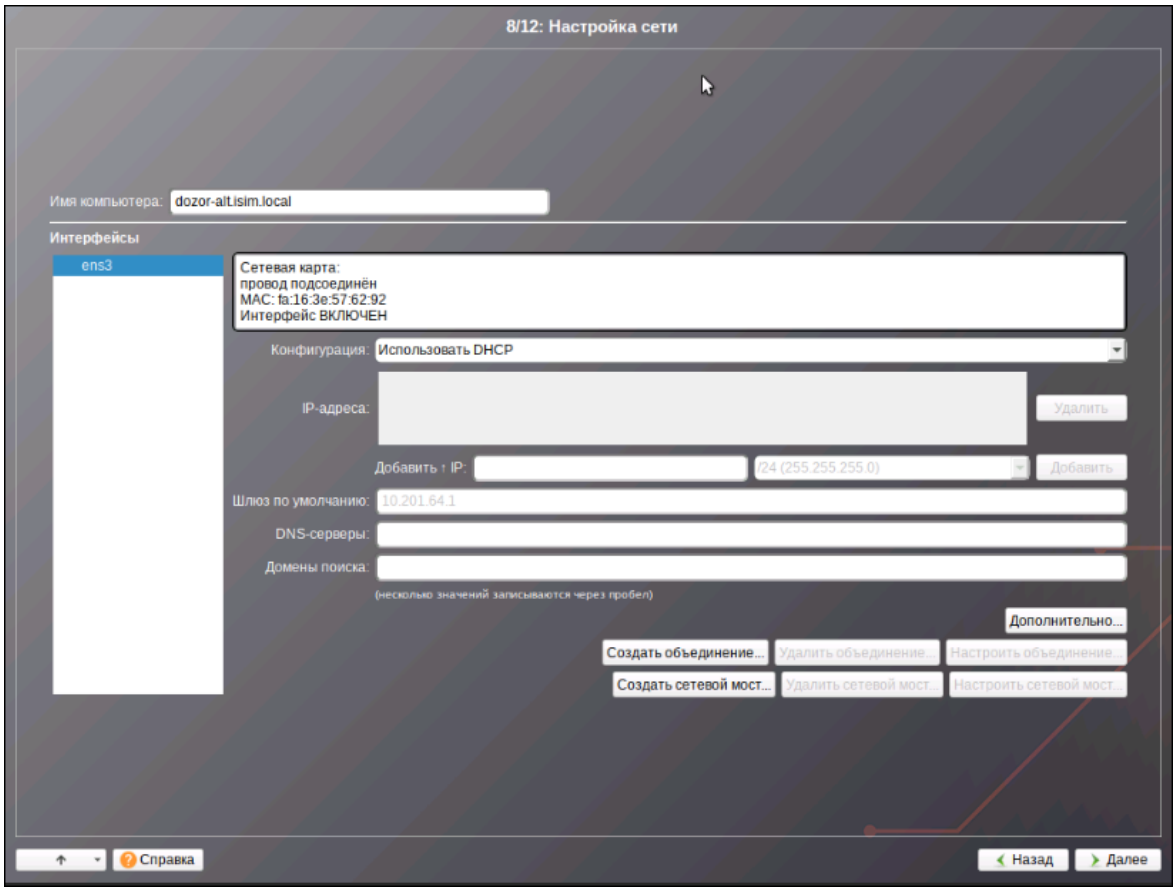


Рис. 5.21. Окно "Настройка сети"

25. Задать пароль учетной записи администратора (**root**) и нажать **Далее**.

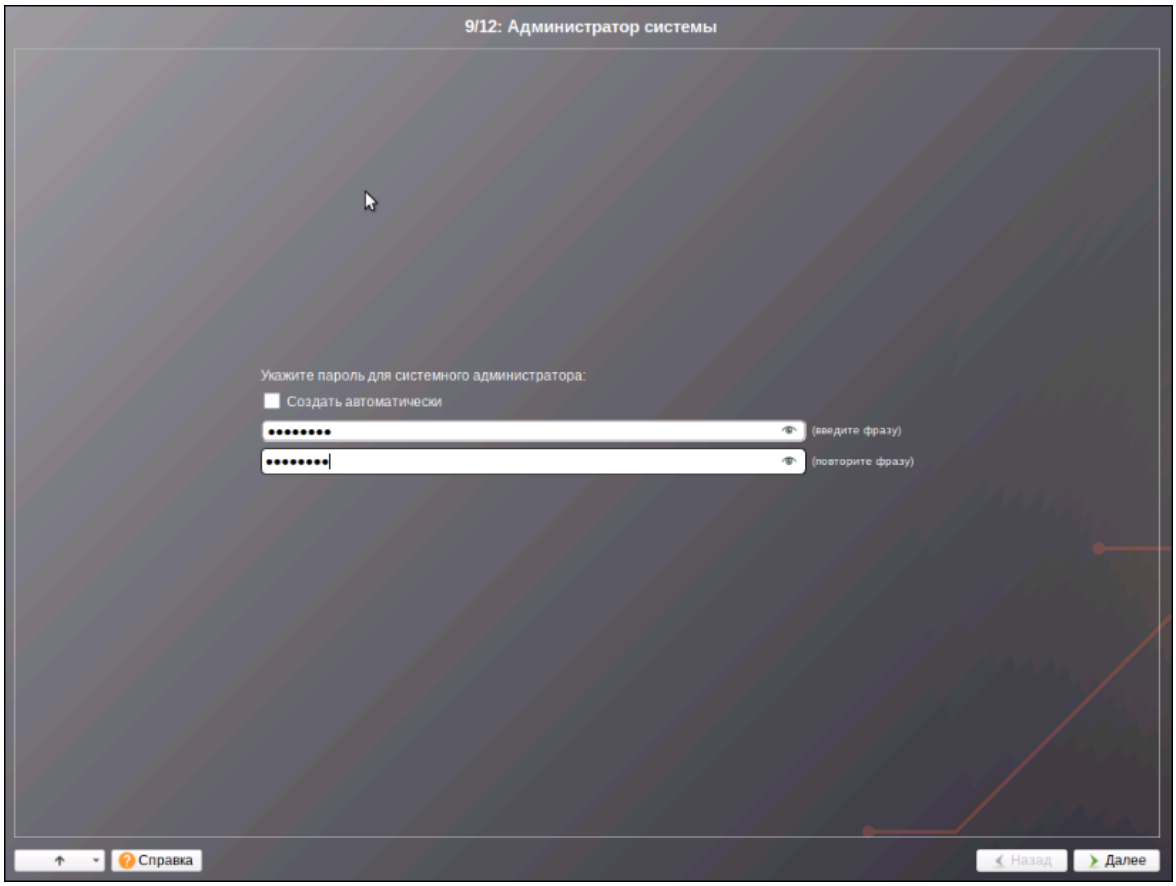


Рис. 5.22. Задание пароля учетной записи администратора (root)

26. При необходимости задать имя и пароль учетной записи системного пользователя. Нажать **Далее**.

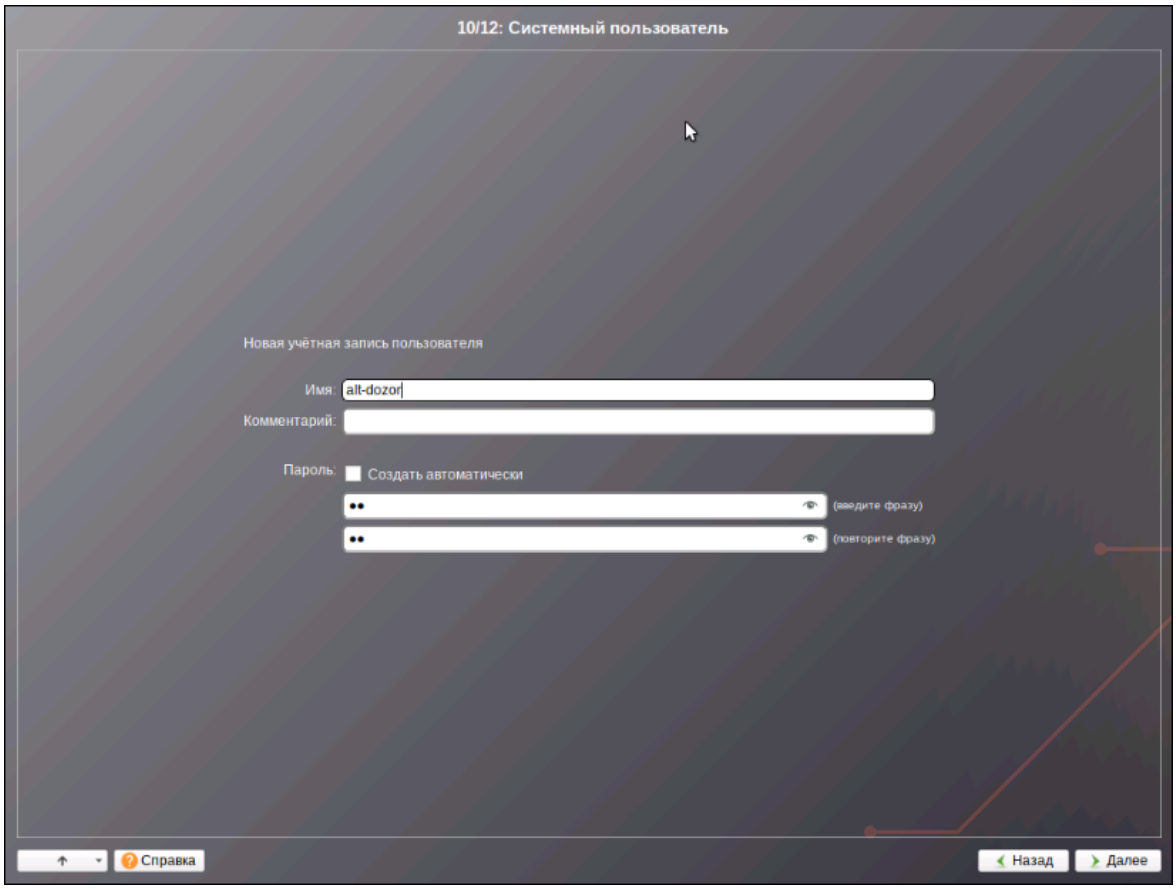


Рис. 5.23. Задание пароля учетной записи системного пользователя

27. Нажать **Завершить**. ОС будет автоматически перезагружена.

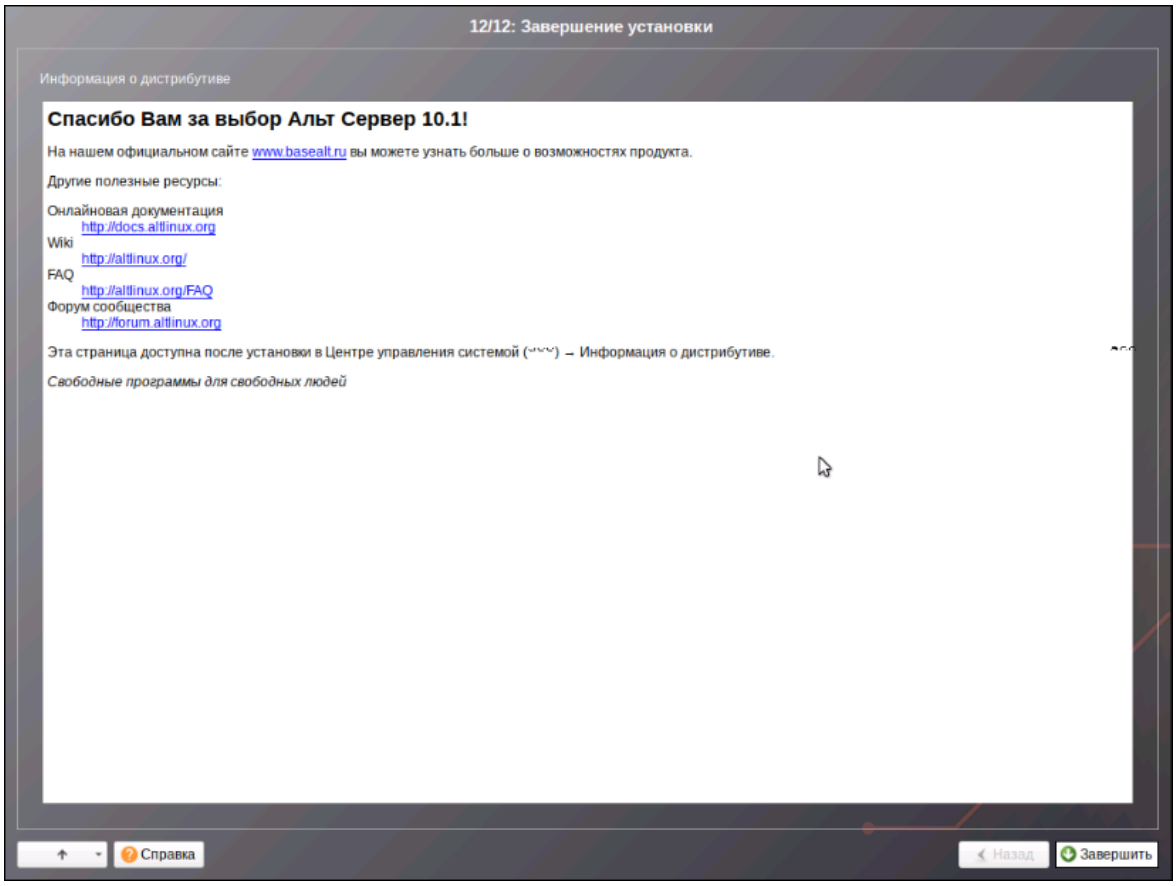


Рис. 5.24. Окно завершения установки

6. Настройка системы и установка Solar Dozor

6.1. Настройка системы

Приведённые в этом разделе процедуры предварительной настройки должны быть выполнены на всех серверах Solar Dozor независимо от выбранной схемы развертывания.

Внимание!

До завершения установки Solar Dozor следует строго придерживаться описанных ниже процедур и не устанавливать какие-либо пакеты или обновления системы. Дистрибутив Solar Dozor содержит все необходимые для работы пакеты, и в случае его установки на ОС с дополнительно установленными пакетами и/или обновлениями не гарантируется корректная работа Solar Dozor.

6.1.1. Настройка SELinux

Необходимо выключить систему принудительного контроля доступа. Для этого следует открыть файл **/etc/sysconfig/selinux** и заменить в нём строку **SELINUX=enforcing** (или **SELINUX=permissive**) на **SELINUX=disabled**, после чего сохранить и закрыть файл, затем перезапустить ОС.

6.1.2. Настройка DNS

Необходимо проверить содержимое следующих файлов настройки DNS на всех узлах Solar Dozor:

- **/etc/hosts**

Файл **/etc/hosts** должен содержать строки для всех узлов кластера Solar Dozor, каждая из которых состоит из IP-адреса узла, его полного (FQDN) и краткого (домен нижнего уровня) доменного имени, например, так:

```
10.199.21.148 dozor7master.company.local dozor7master
10.199.21.149 dozor7filter1.company.local dozor7filter1
10.199.21.150 dozor7filter2.company.local dozor7filter2
```

IP-адрес и записи доменного имени должны быть разделены символом табуляции.

Внимание!

При указании доменного имени узла нельзя использовать символ подчёркивания.

6.1.3. Настройка файловой системы

При наличии внешней СХД необходимо примонтировать её к разделу **/data** master-узла.

Следует убедиться, что раздел **/tmp** на master-узле примонтирован без использования опции **noexec**. Это можно сделать, выполнив команду:

 # mount | grep /tmp | grep noexec

Вывод команды должен быть пустым. В противном случае следует поменять опцию монтирования для раздела **/tmp** и перемонтировать его. Для этого необходимо выполнить следующие действия:

1. Открыть для редактирования файл **/etc/fstab** и найти в нём строку, относящуюся к разделу **/tmp**.

2. Заменить в этой строке опцию **noexec** на **exec**. Сохранить и закрыть файл.

3. Перемонтировать раздел, выполнив команду:

   # mount -o remount,exec /tmp

6.1.4. Настройка синхронизации времени

Синхронизация времени внутри кластера Solar Dozor необходима для его корректной работы. В отсутствие контроллера домена или другого источника точного времени возникнут проблемы из-за разного времени в журналах и метках времени на данных, а также возможны проблемы с работой протокола HTTPS. Для синхронизации времени могут быть использованы один или несколько серверов точного времени, находящихся как в корпоративной сети, так и в сети Интернет.

Для настройки синхронизации времени необходимо на всех узлах Solar Dozor выполнить следующие действия:

1. Найти нужную временную зону, выполнив следующую команду:

   # timedatectl list-timezones

   Для удобства поиска можно воспользоваться сортировкой, например:

   # timedatectl list-timezones | grep Europe

2. Установить нужную временную зону, выполнив команду следующего вида:

   # timedatectl set-timezone <timezone>

   где **<timezone>** – значение, найденное в предыдущем шаге.

3. Удостовериться в правильности настройки временной зоны, выполнив следующую команду:

   # timedatectl

4. Установить пакет **ntp**, выполнив команду:

   # apt-get install ntpd

5. Открыть для редактирования файл **/etc/ntp.conf** и добавить в него одну или несколько строк следующего вида:

   ```
   server <timeserver> iburst
   ```

   где **<timeserver>** – FQDN или IP-адрес NTP-сервера (внешнего или принадлежащего организации). Параметр **iburst** является необязательным и служит для повышения

точности синхронизации за счёт увеличенного количества пакетов, отправляемых при обмене данными с NTP-сервером.

Наличие нескольких записей позволяет продолжать синхронизацию в случае отказа какого-либо из NTP-серверов. Серверы опрашиваются по очереди, в порядке их перечисления в файле **ntp.conf**.

6. Запустить службу NTP и добавить её в автозагрузку, выполнив команды:

   # systemctl start ntpd

   # systemctl enable ntpd

Узнать список работающих используемых серверов точного времени можно выполнив следующую команду:

 # ntpq -p

6.2. Установка Solar Dozor

Табл. 6.1. Контрольный лист действий при одномашинной конфигурации

№ п/п	Наименование действия	Ссылки на разделы	Обязательно	Примечания
1	Установка пакетных файлов Solar Dozor	Раздел 6.2.1. Документ *Описание релиза*.	да	
2	Вход в систему и загрузка лицензии	Разделы 6.4 и 6.5.	да	
3	Назначение ролей узлам	Раздел 8.2.	да	
4	Создание БД инцидентов	Раздел 8.4.	да	
5	Создание БД хранения медиаинформации	Раздел 8.5.	да	
6	Создание БД архива	Раздел 8.3.	см. примечание	Можно создать сколь угодно много БД архива (при желании можно не создавать вовсе).

Табл. 6.2. Контрольный лист действий при распределённой конфигурации

№ п/п	Наименование действия	Ссылки на разделы	Обязательно	Примечания
1	Установка пакетных файлов Solar Dozor	Раздел 6.2.2. Документ *Описание релиза*.	да	
2	Вход в систему и загрузка лицензии	Разделы 6.4 и 6.5.	да	
3	Назначение ролей узлам	Раздел 8.2.	да	
4	Создание БД инцидентов	Раздел 8.4.	да	
5	Создание БД хранения медиаинформации	Раздел 8.5.	да	
6	Создание БД архива	Раздел 8.3.	см. примечание	Можно создать сколь угодно много БД архива (при желании, можно не создавать вовсе).

Ниже описана установка только Solar Dozor. Создание БД архива сообщений, БД событий и инцидентов ИБ и БД, используемой для хранения медиаинформации, описаны в разделах 8.3, 8.4 и 8.5 соответственно.

6.2.1. Установка в одномашинной конфигурации

Для установки Solar Dozor следует выполнить следующие действия:

1. Скопировать полученный от производителя файл архив пакетов установки **solar-dozor-7.12.0-532.alt10.run** на сервер, на котором будет выполнена установка Solar Dozor, например, в каталог **/var/tmp/**.

2. Проверить контрольную сумму загруженного файла, выполнив команды:

   # cd /var/tmp/

   # md5sum solar-dozor-7.12.0-532.alt10.run

   Сопоставить полученное значение с контрольной суммой, приведённой в документе *Описание релиза*. При несовпадении значений прервать установку и связаться с вендором.

3. Настроить сервис **iptables**, выполнив команды:

   iptables -F

   iptables -X

   iptables -t nat -F

   iptables -t nat -X

   iptables -t mangle -F

   iptables -t mangle -X

   iptables -P INPUT ACCEPT

   iptables -P FORWARD ACCEPT

   iptables -P OUTPUT ACCEPT

   /sbin/service iptables save

4. Открыть файлы **/etc/apt/sources.list** и **/etc/apt/sources.list.d/*.list**, и проверить наличие в них репозиториев. При наличии репозиториев следует закомментировать все строки. Сохранить и закрыть файлы. После установки можно снова включить все нужные репозитории.

5. Если была установлена ОС версии 10.1 или 10.2 – запустить установку Solar Dozor, выполнив команду:

   # ./solar-dozor-7.12.0-532.alt10.run -c

6. При необходимости, обновить пакеты операционной системы, выполнив команды:

 # apt-get update

 # apt-get dist-upgrade

 # update-kernel -t std-def

 # reboot

7. Назначить сервер master-узлом, выполнив следующую команду:

   # /opt/dozor/bin/set-role master main

8. Запустить Solar Dozor, выполнив команды:

   # /opt/dozor/bin/shell

   # dsctl boot

После этого следует продолжить работу в GUI Solar Dozor (см. раздел 6.4).

6.2.2. Установка в распределённой конфигурации

Для установки Solar Dozor следует выполнить на каждом сервере следующие действия:

1. Установить Solar Dozor на все узлы согласно инструкциям раздела 6.2.1.
2. Назначить один из серверов master-узлом, выполнив на нём следующую команду:

   # /opt/dozor/bin/set-role master main

3. Запустить Solar Dozor, выполнив следующую команду:

   # /opt/dozor/bin/dsctl boot

4. Назначить все остальные серверы slave-узлами, выполнив на каждом из них команду следующего вида:

   # /opt/dozor/bin/reg-slave <master-host> <name> <role-list>

   где:

   - **<master-host>** – FQDN master-узла.
   - **<name>** – имя регистрируемого slave-узла. Это имя будет отображаться в GUI.

     Примечание

     При указании имени узла нельзя использовать символ подчёркивания и верхний регистр текста.

Внимание!

В некоторых ситуациях (в основном, при клонировании виртуальных машин) могут возникать узлы с одинаковыми идентификаторами. Если узел с таким же именем и идентификатором, как и у вновь регистрируемого узла, уже присутствует в кластере Solar Dozor, то вновь зарегистрированный узел заместит его в описании кластера. При совпадении идентификаторов и различии имён, идентификатор регистрируемого узла будет сгенерирован заново, и он будет корректно добавлен в кластер. Поэтому следует внимательно выбирать имя для регистрируемого узла.

- **<role-list>** – список ролей, назначаемых узлу. Роли перечисляются через пробел. Описание ролей приведено в приложении **Приложение С, *Описание ролей и сервисов***.

Например, если имеется три сервера, один из которых является master-узлом, а на двух других требуется организовать фильтры почтового потока с именами **filter1** и **filter2**, то на каждом из этих двух узлов следует выполнить от имени пользователя **root** или **dozor** соответствующую команду следующего вида:

 # /opt/dozor/bin/reg-slave <master-host> filter1 smtp-filter

 # /opt/dozor/bin/reg-slave <master-host> filter2 smtp-filter

Внимание!

*Если выполнение команды **reg-slave** завершилось с ошибкой, следует проверить правильность синтаксиса команды и её аргументов, исправить возможные ошибки и выполнить команду ещё раз.*

5. Запустить сервисы Solar Dozor на всех slave-узлах, выполнив на каждом из них команду:

 # /opt/dozor/bin/dsctl boot

После этого следует продолжить работу в GUI Solar Dozor (см. раздел **6.4**).

6.3. Установка Solar Dozor в территориально-распределенной схеме работы

Для работы в территориально-распределённом режиме необходимо установить Solar Dozor на все требуемые узлы любым удобным способом, приведённым в разделе **6.2**, а затем создать подкластеры и распределить по ним узлы, как описано в разделе **Настройка общих ресурсов и подкластеров** документа *Руководство по работе с модулем Мультидозор*.

При настройке территориально-распределённой схемы работы Solar Dozor необходимо учитывать следующие положения:

- Сервисы в подкластере должны взаимодействовать с сервисами в этом же подкластере максимально в той мере, насколько это возможно. При необходимости, сервисы подкластера могут взаимодействовать с сервисами вне подкластеров (общие ресурсы).

Взаимодействие сервисов одного подкластера с сервисами другого должно быть исключено.

- Каждый подкластер должен иметь узел с ролью **Сервер лицензирования подкластера**. Такая роль должна быть ровно одна на весь подкластер. Вне подкластеров (на общих ресурсах) такая роль не нужна, её функции выполняет master-узел.

- Хотя бы один узел на общих ресурсах должен иметь роль **Индексатор текста**, независимо от наличия архива сообщений.

- Роль **Сервер действий подкластера** может быть назначена только одному узлу подкластера, и только при наличии хотя бы одного узла с ролью **Сервер архива сообщений** в этом же подкластере. При этом подразумевается, что в таком подкластере имеется собственная БД архива сообщений. Роль **Вспомогательный сервер действий** может быть назначена в подкластере любому количеству узлов, но не узлу с ролью **Сервер действий подкластера**.

- Утилиты, работающие с БД архива сообщений подкластера, могут запускаться только на узлах с ролью **Сервер архива сообщений**. Утилиты для работы с БД, находящимися за пределами подкластеров, можно запускать на master-узле, либо на узлах с ролью **Сервер архива сообщений** за пределами подкластеров.

- Роль **Сервер архива сообщений** следует назначать узлу в комбинации с ролью **Вспомогательный сервер Elasticsearch** (в подкластерах или за их пределами) или **Вспомогательный сервис индексации текста** (в подкластерах). Роли ФХ внутри подкластера или на общих ресурсах следует назначать только если на одном из узлов в этом подкластере или на общих ресурсах имеется роль **Сервис распределённого хранения**.

- Для корректной работы агентов в подкластере рекомендуется назначить роль **Сервер агентов** одному из узлов этого подкластера, а также организовать в нём ФХ.

- Роли **Сервер управления Краулером**, **Анализ поведения (UBA)** и **Контроль рабочего времени** могут быть назначены только одному узлу, и только на общих ресурсах.

6.4. Первый вход в систему

Для входа в GUI Solar Dozor следует ввести в адресной строке браузера адрес **https://<доменное имя master-узла Solar Dozor>** (либо можно использовать доменное имя другого узла которому назначена роль **Локальный веб-сервер**), и подтвердить исключение сертификата безопасности. Появится окно авторизации (см. Рис.6.1):

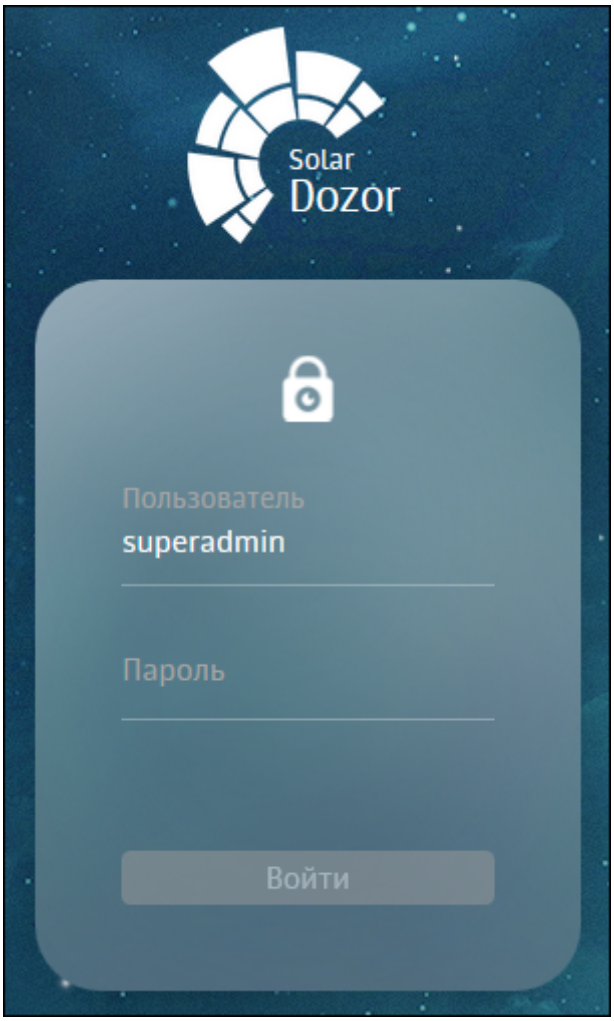


Рис. 6.1. Окно авторизации при входе в систему

В окне авторизации следует указать следующие имя и пароль по умолчанию: **superadmin/superadmin**. После первой авторизации система потребует изменить пароль по умолчанию (см. рисунок Рис.6.2). Следует изменить пароль, указав его дважды.

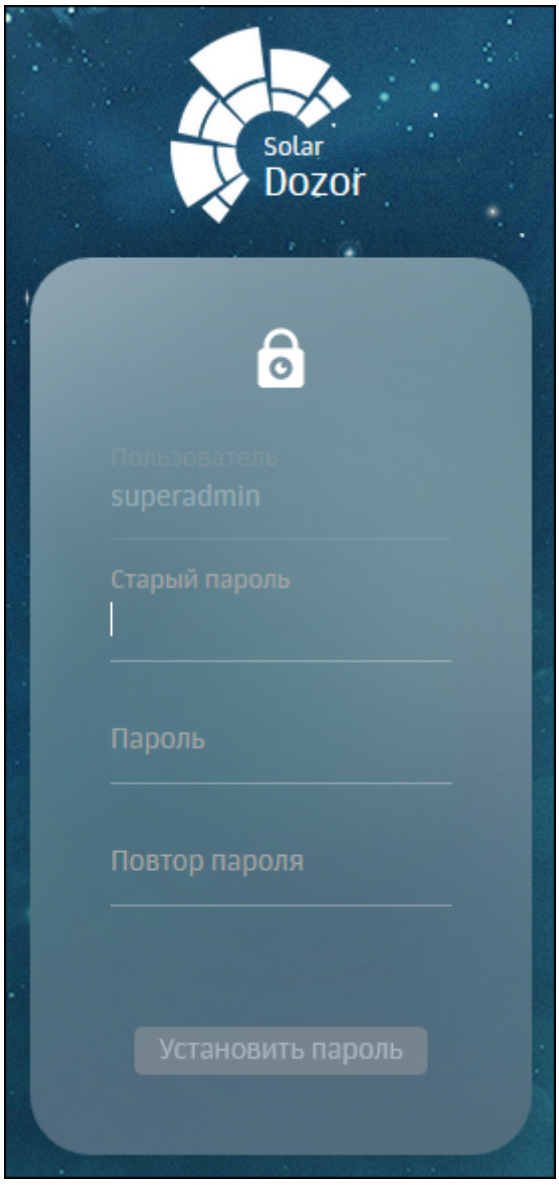


Рис. 6.2. Окно смены пароля

Внимание!

Пароль должен содержать от 6 до 12 символов, а также отвечать критериям сложности. Требования к сложности пароля и метод её вычисления приведены в документе Руководство Системного Администратора, в приложении Требования к паролям учетных записей пользователей.

6.5. Загрузка лицензии

6.5.1. Загрузка лицензии Solar Dozor

После первоначальной смены пароля в верхней части экрана появится уведомление об отсутствии лицензии (см. рисунок Рис.6.3). Для получения файла лицензии следует скопировать указанный в уведомлении идентификатор инсталляции и отправить его в вендорскую службу поддержки Solar Dozor на адрес support@rt-solar.ru.

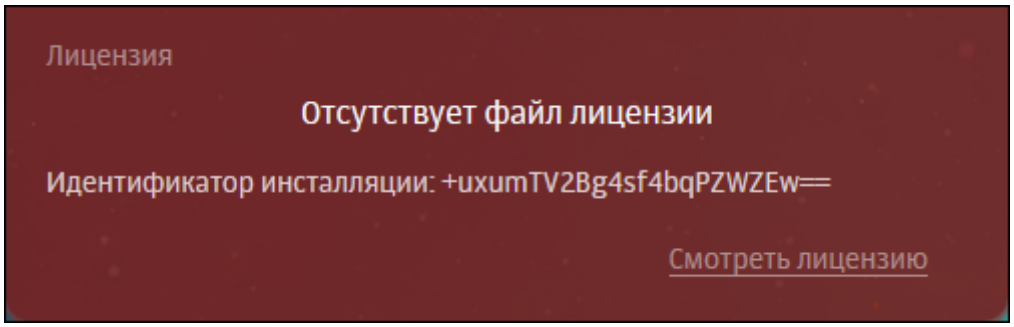


Рис. 6.3. Уведомление об отсутствии лицензии

Для загрузки лицензии следует нажать кнопку **Смотреть лицензию**, и в появившемся окне **Лицензия** нажать кнопку **Загрузить лицензию**. В открывшемся окне проводника указать путь к файлу с лицензией, после чего нажать кнопку **Открыть** (**Open**) и дождаться загрузки лицензии. При этом она автоматически сохранится в файле с именем **license.xml**.

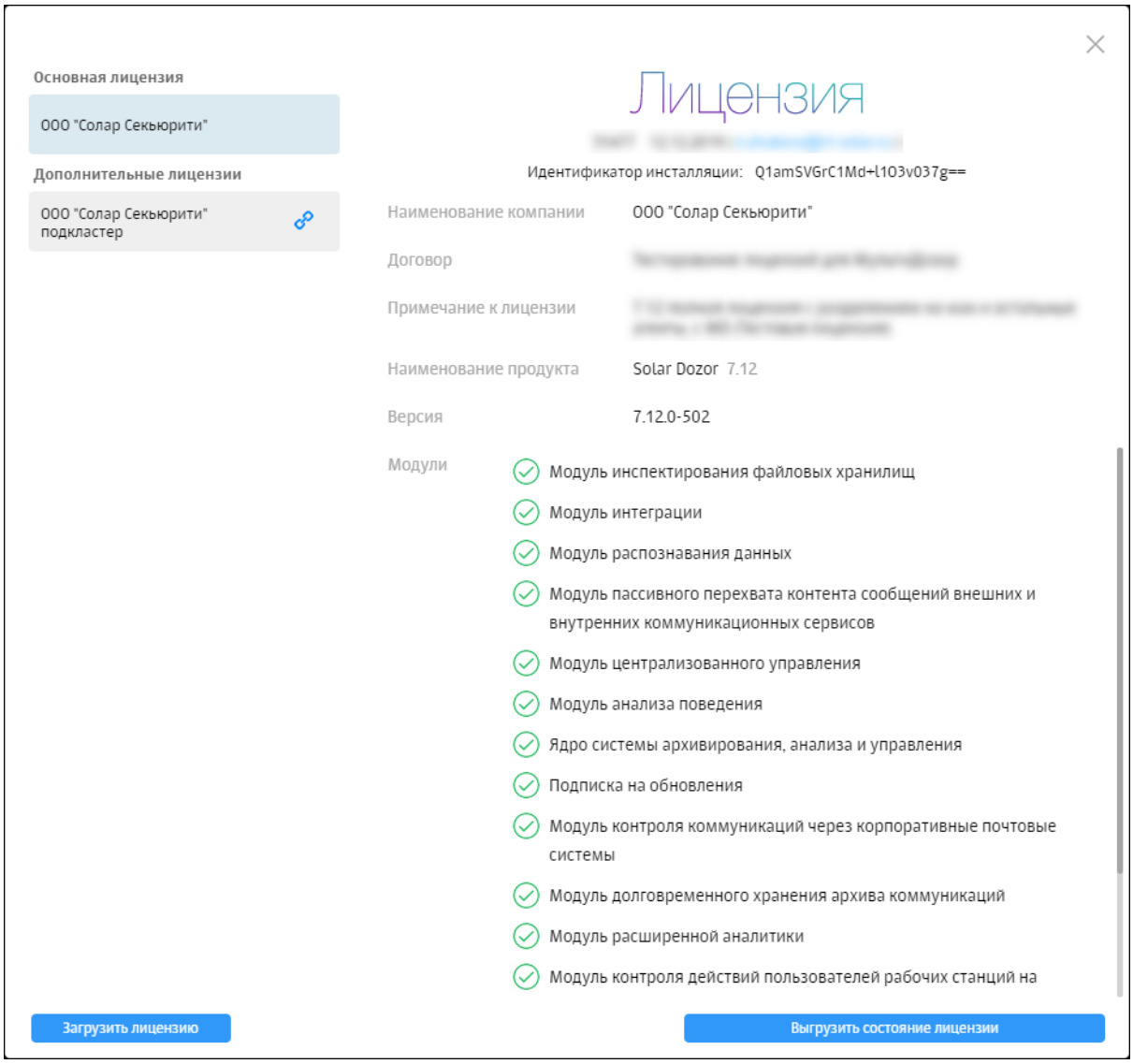


Рис. 6.4. Информация о лицензии Solar Dozor

Для активации территориально-распределенного режима работы Solar Dozor необходимо выполнить следующие действия:

1. Загрузить основную лицензию (master-лицензию) на master-узел.
2. Выполнить настройку подкластеров в соответствии с документом *Руководство системного администратора*.
3. Загрузить лицензии подкластеров.

Изначально после создания подкластера отображается состояние **Лицензия не найдена** (см. Рис.6.3). Для загрузки дополнительных лицензий (лицензий подкластеров) следует выполнить следующие действия:

1. Нажать на значок в правом верхнем углу веб-интерфейса.
2. Выбрать из списка пункт **Лицензия**.
3. В появившемся окне **Лицензия** перейти в раздел требуемого подкластера.
4. Нажать кнопку **Загрузить лицензию**.
5. В открывшемся окне проводника указать путь к файлу с лицензией, после чего нажать кнопку **Открыть** (**Open**) и дождаться загрузки лицензии.

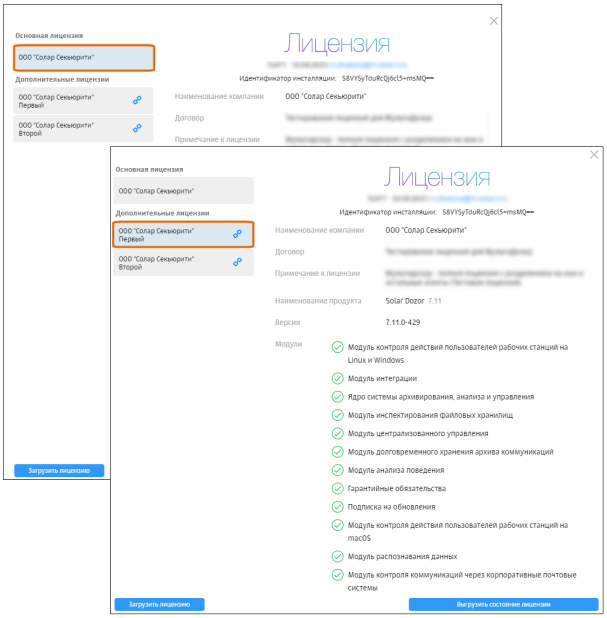


Рис. 6.5. Информация о лицензии при территориально-распределенном режиме работы Solar Dozor

В лицензии применяются следующие условные обозначения:

- – модуль доступен для использования.

-  – требуется внимание к модулю: до окончания разрешённого лицензией срока использования осталось менее 30 дней и/или количественное ограничение модуля превышено не более чем на 20%.

-  – модуль недоступен для использования: истёк или не начался разрешённый лицензией срок использования или количественное ограничение модуля превышено более чем на 20%.

В лицензии также указаны версия и сборка продукта.

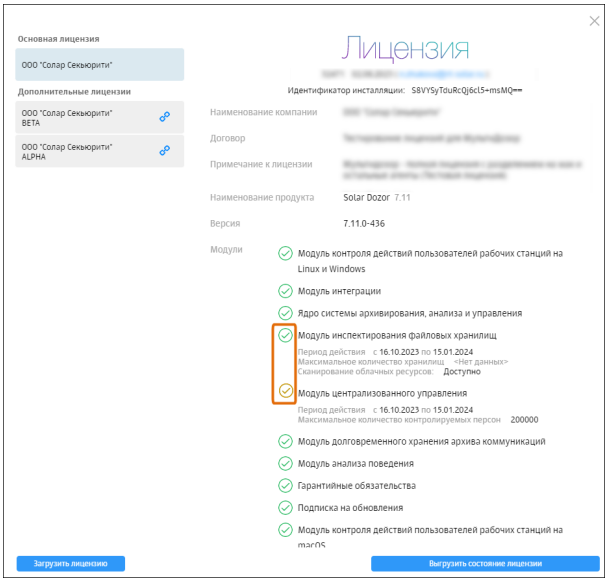


Рис. 6.6. Условные обозначения в лицензии

Внимание!

После замены лицензии с истекшим сроком действия необходимо перезапустить следующие процессы:

- *agent-control-ng*
- *agent-server*
- *archiver-server*
- *mailfilter*
- *smap-smtp-gw*
- *crawler-ccc*
- *crawler-database*
- *crawler-pccc*
- *crawler-processor*
- *crawler-scanner*

- *crawler-snapshot*
- *smap-activemq*

Контроль состояния лицензии осуществляется сервисом **license-server**, входящим в роли **Сервер управления** (**master**) и **Сервер лицензирования подкластера** (**license-server**). Сервис выполняет следующие функции:

- Периодическая проверка идентификатора инсталляции на соответствие указанному в лицензии (по умолчанию – каждые 30 минут).

  В случае несоответствия идентификатора инсталляции, сформированного на основе характеристик аппаратной платформы master-узла, и идентификатора, указанного в лицензии, на экран выводится соответствующее уведомление, а функционирование Solar Dozor прекращается.

- Периодический пересчёт количества активных адресов электронной почты и сравнение его с количеством, указанным в лицензии (по умолчанию – раз в сутки).

  В случае превышения разрешённого лицензией количества активных адресов электронной почты не более чем на 20% на экран выводится соответствующее уведомление, а ресурс **Количество активных адресов** принимает состояние WARNING (см. раздел *Мониторинг состояния ресурсов* документа *Руководство системного администратора*). В случае превышения разрешённого лицензией количества активных адресов электронной почты более чем на 20% на экран выводится соответствующее уведомление, а ресурс **Количество активных адресов** принимает состояние CRITICAL. Функционирование Solar Dozor при этом не прекращается.

  В случае территориально-распределённой инсталляции, при увеличении количества активных адресов электронной почты требуется расширение как основной лицензии, так и лицензии филиала, где было увеличено это количество.

  Адрес электронной почты считается активным, если он принадлежит одному из доменов, указанных в лицензии в качестве внутренних, и является источником хотя бы одного сообщения в архиве за последние 30 дней.

- Периодическая проверка сроков действия модулей.

- Периодическая отправка информации с серверов лицензирования подкластеров на сервер управления.

После загрузки лицензии на каждом узле появляется кэш лицензии. Сервис почтового фильтра (**mailfilter**) обновляет этот кэш раз в пять минут, делая запросы к сервису **license-server**. В случае недоступности сервиса **license-server** сервис почтового фильтра обращается к этому кэшу для проверки лицензионных ограничений. Для сервиса почтового фильтра кэш лицензии остаётся действительным в течение 30 суток с момента последнего обновления. Если кэш лицензии становится недействителен, а сервис **license-server** остается недоступен – сервис почтового фильтра останавливает работу. При этом сервис почтового фильтра продолжает попытки обновить кэш лицензии раз в пять минут, и в случае успеха возобновляет работу.

Аналогичным образом сервер агентов (**agent-server**) делает запросы к сервису **license-server** и обновляет кэш лицензии раз в 10 минут. При неудачной попытке обновления кэша сервер агентов предпринимает новые попытки каждые две минуты. Если с момента последнего обновления кэша лицензии прошёл час или более, то для сервера агентов кэш лицензии становится недействительным, и он деактивирует все зарегистрированные у себя полнофункциональные агенты. При этом сервер агентов продолжает попытки обновить кэш лицензии раз в две минуты, и в случае успеха активирует агенты вновь.

Постоянная лицензия Solar Dozor всегда жёстко привязана к конкретной аппаратной платформе (виртуальной или физической) master-узла Solar Dozor. Для однозначной привязки используется идентификатор инсталляции, представляющий собой особым образом формируемый хэш, зависящий от некоторых уникальных характеристик аппаратного обеспечения master-узла. Идентификатор инсталляции формируется при первом запуске GUI Solar Dozor и передаётся инженерами внедрения в вендорскую службу поддержки, которая на его основе выпускает активированную лицензию для постоянного использования. Изменение хотя бы одной из характеристик master-узла, от которых зависит идентификатор инсталляции, приводит к недействительности выпущенной лицензии и неработоспособности Solar Dozor. При функционировании master-узла в виртуальной среде миграция виртуальной машины приводит к тем же последствиям. В этих случаях необходимо обратиться в вендорскую службу поддержки для повторного выпуска лицензии.

Помимо аппаратных характеристик, на идентификатор инсталляции также влияют значения, записанные в файлах с путями вида **/sys/devices/system/cpu/cpu<num>/online**, где **<num>** – номер ядра процессора. Изменение хотя бы одного из них приводит к изменению идентификатора инсталляции.

Примечание

Идентификатор инсталляции не зависит от характеристик оперативной памяти и жёстких дисков, то есть их замена не приводит к недействительности лицензии.

Примечание

С условиями лицензионного соглашения с конечным пользователем Solar Dozor можно ознакомиться на сайте компании «Solar Security» (по адресу: https://rt-solar.ru/about_company/information/doc-EULA/EULA_Dozor_2023.pdf).

6.5.2. Загрузка лицензий других продуктов

Solar Dozor также позволяет хранить лицензии других продуктов, имеющие тот же формат. Например, продукт DCAP не имеет собственного сервера лицензий и вынужден использовать сервер лицензий Solar Dozor. Загрузка лицензий других продуктов выполняется так же, как и загрузка лицензий Solar Dozor. При загрузке с помощью GUI нескольких лицензий одного и того же продукта необходимо учитывать следующее:

- Без использования распределенного режима (модуль **Мультидозор**) новая лицензия Solar Dozor всегда замещает имеющуюся;

- При использовании распределенного режима новая лицензия Solar Dozor замещает имеющуюся только в случае совпадения идентификатора инсталляции. Отсутствие идентификатора в разных файлах лицензии также считается совпадением;
- Новые лицензии других продуктов всегда замещают имеющуюся лицензию того же продукта.

В директории хранения файлов лицензии не рекомендуется хранить файлы, у которых совпадают комбинации идентификатора инсталляции и имени продукта. Такая ситуация может возникнуть при добавлении файла лицензии напрямую в репозиторий или при загрузке файла лицензии с помощью сервиса другого продукта (например, DCAP). В этом случае будет использоваться файл лицензии с наибольшим значением идентификатора лицензии (поле **license-id**), и только эта лицензия будет отображаться для продукта в GUI.

При просмотре лицензий других продуктов в GUI Solar Dozor для них не будет отображаться список модулей, поскольку Solar Dozor не обладает возможностью чтения соответствующих полей таких лицензий.

7. Настройка Solar Dozor для работы в активном режиме

Для настройки активного режима системы необходимо следующее:

1. Настроить маршрутизацию почтового потока в корпоративной сети таким образом, чтобы не существовало маршрутов между почтовыми серверами организации и внешним почтовым шлюзом в обход серверов Solar Dozor.
2. Настроить серверы фильтрации Solar Dozor для корректного приёма и пересылки почтовых сообщений.

Первая задача возлагается на системного (сетевого) администратора организации и решается им самостоятельно.

Для настройки серверов фильтрации Solar Dozor для корректного приёма и пересылки почтовых сообщений необходимо:

1. Настроить программу отправки **Postfix** (раздел 7.1.1).
2. Создать профиль отправки (раздел 7.2).
3. Настроить политику фильтрации (раздел 7.3).
4. Настроить балансировщик нагрузки на серверы фильтрации (раздел 7.4).
5. Настроить отправку сообщений при ошибках фильтрации (раздел 7.5).

7.1. Настройка программы отправки

Необходимо установить и настроить программу отправки сообщений **Postfix**.

7.1.1. Настройка Postfix

Для настройки Postfix необходимо выполнить на master-узле следующие действия:

1. Перейти в CLI master-узла и установить пакеты **postfix**, **mailx** и **telnet**, если они отсутствуют в системе:

   # apt-get install postfix mailx telnet

2. Открыть для редактирования файл **/etc/postfix/master.cf** и закомментировать с помощью символа **#** следующую строку:

   ```
   #smtp      inet  n       -       n       -       -       smtpd
   ```

3. Открыть для редактирования файл **/etc/postfix/main.cf** и добавить в конец файла следующие строки:

   ```
   # dns_hostname
   myhostname = <node_name>

   # dns_FQDN
   mydomain = <domain_name>

   relayhost = [<relay_IP>]
   ```

```
mailbox_size_limit = 0
message_size_limit = 0

smtp_generic_maps = hash:/etc/postfix/generic
```

где:

- **<node_name>** – имя узла, отображаемое в системных уведомлениях.
- **<domain_name>** – доменное имя узла.
- **<relay_IP>** – IP-адрес узла, через который будет выполняться отправка сообщений за пределы периметра.
- **mailbox_size_limit** – ограничение на размер почтового ящика в байтах. Рекомендуемое значение - **0** (нет ограничения).
- **message_size_limit** – ограничение на размер сообщений в байтах. Рекомендуемое значение - **0** (нет ограничения).
- **/etc/postfix/generic** – путь к конфигурационному файлу, содержащему информацию о подмене почтовых адресов.

4. Открыть файл **/etc/postfix/generic** и добавить в его конец следующую строку:

```
root@dozor.solar.local master@organization.local
```

Вместо адреса **master@organization.local** можно использовать любой другой по усмотрению. Сохранить и закрыть файл.

5. Сохранить и применить настройки, выполнив команды:

 # postmap /etc/postfix/master.cf

 # postmap /etc/postfix/main.cf

 # postmap /etc/postfix/generic

 # postfix reload

 # systemctl enable postfix

Если конфигурация задана верно, то ошибок не возникнет и в каталоге **/etc/postfix/** будут созданы файлы **generic.db**, **main.cf.db** и **master.cf.db**.

6. Проверить, что сервис **postfix** запускается корректно, выполнив команду:

 # systemctl status postfix

Вывод команды не должен содержать ошибок.

7. Проверить связь с узлом отправки сообщений за пределы периметра, выполнив команду:

 # telnet <relay_IP> 25

В результате выполнения должно быть выведено сообщение вида:

```
Connected to <relay_IP>
```

8. Отправить тестовое сообщение, выполнив команду вида:

   # echo "test mail" | mail -s "Check mail" <address>

   где **<address>** – почтовый адрес, на который будет отправлено сообщение с темой **Check mail** и текстом **test mail**.

9. Проверить отправку сообщения, выполнив команду:

   # cat /var/log/maillog | grep <address>

   В найденной строке журнала об успехе будут свидетельствовать значения status=sent и 250 Ok. При этом сообщение придет по указанному адресу с адресом отправителя **master@organization.local**.

После этого необходимо выполнить на всех узлах с ролью **Фильтр почтового потока** следующие действия:

1. Перейти в CLI и установить пакеты **postfix**, **mailx** и **telnet**, если они отсутствуют в системе:

   # yum install postfix mailx telnet

2. Открыть для редактирования файл **/etc/postfix/master.cf** и закомментировать с помощью символа **#** следующую строку:

```
#smtp      inet  n       -       n       -       -       smtpd
```

3. Открыть для редактирования файл **/etc/postfix/main.cf** и добавить в конец файла следующие строки:

```
# dns_hostname
myhostname = <node_name>

# dns_FQDN
mydomain = <domain_name>

relayhost = [<relay_IP>]

mailbox_size_limit = 0
message_size_limit = 0

# Bounce timeout for queue. How long a MAILER-DAEMON message stays in the queue before it is
 considered undeliverable
bounce_queue_lifetime = 30m

# The minamal time between attempts to deliver a deferred message
minimal_backoff_time = 10m
# The maximal time between attempts to deliver a deferred message
maximal_backoff_time = 1h

# How often the queue manager scans the queue for deferred mail
```

```
queue_run_delay = 30m

# Max time to try send a message before return to sender
maximal_queue_lifetime = 3h
# Templates for system messages
bounce_template_file = /etc/postfix/bounce.cf

smtp_generic_maps = hash:/etc/postfix/generic
```

где:

- **<node_name>** – имя узла, отображаемое в системных уведомлениях.
- **<domain_name>** – доменное имя узла.
- **<relay_IP>** – IP-адрес узла, через который будет выполняться отправка сообщений за пределы периметра.
- **mailbox_size_limit** – ограничение на размер почтового ящика в байтах. Рекомендуемое значение - **0** (нет ограничения).
- **message_size_limit** – ограничение на размер сообщений в байтах. Рекомендуемое значение - **0** (нет ограничения).
- **bounce_queue_lifetime** – время жизни для сообщений об ошибках, недоставке и других подобных, в течение которого они будут оставаться в очереди на отправку.
- **minimal_backoff_time** – минимальное время, на которое может быть отложена отправка сообщений, которые не были отправлены из-за временных неисправностей (отсутствие ответа от принимающего сервера или его просьба повторить запрос позже).
- **maximal_backoff_time** – максимальное время, на которое может быть отложена отправка сообщений, которые не были отправлены из-за временных неисправностей.
- **queue_run_delay** – период сканирования очереди сообщений с целью их повторной отправки.
- **maximal_queue_lifetime** – максимальное время, отведённое на попытки отправить сообщение из очереди, прежде чем оно вернётся пользователю с ошибкой.
- **bounce_template_file** – путь к файлу с шаблонами отправки уведомлений об ошибках отправки.
- **/etc/postfix/generic** – путь к конфигурационному файлу, содержащему информацию о подмене почтовых адресов.

Внимание!

Параметры времен, приведенные в этом примере, подходят для большинства случаев. В некоторых случаях может потребоваться более точная подгонка этих параметров. Текущие параметры можно просмотреть, выполнив команду:

 # postconf -n

Параметры по умолчанию можно просмотреть, выполнив команду:

 # postconf -d

4. Открыть файл **/etc/postfix/generic** и добавить в его конец следующую строку:

```
root@dozor.solar.local filter@organization.local
```

Вместо адреса **filter@organization.local** можно использовать любой другой по усмотрению. Сохранить и закрыть файл.

5. Создать файл шаблонов сообщений об ошибках, выполнив команду:

 # touch /etc/postfix/bounce.cf

Заполнить этот файл подготовленным шаблоном, например:

```
failure_template = <<EOF
Charset: UTF-8
From: MAILER-DAEMON (Mail Delivery System)
Subject:
=?UTF-8?B?0J3QtdCy0L7Qt9C80L7QttC90L4g0LTQvtGB0YLQsNCy0LjRgtGMINGB0L7QvtCx0YnQtdC90LjQtQ==?=
Postmaster-Subject: Postmaster Copy: Undelivered Mail

Это почтовая система на сервере $myhostname.

Ваше сообщение не может быть доставлено одному или нескольким получателям.

Для получения дополнительной помощи отправьте письмо на адрес <адрес-техподдержки>.
Приложите данный отчет о проблеме.
Вы можете удалить свой собственный текст из прикрепленного сообщения.

Почтовая система <название организации>.
EOF

delay_template = <<EOF
Charset: UTF-8
Postmaster-Subject: Postmaster Warning: Delayed Mail

Это почтовая система на сервере $myhostname.

###############################################################################
# ЭТО ТОЛЬКО ПРЕДУПРЕЖДЕНИЕ. ВАМ НЕ НУЖНО ПОВТОРНО ОТПРАВЛЯТЬ ВАШЕ СООБЩЕНИЕ #
###############################################################################
Ваше сообщение не удалось доставить.
Попытки отправки будут повторяться, пока не пройдёт $maximal_queue_lifetime часа.

Для получения дополнительной помощи отправьте письмо на адрес <адрес-техподдержки>.
Если вы это сделаете, прикрепите этот отчет о проблеме.
Вы можете удалить свой собственный текст из прикрепленного сообщения.

Почтовая система <название организации>.
EOF

success_template = <<EOF
```

```
Charset: UTF-8
From: MAILER-DAEMON (Mail Delivery System)
Subject:
=?UTF-8?B?0J/QuNGB0YzQvNC+INGD0YHQv9C10YjQvdC+INC00L7RgdGC0LDQstC70LXQvdC+?=


Это почтовая система на сервере $myhostname.

Ваше сообщение было успешно доставлено адресату(ам) перечисленным ниже.
Если возникнут проблемы на стороне получателя, вы получите уведомление об ошибках из
почтовой службы получателя.

Почтовая система <название организации>.
EOF

verify_template = <<EOF
Charset: UTF-8
From: MAILER-DAEMON (Mail Delivery System)
Subject: =?UTF-8?B?0J7RgtGH0LXRgiDQviDQtNC+0YHRgtCw0LLQutC1INC/0LjRgdGM0LzQsA==?=


Это почтовая система на сервере $myhostname.

Прилагается запрошенный вами отчет о доставке почты.

Почтовая система <название организации>.
EOF
```

Следует подставить адрес технической поддержки в организации. Также можно внести любые другие изменения в тела сообщений по усмотрению.

6. Убедиться в отсутствии ошибок в шаблонах сообщений, выполнив команду:

   # postconf -b /etc/postfix/bounce.cf

   В результате выполнения на экран должен быть выведен текст шаблонов сообщений.

7. Сохранить и применить настройки, выполнив команды:

   # postmap /etc/postfix/master.cf

   # postmap /etc/postfix/main.cf

   # postmap /etc/postfix/generic

   # sudo postfix reload

   # systemctl enable postfix

7.1.2. Настройка аутентификации для Postfix

Для настройки аутентификации для **Postfix** необходимо на всех узлах выполнить следующие действия:

1. Установить пакеты, необходимые для настройки аутентификации, выполнив команду:

   # apt-get install nano opensll openssl-devel openssl-libs gcc mailx cyrus-sasl

2. Загрузить архив **cyrus-sasl.2.1.26** по ссылке **https://github.com/cyrusimap/cyrus-sasl/releases/tag/cyrus-sasl-2.1.26**.

3. Распаковать загруженный архив и перейти в каталог **cyrus-sasl.2.1.26/plugins**.

4. Открыть файл **ntlm.c** и найти в нём следующие строки:

```
if (sendv2 &&
 (sendv2[0] == '1'  sendv2[0] == 'y'
(sendv2[0] == 'o' && sendv2[1] == 'n') || sendv2[0] == 't'))
```

   Заменить эти строки на строку:

```
if(1)
```

5. Назначить права на выполнение для скрипта **configure**, выполнив команду:

   chmod +x /cyrus-sasl.2.1.26/configure

6. Перейти в каталог **cyrus-sasl.2.1.26** и сконфигурировать пакет для сборки, выполнив команду:

   # ./configure --enable-ntlm --enable-login

7. Произвести сборку, выполнив команду:

   # make

8. Установить собранный пакет, выполнив команду:

   # make install

9. Создать ссылку на каталог с плагинами, выполнив команду:

   # ln -s /usr/local/lib/sasl2 /usr/lib/sasl2

10. Убедиться, что все плагины загружены, выполнив команду:

    # pluginviewer -c

    На экран будет выведен список загруженных плагинов. Каждая строка, начинающаяся со слова **Plugin** должна содержать статус **[loaded]**.

11. Открыть файл **/etc/postfix/main.cf** и отредактировать конфигурацию **Postfix**, добавив параметры клиента следующего вида:

```
smtp_tls_security_level = encrypt
smtp_tls_policy_maps = hash:/etc/postfix/tls_policy
smtp_tls_loglevel = 2
smtp_tls_CAfile = certs/CA_chain.pem
smtp_sasl_auth_enable = yes
smtp_sasl_tls_security_options = noanonymous
smtpd_sasl_auth_enable = yes
smtpd_sasl_mechanism_filter = login
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_generic_maps = hash:/etc/postfix/generic
sender_canonical_maps = hash:/etc/postfix/canonical
```

12. Создать файл **/etc/postfix/transport** и записать в него строку следующего вида:

    <corp_domain> smtp:<relay_address>

    где **<corp_domain>** – внутренний почтовый домен организации, **<relay_address>** – IP-адрес и порт почтового сервера организации. Пример:

    ```
    organisation.ru smtp:10.10.10.10:1025
    ```

13. Считать конфигурацию и перезапустить сервис **postfix**, выполнив команды:

    # postmap /etc/postfix/transport

    # systemctl reload postfix

14. Создать файл **/etc/postfix/sasl_passwd** и записать в него строку следующего вида:

    <relay_address> <login>:<password>

    где **<relay_address>** – IP-адрес и порт почтового сервера организации, **<login>:<password>** – имя технической учётной записи, от имени которой предполагается отправка уведомлений, и её пароль.

15. Выполнить следующую команду:

    # postmap /etc/postfix/sasl_passwd

    Внимание!

    *Эту команду необходимо выполнять после каждого редактирования файла **/etc/postfix/sasl_passwd**.*

16. Создать файл **/etc/sasl2/smtp.conf** и записать в него следующее:

    ```
    ntlm_v2: yes
    mech_list: ntlm
    ```

7.2. Настройка профиля отправки

Для настройки профиля отправки необходимо выполнить следующие действия:

1. В GUI Solar Dozor перейти в раздел **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Отправка** и в секции **Наборы параметров отправки сообщений** нажать **Добавить**.

2. Задать значения следующих параметров:

    - **Название набора параметров** – ввести произвольное название.
    - **Метод доставки** – **sendmail**
    - **Путь к программе sendmail** – **/usr/sbin/sendmail.postfix**

3. В строке **Файл конфигурации sendmail** нажать кнопку **Добавить** и в появившемся поле ввести значение **/etc/postfix/main.cf**.

4. Нажать **Сохранить**, **Применить**.

5. Перейти в раздел **Политика > Шаблоны и профили** и создать новый профиль отправки для метода **sendmail**:

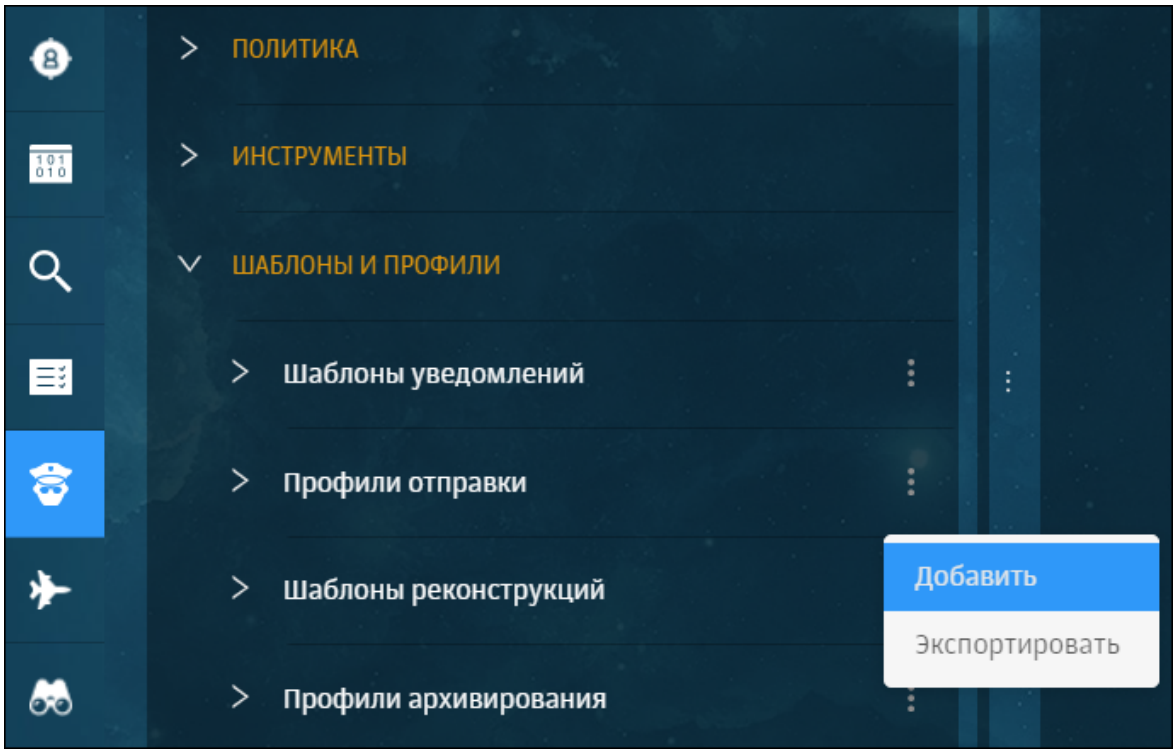


Рис. 7.1. Добавление профиля отправки

6. Ввести название профиля отправки, нажать **Сохранить** и задать значения следующих параметров:

   - **Параметры отправки** – ввести название, выбранное для набора параметров в шаге 2.
   - **Количество попыток отправки** – 1.
   - **Действие по исчерпании попыток** – **Переместить сообщение в err-спул**.

7. Нажать **Сохранить**, **Применить политику**.

7.3. Создание правила политики фильтрации

После создания профиля отправки и настройки программы **Sendmail** следует настроить головное правило политики фильтрации. Для этого необходимо выполнить следующие действия:

1. В GUI Solar Dozor перейти в раздел **Политика > Политика > Наборы правил** и выбрать головной набор правил (отмеченный звёздочкой).

Примечание

*Если головным является набор правил **Архивировать все сообщения** – следует создать новый набор правил и назначить его головным, поскольку набор правил **Архивировать все сообщения** является системным и не может быть изменён.*

2. Добавить правило следующего содержания:

   - **Если** – **Все сообщения**
   - **то** – **Отправить**
   - **Профиль отправки** – указать созданный ранее профиль отправки.
   - **Выполнить**

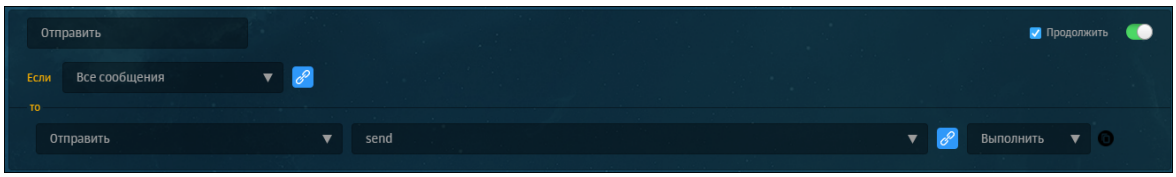


Рис. 7.2. Правило фильтрации для активного режима

3. Нажать **Сохранить**, **Применить политику**.

7.4. Настройка балансировщика

Кластер Solar Dozor может использовать несколько серверов фильтрации. В этом случае для распределения трафика по серверам используют балансировщик.

Балансировщик управляет потоками данных (прозрачно и незаметно для клиентов) и позволяет увеличить производительность Solar Dozor за счет параллельной обработки запросов на нескольких узлах кластера. Балансировщик контролирует работоспособность серверов фильтрации и автоматически отключает узлы от процесса обработки запросов в случае их недоступности.

Для настройки балансировщика HAProxy необходимо выполнить на master-узле следующие действия:

1. Перейти в раздел GUI **Система > Узлы и роли** и назначить одному из узлов роль **Балансировщик**.
2. Нажать кнопку **Применить**.
3. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Прием сообщений** и в секции **Балансировка трафика** нажать **Добавить**.
4. Задать значения следующих параметров:

   - **Название конфигурации балансировки** – ввести произвольное название.

- **Порт для внешних соединений** – порт, на котором сервис балансировки трафика ожидает соединения (по умолчанию 1010).
- **Время ожидания запроса от клиента (с)** – время ожидания запроса от клиента, выраженное в секундах (по умолчанию 10).

  Примечание

  В качестве клиента выступают внешние системы, например SMTP/HTTP/ICAP-серверы.

- **Время ожидания запроса от сервера (с)** – время ожидания запроса от серверов фильтрации, которые задаются в параметре **Узлы для балансировки**. Выражено в секундах (по умолчанию 10).
- **Максимальное количество соединений** – максимальное количество соединений, которое принимает балансировщик от клиента (по умолчанию 1000).
- **Метод балансировки** – алгоритм балансировки трафика (по умолчанию **roundrobin**).

  При значении **roundrobin** нагрузка будет распределена равномерно в соответствии с весом каждого сервера фильтрации Solar Dozor, если таковой указан ниже. При значении **leastconn** запросы будут передаваться серверу с наименьшим количеством подключений. При значении **source** сервер для соединения назначается на основании хэша IP-адреса отправителя запроса и весов серверов.

5. При необходимости, установить параметр **Узлы для балансировки** в значение **Указать вручную** и задать значения следующих параметров:
   - **Тип балансировки** – протокол, по которому распределяется нагрузка между узлами.
   - **Узлы** – добавить одну или несколько записей резервных узлов, предназначенных для балансировки. Запросы от внешних систем будут перенаправляться на эти узлы при недоступности серверов фильтрации Solar Dozor.

     Запись резервного узла имеет следующие параметры:

     - **Сетевой адрес** – FQDN или IP-адрес резервного узла.
     - **Номер порта** – номер порта, на котором резервный узел будет ожидать соединения.
     - **Вес балансировки** – коэффициент, помогающий балансировщику распределять нагрузку между серверами фильтрации. Узел с большим весом будет получать большее число запросов.

       Пример: сервер с весовым коэффициентом 2 будет получать в 2 раза больше запросов, чем сервер с весом, равным 1.

       Пример 2: имеется три сервера фильтрации A, B и C. Сервера A и B имеют вес, равный 1, а сервер C имеет весовой коэффициент 2. При недоступности сервера C нагрузка распределится равномерно между серверами A и B. При восстановлении своей работоспособности сервер C будет получать в 2 раза больше запросов, чем серверы A и B (каждый по отдельности).

6. Нажать **Сохранить** и **Применить**.

7.5. Настройка отправки сообщений при ошибках фильтрации

В Solar Dozor можно настроить отправку сообщений адресатам при ошибках фильтрации. Например, сообщения, которые не успели распаковаться или обработаться политикой за отведенное время, будут доставлены получателям. В этом случае необходимо:

1. Создать профиль отправки.
2. Настроить отправку уведомлений системному администратору о состоянии ресурсов системы.
3. Настроить политику фильтрации.
4. Активировать отправку сообщений адресатам.

7.5.1. Настройка профиля отправки

Для настройки профиля отправки следует выполнить действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Отправка**.
2. В секции **Сервис отправки сообщений** задать значение параметра **Таймаут на сетевое взаимодействие при использовании SMTP** равным 600.
3. В секции **Наборы параметров отправки сообщений** нажать кнопку **Добавить**.
4. Задать значения следующих параметров:
   - **Название набора параметров** – ввести произвольное название.
   - **Метод доставки** – **smtp**.
5. В строке **Соединения SMTP** нажать кнопку **Добавить** и в появившемся поле задать значения следующих параметров:
   - **Протокол SMTP сервера** – **SMTP**.
   - **SMTP сервер** – ввести FQDN или IP–адрес SMTP-сервера, на который будет выполнена отправка.
   - **SMTP порт** – 25.
6. Нажать **Сохранить**, **Применить**.
7. Перейти в раздел **Политика > Шаблоны и профили** и создать новый профиль отправки по протоколу SMTP (см. Рис.7.1).
8. Ввести название профиля отправки, нажать **Сохранить** и задать значения следующих параметров:
   - **Параметры отправки** – ввести название, выбранное для набора параметров на шаге 4.

- **Количество попыток отправки** – 1.
- **Действие по исчерпании попыток** – **Переместить сообщение в err-спул**.

9. Нажать **Сохранить**, **Применить политику**.

7.5.2. Настройка отправки уведомлений о состоянии ресурсов системы

После создания профиля отправки следует настроить отправки уведомлений системному администратору о состоянии ресурсов системы. Для этого следует выполнить действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование > Мониторинг**.
2. В секции **Сервер мониторинга** раскрыть список **Настройки оповещения**.
3. Раскрыть список **Адрес/порт SMTP-сервера** и задать значения следующих параметров:
   - **Сетевой адрес** – имя SMTP-сервера, заданное на шаге 4 раздела 7.5.1.
   - **Номер порта** – 1025.
4. Указать адреса получателей уведомлений в значениях параметров:
   - **Адреса для отправки уведомлений о проблемах чрезвычайной критичности**.
   - **Адреса для отправки уведомлений о проблемах высокой и средней критичности**.
   - **Адреса для отправки уведомлений о проблемах низкой критичности**.
5. Нажать **Сохранить**, **Применить**.

7.5.3. Создание правила политики фильтрации

После создания профиля отправки и настройки отправки уведомлений о состоянии ресурсов следует настроить головное правило политики фильтрации по инструкции в разделе 7.3.

7.5.4. Активация отправки сообщений адресатам

После настройки головного правила политики фильтрации следует активировать отправку сообщений адресатам при ошибках фильтрации. Для этого необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Политика > Политика > Наборы правил > Обработка ошибок**.
2. Отредактировать правило **Ошибки или таймаут обработки** таким образом, чтобы при срабатывании условия **Ошибки или таймаут обработки** выполнялось действие **Отправить** с использованием ранее настроенного профиля отправки.

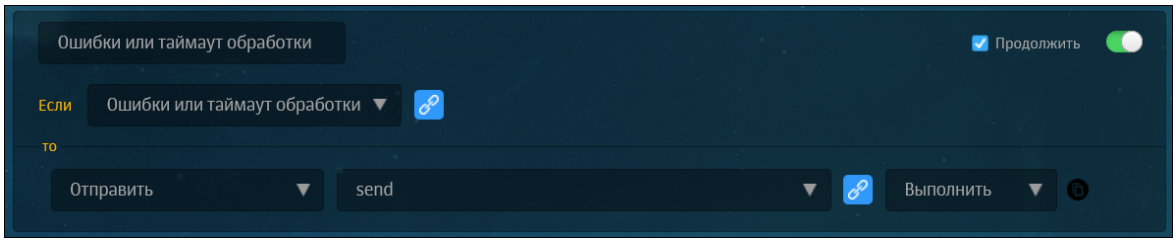


Рис. 7.3. Правило отправки при ошибках

3. Нажать **Сохранить**, **Применить политику**.

8. Первичная настройка Solar Dozor

8.1. Настройка контроля целостности

Для контроля целостности используется скрипт **check_dozor**, который при вызове пересчитывает контрольные суммы неизменяемых исполняемых файлов и сравнивает их с контрольными суммами, хранящимися в БД пакетного менеджера ОС. При несоответствии значений контрольных сумм хотя бы для одного проверяемого файла скрипт отправляет почтовое сообщение с результатами проверки по адресам, заданным в конфигурации. Сообщение с результатами проверки содержит следующую информацию:

- Сетевое имя узла, на котором было обнаружено несоответствие контрольных сумм.
- Данные об ОС.
- Дата и время выполнения проверки.
- Сводная таблица с результатами пересчёта контрольных сумм по всем установочным пакетам Solar Dozor.

Для получения уведомлений о результатах регулярного контроля целостности необходимо выполнить следующие действия:

1. Перейти в GUI и открыть раздел **Система > Конфигурация > Основные настройки > Работа системы**, секцию настроек **Общие настройки системы**, развернуть список **Адреса получателей в системных сообщениях** и задать значения параметров:
   - **Имя почтового ящика** – задать имя почтового ящика (без домена), на который будет отправлено уведомление в случае аварийной остановки системы при несовпадении контрольных сумм в результате проверки целостности.
   - **Имя почтового домена** – задать домен, в котором находится почтовый ящик, заданный в предыдущем параметре.
2. При необходимости, создать дополнительные записи с помощью кнопок **Копировать** или **Добавить** и повторить действия предыдущего шага.
3. Нажать **Сохранить**, **Применить**.

Механизм контроля целостности по умолчанию включен. Для отключения механизма контроля целостности необходимо создать файл **/opt/dozor/SKIP_CHECK_MODE**. Пока этот файл существует – никакие проверки целостности не будут выполняться ни в автоматическом режиме, ни в ручном.

8.2. Назначение ролей узлам

Набор функций, выполняемых каждым узлом кластера Solar Dozor, определяется списком назначенных ему ролей. Каждая роль отражает конкретную прикладную задачу: приём и обработка почтовых сообщений, поиск по архиву сообщений, индексация событий и инцидентов ИБ, и другие. Для решения таких задач используются процессы Solar Dozor. Список процессов, запускаемых на узле Solar Dozor, определяется набором ролей, назначенных этому узлу. Подробная информация о составе ролей приведена в **Приложение С, *Описание ролей и сервисов***.

8.2.1. Назначение ролей с помощью GUI

Для назначения ролей узлам используется вкладка **Система > Узлы и роли**, содержащая информацию о состоянии и ролях всех узлов кластера Solar Dozor. Для назначения узлу какой-либо роли следует щёлкнуть мышью в поле **Роли узла** и выбрать в раскрывающемся списке одну или несколько ролей для узла, а затем щёлкнуть мышью на любой области за пределами списка. Для снятия с узла какой-либо роли следует нажать на крестик на плашке с названием этой роли.

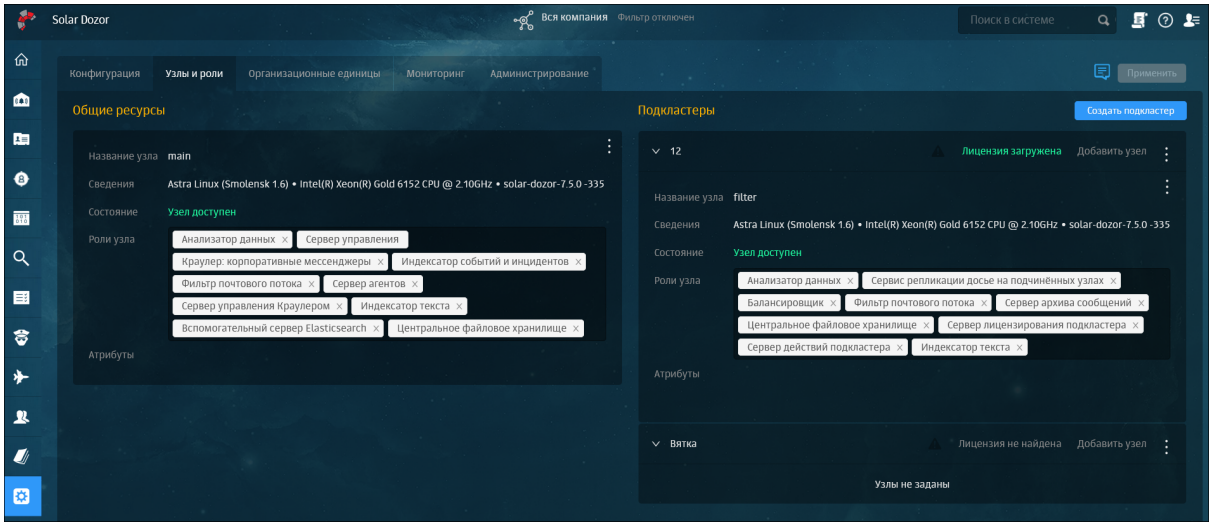


Рис. 8.1. Назначение ролей

Для отображения списка узлов используется пагинация, которая располагается в нижней части интерфейса. На одной странице может быть одновременно отображено не более пяти узлов (как при использовании модуля **Мультидозор**, так и без него).

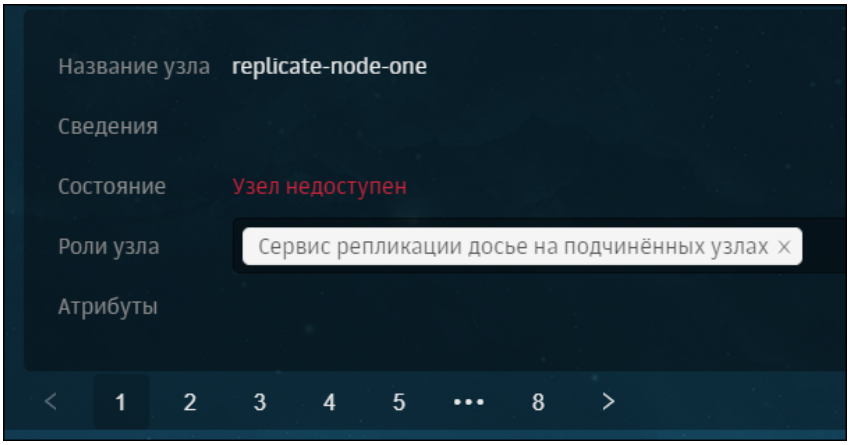


Рис. 8.2. Разбиение на страницы

Если в системе имеется более пяти узлов, в правой верхней части экрана отображается поле **Поиск по узлам**.

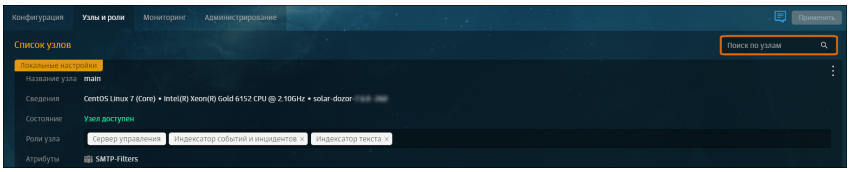


Рис. 8.3. Поиск узлов

Минимальный набор ролей для нормального функционирования Solar Dozor:

- **Сервер управления** – роль будет назначена одному из узлов в процессе установки.
- **Хранилище индексов событий и инцидентов** – роль необходима для хранения индексов событий и инцидентов ИБ. Необходимо назначить эту роль master-узлу.
- **Индексатор текста** – роль необходима для индексирования сообщений в архиве и хранения индексов. При назначении этой роли узлам Solar Dozor следует руководствоваться информацией из раздела 8.8.
- **Фильтр почтового потока** – роль необходима для фильтрации и отправки сообщений согласно заданной политике. Следует назначать эту роль высокопроизводительным серверам, по возможности – двум и более с использованием балансировщика нагрузки.
- **Мониторинг локального почтового шлюза** – роль необходима для того, чтобы система мониторинга могла отслеживать состояние сервиса почтового шлюза на тех узлах, где его функционирование необходимо. В большинстве случаев такие узлы имеют роли **Сервер управления**, **Балансировщик** и **Фильтр почтового потока** (особенно при реализации активного режима работы Solar Dozor).
- **Центральное файловое хранилище** – роль необходима для хранения тел и текстовых частей сообщений архива, снимков экрана и вложений, отображаемых в большой карточке персоны.
- **Анализатор данных** – роль необходима для работы сервисов цифровых отпечатков, идентификаторов и извлечения текстов и метаинформации из вложений.

8.2.2. Назначение ролей с помощью CLI

Для получения списка ролей и доступных узлов необходимо выполнить следующую команду:

 # /opt/dozor/bin/set-role

На экран будет выведена информация следующего вида:

```
Available roles:
 - api-gateway
 - master
 - storage
 - ocr
 - god-server
 - cassandra
 - analyzer
 - traffic-agent
 - abook-slave
 - agent-server
```

```
- fsng-client
- fsng-storage
- text-indexer
- historic-text-indexer
- incident-indexer
- historic-incident-indexer
- local-incident-daemon
- elasticsearch
- smtp-filter
- action-server
- action-server-master
- category-server
- im-crawler
- crawler-x
- crawler-x-master
- uba-server
- time-control
- balancer
- software-center
- license-server
- indexer-only
- historic-indexer-only
- webserver-local
- mail-gw
- media-processor
Available nodes:
- 0f676af8-e25d-481e-a193-2aaecb2a2eed filter
- main main
```

Для назначения узлу какой-либо роли или списка ролей следует выполнить команду следующего вида:

 # /opt/dozor/bin/set-role <role-list> <name>

где **<role-list>** – роли, перечисленные через пробел, а **<name>** – имя узла Solar Dozor. Имена узлов перечислены в списке **Available nodes** при выполнении команды **set-role** (последнее значение в строке).

Внимание!

*При выполнении команды на master-узле следует убедиться, что среди назначаемых ролей есть **master**, а в качестве имени узла следует указать **main**.*

Для получения списка ролей, назначенных узлу, необходимо выполнить следующую команду:

 # /opt/dozor/bin/get-role

Скрипт **get-role** имеет следующий формат:

get-role [<node-name> | total | list]

где **<node-name>** – имя узла, список ролей которого требуется получить. Команда **get-role** без аргументов выводит на экран список ролей текущего узла.

Команда
get-role total
выводит на экран списки ролей всех узлов кластера.

Команда
get-role list
выводит на экран список доступных ролей.

8.3. Создание и настройка БД архива PostgreSQL

В Solar Dozor может быть создано сколь угодно много БД архива сообщений (под управлением СУБД PostgreSQL). Для создания БД архива сообщений необходимо сначала настроить схему соединения с БД (раздел 8.3.1), а затем создать схему БД (раздел 8.3.2).

8.3.1. Настройка схемы соединения с БД

Для настройки схемы соединения с БД PostgreSQL необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Доступ к данным** и в секции **Схемы соединений с БД** добавить новую запись с помощью кнопки **Добавить**.

2. Установить следующие значения параметров для новой записи:

   - **Имя схемы соединения с базой данных** – указать значение вида **db-conn-<n>**, где **<n>** – значение параметра **id** для этой записи (например, **db-conn-4**).
   - **Включено** – установить флажок.
   - **Настройки использования соединения с БД**:
     - **Использовать БД для поиска по архиву**, **Использовать БД для архивирования сообщений** – установить флажки.
     - **Использовать БД для архивирования по умолчанию** – установить флажок. Подробнее об использовании этого флажка см. документ *Руководство пользователя*, раздел *Профили архивирования*.
   - **Тип базы данных** – оставить значение **pgsql**.
   - **Настройки соединения с базой**:
     - **Сетевое имя сервера базы данных** – указать FQDN или IP-адрес узла, на котором предполагается размещение базы данных архива.
     - **Сетевой порт сервера базы данных** – указать порт, на котором БД архива будет ожидать соединения. Порт не должен быть занят никаким другим сервисом на данном узле (см. раздел 4.4).
     - **Имя базы данных** – указать имя базы данных. К этому значению предъявляются те же требования, что и к именованию каталогов в ОС. Рекомендуется выбирать имя, отражающее назначение создаваемой БД (например, **archive-01**).

- **Пользователь базы данных** – указать имя **dozor**.
- **Пароль пользователя базы данных** – рекомендуется задать уникальный пароль для доступа к БД. Если оставить значение по умолчанию – доступ к БД будет осуществляться без пароля.

- **Использование секционирования** – установить значение **используется**, если требуется секционирование БД, и задать подчинённые параметры по усмотрению (описание параметров и подробная информация о секционировании в БД PostgreSQL приведены в документе *Руководство системного администратора*, раздел *Секционирование БД PostgreSQL*).

3. Нажать **Сохранить** и **Применить**.

8.3.2. Создание схемы БД

После настройки соединения необходимо создать схему БД, выполнив следующие действия:

1. Подключиться по протоколу SSH к узлу, указанному в параметре **Сетевое имя сервера базы данных** при настройке схемы соединения с БД.

2. Переключиться на работу от имени пользователя **dozor**, запустить интерпретатор команд shell и перейти в каталог **/opt/dozor/smap/schema/pgsql/**, выполнив следующие команды:

   # su - dozor

   $ /opt/dozor/bin/shell

   $ cd /opt/dozor/smap/schema/pgsql/

3. Создать схему БД с помощью скрипта **create-database.sh**, выполнив команду:

   $ ./create-database.sh <path> -con <conn>

   где **<path>** – каталог, в котором создаётся БД (например, **/data/base/smap-archive/**), а **<conn>** – имя схемы соединения с БД, определённое в настройках соединения (например, **db-conn-4**).

4. Переключиться на работу от имени пользователя **root** и запустить командную оболочку, выполнив команды:

   $ exit

   $ su - root

   # /opt/dozor/bin/shell

5. Перейти в каталог **<path>** (**/data/base/smap-archive/** в данном примере) и отредактировать конфигурационный файл **pg_hba.conf** таким образом, чтобы он содержал строки, определяющие доступ к узлу БД с других узлов кластера Solar Dozor. Пример таких строк в случае использования пароля для доступа к БД:

```
host all all <master-host> scram-sha-256
host all all <filter-host> scram-sha-256
```

где **<master-host>** – IP-адрес или FQDN master-узла, **<filter-host>** – IP-адрес или FQDN дополнительного узла фильтрации, например:

```
host all all master.dozor.local scram-sha-256
host all all filter1.dozor.local scram-sha-256
```

При использовании IP-адресов необходимо также использовать маску подсети, например:

```
host all all 192.168.100.2/32 scram-sha-256
host all all 192.168.100.3/32 scram-sha-256
```

Пример строк в случае отказа от использования пароля для доступа к БД (не рекомендуется):

```
host all all <master-host> trust
host all all <filter-host> trust
```

где **<master-host>** – IP-адрес или FQDN master-узла, **<filter-host>** – IP-адрес или FQDN дополнительного узла фильтрации, например:

```
host all all master.dozor.local trust
host all all filter1.dozor.local trust
```

При использовании IP-адресов необходимо также использовать маску подсети, например:

```
host all all 192.168.100.2/32 trust
host all all 192.168.100.3/32 trust
```

6. В этом же каталоге открыть конфигурационный файл **postgresql.conf** и найти строку с параметром **lc_messages**. Строка должна выглядеть следующим образом:

   ```
   lc_messages = 'C'
   ```

   Если параметр имеет любое другое значение, следует заменить его на **'C'** (заглавная латинская буква C, заключённая в прямые апострофы). Сохранить и закрыть файл.

7. После создания схемы БД PostgreSQL в каталоге **/opt/dozor/smap/schema/pgsql** создаётся скрипт **dozor-postgresql.service**, в котором записывается пользователь, от имени которого создана БД, а также каталог и порт, на котором работает БД. Необходимо скопировать скрипт **dozor-postgresql.service** в каталог **/etc/systemd/system/** и переименовать его, например в **archive.service**:

   ~$ sudo cp /opt/dozor/smap/schema/pgsql/dozor-postgresql.service /etc/systemd/system/archive.service

8. От имени пользователя **root** выполнить следующие команды:

   ~$ sudo systemctl daemon-reload

   ~$ sudo systemctl enable archive.service

   ~$ sudo systemctl start archive.service

9. Перезагрузить процессы Solar Dozor, выполнив команду:

$ /opt/dozor/bin/dsctl restart

Если при настройке соединения с БД для параметра **Использование секционирования** было задано значение **используется**, то необходимо настроить автоматическое создание секций с помощью планировщика **cron**. Для этого необходимо выполнить следующие действия:

1. На master-узле открыть расписание планировщика (при запросе системы выбрать редактор **vim**):

   # crontab -u dozor -e

2. Нажать клавишу **i** и добавить в расписание после комментария **### End: schedule of crontab entry ###** следующую строку:

   ```
   0 0 * * * bash /opt/dozor/smap/schema/pgsql/shell/part-control -con <conn> > /dev/null 2>&1
   ```

   где **<conn>** – имя схемы соединения с БД, определённое в настройках соединения (например, **db-conn-4**).

3. Нажать клавишу **Esc**, ввести **:wq** и нажать **Enter**.

8.4. Настройка БД для хранения событий и инцидентов ИБ

Для хранения событий и инцидентов ИБ Solar Dozor использует БД PostgreSQL. Для настройки БД событий и инцидентов ИБ необходимо выполнить следующие действия:

1. Убедиться, что хотя бы одному узлу назначена роль **Хранилище индексов событий и инцидентов** (см. раздел 8.2).

2. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > События и инциденты** и в секции **Настройки подключений к хранилищам инцидентов (PostgreSQL)** задать следующие значения параметров:

   - **Имя схемы соединения с базой данных** – указать произвольное имя схемы соединения с создаваемой БД.

   - **Подкластер** – оставить значение **Нет**, если БД создается для общих ресурсов, или установить значение **Да**, если БД создается для какого-либо подкластера. Во втором случае появляется параметр, в котором следует указать этот подкластер.

3. Раскрыть группу параметров **Настройки соединения с базой** и задать следующие значения параметров:

   - **Сетевое имя сервера базы данных** – указать FQDN или IP-адрес узла, на котором предполагается размещение БД.

   - **Сетевой порт сервера базы данных** – указать порт, на котором БД будет ожидать соединения. Порт не должен быть занят никаким другим сервисом на данном узле (см. раздел 4.4).

   - **Имя базы данных** – указать имя БД. К этому значению предъявляются те же требования, что и к именованию каталогов в ОС. Рекомендуется выбирать имя, отражающее назначение создаваемой БД (например, **dozor-event**).

- **Пользователь базы данных** – указать имя **dozor**.
- **Пароль пользователя базы данных** – задать пароль пользователя **dozor** для подключения к БД.

4. Нажать **Сохранить** и **Применить**.
5. Перейти в CLI на узле, на котором предполагается размещение БД событий и инцидентов (или на любом узле Solar Dozor, если БД предполагается разместить на внешнем сервере), переключиться на работу от имени пользователя **dozor**, выполнив команду:

   # sudo su - dozor
6. Загрузить командную оболочку, выполнив команду:

   $ /opt/dozor/bin/shell
7. Создать схему БД с помощью скрипта **create-database.sh**, выполнив команду:

   $ /opt/dozor/smap/schema/pgsql/create-database.sh <db_path> <db_port> <db_name> <db_pass> <db_host> --empty-db

   где:

   - **<db_path>** – путь к каталогу БД (например, **/data/base/incident/**).
   - **<db_port>** – номер порта, заданный в конфигурации (например, 5436).
   - **<db_name>** – имя БД, заданное в конфигурации (например, **dozor-event**).
   - **<db_pass>** – пароль для доступа к БД, заданный в конфигурации.
   - **<db_host>** – адрес узла для размещение БД, заданный в конфигурации (например, 127.0.0.1 или 10.31.10.12). Можно не указывать, если БД создается на текущем узле.

   Внимание!

   Об успешном создании схемы БД свидетельствуют следующие строки в выводе команды:

   Creating control script...
   Control script "/opt/dozor/smap/schema/pgsql/dozor-postgresql" created.
   Copy it to /etc/systemd/system/dozor-postgresql.service
   And run: 'systemctl daemon-reload; systemctl enable dozor-postgresql.service;
   systemctl start dozor-postgresql.service'
   Stop database service ...

   *При наличии сообщений об ошибках в выводе команды следует удалить каталог базы данных (в данном примере – с помощью команды **$ rm -rf /data/base/incident/**), и убедиться в правильности выполнения предыдущих шагов.*
8. Завершить работу интерпретатора shell, выполнив команду:

   $ exit

9. Настроить доступ к БД с других узлов кластера: перейти в каталог БД (в данном примере – **/data/base/incident**) и отредактировать конфигурационный файл **pg_hba.conf** таким образом, чтобы он содержал строку следующего вида:

   ```
   host all all <IP>/<mask> scram-sha-256
   ```

   где **<IP>** – IP-адрес подсети, с узлов которой БД инцидентов будет принимать соединения, а **<mask>** – маска этой подсети, например:

   ```
   host all all 10.31.0.0/16 scram-sha-256
   ```

10. Настроить БД на прослушивание сети на внешнем интерфейсе. Если при создании БД был указан внешний IP-адрес – то БД уже настроена. Если при создании БД был указан локальный адрес (или не указан вовсе) – в том же каталоге отредактировать конфигурационный файл **postgresql.conf** так, чтобы он содержал строку следующего вида:

    ```
    listen_addresses = '<IP-interface>'
    ```

    где **<IP-interface>** – IP-адрес сетевого интерфейса, который БД инцидентов будет использовать для приёма соединений, например:

    ```
    listen_addresses = '10.31.10.12'
    ```

11. Завершить работу от имени пользователя **dozor**, выполнив команду:

    $ exit

12. После создания схемы БД PostgreSQL в каталоге **/opt/dozor/smap/schema/pgsql** создаётся скрипт **dozor-postgresql.service**, в котором записывается пользователь, от имени которого создана БД, а также каталог и порт, на котором работает БД. Необходимо скопировать скрипт **dozor-postgresql.service** в каталог **/etc/systemd/system/** и переименовать его, например, в **event.service**:

    # cp /opt/dozor/smap/schema/pgsql/dozor-postgresql.service /etc/systemd/system/event.service

13. От имени пользователя **root** выполнить следующие команды:

    # systemctl daemon-reload

    # systemctl enable event.service

    # systemctl start event.service

14. Перезапустить сервис индексатора инцидентов, выполнив следующую команду:

    # /opt/dozor/bin/dsctl restart incident-daemon

После этого БД событий и инцидентов должна начать свою работу. Чтобы в этом убедиться, необходимо открыть раздел **Система > Конфигурация > Расширенные настройки > События и инциденты** и в секции **Настройки подключений к хранилищам инцидентов (PostgreSQL)** нажать кнопку **Проверить**.

8.5. Настройка сервера хранения медиаинформации

Сервер хранения медиаинформации (далее – медиасервер) предназначен для хранения метаданных изображений (в том числе снимков экрана), звукозаписей и видеозаписей, присылаемых агентами. Письма, содержащие медиаинформацию от агентов, не обрабатываются фильтром почтового потока. После их обработки сервером агентов медиаинформация из таких писем сохраняется в ФХ, а метаданные – в заданной существующей БД PostgreSQL, где медиасервер создаёт отдельное табличное пространство с секционированием. Медиасервер самостоятельно создаёт новые секции и удаляет старые по истечении заданного срока хранения.

Для корректного отображения медиаинформации в интерфейсе Solar Dozor следует согласовать ротацию метаданных с ротацией медиаинформации. Для этого следует установить одинаковые значения для связанных параметров:

- снимки экрана:
  - Раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**, секция **Хранение медиаинформации**, параметр **Срок хранения снимков (д)**.
  - Раздел GUI **Система > Конфигурация > Основные настройки > Доступ к данным**, секция **Файловое хранилища**, группа параметров **Настройка ротации**, список с параметром **Volume Group** – **agent-media**, параметр **Время жизни до ротации (д)**.
- аудиозаписи:
  - Раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**, секция **Хранение медиаинформации**, параметр **Срок хранения аудиозаписей (д)**.
  - Раздел GUI **Система > Конфигурация > Основные настройки > Доступ к данным**, секция **Файловое хранилища**, группа параметров **Настройка ротации**, список с параметром **Volume Group** – **audio**, параметр **Время жизни до ротации (д)**.
- записи экранов:
  - Раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**, секция **Хранение медиаинформации**, параметры **Срок хранения записей экрана (д)** и **Срок хранения списков процессов приложений (д)**.
  - Раздел GUI **Система > Конфигурация > Основные настройки > Доступ к данным**, секция **Файловое хранилища**, группа параметров **Настройка ротации**, список с параметром **Volume Group** – **screen-video**, параметр **Время жизни до ротации (д)**.

Для хранения медиаинформации Solar Dozor использует БД PostgreSQL. Для настройки БД для хранения медиаинформации необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** и в секции **Хранение медиаинформации** установить следующие значения параметров:

- **База данных (PostgreSQL)** – **Специальная БД**.
- **Сетевое имя сервера базы данных** – указать FQDN или IP-адрес узла, на котором предполагается размещение БД, используемой для хранения информации о задачах сервиса **agent-media-server**.
- **Сетевой порт сервера базы данных** – указать порт, на котором БД для хранения медиаинформации будет ожидать соединения. Порт не должен быть занят никаким другим сервисом на данном узле (см. раздел 4.4).
- **Имя базы данных** – указать имя БД. К этому значению предъявляются те же требования, что и к именованию каталогов в ОС. Рекомендуется выбирать имя, отражающее назначение создаваемой БД (например, **dozor-media**).
- **Пользователь базы данных** – указать имя **dozor**.
- **Пароль пользователя базы данных** – задать пароль пользователя **dozor** для подключения к БД для хранения медиаинформации.

2. Нажать **Сохранить** и **Применить**.
3. Перейти в CLI на узле, на котором предполагается размещение БД для хранения медиаинформации (или на любом узле Solar Dozor, если БД предполагается разместить на внешнем сервере) и переключиться на работу от имени пользователя **dozor**, выполнив команду:

   # sudo su - dozor
4. Запустить командную оболочку, выполнив команду:

   $ /opt/dozor/bin/shell
5. Создать схему БД с помощью скрипта **create-database.sh**, выполнив команду:

   $ /opt/dozor/smap/schema/pgsql/create-database.sh <db_path> <db_port> <db_name> <db_pass> <db_host> --empty-db

   где:

   - **<db_path>** – путь к каталогу БД (например, **/data/base/media/**).
   - **<db_port>** – номер порта, заданный в конфигурации (например, 5438).
   - **<db_name>** – имя БД, заданное в конфигурации (например, **dozor-media**).
   - **<db_pass>** – пароль для доступа к БД, заданный в конфигурации.
   - **<db_host>** – адрес узла для размещение БД, заданный в конфигурации (например, 127.0.0.1 или 10.31.10.12). Можно не указывать, если БД создается на текущем узле.

   Внимание!

   Об успешном создании схемы БД свидетельствуют следующие строки в выводе команды:

Creating control script...
Control script "/opt/dozor/smap/schema/pgsql/dozor-postgresql" created.
Copy it to /etc/systemd/system/dozor-postgresql.service
And run: 'systemctl daemon-reload; systemctl enable dozor-postgresql.service;
systemctl start dozor-postgresql.service'
Stop database service ...

*При наличии сообщений об ошибках в выводе команды следует удалить каталог базы данных (в данном примере – с помощью команды **$ rm -rf /data/base/media/**), и убедиться в правильности выполнения предыдущих шагов.*

6. Завершить работу интерпретатора shell, выполнив команду:

   $ exit

7. Настроить доступ к БД с других узлов кластера: перейти в каталог БД (в данном примере – **/data/base/media**) и отредактировать конфигурационный файл **pg_hba.conf** таким образом, чтобы он содержал строку следующего вида:

   ```
   host all all <IP>/<mask> scram-sha-256
   ```

   где **<IP>** – IP-адрес подсети, с узлов которой БД для хранения медиаинформации будет принимать соединения, а **<mask>** – маска этой подсети, например:

   ```
   host all all 10.31.0.0/16 scram-sha-256
   ```

8. Настроить БД на прослушивание сети на внешнем интерфейсе. Если при создании БД был указан внешний IP-адрес – то БД уже настроена. Если при создании БД был указан локальный адрес (или не указан вовсе) – в том же каталоге отредактировать конфигурационный файл **postgresql.conf** так, чтобы он содержал строку следующего вида:

   ```
   listen_addresses = '<IP-interface>'
   ```

   где **<IP-interface>** – IP-адрес сетевого интерфейса, который БД для хранения медиаинформации будет использовать для приема соединений, например:

   ```
   listen_addresses = '10.31.10.12'
   ```

9. Завершить работу от имени пользователя **dozor**, выполнив команду:

   $ exit

10. После создания схемы БД PostgreSQL в каталоге **/opt/dozor/smap/schema/pgsql** создаётся скрипт **dozor-postgresql.service**, в котором записывается пользователь, от имени которого создана БД, а также каталог и порт, на котором работает БД. Необходимо скопировать скрипт **dozor-postgresql.service** в каталог **/etc/systemd/system/** и переименовать его, например в **media.service**:

    # cp /opt/dozor/smap/schema/pgsql/dozor-postgresql.service /etc/systemd/system/media.service

11. От имени пользователя **root** выполнить следующие команды:

 # systemctl daemon-reload

 # systemctl enable media.service

 # systemctl start media.service

12 Перезапустить сервис хранения медиаинформации, выполнив следующую команду:

 # /opt/dozor/bin/dsctl restart agent-media-server

После этого БД для хранения медиаинформации должна начать свою работу. Чтобы в этом убедиться, необходимо открыть раздел **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение** и в секции **Хранение медиаинформации** нажать кнопку **Проверить**.

8.6. Настройка синхронизации Досье

8.6.1. Синхронизация с FreeIPA

Для настройки синхронизации данных Досье с существующей структурой каталогов 389 Directory Server необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Взаимодействие**, добавить новый источник (либо отредактировать шаблон **389 Directory Server Example**) в секции **Источники данных досье** и задать значения следующих параметров:

   - **Название источника** – указать произвольное название источника данных 389 Directory Server. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
   - **Синхронизация включена** – установить флажок.
   - **Параметры доступа к источнику данных** – **ldap**
   - **DN пользователя** – DN учётной записи с правами чтения каталога 389 Directory Server.
   - **Пароль пользователя** – пароль учётной записи, указанной в предыдущем параметре. Пароль не должен содержать кириллицы, символов «\», «/», «**{**», «**}**», «**[**», «**]**», «**(**», «**)**» и пустых символов.
   - **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например – **ldap://ldap.organization.local:389**).
   - **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов AD организации.
   - **Атрибут, содержащий уникальный идентификатор записи (UUID)** – **nsUniqueId**
   - **Атрибут, содержащий номер последнего изменения записи** – **entryUsn**
   - **Атрибут RootDSE, содержащий идентификатор сервера** – **netscapemdsuffix**

- **Атрибут RootDSE, содержащий номер последнего изменения содержимого – lastusn**

2. Раскрыть список **Список соответствий атрибутов** и при необходимости добавить и/или исправить соответствия между атрибутами 389 Directory Server и атрибутами досье.

3. Нажать **Сохранить** и **Применить**.

4. Выполнить принудительную синхронизацию Досье с источниками, нажав кнопку **Синхронизировать**:

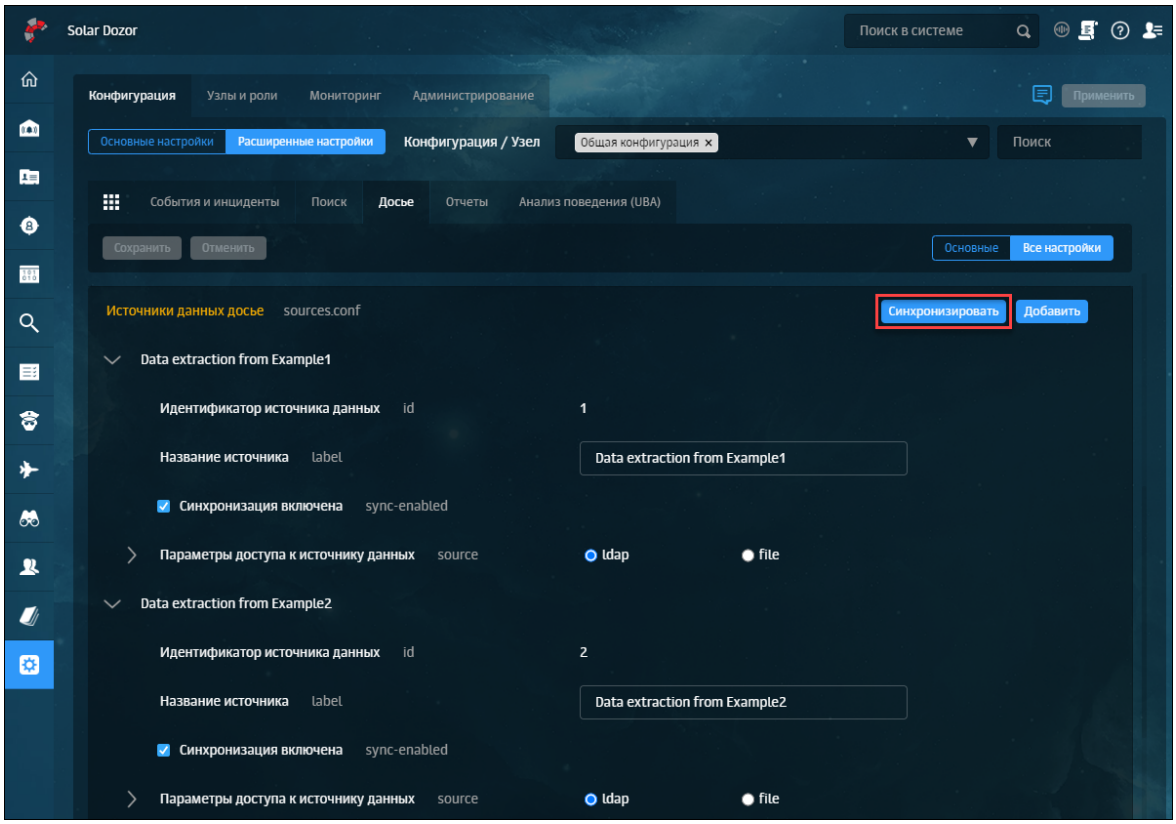


Рис. 8.4. Кнопка принудительной синхронизации Досье

5. Дождаться уведомления об успешности синхронизации.

8.6.2. Синхронизация с ALD Pro

Solar Dozor имеет возможность синхронизировать данные Досье с ALD Pro версии 1.3.0. Для настройки синхронизации данных Досье с существующей структурой каталогов ALD Pro необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Взаимодействие**, добавить новый источник (либо отредактировать шаблон **ALD Pro**) в секции **Источники данных досье** и задать значения следующих параметров:

   - **Название источника** – указать произвольное название источника данных ALD Pro. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.

- **Синхронизация включена** – установить флажок.
- **Параметры доступа к источнику данных** – **ldap**
- **DN пользователя** – DN учётной записи с правами чтения каталога ALD Pro.
- **Пароль пользователя** – пароль учётной записи, указанной в предыдущем параметре. Пароль не должен содержать кириллицы, символов «\», «/», «**{**», «**}**», «**[**», «**]**», «**(**», «**)**» и пустых символов.
- **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например – **ldap://ldap.organization.local:389**).
- **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов ALD Pro организации.
- **Атрибут, содержащий уникальный идентификатор записи (UUID)** – **nsUniqueId**
- **Атрибут, содержащий номер последнего изменения записи** – **entryUsn**
- **Атрибут RootDSE, содержащий идентификатор сервера** – **netscapemdsuffix**
- **Атрибут RootDSE, содержащий номер последнего изменения содержимого** – **lastusn**

2. Раскрыть список **Список соответствий атрибутов** и при необходимости добавить и/или исправить соответствия между атрибутами ALD Pro и атрибутами досье.
3. Нажать **Сохранить** и **Применить**.
4. Выполнить принудительную синхронизацию Досье с источниками, нажав кнопку **Синхронизировать**:

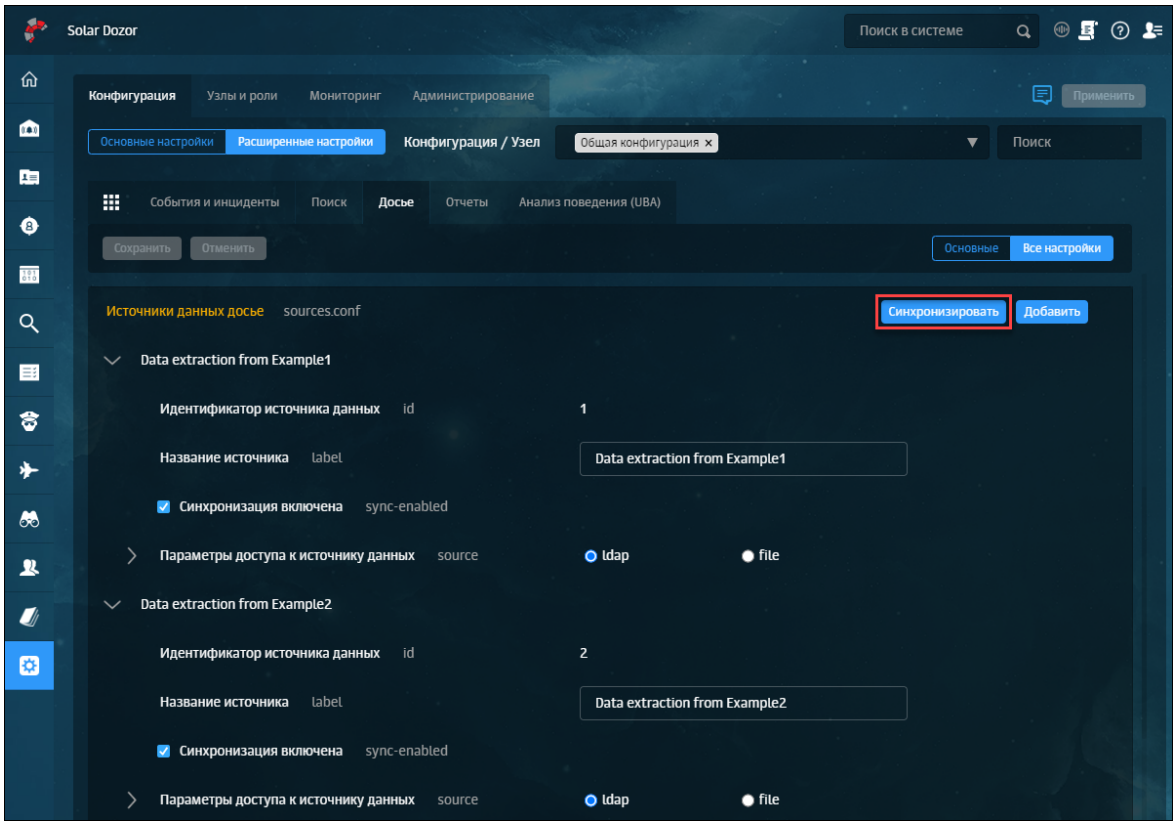


Рис. 8.5. Кнопка принудительной синхронизации Досье

5. Дождаться уведомления об успешности синхронизации.

8.6.3. Синхронизация со службами каталогов без шифрования

Для настройки синхронизации данных Досье с существующей структурой каталогов Active Directory без использования шифрования необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Взаимодействие**, добавить новый источник (либо отредактировать шаблон **AD example**) в секции **Источники данных досье** и задать значения следующих параметров:

   - **Название источника** – указать произвольное название источника данных AD. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
   - **Синхронизация включена** – установить флажок.
   - **Параметры доступа к источнику данных** – **ldap**
   - **DN пользователя** – имя учётной записи с правами чтения каталога AD. Имя указывается вместе с доменом (например – **admin@organization.local**).
   - **Пароль пользователя** – пароль учётной записи, указанной в предыдущем параметре. Пароль не должен содержать кириллицы, символов «\», «/», «**{**», «**}**», «**[**», «**]**», «**(**», «**)**» и пустых символов.

- **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например – **ldap://ldap.organization.local:389**).
- **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов AD организации.
- **Атрибут, содержащий уникальный идентификатор записи (UUID) – objectGuid**
- **Атрибут, содержащий номер последнего изменения записи – UsnChanged**
- **Атрибут RootDSE, содержащий идентификатор сервера – dnsHostname**
- **Атрибут RootDSE, содержащий номер последнего изменения содержимого – highestcommittedusn**

2. Раскрыть список **Список соответствий атрибутов** и при необходимости добавить и/или исправить соответствия между атрибутами AD и атрибутами досье.
3. Нажать **Сохранить** и **Применить**.
4. Выполнить принудительную синхронизацию Досье с источниками, нажав кнопку **Синхронизировать**:

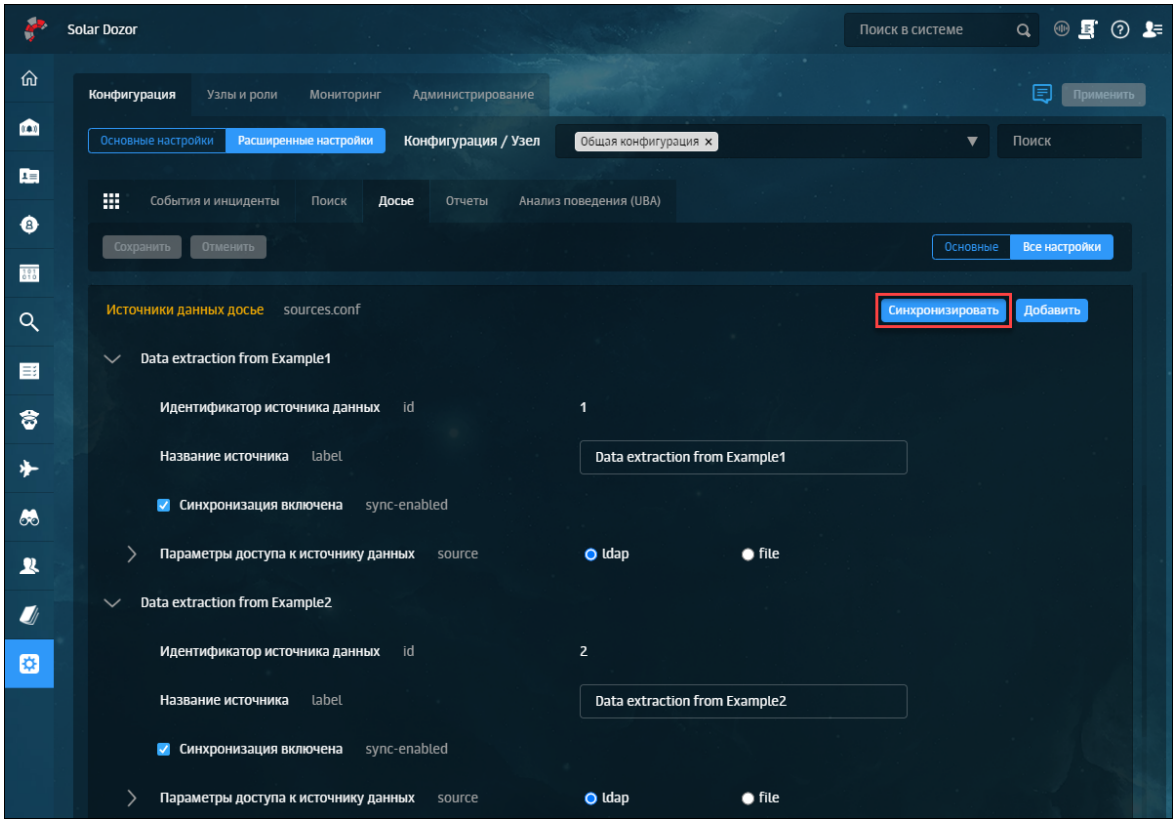


Рис. 8.6. Кнопка принудительной синхронизации Досье

5. Дождаться уведомления об успешности синхронизации.

8.6.4. Синхронизация со службой LDAP с TLS

Установка сертификата организации на контроллере домена позволяет службе LDAP прослушивать и автоматически принимать подключения по протоколу TLS.

Для настройки синхронизации данных Досье с существующей структурой каталогов той или иной службы LDAP с использованием шифрования по протоколу TLS необходимо создать сертификат службы LDAPS, а затем импортировать его в Solar Dozor. Поддерживаются версии TLS 1.2 и выше.

Для установки сертификата LDAPS в Solar Dozor необходимо выполнить следующие действия (пример для Active Directory):

1. Выгрузить сертификат в формате PEM из LDAP-сервера организации, выполнив команду следующего вида:

   # openssl s_client -connect <ip_ldap>:636 </dev/null | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > /var/tmp/<name>.pem

   где **<ip_ldap>** – IP-адрес LDAP-сервера (FQDN недопустим), **<name>** – произвольное имя файла сертификата.

2. Проверить выгруженный сертификат, выполнив команду следующего вида:

   # openssl x509 -in /var/tmp/<name>.pem -noout -text

3. Создать хранилище и загрузить сертификат в него, выполнив команду следующего вида:

   # keytool -import -v -trustcacerts -alias "<name_cert>" -file /var/tmp/<name>.pem -keystore /opt/dozor/etc/ldap.jks -deststoretype JKS

   где **<name_cert>** – имя сертификата (указывается в кавычках), **<name>** – имя файла сертификата. В процессе выполнения команды система предложит ввести новый пароль хранилища и подтвердить его, а также при добавлении сертификата в хранилище будет необходимо ввести **yes**.

4. Перезапустить сервис **monitor-ng**, выполнив команду:

   # /opt/dozor/bin/dsctl restart monitor-ng

5. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Взаимодействие**, добавить новый источник (либо отредактировать имеющийся шаблон) в секции **Источники данных досье** и задать значения следующих параметров:

   - **Название источника** – указать произвольное название источника данных AD. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
   - **Параметры доступа к источнику данных** – **ldap**
   - **DN пользователя** – имя учётной записи с правами чтения каталога AD. Имя указывается вместе с доменом (например – **admin@organization.local**).

- **Пароль пользователя** – пароль учётной записи, указанной в предыдущем параметре. Пароль не должен содержать кириллицы, символов «\», «/», «{», «}», «[», «]», «(», «)» и пустых символов.
- **URL LDAP сервера** – FQDN LDAP-сервера организации с указанием протокола и порта (например – **ldaps://ldap.organization.local:636**). IP-адрес недопустим.
- **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов AD организации.

6. Раскрыть список **Список соответствий атрибутов** и при необходимости добавить и/или исправить соответствия между атрибутами AD и атрибутами досье.
7. Нажать **Сохранить** и **Применить**.
8. Выполнить принудительную синхронизацию Досье с источниками, нажав кнопку **Синхронизировать**:

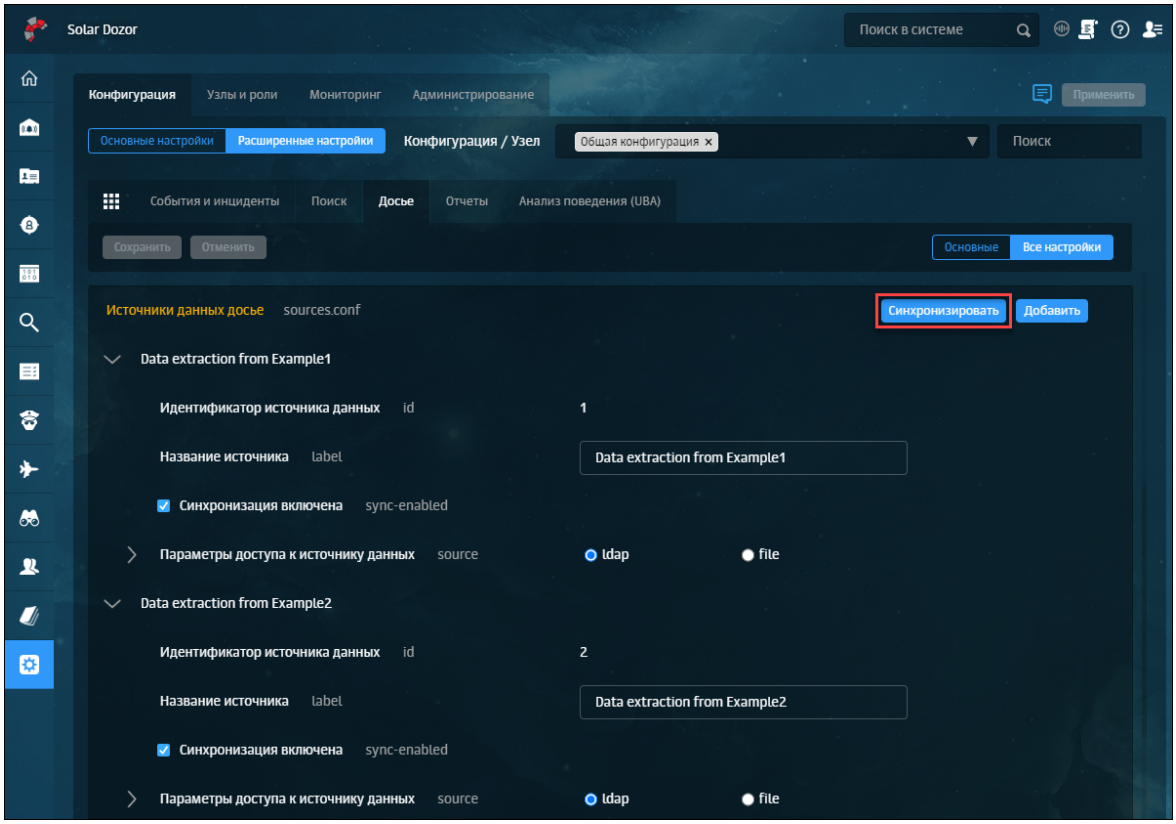


Рис. 8.7. Кнопка принудительной синхронизации Досье

9. Дождаться уведомления об успешности синхронизации.

8.6.5. Синхронизация со сторонним Досье

Досье Solar Dozor может работать в подчинённом режиме, то есть использовать Досье другого кластера Solar Dozor или Solar webProxy. Для этого сторонний кластер должен иметь собственное хранилище Досье. В этом режиме локальный кластер Solar Dozor подключается к Досье стороннего кластера и загружает в оперативную память локальную копию Досье. Все изменения, вносимые в Досье со стороны любого из кластеров, стано-

вятся доступными со стороны другого кластера. В подчинённом режиме нельзя подключиться к Досье кластера, также использующего подчинённый режим.

Для настройки синхронизации данных Досье Solar Dozor с Досье Solar webProxy или Solar Dozor необходимо выполнить следующие действия:

1. На master-узле и всех slave-узлах, имеющих роль **Сервис репликации досье на подчинённых узлах** (**abook-slave**), перейти в CLI и выполнить команду:

   # /opt/dozor/abook-daemon/bin/reg-abook-slave <host>

   где **<host>** – FQDN master-узла кластера Solar Dozor или Solar webProxy, с Досье которого будет выполняться синхронизация. При выполнении команды система запросит пароль пользователя **root** на удалённом master-узле.

2. Перейти в GUI, выбрать раздел **Система > Конфигурация > Расширенные настройки > Досье**, и в секции **Сервис доступа к Досье** задать значения следующих параметров:

   - **Режим работы сервера** – **Подчиненный**
   - **Сетевой адрес** – FQDN master-узла кластера Solar Dozor или Solar webProxy, с Досье которого будет выполняться синхронизация.
   - **Номер порта** – порт, на котором сервис **abook-daemon** ожидает соединения по HTTPS (по умолчанию – 2269).

3. Нажать **Сохранить**, **Применить**.

4. Перезапустить сервис **abook-daemon** на локальном и удалённом master-узлах.

8.6.6. Синхронизация с локальным источником

Досье Solar Dozor может быть обновлено с помощью табличных файлов, содержащих данные организационно-штатной структуры (ОШС) для персон и групп. Такие файлы могут быть получены из внешних систем, и должны соответствовать следующим требованиям:

- Таблица персон и таблица групп сохранены каждая в отдельном файле
- Файлы имеют формат CSV и кодировку UTF-8
- Первая строка каждого файла содержит заголовки столбцов
- Разделителем столбцов является точка с запятой
- Разделителем элементов списка является запятая, все элементы в списке должны быть заключены в квадратные скобки, например: [группа1,группа2,группа3]
- Размер каждого файла не превышает 100 МБ

Таблица групп должна содержать три столбца:

1. **id** – уникальный идентификатор группы.

2. **pid** – идентификатор родительской группы. Такой идентификатор должен существовать среди групп в столбце **id**, за единственным исключением, когда группа является корневой, и в этом случае не имеет никакой родительской группы (см. пример ниже).

3. **group** – название группы.

Пример таблицы групп:

Табл. 8.1. Таблица групп

id	pid	group
1		ПАО "Вектор"
11	1	Московский офис
12	11	Совет директоров
13	11	Аппарат генерального директора
111	11	Исполнительный аппарат
1111	111	Пресс-служба
1112	111	АХО
1113	111	Секретариат
1114	111	Коммерческая служба
11141	1114	Отдел маркетинга

Таблица персон обязательно должна содержать следующие столбцы:

- **id** – уникальный идентификатор персоны.
- **group-id** – идентификатор группы персоны.
- **fullname** – имя персоны.
- **title** – должность персоны.

Таблица персон также может иметь и другие столбцы, в зависимости от требований к полноте данных о персонах. Пример таблицы персон:

Табл. 8.2. Таблица персон

id	group-id	fullname	title	email
1	13	Иванов Иван Иванович	Генеральный директор	i.ivanov@vector.su
2	111	Петров Петр Петрович	Главный бухгалтер	p.petrov@vector.su
3	111	Егоров Егор Егорович	PR-директор	e.egorov@vector.su
5	21	Кузнецова Анна Ивановна	Офицер ИБ	a.kuznetsova@vector.su
6	111	Попова Елена Алексеевна	Исполнительный директор	e.popova@vector.su
78	11	Смирнова Екатерина Александровна	Директор Московского офиса	e.smirnova@vector.su

Таблица персон должна удовлетворять следующим критериям:

- У каждой персоны должна быть указана должность.

- Идентификатор группы персон должен существовать в таблице групп.

Таблица персон может содержать столбец с изображениями (**image_preview**). В ячейках такого столбца следует размещать текстовое base64-представление изображения, полученное из формата **.png**.

После создания файлов с таблицами групп и персон следует разместить их на файловой системе master-узла, а затем выполнить следующее:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Досье > Источники данных досье**.
2. Нажать кнопку **Добавить** и для появившейся группы параметров задать значения:
   - **Название источника** – ввести произвольное значение.
   - **Параметры доступа к источнику данных** – **file**.
   - **Каталог с данными ОШС** – ввести путь к файлам с таблицами групп и персон.
   - **Файл со списком групп** – ввести имя файла с таблицей групп.
   - **Файл со списком сотрудников** – ввести имя файла с таблицей персон.
3. Нажать **Сохранить**, **Применить**, затем **Синхронизировать**.
4. Перейти в раздел **Досье** и проверить наличие новых данных о персонах и группах.

При синхронизации данных могут возникнуть ошибки импорта. Сведения об ошибках содержатся в файле **/data/spool/abook-daemon/org_structure/errors.log** и в разделе GUI **Досье > Организационная структура > Ошибки импорта данных**.

8.7. Настройка планировщика

Для выполнения заданий по расписанию используется планировщик **cron**. После установки Solar Dozor расписание **cron** выглядит следующим образом:

- для пользователя **root**:

```
0 */12 * * * /opt/dozor/bin/check_dozor
```

- для пользователя **dozor**:

```
* * * * * accept-settings mode slave 2>&1 | logger -t dozor -i -p cron.warn
* * * * * accept-policy mode slave 2>&1 | logger -t dozor -i -p cron.warn
* * * * * counters-stat mode slave 2>&1 | logger -t dozor -i -p cron.warn
10 4 * * * dump-settings name daily password "" 2>&1 | logger -t dozor -i -p cron.warn
5 1 * * * send-vendor-report | logger -t dozor -i -p cron.warn
5 15 * * * gen-bug-report | logger -t dozor -i -p cron.warn
25 4 * * * do-logrotate || logger -t dozor "logrotate exited abnormally"
```

Данное расписание соответствует следующим заданиям:

- Вызов скрипта **accept-settings** на slave-узлах раз в минуту. Это задание предназначено для распространения конфигурации Solar Dozor по slave-узлам.

- Вызов скрипта **accept-policy** на slave-узлах раз в минуту. Это задание предназначено для распространения политики фильтрации Solar Dozor по slave-узлам.
- Вызов скрипта **counters-stat** на slave-узлах раз в минуту. Это задание предназначено для сбора метрик ОС и приложений.
- Вызов скрипта **dump-settings** на всех узлах раз в сутки. Это задание предназначено для сохранения репозитория настроек конфигурации в каталог **/data/backups/dozor/**.
- Вызов скрипта **send-vendor-report** на всех узлах раз в сутки. Это задание предназначено для отправки диагностических данных вендору.
- Вызов скрипта **gen-bug-report** на всех узлах раз в сутки. Это задание предназначено для создания отчёта об ошибках.
- Вызов скрипта **do-logrotate** на всех узлах раз в сутки. Это задание предназначено для ротации журнальных файлов, находящихся в каталоге **/opt/dozor/var/log/** (журнальные файлы утилит).
- Вызов скрипта **check_dozor** на всех узлах два раза в сутки (полдень и полночь). Это задание предназначено для подсчёта контрольных сумм неизменяемых исполняемых файлов.

8.8. Настройка индексатора

8.8.1. Общая настройка индексатора

Для текстового поиска по досье, архиву сообщений и архиву событий ИБ используется поисковый движок Elasticsearch (далее – ES).

Сервис **indexer–ng** выполняет индексацию сообщений в архиве. Данный сервис используется ролями **Индексатор текста** и **Вспомогательный сервис индексации текста**. Записи о сообщениях хранятся в таблице **message** БД архива. Версия сообщений определяется параметром **message_version** таблицы. Значение по умолчанию равно 1. Оно увеличивается при изменении информации в сообщении (добавлении и удалении пометок, отправки уведомлений и т. д.).

Параметр **index_version** задает версию сообщения, которую хранит сервис **indexer–ng**. При этом если значение **index_version** равно 0, то сообщение ранее не индексировалось.

Работа индексатора заключается в преобразовании сообщений, хранящихся в БД архива, в документы Elasticsearch. В случае изменения, архивирования и удаления сообщений сервис индексации данных получает уведомления от сервера архивации. Далее индексатор с заданной периодичностью сканирует БД архива и выполняет поиск сообщений, у которых различаются значения параметров **message_version** и **index_version**. Периодичность задается в параметре **Период плановой индексации (Ч)** (секция **Индексация сообщений в архиве**, раздел GUI **Конфигурации > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**) и по умолчанию равна одному часу. После этого выполняется синхронизация индексов на индексаторе, и обновляется значение параметра **index_version**.

Сервис **indexer–ng** проверяет данные архива на наличие индексов. В случае их отсутствия индексатор текста выполняет сброс значения параметра **index_version** таблицы **message**. Далее запускается индексация сообщений в БД архива.

При переходе независимых инсталляций Solar Dozor в территориально-распределенные (при наличии работающего модуля **Мультидозор**), а также при обновлении версии Solar Dozor необходимо обеспечить корректность работы быстрого поиска. Для этого следует привести устаревшие индексы к определенному формату. Это делается с помощью настройки обновления устаревших индексов, которые задаются в группе параметров **Ежедневная фоновая миграция устаревших индексов сообщений** (секция **Индексация сообщений в архиве**, раздел GUI **Система > Конфигурация > Расширенные настройки > Поиск**). Необходимо раскрыть группу параметров, установить флажки **Включена для сообщений** и **Включена для бесед**, и задать час начала и окончания фоновой миграции устаревших индексов в параметрах **Время начала** и **Время окончания**. То же самое следует выполнить для событий и инцидентов ИБ в группе параметров **Ежедневная фоновая миграция устаревших индексов** (секция **Сервис хранения и индексации событий и инцидентов**, раздел GUI **Система > Конфигурация > Расширенные настройки > События и инциденты**).

Внимание!

Следует учитывать, что во время выполнения обновления индексов сообщения могут пропадать из списков результатов быстрого поиска.

Внимание!

*Настройка фоновой миграции устаревших индексов бесед, включаемая флажком **Включена для бесед**, может корректно работать только в комбинации с флажком **Включена для сообщений**.*

Работа ES обеспечивается сервисом **smap-elasticsearch**. Этот сервис используется ролями **Индексатор текста**, **Хранилище индексов событий и инцидентов** и **Вспомогательный сервер Elasticsearch**. В распределённой конфигурации Solar Dozor ES может образовывать собственный кластер, то есть иметь распределённую конфигурацию, если его сервис запущен на нескольких узлах.

В зависимости от назначенной роли, узлы Solar Dozor выполняют следующие задачи:

- **Индексатор текста** – создание и хранение индексов архива сообщений, поиск по архиву сообщений.
- **Вспомогательный сервис индексации текста** – создание индексов хранения сообщений без хранения.
- **Хранилище индексов событий и инцидентов** – создание и хранение индексов архива инцидентов, поиск по архиву инцидентов.
- **Вспомогательный сервер Elasticsearch** – участие в кластере ES для решения некоторых служебных задач (см. ниже).

Если два или более узлов имеют роль **Индексатор текста**, то они будут делить индексы между собой для равномерного использования ресурсов кластера (то же справедливо для роли **Хранилище индексов событий и инцидентов**).

Роль **Вспомогательный сервер Elasticsearch** предназначена для следующих целей:

- Выведение узла из кластера ES без потери данных. Если узел имеет роль **Индексатор текста** и/или **Хранилище индексов событий и инцидентов**, и требуется освободить его от этой роли без потери хранящихся на нём индексов, то необходимо выполнить следующие действия:

  1. Назначить узлу роль **Вспомогательный сервер Elasticsearch**.

  2. Снять с узла роли **Индексатор текста** и/или **Хранилище индексов событий и инцидентов**.

  3. Дождаться окончания переноса индексов на другие узлы кластера ES. Проверить наличие индексов на узле можно с помощью CLI, выполнив следующую команду:

     elastictool -i

     Об окончании переноса свидетельствует значение **0** в столбце **Size**.

  4. При необходимости, снять с узла роль **Вспомогательный сервер Elasticsearch**.

- Исключение конфликтов внутри кластера ES. Некоторые внутренние решения (например, выбор ведущего узла) узлы ES принимают большинством. Если кластер ES состоит из двух узлов, и один из них по каким-либо причинам не отвечает на запросы (например, выключен или перегружен), то решение не может быть принято, поскольку оставшийся узел не составляет большинства из двух. Для исключения такой ситуации следует назначить роль **Вспомогательный сервер Elasticsearch** ещё одному узлу. Сама по себе эта роль практически не создаёт дополнительной нагрузки на узел Solar Dozor, поэтому её можно назначить любому узлу, который имеет хотя бы минимальный резерв производительности.

Настройку ES следует выполнять при следующих условиях:

- Узлу назначена роль **Вспомогательный сервер Elasticsearch.**

- Требуется корректировка производительности сервиса **smap-elasticsearch**.

Настройка ES производится в следующих секциях:

- **Сервис хранения и индексации событий и инцидентов** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > События и инциденты**);

- **Сервис поиска и индексации Elasicsearch** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**);

- **Производительность сервиса поиска и индексации сообщений и инцидентов** (раздел GUI **Конфигурации > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**).

Рекомендуемые значения параметров секций **Производительность сервиса поиска и индексации сообщений и инцидентов** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**) и **Сервис хранения и индексации событий и инцидентов** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > События и инциденты**):

- **Количество shard-ов** – количество шардов базы данных индексов ES. Рекомендуемое значение параметра равно числу узлов в кластере ES (то есть по одному шарду на узел). Если на узлах кластера ES нет высоконагруженных сервисов и имеется запас производительности, допускается выделить по два шарда на узел; в этом случае, рекомендуемое значение параметра составит количество узлов в кластере ES, умноженное на 2. Максимальное значение рассчитывается исходя из того, что общее число шардов по всем индексам за требуемый срок хранения не должно превышать 500. Один шард содержит индексы за неделю. Таким образом, для расчёта максимального значения необходимо разделить 500 на требуемый срок хранения, выраженный в неделях, и округлить вниз до целого. В качестве значения параметра следует указать меньшее из рекомендуемого и максимального значений.

  Пример: имеется 5 узлов, их производительность достаточно высока, требуется хранить индексы за 52 недели (год). Рекомендуемое значение составляет 10 (по два шарда на узел). Максимальное значение составляет 9 (целая часть результата деления 500 на 52). Тогда в качестве значения параметра следует указать 9.

  Пример: имеется 2 узла, их производительность достаточно высока, требуется хранить индексы за 52 недели (год). Рекомендуемое значение составляет 4 (по два шарда на узел). Максимальное значение составляет 9 (целая часть результата деления 500 на 52). Тогда в качестве значения параметра следует указать 4.

- **Число копий** – количество копий индексов ES. Значение по умолчанию – 0, то есть все индексы хранятся в единственном экземпляре. Увеличивать это значение имеет смысл только в случае распределённой конфигурации кластера ES. Использование копий индексов ES позволяет повысить производительность работы ES, поскольку становится возможным параллельный доступ к индексам на разных узлах, но при этом кратно повышаются требования к объёму физических носителей данных на узлах. Копии индексов всегда хранятся на разных узлах, то есть на одном узле не может быть двух и более копий одних и тех же индексов, поэтому максимальное значение этого параметра равняется числу узлов кластера ES, уменьшенному на единицу.

- **Периодичность обновления индекса (с)** – периодичность обновления индекса ES в секундах. Значение по умолчанию – 30, то есть индекс становится доступным для чтения и использования через тридцать секунд после его помещения в базу данных ES. Это значение нормально для штатной работы ПК Solar Dozor, однако в отдельных сценариях (например, единовременная индексация базы данных с большими объёмами данных) это может привести к значительному ухудшению производительности. В подобных случаях рекомендуется временно увеличивать это значение до окончания создания индекса.

Рекомендуемые значения параметров секции **Сервис поиска и индексации Elasicsearch** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**):

- **Прекратить размещение новых индексов, если свободного места меньше (МБ)** – минимальный размер свободного места на файловой системе в мегабайтах, при котором происходит размещение новых индексов ES. Если свободного места на узле станет меньше указанного значения, ES на этом узле прекратит размещение новых индексов. Значение следует выбирать исходя из условий эксплуатации Solar Dozor. Значение по умолчанию: 1024.

- **Переносить данных на другие узлы если свободного места меньше (МБ)** – максимальный размер свободного места на файловой системе узла кластера ES в мега-

байтах, при котором происходит принудительный перенос данных на другие узлы. Если свободного места на узле станет меньше указанного значения, ES на этом узле будет пытаться переносить индексы на другие узлы кластера до тех пор, пока не будет освобождён указанный объём. Значение следует выбирать исходя из условий эксплуатации Solar Dozor. Значение по умолчанию: 512.

- **Репликация с учётом размещения серверов в стойках** – при включении этого параметра копии индексов ES сохраняются на узлах с учётом их физического размещения в серверных стойках. На узлах, размещённых в одной стойке, совокупно будет находиться одна полная копия индексов или её часть, без дублирования. Принадлежность узла к той или иной стойке следует указать во вкладке **Система > Узлы и роли**, открыв вспомогательное меню этого узла и выбрав пункт **Атрибуты**. Количество копий индексов ES не должно превышать количество стоек, содержащих узлы кластера ES.

Для остальных параметров рекомендуется оставить значения по умолчанию.

Рекомендуемые значения параметров секции **Производительность сервиса поиска и индексации сообщений и инцидентов** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск**):

- **Размер памяти (ГБ)** – объём оперативной памяти в гигабайтах, выделяемой для сервиса **smap-elasticsearch** на каждом узле кластера ES. Значение по умолчанию: 4. Рекомендуется увеличить это значение на столько, сколько полных или неполных десятков миллионов сообщений содержится в архиве. Например, если в архиве содержится 35 миллионов сообщений, то в качестве значения параметра рекомендуется установить 8. Максимально допустимое значение – половина всей имеющейся оперативной памяти сервера, но не более 128 ГБ.

После установки значений параметров конфигурационных файлов необходимо нажать **Сохранить** на вкладках каждого из них, а затем нажать **Применить** на вкладке любого из них.

8.8.2. Настройка индексации оперативных и исторических данных

Для оптимизации работы с архивом сообщений и хранилищем событий и инцидентов ИБ используется механизм разделения данных на оперативные и исторические. При использовании этого механизма оперативными считаются данные не старше некоторого заданного значения в неделях, а историческими – все остальные. При неиспользовании этого механизма все данные считаются оперативными. Оперативные и исторические данные хранятся и индексируются разными сервисами на разных узлах.

Примечание

Узел может хранить оперативные и исторические данные одного типа (сообщения архива или события и инциденты ИБ), но в этом случае теряется смысл их разделения.

Для использования механизма оперативных и исторических данных необходимо выполнить следующие шаги:

1. Перейти в раздел GUI **Система > Узлы и роли** и назначить роль **Индексатор текста** тем узлам, на которых необходимо хранить и выполнять индексацию оперативных сообщений архива.

2. Назначить роль **Хранилище индексов событий и инцидентов** тем узлам, на которых необходимо хранить и выполнять индексацию оперативных событий и инцидентов ИБ.

3. Назначить роль **Индексатор исторических сообщений** тем узлам, на которых необходимо хранить и выполнять индексацию исторических сообщений архива.

4. Назначить роль **Хранилище индексов исторических событий и инцидентов** тем узлам, на которых необходимо хранить исторические события и инциденты ИБ.

5. Назначить роль **Вспомогательный сервис индексации текста** тем узлам, на которых необходимо только выполнять индексацию оперативных сообщений архива, без хранения индексов.

6. Назначить роль **Вспомогательный индексатор исторических сообщений** тем узлам, на которых необходимо только выполнять индексацию исторических сообщений архива, без хранения индексов.

7. При необходимости, назначить некоторым узлам роль **Вспомогательный сервер Elasticsearch** для исключение конфликтов внутри кластера ES, как описано в разделе 8.8.1.

8. Перейти в раздел **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > Поиск** и в секции **Индексация сообщений в архиве** переключить параметр **Разделять оперативные и исторические данные** в значение **Разделять**. Для появившегося параметра **Период хранения в оперативном архиве** установить значение в неделях, которое будет определять максимальный возраст сообщения в архиве, после которого оно переходит из оперативных в исторические.

9. Перейти в раздел **Система > Конфигурация > Расширенные настройки > Настройка средств мониторинга и анализа нарушений > События и инциденты** и в секции **Сервис хранения и индексации событий и инцидентов** переключить параметр **Разделять оперативные и исторические данные** в значение **Разделять**. Для появившегося параметра **Период хранения в оперативном архиве** установить значение в неделях, которое будет определять максимальный возраст события или инцидента ИБ, после которого оно переходит из оперативных в исторические.

10. Нажать **Сохранить** и **Применить**.

После этого индексаторы на узлах приступят к маркировке оперативных и исторических данных, а сервис ES начнет распределение индексов по заданным узлам. Пользоваться системой можно сразу же.

8.9. Настройка файлового хранилища

Создание схемы БД и настройка соответствующих соединений в конфигурации Solar Dozor позволяет архивировать и хранить сообщения в БД архива. Помимо БД, сообщения можно хранить в файловой системе, для чего на одном или нескольких узлах организуется файловое хранилище (далее – ФХ). На одном или нескольких узлах необходимо

настроить центральное ФХ, куда будут записываться данные с локальных ФХ, организованных на других узлах.

Архитектура ФХ подробно описана в приложении **Приложение D, *Описание файлового хранилища***.

Использование ФХ по умолчанию включено. Необходимо либо выключить использование ФХ, либо назначить каким-либо узлам кластера роли, относящиеся к файловому хранилищу и затем настроить работу ФХ.

Для настройки ФХ необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Узлы и роли** и назначить роль **Центральное файловое хранилище** всем узлам, на которых предполагается производить долгосрочное хранение и ротацию данных. Рекомендуется назначить эту роль узлу, к которому примонтирована СХД.

2. Назначить роль **Локальное файловое хранилище** всем узлам, на которых предполагается осуществлять временное хранение сообщений с последующим переносом в центральное ФХ. Рекомендуется назначить эту роль всем узлам с ролью **Фильтр почтового потока**.

3. Перейти в раздел **Система > Конфигурация > Расширенные настройки > Хранение** и в секции **Настройки файлового хранилища** задать значения следующих параметров:

   - **Gzip-компрессия при размещении** – рекомендуется оставить включенным для экономии места на диске.

   - **Вывод отладочной информации** – включить при необходимости диагностики ФХ.

   - **Режим распределения по хранилищам при переносе** – выбрать алгоритм распределения данных по хранилищам при их переносе. Принимает значения: **Приоритет скорости** и **Равномерное распределение**. Значение по умолчанию: **Приоритет скорости**.

     При выбранном значении **Приоритет скорости** данные переносятся в центральные ФХ с той скоростью, с которой они могут быть приняты. Более быстрый сервер забирает на себя больше данных. Неработающие узлы исключаются из переноса. Этот режим наиболее производительный, но может приводить к дисбалансу объемов хранения между хранилищами.

     При выбранном значении **Равномерное распределение** на каждое центральное ФХ переносится одинаковое количество контейнеров. Медленный узел замедляет процесс переноса. Неработающий узел практически останавливает процесс переноса. Этот режим дает равномерное распределение данных по хранилищам, но скорость переноса фактически ограничена скоростью самого медленного узла.

     Рекомендуется выбрать значение по умолчанию.

   - **Разрешенные часы переноса данных из локального файлового хранилища в центральное**:

     - **Час начала (timezone сервера)** – час, начиная с которого будет выполняться перенос данных из локального ФХ в центральное.

- **Час окончания (timezone сервера)** – последний час, в течение которого будет выполняться перенос. Например, если задано значение 17, то данные будут переноситься вплоть до момента 17:59:59.

- **Настройка переноса контейнеров** – нажать кнопку **Добавить** в строке параметра:
  - **Volume Group** – **vg-000000**
  - **Время жизни до переноса** – минимальное время нахождения данных в локальном ФХ до переноса. Значение по умолчанию **0 дн. 0 ч.** означает, что данные будут перенесены в центральное ФХ при первой же возможности.

- **Настройка ротации**:
  - **Volume Group** – **vg-000000**
  - **Время жизни до ротации** – период времени в днях, по истечении которого после помещения данных в центральное ФХ происходит их ротация (удаление или архивирование).
  - **Рекомендуемый размер файла архива (МБ)** – максимальный размер файла в мегабайтах, помещаемого в архив при ротации, если параметр **Режим ротации** имеет значение **Локальная файловая система** или **Внешний FTP сервер**.
  - **Критический объем свободного места (МБ)** – минимальный размер свободного пространства на узле центрального ФХ в мегабайтах. Если размер свободного пространства становится меньше этого значения, система производит внеочередную ротацию в момент 3:00:00 ближайших суток.
  - **Gzip компрессия архива** – Gzip-компрессия при сохранении данных в центральное ФХ. Включить, если это требуется.
  - **Режим ротации** – установить одно из следующих значений:
    - **Удалить, не архивировать** – данные при ротации будут удалены.
    - **Локальная файловая система** – данные при ротации будут отключены от ФХ и помещены в каталог, указанный в параметре **Путь**.
    - **Внешний FTP сервер** – данные при ротации будут отключены от ФХ и помещены заданный каталог на заданном FTP-сервере:
      - **Сетевой адрес** – адрес FTP-сервера организации.
      - **Номер порта** – порт, на котором FTP-сервер ожидает соединения.
      - **Режим FTP** – режим работы, на который настроен FTP-сервер (активный или пассивный).
      - **Пользователь** – имя пользователя для соединения с FTP-сервером.
      - **Пароль** – пароль этого пользователя.
      - **Путь на FTP-сервере** – путь к каталогу на FTP-сервер, в который будут сохраняться данные при ротации.

- **Периодичность ротации** – выбрать **Ежедневно**, **Еженедельно** или **Ежемесячно**, после чего задать значения следующих параметров:
  - **День месяца**
  - **День недели**
  - **Час**
  - **Минута**

4. В секции **Тома файлового хранилища** задать значения следующих параметров:
   - **Группа томов** – **vg-000000**
   - **Идентификатор тома** – задать идентификатор тома. Рекомендуется выбирать значение с учётом возможного создания других томов.
   - **Только для чтения** – включить, если требуется запретить запись данных в этот том.

     Внимание!

     Ротация тома (если включена) выполняется независимо от значения этого параметра.
   - **Разрешить ротацию тома** – включить, если требуется ротация этого тома в соответствии с заданными на предыдущем шаге параметрами.
   - **Путь, по которому размещены данные** – путь к каталогу данных ФХ на файловой системе.
5. При необходимости, добавить новый том с помощью кнопки **Добавить** и повторить предыдущий шаг.
6. Нажать **Сохранить** и **Применить**.

8.10. Настройка перехвата сообщений из Express

В Solar Dozor реализован перехват сообщений из корпоративного мессенджера Express. Для настройки перехвата необходимо выполнить следующие действия:

1. Обновить мессенджер Express до актуальной версии согласно официальной документации по ссылке https://express.ms/admin_guide_update.pdf.
2. Перейти в GUI Solar Dozor, раздел **Система > Расширенные настройки > Обработка сообщений** и открыть секцию **Сервис фильтрации сообщений**.
3. Раскрыть группу настроек **ICAP-интерфейс** и задать следующие значения:
   - **Включить ICAP-интерфейс** – установить флажок.
   - **Порт ICAP-интерфейса** – указать любой незанятый номер сетевого порта.
   - **Обрабатывать только указанные MIME-типы** – снять флажок.

4. В той же группе, в зависимости от возможностей по обработке ошибок снять или установить флажки для параметров:

   - **Не обрабатывать сообщения с пустым телом**
   - **Выдавать ответ с кодом 200/204 при ошибках обработки**

5. Убедиться, что на серверах обработки сообщений Express существует файл схемы преобразования по пути **/opt/dozor/smap/mapping/express.edn**. В противном случае поместить файл в данный каталог и задать для него права на чтение. Содержимое файла должно быть следующим:

```
{
 ["x-dozor-mapping-schema" "Express"]
 [
  [:address-info :source] [:header "x-plain-authenticated-user" :extract #".+\\(.+)" :as-login]
  [:address-info :source] [:header "x-plain-authenticated-user" :extract #".+\\(.+)" :as-im]
  [:address-info :source] [:header "x-plain-authenticated-user" :extract #"(^[1-9]+[0-9]*$)" :as-im]
  [:address-info :destination] [:header "x-recipient-user-login" :as-list :extract #".+\\(.+)" :as-login]
  [:address-info :destination] [:header "x-recipient-user-login" :as-list :extract #".+\\(.+)" :as-im]
 [:address-info :destination] [:header "x-recipient-user-login" :as-list :extract #"(^[1-9]+[0-9]*$)" :as-im]

  :subject [:header "x-groups-channels-name"]
  :subject [:header "subject"]
  :headers [:header "x-application" :as-header "x-agent-application-name"]
  :headers [:header "x-groups-channels-id" :as-header "x-agent-chat-id"]
  :recv-date [:header "x-message-date" :or-now :as-date]
  :comp-date [:header "x-message-date" :or-now :as-date]
  :type [:const "endpoint/im"]
  :comm-channel [:const "im"]
  :filename [:header "x-file-name"]]
}
```

6. Перезапустить сервис **mailfilter**, выполнив в CLI следующие команды:

   # /opt/dozor/bin/shell

   # dsctl restart mailfilter

7. Перейти в CLI сервера Express и выполнить от имени пользователя **root** команды:

   cd /opt/express

   mkdir -p dlps_keys/storage && chown -R 888:888 dlps_keys

8. Открыть файл настроек **/opt/express/settings** и добавить в него следующие строки:

```
dlps_enabled: true
dlps_env_override:
  DLPS_ICAP_CLIENT_HOST: <dozor_ip>
  DLPS_ICAP_CLIENT_PORT: <dozor_port>
dlps_icap_additional_headers:
  client_ip: <express_ip>
  server_ip: <dozor_ip>
  network_segment: CTS
  application: Express
```

```
dlps_icap_client_host: <dozor_ip>
dlps_icap_client_port: <dozor_port>
```

где:

- **<dozor_ip>** – IP-адрес узла Solar Dozor с ролью **Фильтр почтового потока** или **Балансировщик** (см. раздел). В этом файле настроек можно задать только один такой узел.
- **<dozor_port>** – порт, на котором этот узел ожидает соединения по протоколу ICAP (заданный на шаге 3).
- **<express_ip>** – IP-адрес бэкенд-сервера Express.

9. Перезагрузить контейнеры Express, выполнив команды:

   cd /opt/express

   dpl -d

   dpl --dc restart

   В каталоге **/opt/express/dlps_keys** будет создан файл ключа с расширением **.key**.

10. Перейти в GUI сервера Express, перейдя по адресу https://express.mydomail.ltd/dlps/. При входе использовать имя пользователя **admin** и пароль **admin**. Настоятельно рекомендуется изменить пароль на более надёжный.

11. Перейти в раздел **Общие** и установить флажки для следующих параметров:

    - **DLPS**
    - **Отправлять события режима конфиденциальной переписки**

12. Перейти в раздел **Настройки** и установить флажки для следующих параметров:

    - **Интеграция с Solar Dozor**
    - **Режим отладки интеграции с Solar Dozor** (если требуется ведение журналов отладки на стороне Express)

13. Перейти в раздел GUI Solar Dozor **Справочники > Приложения**, открыть вкладку **Справочник приложений** и нажать кнопку **Добавить приложение**. В появившемся окне **Добавить приложение** задать название **Express** и родительскую категорию **Общение > Мессенджеры и чаты**. Нажать **Сохранить**.

14. Выбрать в справочнике созданное приложение **Express** и добавить в список процессов значение **Express**.

8.11. Настройка перехвата сообщений из VK Teams

В Solar Dozor реализован перехват сообщений из корпоративного мессенджера VK Teams. Для настройки перехвата необходимо выполнить следующие действия:

1. Перейти в GUI Solar Dozor и открыть раздел **Система > Конфигурация > Расширенные настройки > Обработка сообщений**. Перейти в секцию **Сервис фильтрации сооб-**

щений, раскрыть группу параметров **ICAP-интерфейс** и установить флажок **Включить ICAP-интерфейс**. Изменить порт по умолчанию, если это необходимо. Нажать **Сохранить**, **Применить**.

2. Настроить синхронизацию Досье с тем же источником, который использует VK Teams. Настройка синхронизации Досье описана в разделе 8.6.

3. Настроить правила политики для обработки перехватов. Если не требуется обрабатывать перехваты типа **веб-запрос**, то их можно отфильтровать правилом политики по заголовку **Host** со значением **VkTeams**.

4. Перейти на сервер **VK Teams**, открыть конфигурационные файлы **/usr/local/etc/gbld-st-1.conf** и **/usr/local/etc/gbld-mchat-1.conf**, и добавить в каждый из них следующие строки (либо изменить значение **false** на **true**, если такие строки уже есть):

```
gbld.check_dlp true
gbld.check_dlp_sync true
```

5. Указать конечную точку сервера Solar Dozor, выполнив команду:

   etcdctl --endpoints=<host_etcd>:<port_etcd> put /vars/services/plumber/development/public/service/DLP/ICAP/address icap:\\/<dozor_mailfilter>:<dozor_port>/icap/spool

   где **<host_etcd>:<port_etcd>** – FQDN и порт сервера VK Teams, **<dozor_mailfilter>:<dozor_port>** – IP-адрес и порт узла Solar Dozor с ролью **Фильтр почтового потока**. Пример:

```
etcdctl --endpoints=etcd.organization.local:2379 put
/vars/services/plumber/development/public/service/DLP/ICAP/address
icap:\\192.168.106.71:2344/icap/spool
```

6. Перезапустить сервис **plumber**, выполнив команду:

   kubectl -n plumber scale deployment plumber --replicas=1

7. Перезапустить сервисы **gbld-st** и **gbld-mchat**, выполнив команду:

   systemctl restart gbld-st-1 gbld-mchat-1

8. Открыть конфигурационный файл **/usr/local/etc/go.files.icq.com/files.icq.com.config.yaml** и добавить в него следующие строки:

```
DLP:
isActive: true
syncSend: true
resortClient:
timeout: "3s"
```

9. Перезапустить сервис **gofiles_httpd**, выполнив команду:

   systemctl restart gofiles_httpd

8.12. Настройка перехвата сообщений из Cisco Webex Teams

В Solar Dozor реализован перехват сообщений из корпоративного мессенджера Cisco Webex Teams с помощью официального API. Для настройки перехвата необходимо выполнить следующие действия:

1. Перейти по ссылке **https://developer.webex.com/my-apps/new/integration** и авторизоваться в системе под учётной записью с правами **Compliance Officer**.

2. На открывшейся странице в поле Redirect URI(s) указать адрес (IP или FQDN) и порт сервера Solar Dozor, на котором будут выполняться перехваты сообщений. Пример: **https://filter.dozor.organization.ru:9090**.

   Внимание!

   Номер порта 9090 не может быть изменён и должен быть разрешён пакетным фильтром.

   Внимание!

   *Выбранный сервер Solar Dozor должен иметь роль **Фильтр почтового потока**. В территориально-распределённой схеме работы (модуль **Мультидозор**) этот сервер должен находиться на общих ресурсах.*

3. Включить следующие флажки:

   - **spark:people_read**
   - **spark-admin:people_read**
   - **spark-compliance:events_read**
   - **spark-compliance:rooms_read**
   - **spark-compliance:messages_read**
   - **spark-compliance:memberships_read**

4. Заполнить остальные обязательные поля значениями по усмотрению или согласно реалиям организации.

5. Нажать **Add Integration**.

6. Сохранить значения полей **CLIENT_ID** и **CLIENT_SECRET** для будущего использования.

7. Если на сервере Solar Dozor, выбранном для выполнения перехватов, нет доступа к адресам **https://webexapis.com/** и **https://developer.webex.com/**, следует задать на этом сервере переменную окружения https_proxy, выполнив в CLI команду следующего вида:

   # export https_proxy=http://<proxy.host:port>/

   где **<proxy.host:port>** – адрес (IP или FQDN) и порт прокси-сервера организации.

8. Запустить на этом сервере команду следующего вида:

   # wereg.py -n <hostname> -i <CLIENT_ID> -s <CLIENT_SECRET> -t <path>

   где **<hostname>** – адрес (IP или FQDN) этого сервера, **<CLIENT_ID>** и **<CLIENT_SECRET>** – соответствующие значения полей, сохранённые на шаге 6, **<path>** – произвольный путь к каталогу, в который будет записан файл **token.json** в результате выполнения команды (например, **/opt/dozor/share/im-crawler/token.json**).

   Внимание!

   *Файл **token.json** необходим для идентификации опрашивающего сервера Solar Dozor на стороне серверов Webex. При отсутствии обращений серверов Solar Dozor к серверам Webex с помощью этого файла в течение более 90 суток, файл становится недействительным. Для создания нового такого файла необходимо повторно выполнить этот шаг инструкции.*

9. В результате выполнения команды на экран будет выведен URL, по которому нужно будет перейти с помощью браузера. Пример вывода:

   ```
   Please point your browser to following url:
   https://webexapis.com/v1/authorize?response_type=code&client_id=
   C93071de24cda52557c925dc0341d2cb6e1c736579b4d58b93c94edb64eacf84b&
   redirect_uri=https%3A%2F%2Fexample.organization.local%3A9090%2Fauth&scope=
   spark-compliance%3Aevents_read%20spark-compliance%3Amessages_read%20
   spark-compliance%3Arooms_read%20spark%3Apeople_read%20spark-admin%3A
   people_read%20spark-compliance%3Amemberships_read%20spark%3Akms&state=
   c8f61ebb8f484ee68df09754763416bc
   Waiting for request on https://example.organization.local:9090/auth
   ```

   Следует перейти по первой, «длинной» ссылке.

10. Проверить владельца файла **token.json**, выполнив команду следующего вида:

    # ls -l <path>

    Файлом должны владеть пользователь **dozor** и группа **dozor**. Если это не так, то сменить владельца файла **token.json**, выполнив команду следующего вида:

    # chown dozor:dozor <path>

    где **<path>** – путь, заданный в шаге 8 (например, **/opt/dozor/share/im-crawler/token.json**).

11. Перейти в GUI Solar Dozor и открыть раздел **Система > Основные настройки > Работа системы**, пролистать до секции **Загрузка сообщений из корпоративных мессенджеров**. Задать значения следующих параметров:

    - **Настройки прокси-сервера** – если для доступа к адресу **https://webexapis.com/** требуется соединение через прокси-сервер, то выбрать значение **Настройка прокси-сервера**, и в раскрывшемся списке задать значения параметров:
      - **Адрес прокси-сервера** – адрес (IP или FQDN) прокси-сервера, через который предполагается соединяться с узлом **webexapis.com**.

- **Порт прокси-сервера** – номер порта, на котором этот прокси-сервер ожидает соединения.
- **Логин для Basic-аутентификации на прокси-сервере** – имя учётной записи пользователя для авторизации на прокси-сервере.
- **Пароль для Basic-аутентификации на прокси-сервере** – пароль этой учётной записи.

- **Файл с токеном доступа** – указать путь **<path>**, заданный в шаге 8.
- **Client ID** – указать значение **CLIENT_ID**, сохранённое в шаге 6.
- **Client Secret** – указать значение **CLIENT_SECRET**, сохранённое в шаге 6.

12 При необходимости, задать дополнительные параметры конфигурации. Для этого открыть раздел **Система > Расширенные настройки > File Crawler**, пролистать до секции **Загрузка сообщений из корпоративных мессенджеров**, и задать значения следующих параметров:

- **Уровень журналирования** – выбрать требуемую степень подробностей журналируемых данных.
- **Время актуальности данных в кэше** – периодичность в секундах, с которой обновляется список участников беседы, для которой выполняется перехват сообщений. Значение по умолчанию – 3600 (один час).
- **Каталог для временных файлов** – задать каталог для временных файлов сервиса.
- **Максимальный размер загружаемых файлов** – максимальный размер файлов в мегабайтах, передаваемых в беседах, для которых будет выполняться загрузка и фильтрация по политике безопасности. Solar Dozor не обрабатывает файлы размером более 500 МБ. Значение по умолчанию – 100.

Примечание

Существует возможность ограничить максимальный размер передаваемых файлов на стороне мессенджера Webex и таким образом обеспечить загрузку и фильтрацию всех переданных в беседах файлов.

- **Загружать историю сообщений за последние** – задать промежуток времени, за который требуется загрузить сообщения из истории. Возможные значения: **1 день**, **5 дней**, **10 дней**, **30 дней**, **60 дней**, **90 дней**, **Все возможные**.
- **Сообщения и файлы** – выбрать один из двух вариантов:
  - **Только ранее не загруженные** – при загрузке истории сообщений будут учтены сообщения, уже имеющиеся в архиве, и повторно загружены не будут. Такой вариант подходит при увеличении выбранного периода истории.
  - **Все за выбранный период** – сообщения за выбранный период истории будут загружены независимо от того, были ли они помещены в архив ранее. Такой

вариант можно применить при необходимости перефильтрации сообщений в архиве.

- **Интервал обновления** – периодичность в секундах, с которой Solar Dozor опрашивает сервер Webex в ожидании новых сообщений.

Внимание!

Производителем корпоративного мессенджера установлено ограничение на количество запросов в единицу времени, отправляемых на сервер Webex. При достижении предела сообщения перестают загружаться в Solar Dozor. По умолчанию таймаут загрузки сообщений с сервера действует в течение минуты, при этом производитель может установить более длительный период. По истечении этого времени загрузка сообщений возобновляется.

13. Нажать **Сохранить**, **Применить**.

14. Перейти в раздел **Система > Узлы и роли** и назначить выбранному узлу роль **Краулер: корпоративные мессенджеры**. Этот узел также должен иметь роль **Фильтр почтового потока**. В территориально-распределённой схеме работы (модуль **Мультидозор**) этот узел должен находиться на общих ресурсах.

Внимание!

Серверы Cisco Webex, от которых Solar Dozor получает сообщения, испытывают переменную нагрузку в зависимости от времени суток, дня недели и других обстоятельств (в том числе непредсказуемых), вследствие чего время между возникновением сообщения в беседе и его попаданием в Solar Dozor может составлять от нескольких минут до 24 часов.

8.13. Настройка передачи информации в пользовательский сервер Zabbix

По умолчанию slave-узлы кластера Solar Dozor принимают соединения от сервера мониторинга Zabbix, который функционирует на master-узле. Чтобы slave-узлы принимали соединения от пользовательского сервера, необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование > Мониторинг > Агенты мониторинга**.

2. Задать значения параметров:

   - **Порт** – 10050.

   - **Пользовательский сервер мониторинга (для пассивных проверок)** – пользовательские серверы мониторинга, используемые для пассивных проверок, т.е. упрощенных запросов. В качестве значения задается список перечисленных через запятую IP-адресов или имен узлов, допускается использование маски CIDR в формате **X.X.X.X/N**.

     Примеры значений:

```
127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.domain
```

- **Пользовательский сервер мониторинга (для активных проверок)** – пользовательские серверы мониторинга, используемые для активных проверок, которые требуют более сложной обработки. В качестве значения задается список перечисленных через запятую пар **IP-адрес:порт** или **Имя узла: порт**. Не допускается использование пробелов. Если значение не указано, активные проверки отключены.

3. Для сбора дополнительной статистики по параметрам из каталога **/etc/zabbix/zabbix_agentd.d/** установить флажок **Читать системную конфигурацию zabbix-agent (/etc/zabbix/zabbix_agentd.d/)**.

4. Нажать **Сохранить** и **Применить**.

Чтобы получать статистику по показателям, проверка которых по умолчанию не предопределена в сервере мониторинга Zabbix, следует создать пользовательские параметры **Userparameter**.

Примечание

*За рекомендациями относительно настройки **Userparameter** следует обращаться к руководству по Zabbix.*

Примечание

*Созданные пользователем параметры **Userparameter** не будут работать, если конфигурационные файлы с их описанием отсутствуют в каталоге **/etc/zabbix/zabbix_agentd.d**. При добавлении дублирующихся **Userparameter** пользовательский сервер Zabbix не будет работать.*

8.14. Настройка распознавания графических объектов

Для корректного функционирования сервиса распознавания графических объектов необходимо, чтобы процессор поддерживал набор инструкций **avx**, **avx2** и **avx512**. Проверить наличие этой поддержки можно с помощью следующей команды:

 # grep avx /proc/cpuinfo

Вывод команды должен быть непустым.

Внимание!

*Сервис **god-server** работает на серверах с поддержкой CPU/GPU и не работает на серверах с поддержкой QEMU. Изображения формата **JPEG2000** не обрабатываются.*

Для настройки распознавания графических объектов необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Узлы и роли** и назначить одному из узлов роль **Распознавание графических объектов**.

Внимание!

Настоятельно рекомендуется использовать сервер с графическими процессорами. Чем больше графических процессоров будет на сервере – тем производительнее будет сервис распознавания графических объектов. При отсутствии сервера с графическими процессорами следует выделить сервер с наибольшим количеством запаса производительности центрального процессора.

2. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Обработка сообщений**.

3. В секции **Сервис фильтрации сообщений** задать значение параметра **Таймаут при взаимодействии с сервером определения графических объектов** равным 30.

4. В секции **Сервис определения графических объектов** задать значения параметров:

- **Локальный порт, на котором сервер будет принимать соединения** – 9303.
- **Максимальное количество обработчиков, выполняющих распознавание** – количество экземпляров обработчика, одновременно выполняющих распознавание графических объектов. Для каждого экземпляра организуется очередь сообщений для обработки, максимальное количество сообщений в очереди – 100. Значение по умолчанию: 0 (количество экземпляров обработчика будет равно количеству ядер процессора).
- **Количество GPU** – количество графических процессоров, используемых для распознавания графических объектов. Значение по умолчанию: 0 (будут использованы все графические процессоры сервера).
- **Уровень журналирования** – включить при необходимости диагностики работы сервиса.
- **Каталог для временных файлов** – оставить значение **/data/temp/god**.
- **Настройки ограничений на параметры графических изображений** – настроить исходя из объема передаваемых данных.

Внимание!

Максимальное ограничение на объем файлов изображений – 100 МБ, даже если задано значение выше или не задано вовсе.

Примечание

Подробное описание параметров конфигурации сервиса распознавания графических объектов приведено в документе Руководство системного администратора, приложение Параметры конфигурации Solar Dozor.

5. Перейти в раздел GUI **Политика > Инструменты > Графические шаблоны** и меню действий с этим разделом выбрать пункт **Добавить** (Рис.8.8).

6. В открывшемся окне ввести название шаблона (например, **Все печати**) и нажать кнопку **Сохранить** (Рис.8.8).

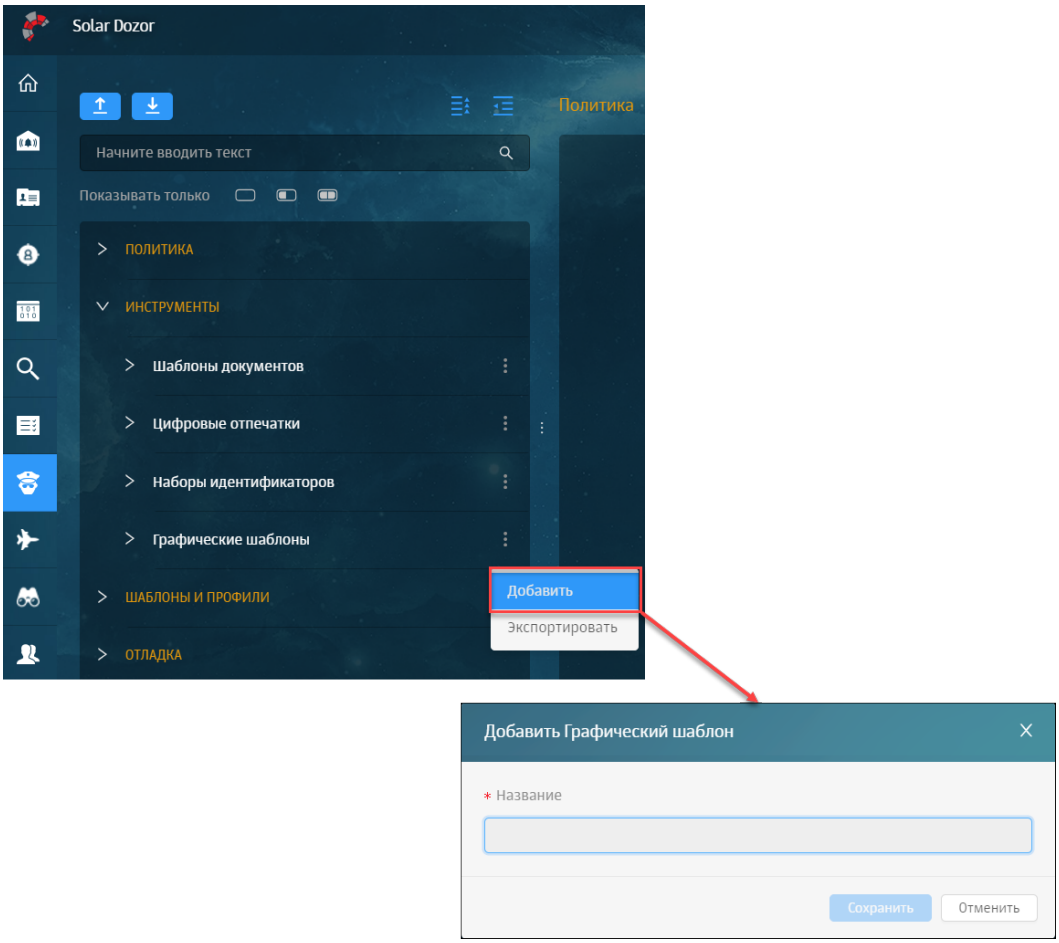


Рис. 8.8. Создание графического шаблона

7. В правой части экрана выбрать режим проверки, указать типы и минимальное количество объектов, необходимое для срабатывания условия политики (Рис.8.9). Нажать **Сохранить**.

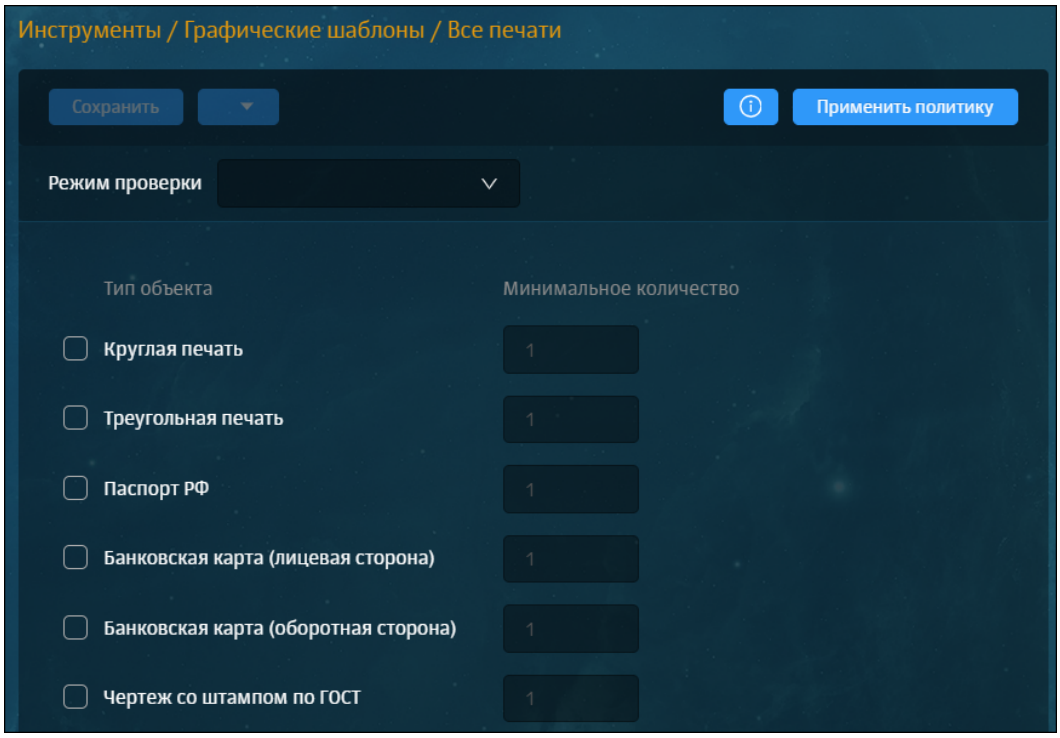


Рис. 8.9. Пример настройки графического шаблона

8. В меню действий с разделом GUI **Политика > Политика > Условия** выбрать пункт **Добавить** (Рис.8.10).

9. В открывшемся окне ввести название условия (например, **Условие для печатей**) и нажать кнопку **Сохранить** (Рис.8.10).

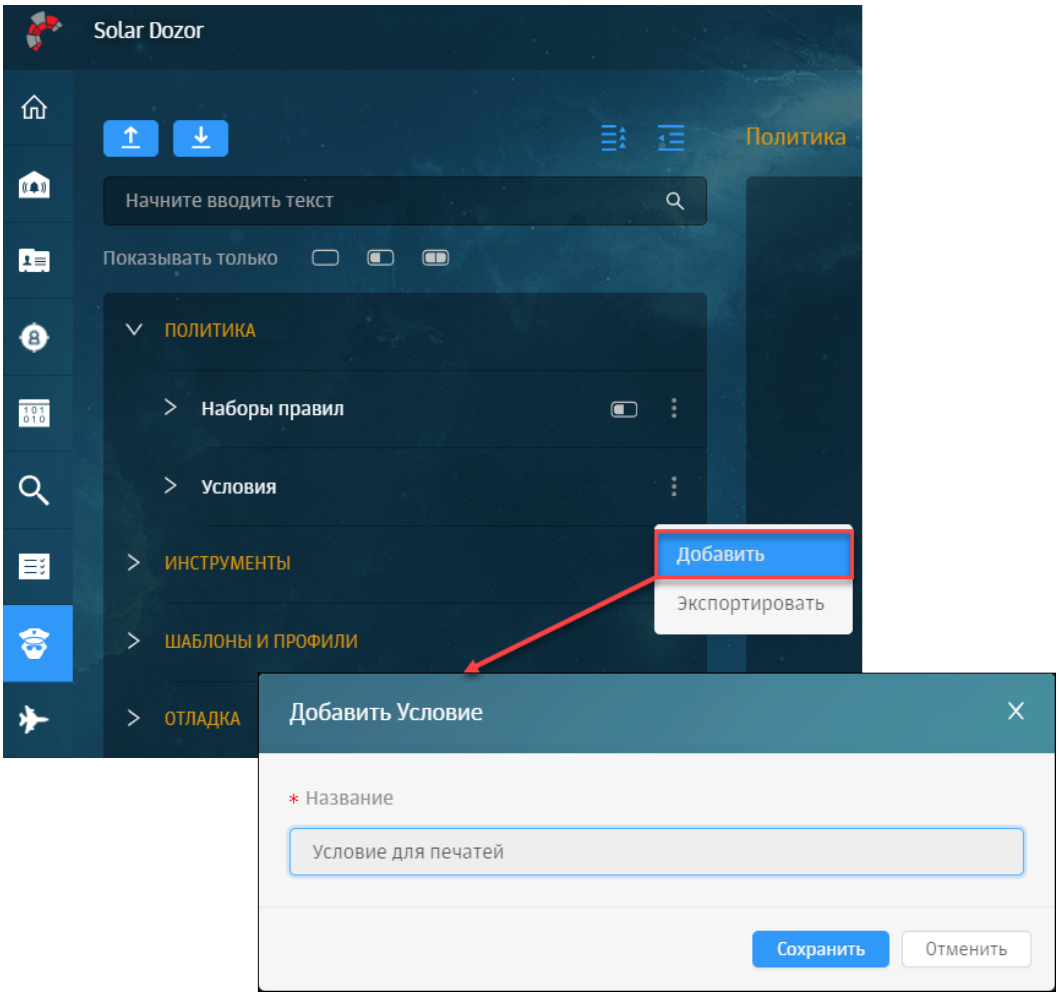


Рис. 8.10. Создание условия

10. В правой части экрана задать элементы условия (Рис.8.11), например:

- **Графический шаблон: Результат проверки**;
- **Соответствует**;
- **Все печати**.

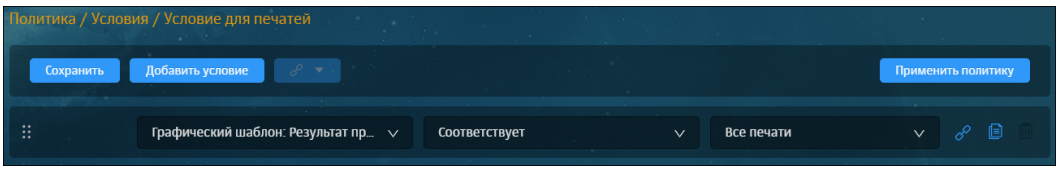


Рис. 8.11. Настройка условия

11. Нажать кнопку **Сохранить** (Рис.8.11).

12. В меню действий с разделом GUI **Политика > Политика > Наборы правил** выбрать пункт **Добавить** (Рис.8.12).

13. В открывшемся окне ввести название набора правил (например, **Правило для печатей**) и нажать кнопку **Сохранить** (Рис.8.12).

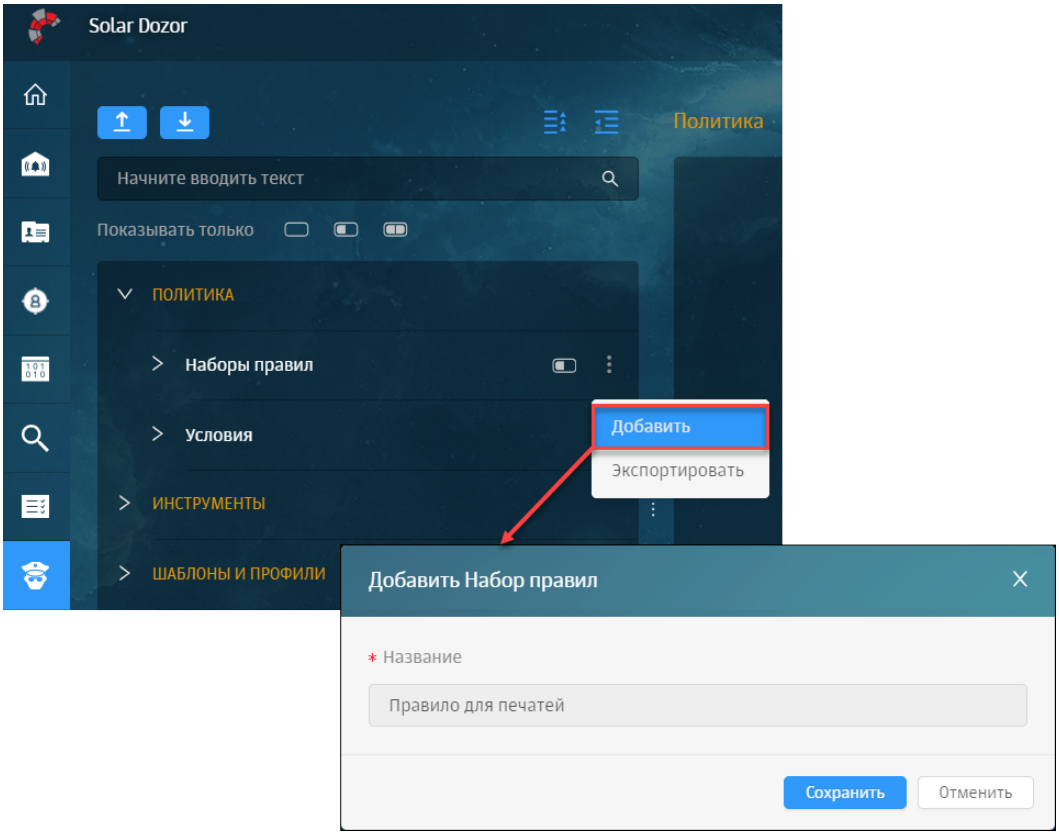


Рис. 8.12. Создание набора правил

14. В правой части экрана указать элементы правила (Рис.8.13):

- Название правила: **Правило для печатей**;
- Если: **Условие для печатей**;
- то: **Поместить в архив / Поместить в архив / Выполнить**.

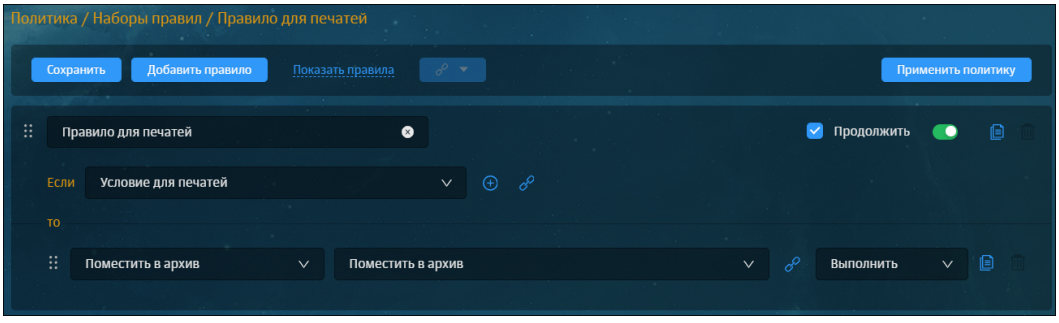


Рис. 8.13. Настройка набора правил "Управление печатями"

15. Нажать **Сохранить**, **Применить политику**.

8.15. Настройка сервиса интеграции

В Solar Dozor реализован сервис интеграции, предоставляющий единую точку входа для взаимодействия с внешним ПО. Текущая реализация позволяет внешнему ПО применять политику фильтрации, работать со списками слов, управлять событиями информационной безопасности, а также выполнять другие действия. В дальнейших релизах спектр возможностей будет расширяться.

Для работы сервиса интеграции требуется соответствующая лицензия.

Сервис интеграции является внутренним сервисом Solar Dozor и пользуется доверенным доступом к данным. Сервис интеграции не связан с именами учетных записей Solar Dozor и их паролями, поэтому настоятельно рекомендуется учитывать следующее:

- При использовании сервиса интеграции следует разрешить порт, назначенный этому сервису (по умолчанию – 33033) только тем узлам, которые будут участвовать во взаимодействии.
- При использовании сервиса интеграции следует использовать интеграционные ключи (см. ниже) во избежание несанкционированного доступа.
- Любой сервер Solar Dozor, которому назначена роль **Сервер интеграции**, является точкой доступа. Не назначайте эту роль тем серверам, на которых не предполагается использовать функциональность сервиса интеграции.
- При использовании сервиса интеграции следует запретить выбранный сетевой порт (см. ниже) на всех узлах сетевой инфраструктуры организации, на которых не предполагается использование сервиса интеграции.

Для запуска сервиса интеграции необходимо назначить одному или нескольким узлам роль **Сервер интеграции**. После этого необходимо перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Вспомогательные сервисы** и в секции **Сервис интеграции** задать значения параметров:

- **Вывод отладочной информации** – включить, если требуется вывод отладочной информации о работе сервиса интеграции в его журнал.
- **Порт сервиса интеграции** – задать порт, на котором сервис интеграции будет ожидать соединения с внешним клиентом. Следует убедиться, что этот порт не закрыт никаким сетевым ПО. Значение по умолчанию: 33033.
- **Использовать защищенное соединение** – рекомендуется оставить включенным. В этом случае сервис интеграции будет принимать запросы от внешнего клиента только в случае установки защищенного соединения по протоколу HTTPS.
- **Таймаут взаимодействия с веб-сервером** – таймаут в секундах, в течение которого сервис интеграции ожидает ответа от веб-сервера на запрос, полученный от внешнего клиента. Если веб-сервер не успеет ответить за это время – сервис интеграции возвращает внешнему клиенту ошибку HTTP 502.
- **Таймаут взаимодействия с сервером лицензирования** – таймаут в секундах, в течение которого сервис интеграции ожидает ответа от сервера лицензирования. Если сервис активен, то он запрашивает лицензию раз в час. Если сервис не получил

лицензию и/или неактивен, то он запрашивает лицензию раз в пять минут. Неактивный сервис не принимает запросов от внешнего клиента.

- **Интеграционные ключи** – при желании, добавить одну или несколько строк, содержащих произвольные последовательности символов. API сервиса интеграции будет ожидать одну из этих строк от внешнего клиента для его авторизации.

Также в секции JVM сервиса интеграции можно задать значения параметров:

- **Максимальное количество оперативной памяти (МБ)** – максимальное количество оперативной памяти в мегабайтах, выделяемой для сервиса интеграции.
- **Снимать дампы памяти при критических ошибках** – включить, если требуется сохранение дампа памяти сервиса интеграции в случае ошибки исчерпания памяти.
- **Каталог для записи дампов памяти** – путь к каталогу для записи дампов памяти.

С описанием API можно ознакомиться в интерфейсе Solar Dozor по адресу вида **https://dozor.organization.local:33033/docs**, подставляя актуальные значения адреса и порта узла, на котором запущен сервис интеграции. В этом же интерфейсе можно выполнять запросы к сервису интеграции в интерактивном режиме. Например, для применения политики следует раскрыть группу запросов **Политика**, раскрыть запрос **Применить политику**, нажать **Try it out** и нажать **Execute**.

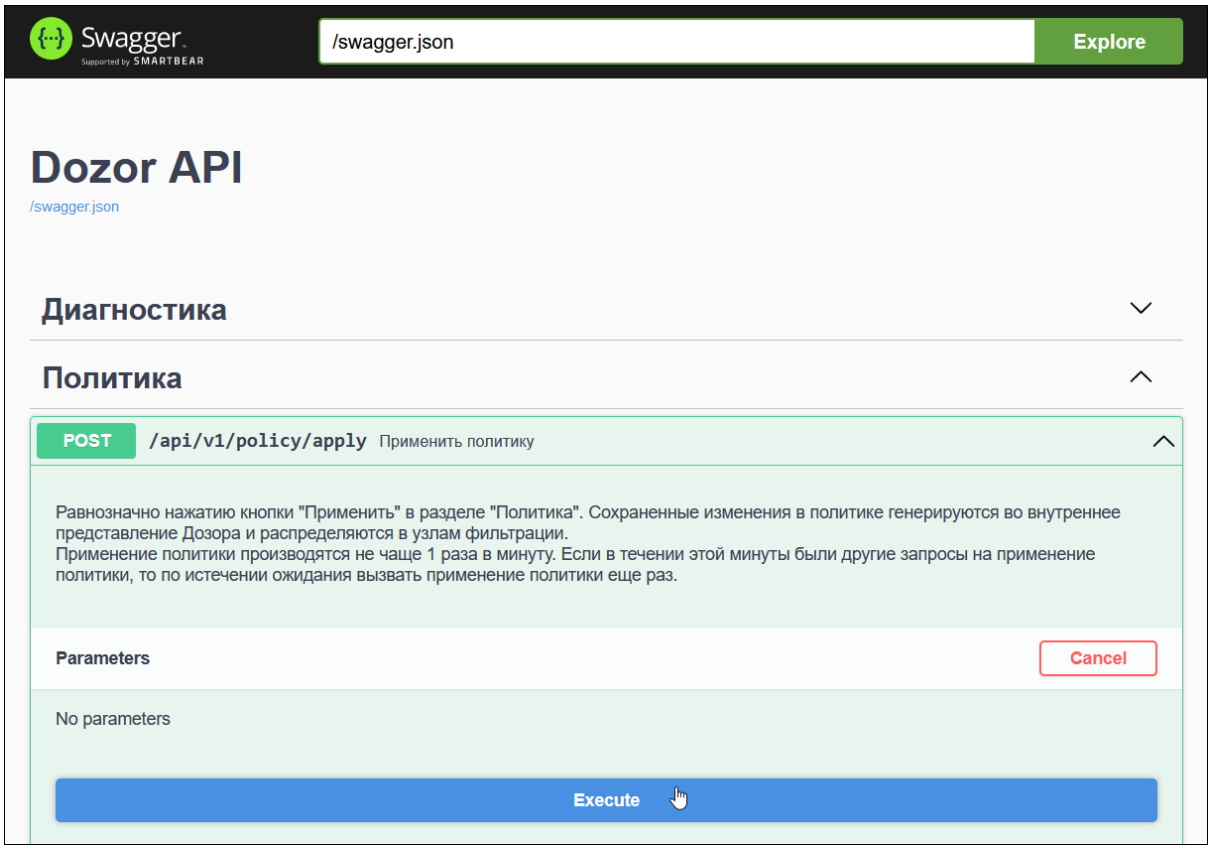


Рис. 8.14. Запрос Применить политику

После выполнения запроса на экран будет выведена следующая информация:

- **Curl** – текст запроса, с помощью которого можно выполнить этот же запрос из командной строки, используя утилиту **cURL**.
- **Request URL** – адрес, на который внешний клиент может отправить запрос с помощью каких-либо других средств.
- **Server response** – ответ сервера на отправленный запрос. Содержит стандартный код состояния HTTP и подробности:
  - **Response body** – тело ответа. Выводится, если предусмотрено синтаксисом ответа сервера на запрос.
  - **Response headers** – заголовки ответа.
- **Responses** – список кодов состояния HTTP и описаний всех возможных ответов сервера на запрос.

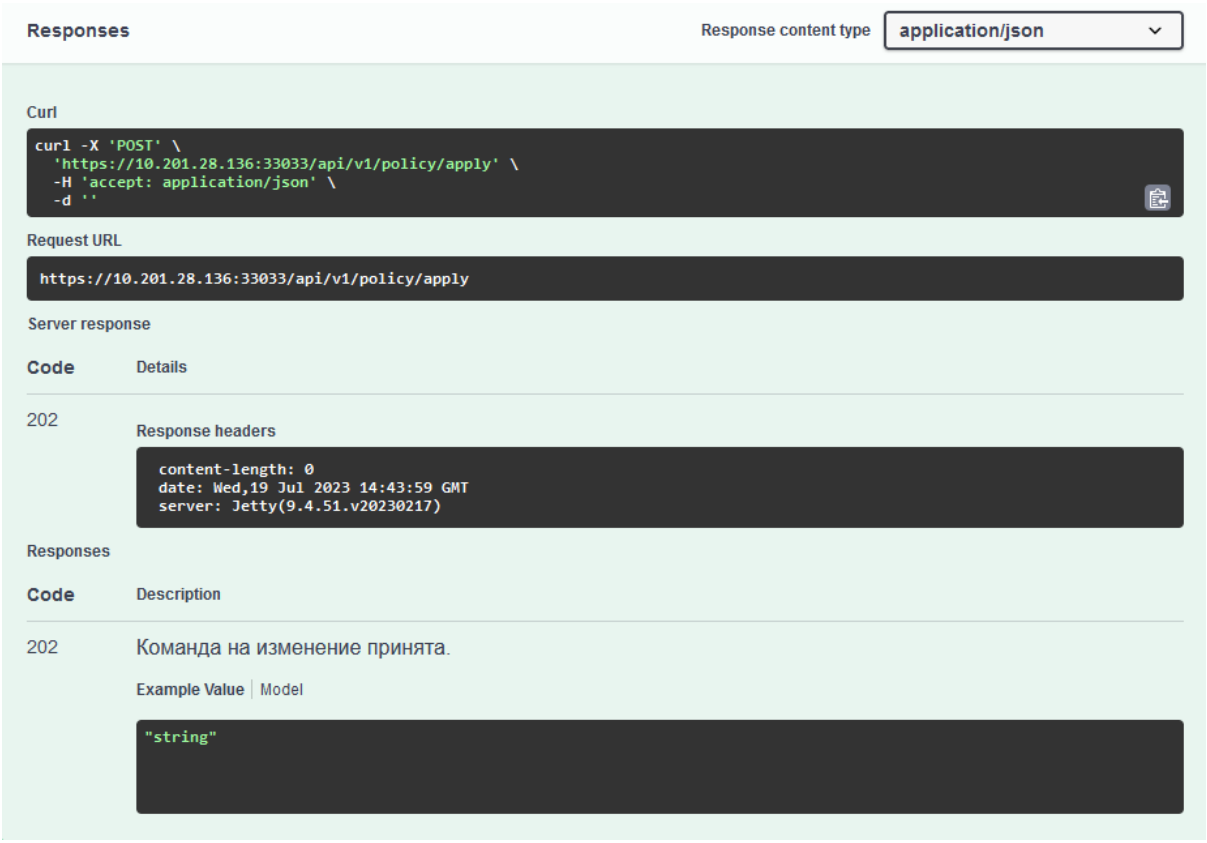


Рис. 8.15. Результат выполнения запроса Применить политику

Для авторизации внешнего клиента сервисом интеграции можно использовать интеграционный ключ. Настоятельно рекомендуется задать такие ключи – для этого следует задать в конфигурации один или несколько таких ключей, как описано выше, после чего сервис интеграции будет ожидать один из ключей в качестве значения заголовка **Autorization: apikey** каждого запроса со стороны внешнего клиента, например:

```
Autorization: apikey WKOHqszQNav+GGFhcYtwZnSvN7cy21LC
```

Ключ можно создать любым доступным способом: придумать самостоятельно или сгенерировать аппаратно, например, с помощью команды вида:

openssl rand -base64 24

Пример вывода команды:

```
WKOHqszQNav+GGFhcYtwZnSvN7cy21LC
```

К полученному результату можно добавить какую-либо осмысленную часть, например, название организации.

Если не задать интеграционные ключи – то любой клиент, находящийся в одной сети с соответствующим сервером Solar Dozor, для которого открыт соответствующий сетевой порт, сможет получить доступ к API этого сервера и выполнить на нём любые доступные действия, в том числе вредоносные.

Сервис интеграции имеет ограничение на количество входящих запросов от внешних клиентов – 100 запросов в минуту. При превышении количества запросов сервис отдает ответ с кодом **429 Too Many Requests**. Следует учитывать это ограничение при разработке внешнего клиента сервиса интеграции.

Подробная справка об использовании сервиса интеграции приведена в документе *Описание API универсального интеграционного модуля*.

8.16. Выпуск сертификата организации для web-интерфейса

Если в организации имеется собственный УЦ, можно использовать его сертификат для установления соединения с GUI Solar Dozor.

Примечание

Если в организации имеется сертификат формата PFX, следует убедиться, что пароль для ключа вам известен. Для этого необходимо загрузить командную оболочку Solar Dozor, а затем запросить информацию о сертификате, выполнив команды:

 # /opt/dozor/bin/shell

 # openssl pkcs12 -in <cert.pfx> -info

где ***<cert.pfx>*** *– имя сертификата с полным путем к нему. Во время выполнения команда запросит пароль для контейнера. После ввода пароля на экран будет выведена информация о контейнере. Затем будет запрошен пароль для ключа. При вводе правильного пароля для ключа на экран будет выведена информация о ключе. Если пароль неизвестен – следует либо запросить пароль у выпускающего подразделения организации, либо перевыпустить сертификат. Этот пароль должен содержать только буквы и/или цифры. После этого следует конвертировать сертификат в формат JKS, выполнив команду в каталоге с этим сертификатом:*

 # keytool -importkeystore -srckeystore <cert.pfx> -srcstoretype pkcs12 -destkeystore WEB.jks -deststoretype JKS

Во время выполнения команда запросит установить пароль для нового контейнера. Следует установить пароль, совпадающий с паролем для ключа. После этого необходимо перейти к шагу ***15****.*

Для выпуска сертификата организации необходимо выполнить следующие действия на master-узле Solar Dozor:

1. Загрузить командную оболочку Solar Dozor, выполнив команду:

   # /opt/dozor/bin/shell

2. Открыть CLI и перейти во временный каталог (например, **/var/tmp/**), выполнив команду:

   # cd /var/tmp

3. Перед тем как создавать сертификат пользователя, сгенерировать закрытый ключ для него. Для этого необходимо запустить программу openssl с указанием имени файла создаваемого ключа:

   # openssl genrsa -out dz.key -aes256 2048

   В результате работы на экран будет выведено следующее сообщение:

   ```
   Generating RSA private key, 4096 bit long modulus
   ..................++
   ..........................................................................++
   e is 65537 (0x10001)
   Enter pass phrase for dz.key:
   Verifying - Enter pass phrase for dz.key:
   ```

   В ходе выполнения программы генерации на экран выводится приглашение ввести кодовое слово для создаваемого ключа – **Enter pass phrase for dz.key:**. Оно может состоять только из букв и/или цифр (спецсимволы не допускаются). После чего необходимо дважды (второй раз для проверки) ввести с клавиатуры кодовое слово длиной не менее 4 символов (например: **123456**). Данное слово необходимо запомнить.

4. Создать в текущем каталоге файл с именем **openssl.cnf** и записать в него следующие данные:

   ```
   [ req ]
   req_extensions = v3_req
   distinguished_name = req_distinguished_name
   promt=yes
   [ req_distinguished_name ]
   countryName                 = Country Name (2 letter code)
   countryName_default             = RU

   stateOrProvinceName             = State or Province Name (full name)
   stateOrProvinceName_default     = Moscow

   localityName                = Locality Name (eg, city)
   localityName_default            = Moscow

   0.organizationName              = Organization Name (eg, company)
   0.organizationName_default      = Organization

   organizationalUnitName          = Organizational Unit Name (eg, section)
   organizationalUnitName_default  = Dept

   commonName                  = Common Name (eg, your name or your server\'s hostname)
   commonName_default              = proxy.org.com
   ```

```
emailAddress                    = Email Address
emailAddress_default            = support@org.com

[ v3_req ]
basicConstraints = critical, CA:true
#basicConstraints = CA:false
#keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[ alt_names ]
DNS.0 = proxy.org.com
IP.0 = 192.168.10.15
```

Выделенные жирным значения параметров следует заменить на актуальные значения в организации:

- **countryName_default** – двухбуквенный код страны.
- **stateOrProvinceName_default** – регион.
- **localityName_default** – город.
- **organizationName_default** – название организации.
- **organizationalUnitName_default** – название подразделения, департамента и т. д.
- **commonName_default** – FQDN master-узла.
- **emailAddress_default** – контактный адрес электронной почты организации.
- **DNS.0** – FQDN master-узла.
- **IP.0** – IP-адрес master-узла.

5. Сгенерировать запрос на подпись сертификата, выполнив команду:

   # openssl req -new -key dz.key -out name.csr -config openssl.cnf

   В процессе выполнения команды система потребует ввести кодовое слово, заданное на шаге 3.

6. Зайти на портал УЦ Windows и нажать **Request a certificate**.

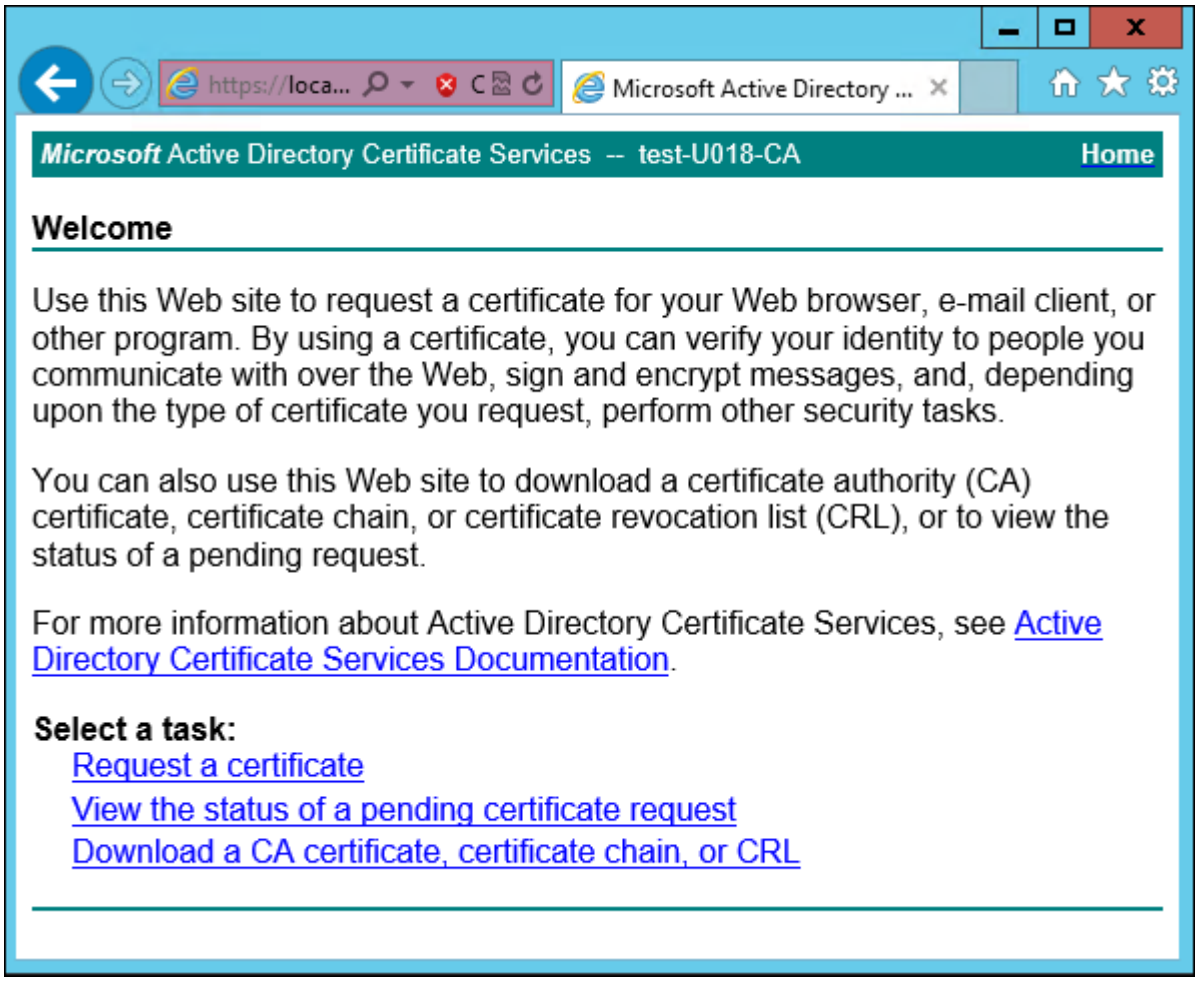


Рис. 8.16. Экран приветствия УЦ Windows

7. Нажать **advanced certificate request**.

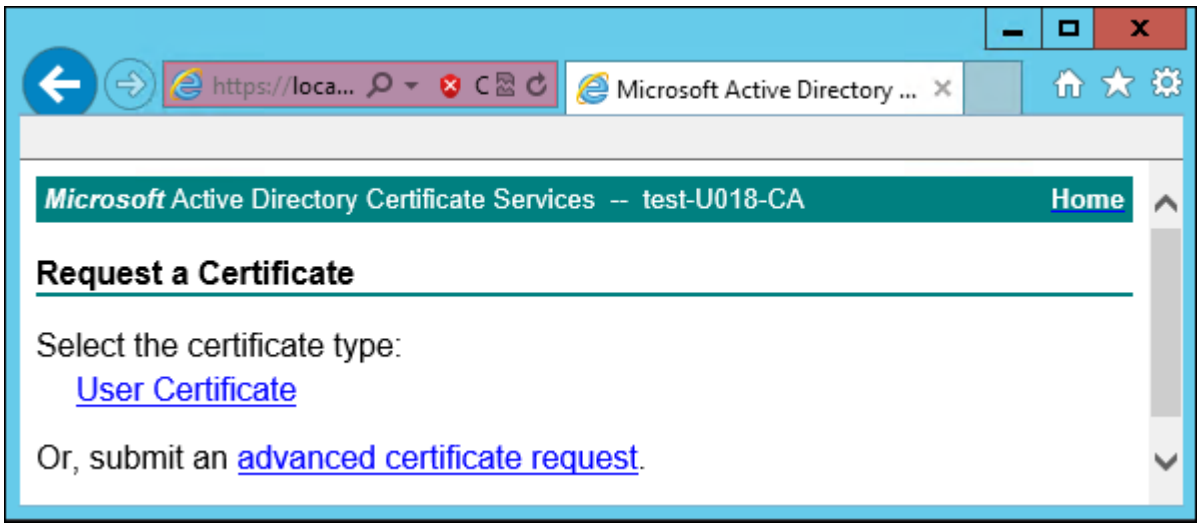


Рис. 8.17. Экран запроса сертификата

8. Нажать **Submit a certificate request by using...**.

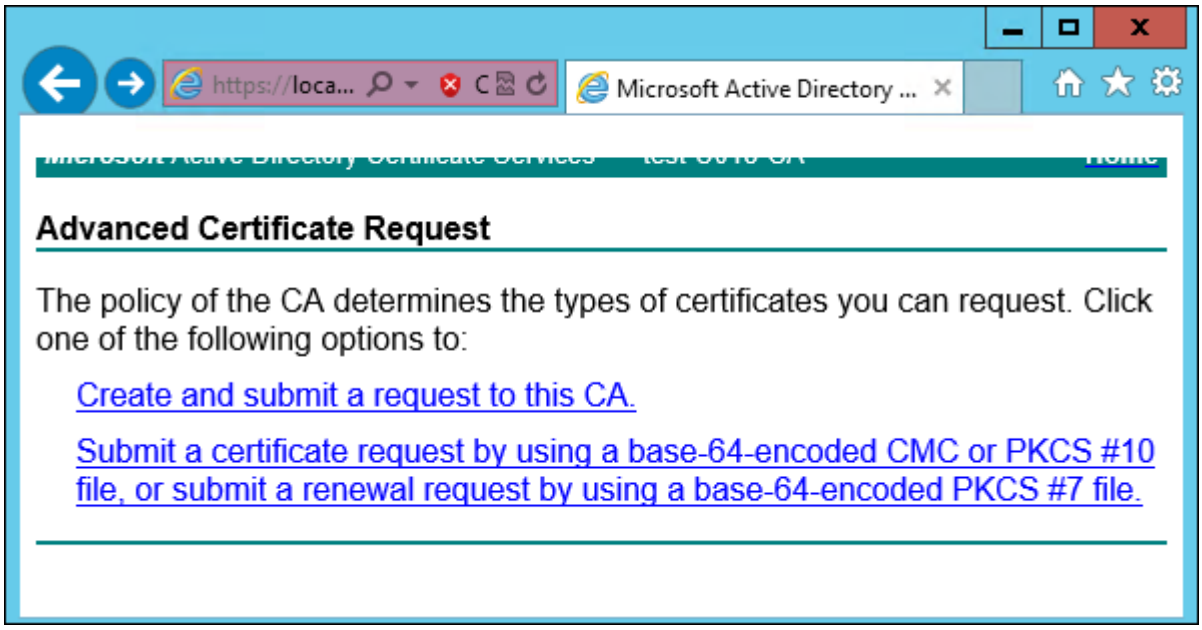


Рис. 8.18. Экран особого запроса сертификата

9. Выбрать шаблон сертификата **Веб-сервер** и вставить в поле **Base-64** содержимое файла, созданного на шаге 4. Нажать **Выдать**.

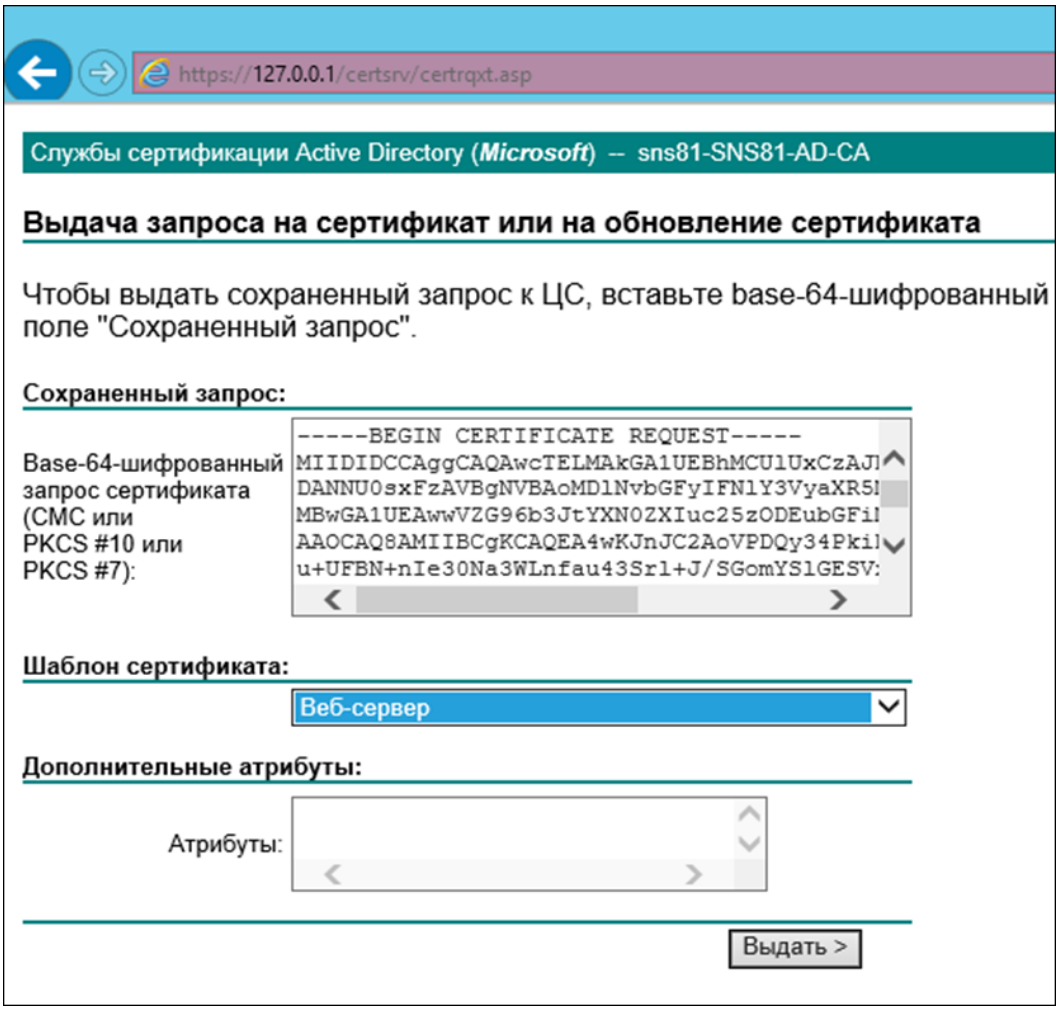


Рис. 8.19. Экран атрибутов сертификата

10. Нажать **Download certificate**. Сохранить файл сертификата с именем **dz.cer** во временный каталог, выбранный на шаге 2.

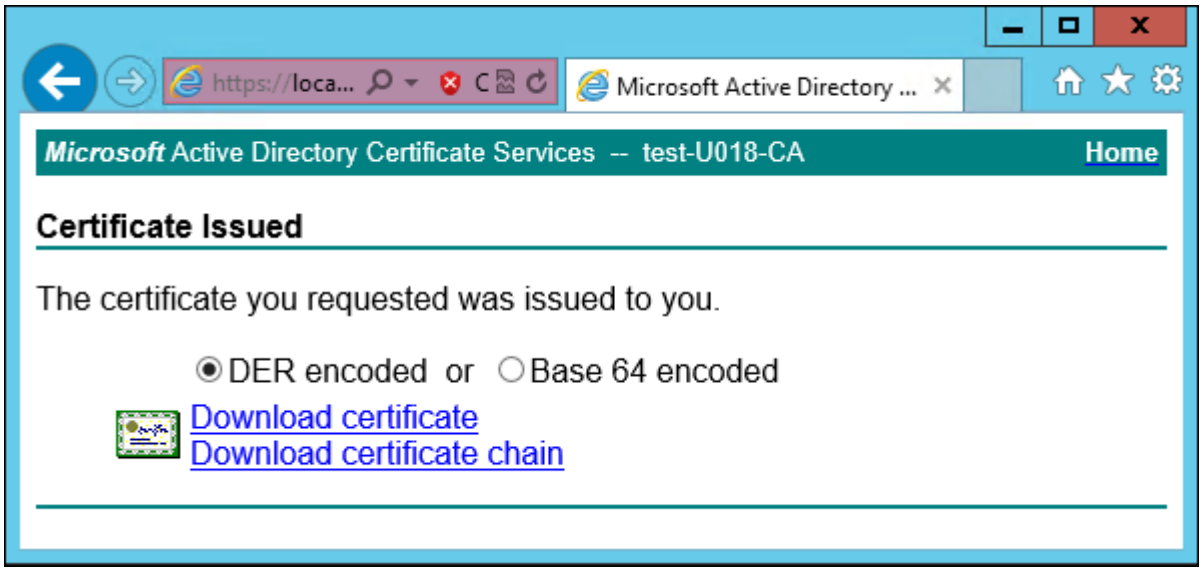


Рис. 8.20. Экран выдачи сертификата

11. Перейти на главную страницу портала УЦ и нажать **Download a CA certificate, certificate chain or CRL**. Сохранить сертификат УЦ с именем **ca.cer** в тот же каталог.

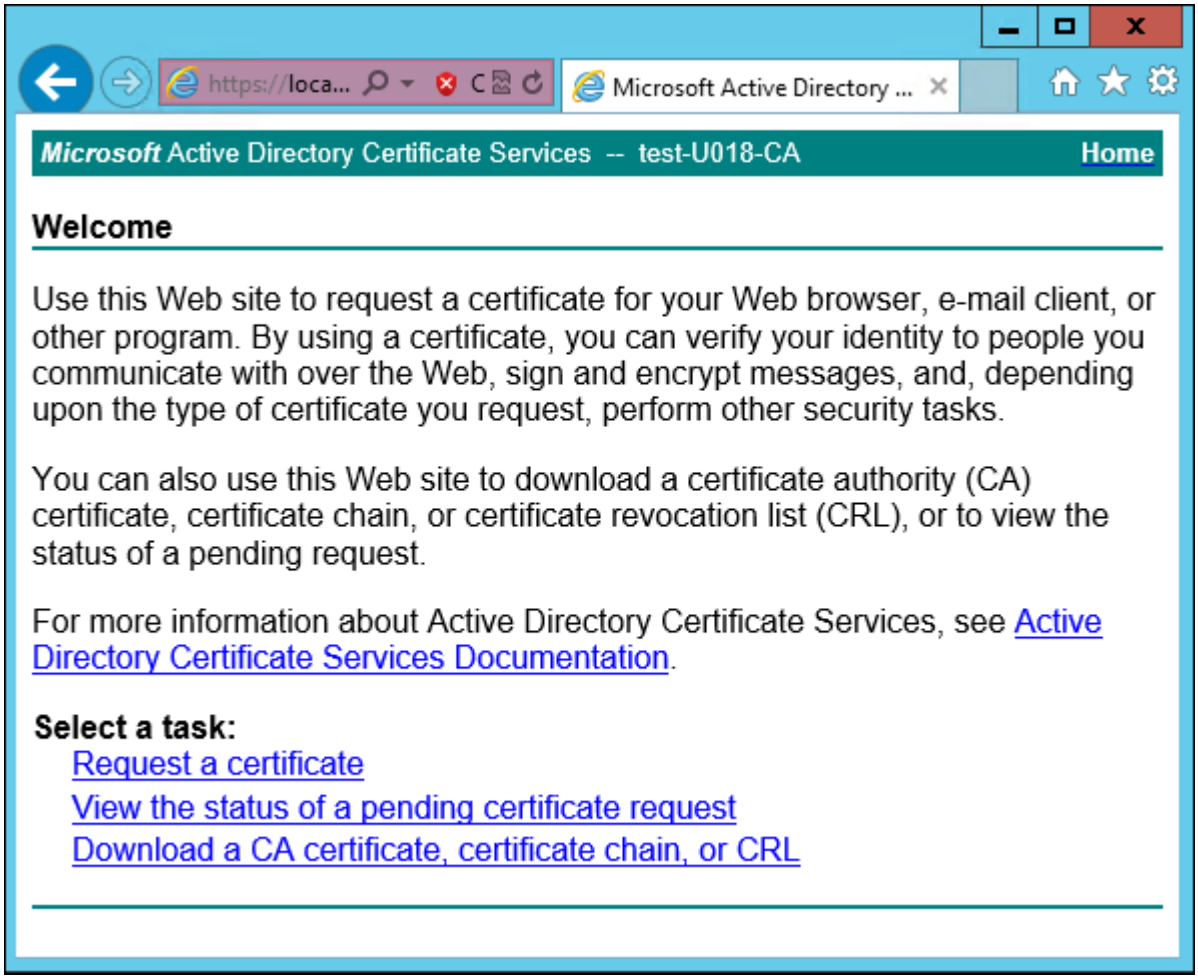


Рис. 8.21. Экран приветствия УЦ Windows

12. Вернуться в CLI Solar Dozor, перейти в выбранный временный каталог и сконвертировать загруженные сертификаты в формат PEM, выполнив команды:

    # openssl x509 -inform der -in dz.cer -out dz.pem

    # openssl x509 -inform der -in ca.cer -out ca.pem

13. Объединить сертификаты и ключ в сертификат pkcs12, выполнив команду:

    # openssl pkcs12 -export -out dz.p12 -inkey dz.key -in dz.pem -certfile ca.pem

    В ходе выполнения команды будет предложено сначала ввести кодовое слово, заданное на шаге 3, а затем указать пароль для экспорта, например: **secret**, и подтвердить его:

    ```
    Enter pass phrase for dz.key:
    Enter Export Password:
    Verifying - Enter Export Password:
    ```

14. Импортировать Java-хранилище сертификатов, выполнив команду вида:

    # keytool -importkeystore -deststorepass <password> -destkeypass <password> -destkeystore WEB.jks -srckeystore dz.p12 -srcstorepass <password>

    где **<password>** – пароль для экспорта, указанный на предыдущем шаге.

15. Скопировать Java-хранилище в каталог Solar Dozor, выполнив команду:

    # cp WEB.jks /opt/dozor/etc/ssl/

16. Сменить владельца хранилища, выполнив команду вида:

    # chown dozor:dozor /opt/dozor/etc/ssl/WEB.jks

17. Проверить, что сертификат находится в хранилище, выполнив команду вида:

    # keytool -list -keystore /opt/dozor/etc/ssl/WEB.jks

    О наличии сертификата в хранилище будет свидетельствовать вывод следующего вида:

    ```
    1, Jul 10, 2020, PrivateKeyEntry,
    Certificate fingerprint (SHA1): B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
    ```

18. Перейти в GUI, выбрать раздел **Система > Конфигурация > Расширенные настройки > Администрирование системы > Интерфейс**, перейти в секцию **Параметры сервера веб-интерфейса** и задать значения следующих параметров:

    - **Путь к хранилищу ключей и сертификатов** – **/opt/dozor/etc/ssl/WEB.jks**
    - **Пароль к хранилищу ключей** – пароль.

19. Перезапустить сервис **webserver**, выполнив в CLI следующие команды:

 # /opt/dozor/bin/shell

 # dsctl restart webserver

8.17. Проверка работоспособности настроенного Solar Dozor

Для проверки работоспособности архива сообщений установленного Solar Dozor необходимо выполнить следующие действия:

1. Перезапустить на каждом из узлов процессы Solar Dozor, выполнив от имени пользователя **root** следующую команду:

   # /opt/dozor/bin/dsctl restart

   Следует дождаться завершения перезапуска процессов Solar Dozor – об этом будет свидетельствовать возвращение приглашения командной строки.

2. Отправить тестовое сообщение на сервер Solar Dozor. Ниже приведён листинг команд, выполняемых для отправки сообщения:

   telnet 127.0.0.1 1025

   ```
   Trying 127.0.0.1...
   Connected to localhost.
   Escape character is '^]'.
   220 Z-2 Firewall 2.6.17 SMTP proxy ready to service
   ```

   helo localhost

   ```
   250 Pleased to meet you, localhost
   ```

   mail from: solar@solar.ru

   ```
   250 Sender OK
   ```

   rcpt to: solar@solar.ru

   ```
   250 Recipient OK
   ```

   data

   ```
   354 OK enter mail, end with <CRLF>.<CRLF>
   ```

   From: solar@solar.ru

   To: solar@solar.ru

   Subject: first letter

   <Пустая строка>

   Say hello to my little friend!

   .

   ```
   250 Message accepted for delivery (norm-d5d73742-fd4f-11df-8720-000c29e6dd7f)
   ```

quit

```
221 Closing connection
Connection closed by foreign host.
```

Примечание

Команды и другой текст, вводимые пользователем с клавиатуры, выделены моноширинным шрифтом; ответы сервера и другая выводимая системой на экран информация подсвечены серым цветом.

3. Запустить веб-интерфейс администратора Solar Dozor, указав в адресной строке браузера адрес **https://<IP-адрес сервера ПК Solar Dozor>**

   Продолжить открытие веб-узла, проигнорировав предупреждение браузера об ошибке сертификата безопасности или недоверенном соединении, и принять предлагаемый сертификат.

4. Ввести в соответствующие поля имя учётной записи и пароль администратора.

5. Выбрать раздел **Поиск**. На экране отобразятся инструменты поиска (см. Рис.8.22).

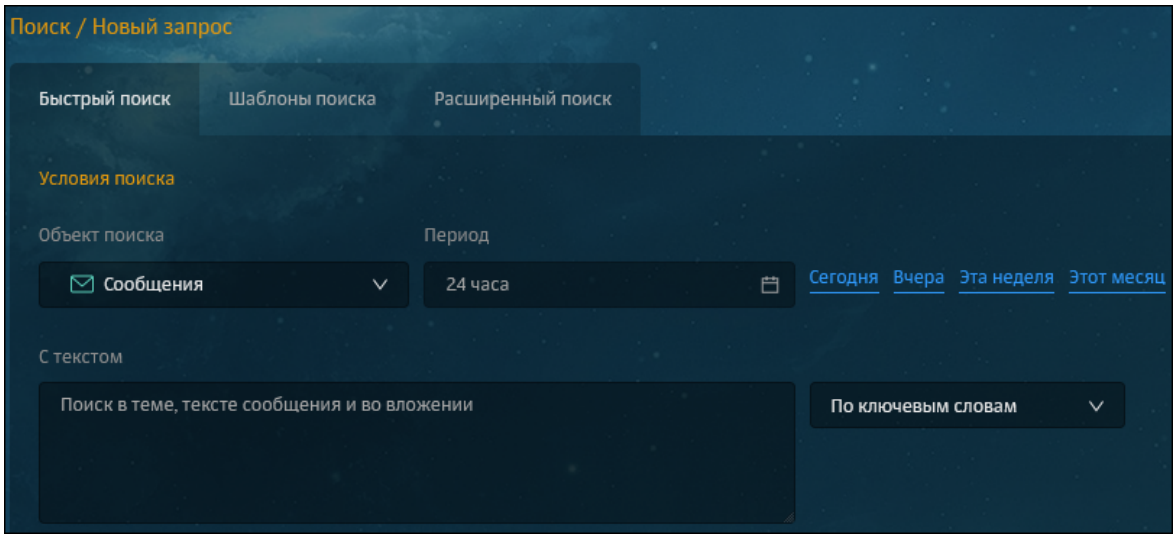


Рис. 8.22. Раздел Поиск

6. Поле **Объект поиска** оставить в значении **Сообщения**, в поле **С текстом** ввести **Say hello my friend**, и нажать кнопку **Найти**.

   На экране отобразится список результатов поиска с подсветкой совпадений (см. Рис.8.23)

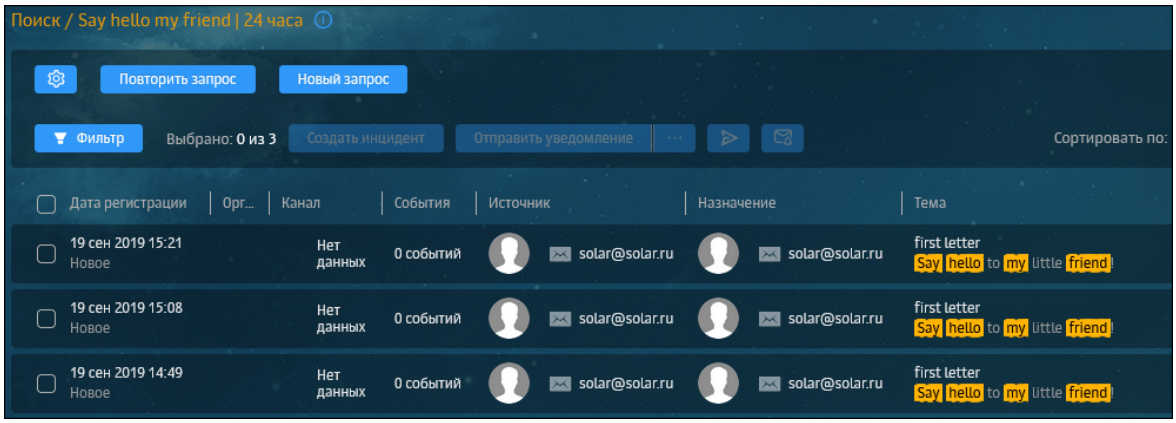


Рис. 8.23. Результат поиска

Для проверки работоспособности файлового хранилища установленного Solar Dozor необходимо выполнить следующие действия:

1. Проверить правильность настроек локальных ФХ и центрального ФХ.

2. Убедиться в том, что сервисы **filestorage-ng** и **skvt-cassandra**, обеспечивающие работу ФХ, находятся в состоянии **Запущен**.

3. Найти идентификатор контейнера отправленного письма (**vID**) в одном из журнальном файле архиватора (**archiver**), выполнив команду:

   # /opt/dozor/bin/seelog archiver

   На экране появится список следующего вида:

```
2015-12-11 11:47:50.233774500 support:info (8886) {f41c1342-ec81-11e3-b6e7-0050569900e4}
message f41c1342-ec81-11e3-b6e7-0050569900e4 archived successfully id=2.201406051147454239
 time=4493 msec msg_size=6199 bytes
2015-12-11 11:47:52.450357500 support:info (6534) {f46cc40e-ec81-11e3-9e66-0050569900e4}
message f46cc40e-ec81-11e3-9e66-0050569900e4 archived successfully id=3.201406051147500332
 time=1810 msec msg_size=7357 bytes
2015-12-11 11:47:52.581030500 support:info (12533) {f46f7be0-ec81-11e3-9e66-0050569900e4}
message f46f7be0-ec81-11e3-9e66-0050569900e4 archived successfully id=3.201406051147470345
 time=5409 msec msg_size=6860 bytes
2015-12-11 11:47:55.316807500 support:info (8886) {f4238fbe-ec81-11e3-b6e7-0050569900e4}
message f4238fbe-ec81-11e3-b6e7-0050569900e4 archived successfully id=3.201406051147530364
 time=1856 msec msg_size=5606 bytes
2015-12-11 11:47:59.487845500 support:info (6534) {f4937054-ec81-11e3-b387-0050569900e4}
message f4937054-ec81-11e3-b387-0050569900e4 archived successfully id=2.201406051147554240
 time=3864 msec msg_size=134732 bytes
2015-12-11 11:47:59.748163500 support:info (12533) {f411273e-ec81-11e3-b6e7-0050569900e4}
message f411273e-ec81-11e3-b6e7-0050569900e4 archived successfully id=2.201406051147554241
 time=4020 msec msg_size=2852 bytes
```

4. Выбрать из этого списка нужное письмо и соответствующий ему идентификатор контейнера **vID** (в фигурных скобках).

5. Создать конфигурационный файл командной оболочки языка запросов к Cassandra, выполнив команду:

 # touch /var/tmp/cqlshrc

Записать в этот файл следующее содержимое:

```
[connection]
factory = cqlshlib.ssl.ssl_transport_factory

[ssl]
certfile = /opt/dozor/etc/ssl/ca.crt
userkey = /opt/dozor/etc/ssl/bus.key
usercert = /opt/dozor/etc/ssl/bus.pem
version = TLSv1_2
```

Сохранить и закрыть файл.

6. Подключиться к базе данных индексов ФХ следующей командой:

   # /opt/dozor/cassandra/bin/cqlsh -k filestorage <hostname> --ssl --cqlsh /var/tmp/cqlshrc

   где <**hostname**> – имя узла, на котором размещено ФХ.

7. Ввести следующий запрос:

   select url from vids where vid='vg-000000/<vID>';

   где <**vID**> – идентификатор контейнера.

   На экране появится результат вида:

```
 url
----------------------------------------------------------------------------------------------------
 https://Dozor6:2266/_storage/main/2015/12/11/09/20/4abda222-9fe8-11e5-afb8-005056882665/

(1 rows)
```

8. Отключиться от базы данных командой **logout**. Перейти в каталог с контейнером командой вида:

   cd /data/storage/vg-000000/fs-1/2015/12/11/09/20/<vID>/data/

   где **/data/storage/vg-000000/fs-1/** – путь к файловому хранилищу, заданный в секции **Каталоги файлового хранилища** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка обеспечивающих средств > Хранение**). Вместо **2015/12/11/09/20/<vID>/** следует подставить соответствующую часть пути, полученного в предыдущем шаге.

9. Выполнить команду **ls -la**. В результате на экране появится информация следующего вида:

```
ds-mode@Dozor6
/data/storage/vg-000000/fs-1/2015/12/11/09/20/4abda222-9fe8-11e5-afb8-005056882665/data # ls
 -la
итого 12
drwxr-xr-x 2 dozor dozor 4096 Dec 11 12:20 .
```

```
drwx------ 4 dozor dozor 4096 Dec 11 12:20 ..
-rw-r--r-- 1 dozor dozor  196 Dec 11 12:20 body.gz
```

Последняя строка свидетельствует о том, что тело сообщения содержится в контейнере, и, следовательно, ФХ работает корректно.

9. Работа модуля S/MIME

Модуль **S/MIME** предназначен для шифрования и дешифрования сообщений и уведомлений, отправляемых и получаемых Solar Dozor.

При хранении сертификатов в файлах поиск сертификата выполняется по имени файла в каталоге, указанном в значении параметра **Директория для ключей и сертификатов S/MIME** (секция **Хранилище ключей S/MIME** раздела GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации перехваченных данных и детектирования критичной информации > Обработка сообщений**). Имена файлов должны содержать email-адрес, например **<email@domain.com>-cert.pem**. Сертификаты должны иметь формат **PEM (BASE64)** с разделителями следующего вида:

```
-----BEGIN CERTIFICATE-----
<Certificate_body>
-----END CERTIFICATE-----
```

Различные сертификаты в файле размещены один за другим.

Для шифрования сообщений и уведомлений, отправляемых из Solar Dozor, следует использовать в правилах фильтрации профиль отправки с установленным флажком **Зашифровать** (подробнее см. документ *Руководство пользователя*). При установленном флажке выполняется поиск сертификатов всех получателей уведомления. Если сертификаты для всех получателей найдены, то сообщение/уведомление шифруется открытыми ключами всех получателей. То есть в сообщении с уведомлением для каждого получателя содержится блок данных, который может быть расшифрован закрытым ключом данного получателя. После этого сообщение с уведомлением отправляется в соответствии с набором параметров отправки, который задан в профиле.

Если хотя бы для одного получателя сертификат не найден, действие зашифрованное уведомление не может быть отправлено. В таком случае генерируется ошибка, а сообщение перемещается в **err-spool**.

Для отправки зашифрованных уведомлений необходимо выполнить следующие действия:

1. Проверить, что указанный в параметре **Директория для ключей и сертификатов S/MIME** каталог с сертификатами пользователей существует (по умолчанию **/opt/dozor/etc/keystores**).

   В противном случае необходимо создать каталог, выполнив команду от имени пользователя **dozor**:

   $ mkdir /opt/dozor/etc/keystores

2. Сохранить и применить конфигурацию.

3. Скопировать файлы сертификатов в **/opt/dozor/etc/keystores**.

4. Перезапустить все процессы (раздел GUI **Система > Администрирование > Процессы**).

5. Создать профиль отправки (раздел GUI **Политика > Шаблоны и профили > Профили отправки**).

6. Создать шаблон уведомлений (раздел GUI **Политика > Шаблоны и профили > Шаблоны уведомлений**).

7. Создать условие (раздел GUI **Политика > Политика > Условия**), при котором необходимо отправлять зашифрованное уведомление.

8. Создать правило фильтрации **Отправить зашифрованное уведомление** (раздел GUI **Политика > Политика > Наборы правил**) с созданными условием, шаблонами отправки и уведомлений. Сделать правило головным.

9. Применить политику.

Расшифровка зашифрованного сообщения выполняется на этапе его распаковки. Дешифрование осуществляется распаковщиком соответствующего MIME-типа (**application/x-pkcs7-mime**). Такая схема обладает следующими особенностями:

- Единый механизм распаковки для всех типов данных (в том числе и для зашифрованных).
- Поддержка «ленивой» распаковки для шифрованных данных (дешифрование только при обращении к данным).
- Исходное сообщение не удаляется и не изменяется при дешифровании, можно осуществлять доставку исходного сообщения.
- В архиве сообщение доступно «как есть», можно осуществлять доставку из архива.
- В архиве доступны текстовые представления зашифрованных частей «открытым текстом», можно читать в архиве и осуществлять контекстный поиск.
- Из архива можно получить зашифрованные части в расшифрованном виде (дешифрование выполняется при извлечении из архива).

Для дешифрования требуются сертификаты и секретные ключи пользователей, а также файл с паролем от хранилища ключей.

При хранении закрытых ключей в файлах поиск осуществляется по имени файла в каталоге, указанном в конфигурации. Имена файлов должны иметь вид:

<Email-адрес>-key.pem

Например:

user@host.example-key.pem.

Ключи должны иметь формат **PEM (BASE64)** с разделителями:

"-----BEGIN RSA PRIVATE KEY-----" и **"-----END RSA PRIVATE KEY-----"**

Имя файла с паролем хранилища ключей должно иметь вид:

<Email-адрес>.password

Например:

user@host.example.password

Все закрытые ключи могут быть зашифрованы одним паролем. В этом случае в конфигурации указывается имя файла с общим паролем.

Подготовка к использованию возможности отправки и получения шифрованных сообщений и уведомлений состоит из следующих этапов:

1. Генерация ключей и сертификатов пользователей (см. раздел 9.1).
2. Настройка модуля **S/MIME** (см. раздел 9.2).
3. Настройка почтового клиента (см. раздел 9.3).

9.1. Генерация ключей и сертификатов пользователей

Сгенерировать ключи для шифрования почтовых сообщений можно с помощью программы **openssl**. Для этого необходимо выполнить следующие действия:

1. Создать каталог, в котором будут размещаться файлы ключей и сертификатов, например, **/home/ssl**. Для этого выполнить следующую команду от имени пользователя **dozor**:

   $ mkdir /home/ssl

2. Перейти в созданный каталог, выполнив команду:

   $ cd /home/ssl

3. Перед тем как создавать сертификат пользователя, сгенерировать закрытый ключ для него. Для этого необходимо запустить программу **openssl** с указанием имени файла создаваемого ключа. Действия выполнять от пользователя **dozor**. Формат команды для запуска следующий:

   $ openssl genrsa -des3 -out <key_filename> 4096

   где:

   - **<key_filename>** – имя создаваемого файла с расширением **.key**, например **cert.key**;
   - 4096 – размер ключа в битах.

   В результате выполнения команды на экран будет выведено сообщение следующего вида:

```
Generating RSA private key, 4096 bit long modulus
.....++
.....................................................................................................................++
e is 65537 (0x10001)
Enter pass phrase for cert.key:
Verifying - Enter pass phrase for cert.key:
```

   В ходе выполнения программы генерации на экран выводится приглашение ввести кодовое слово для создаваемого ключа – **Enter pass phrase for cert.key:**. После чего необходимо дважды (второй раз для проверки) ввести с клавиатуры кодовое слово длиной не менее 4 символов. Данное слово необходимо запомнить.

4. Создать csr-файл запроса на сертификат. Это файл нужен для проверки и идентификации. Для этого выполнить следующую команду от имени пользователя **dozor**:

   $ openssl req -new -key cert.key -out cert.csr

   После появления сообщения:

   ```
   Enter pass phrase for cert.key:
   ```

   необходимо ввести с клавиатуры кодовое слово, указанное на предыдущем шаге. После чего на экран будет выведено приглашение ввести информацию, которая будет включена в сертификат. Главное – указать почтовый адрес, для которого создается пара закрытый ключ – сертификат. Остальные параметры можно не указывать, для этого достаточно в каждой строчке ввести символ «.» (точка).

   ```
   You are about to be asked to enter information that will be incorporated
   into your certificate request.
   What you are about to enter is what is called a Distinguished Name or a DN.
   There are quite a few fields but you can leave some blank
   For some fields there will be a default value,
   If you enter '.', the field will be left blank.
   -----
   Country Name (2 letter code) [AU]:.
   State or Province Name (full name) [Some-State]:.
   Locality Name (eg, city) []:.
   Organization Name (eg, company) [Internet Widgits Pty Ltd]:.
   Organizational Unit Name (eg, section) []:.
   Common Name (e.g. server FQDN or YOUR name) []:
   Email Address []:admin@example.com

   Please enter the following 'extra' attributes
   to be sent with your certificate request
   A challenge password []:.
   An optional company name []:.
   ```

5. Подписать созданный csr-файл созданным ранее ключом. Для этого выполнить следующую команду от имени пользователя **dozor**:

   $ openssl x509 -req -days 365 -in cert.csr -signkey cert.key -out cert.crt

   В результате выполнения команды будет проведена проверка подписи и на экран выведены данные о сертификате, указанные ранее, в частности адрес электронной почты, для которого он создается:

   ```
   Signature ok
   emailAddress=admin@example.com
   Getting Private key
   Enter pass phrase for cert.key:
   ```

   В завершении потребуется ввести кодовое слово, заданное ранее.

6. Сконвертировать полученный файл сертификата в формат **.p12**, пригодный для импорта в программу-почтовый клиент. Для этого выполнить следующую команду от имени пользователя **dozor**:

   $ openssl pkcs12 -export -in cert.crt -inkey cert.key -name <name> -out cert.p12

где в качестве параметра **<name>** следует указать реальное имя пользователя (например, **admin**), для которого создается сертификат, чтобы в дальнейшем не возникло путаницы.

В ходе выполнения команды будет предложено сначала ввести кодовое слово, заданное ранее, а затем указать пароль для экспорта и подтвердить его.

```
Enter pass phrase for cert.key:
Enter Export Password:
Verifying - Enter Export Password:
```

Заданный пароль для экспорта необходимо запомнить, так как он используется для экспорта созданного сертификата в почтовую программу.

7. В результате выполнения указанных действий в созданном каталоге должно быть 4 файла с расширениями **.crt**, **.csr**, **.key**, **.p12**, наличие которых можно проверить, выполнив команду **ls** от имени пользователя **dozor**. Формат команды следующий:

   $ ls -1

   В результате выполнения команды на экран будет выведен список файлов в каталоге **/home/ssl**.

   ```
   cert.crt
   cert.csr
   cert.key
   cert.p12
   ```

8. Файл с расширением **.p12** следует переименовать так, чтобы его имя имело вид **<email>.p12**, где **<email>** – электронный адрес пользователя, для которого был создан сертификат. Этот файл необходимо импортировать в почтовый клиент, чтобы было возможным с ее помощью открывать сообщения, зашифрованные сгенерированным ключом (подробнее см. 9.3). Также его следует разместить в каталоге, указанном в параметре **Директория для ключей и сертификатов S/MIME** (см. 9.1).

9. Если в системе используется несколько сертификатов, созданных по этой процедуре, и для них заданы неодинаковые пароли для экспорта, то для каждого файла с расширением **.p12** следует создать одноимённый файл с расширением **.password**, записать в него пароль для экспорта в открытом виде, и разместить в том же каталоге.

   Примечание

   *Если один из паролей для экспорта повторяется чаще остальных – то можно указать его в параметре **Пароль по умолчанию для хранилищ ключей S/MIME** (см. 9.1), и не создавать файл с расширением **.password**.*

9.2. Настройка модуля S/MIME

После генерации ключей и сертификатов пользователей переименованные файлы следует скопировать в каталог, определенный параметром конфигурации **Директория для ключей и сертификатов S/MIME** секции **Хранилище ключей S/MIME** (раздел GUI **Система > Конфигурация > Расширенные настройки > Настройка средств фильтрации**

перехваченных данных и детектирования критичной информации > Обработка сообщений).

Рис. 9.1. Настройка параметров S/MIME

В значении параметра **Пароль по умолчанию для хранилищ ключей S/MIME** необходимо указать пароль, которым зашифрованы все закрытые ключи пользователей.

9.3. Настройка почтового клиента

В данном разделе описывается экспорт сгенерированного сертификата пользователя в программу - почтовый клиент и настройка почтового клиента для работы с зашифрованными почтовыми сообщениями. Такая настройка необходима, чтобы иметь возможность открывать зашифрованные уведомления, отправляемые из интерфейса Solar Dozor. Приводится описание настройки для почтовых клиентов Microdoft Outlook и Mozilla Thunderbird.

9.3.1. Настройка Microsoft Outlook

Для импорта ключа шифрования и настройки почтового клиента Microsoft Outlook на работу с зашифрованными сообщениями необходимо выполнить следующие действия:

1. Выбрать пункт меню **Файл > Параметры > Центр управления безопасностью** и нажать кнопку **Параметры центра управления безопасностью** (Рис.9.2).

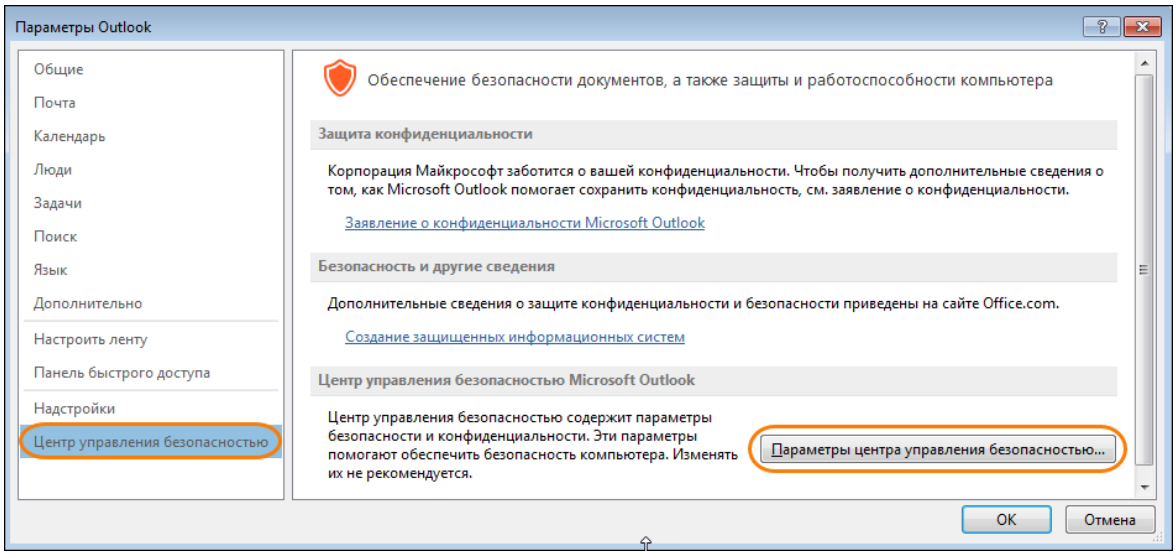


Рис. 9.2. Окно Параметры Outlook

2. В открывшемся окне в меню слева выбрать пункт **Защита электронной почты** (Рис.9.3):

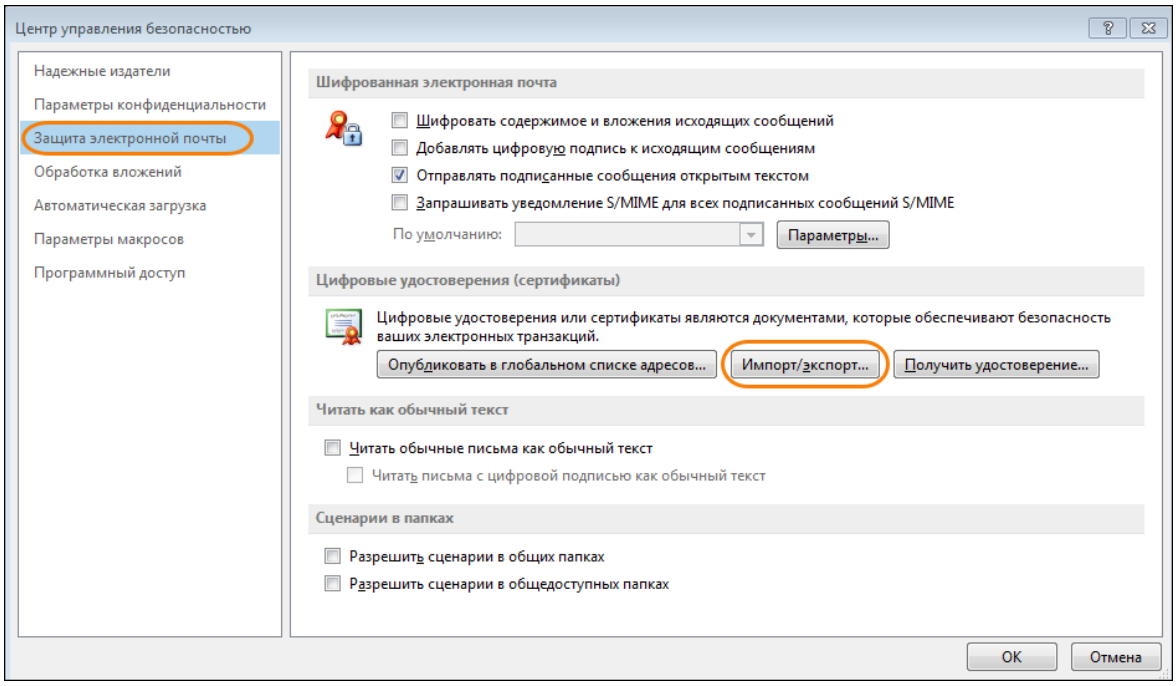


Рис. 9.3. Окно Центр управления безопасностью

3. В правой части окна в разделе **Цифровые удостоверения (сертификаты)** нажать кнопку **Импорт/экспорт** (Рис.9.3).

4. В открывшемся окне **Импорт/экспорт цифрового удостоверения** установить переключатель **Импортировать имеющееся цифровое удостоверение из файла** (Рис.9.4):

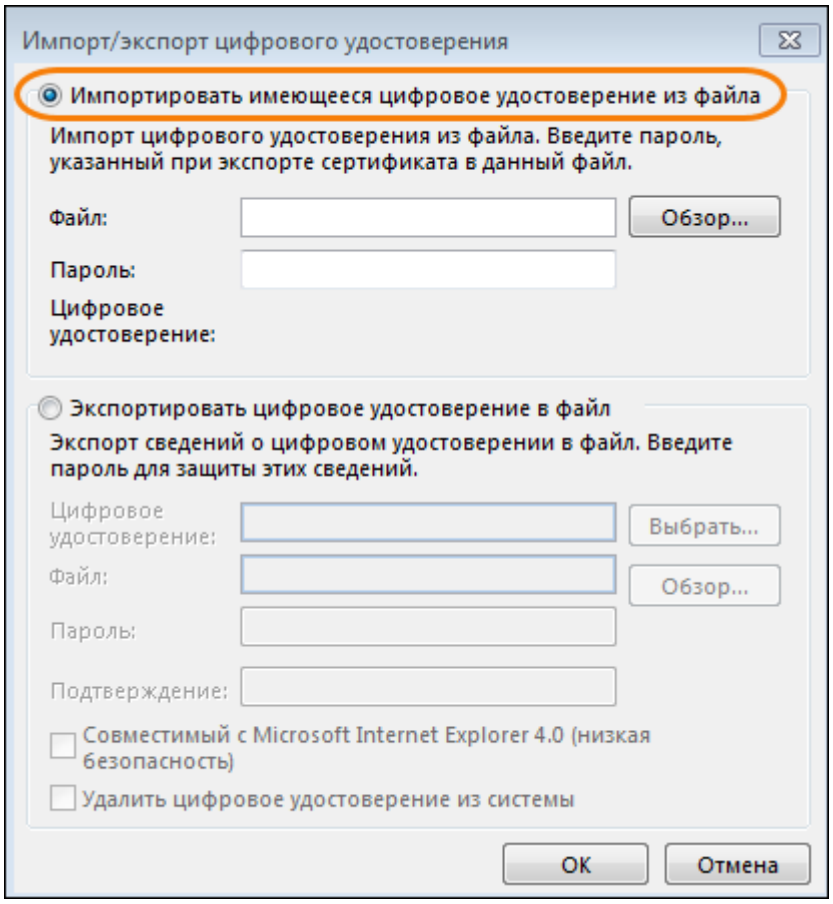


Рис. 9.4. Окно Импорт/экспорт цифрового удостоверения

5. Нажать кнопку **Обзор** и в открывшемся окне Проводника найти на жестком диске компьютера файл с сертификатом в формате **.p12**, созданный ранее и нажать кнопку **Открыть**:

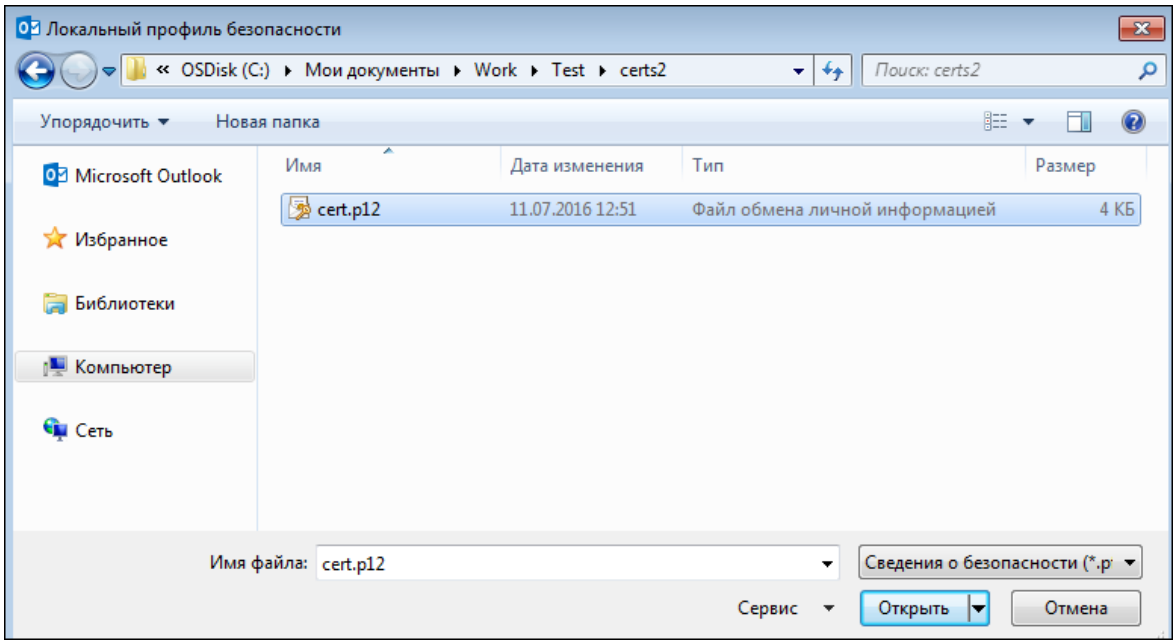


Рис. 9.5. Файл сертификата в формате .p12

6. В окне **Импорт/экспорт цифрового удостоверения** в поле **Файл** появится путь к указанному файлу (Рис.9.6). В поле **Пароль** необходимо ввести пароль для экспорта, указанный на шаге 6 в ходе генерации цифрового сертификата.

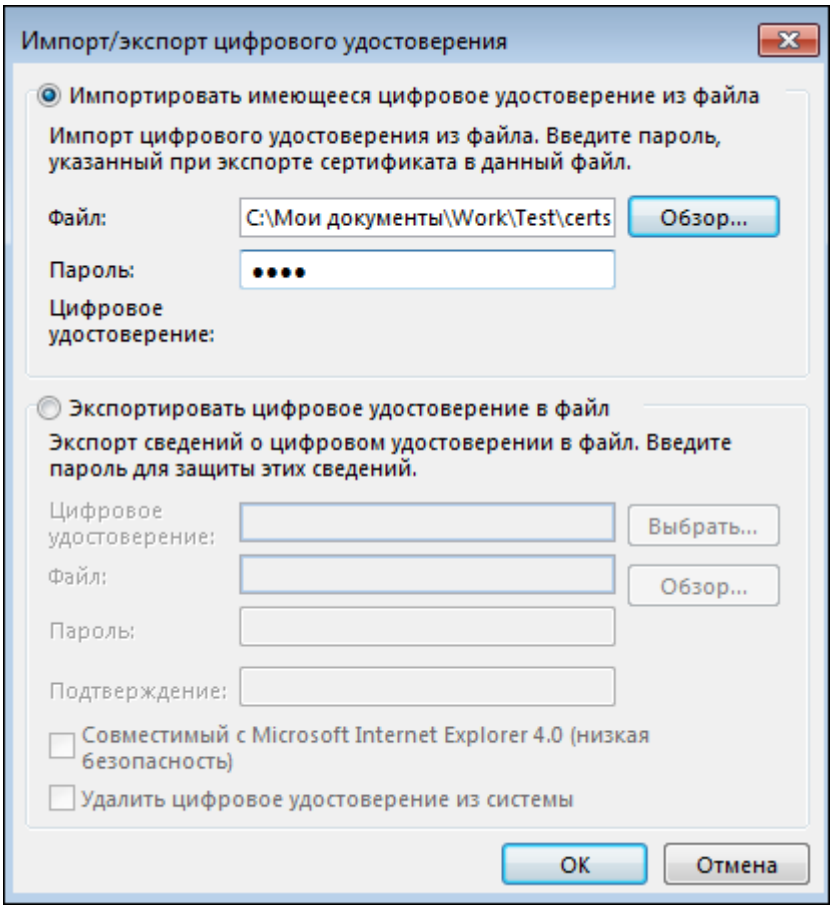


Рис. 9.6. Данные для импорта сертификата

7. Для завершения импорта сертификата нажать в окне **Импорт/экспорт цифрового удостоверения** кнопку **OK**.

8. На экране появится окно **Импорт нового закрытого ключа обмена** (Рис.9.7) с сообщением о том, что будет установлен средний уровень безопасности и кнопкой **Уровень безопасности**, при нажатии на которую можно выбрать средний или высокий уровень безопасности. Чтобы завершить импорт закрытого ключа без изменения уровня безопасности, следует нажать кнопку **OK**:

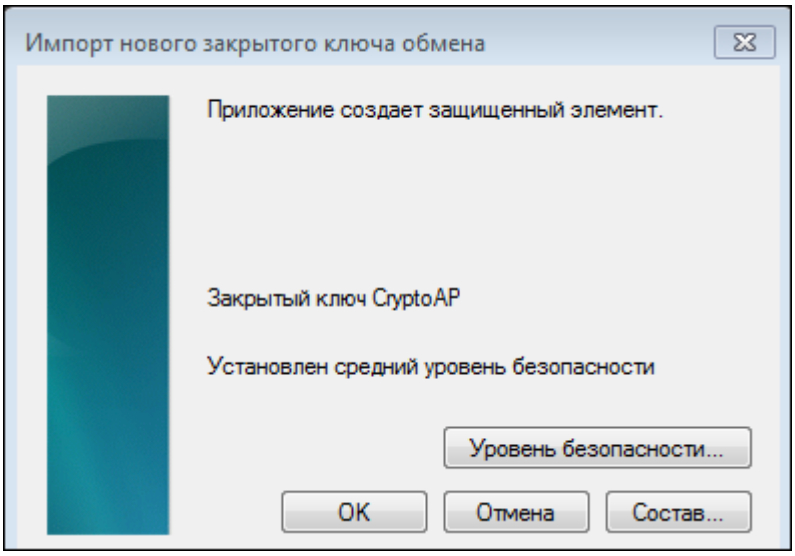


Рис. 9.7. Импорт нового закрытого ключа

9. При нажатии кнопки **Уровень безопасности** открывается окно, содержащее два переключателя для выбора уровня безопасности (Рис.9.8).:

   - **Средний** – при работе запрашивается только разрешение пользователя.
   - **Высокий** – при работе запрашивается разрешение с паролем.

   Для изменения уровня безопасности следует установить соответствующий переключатель и нажать кнопку **Далее**:

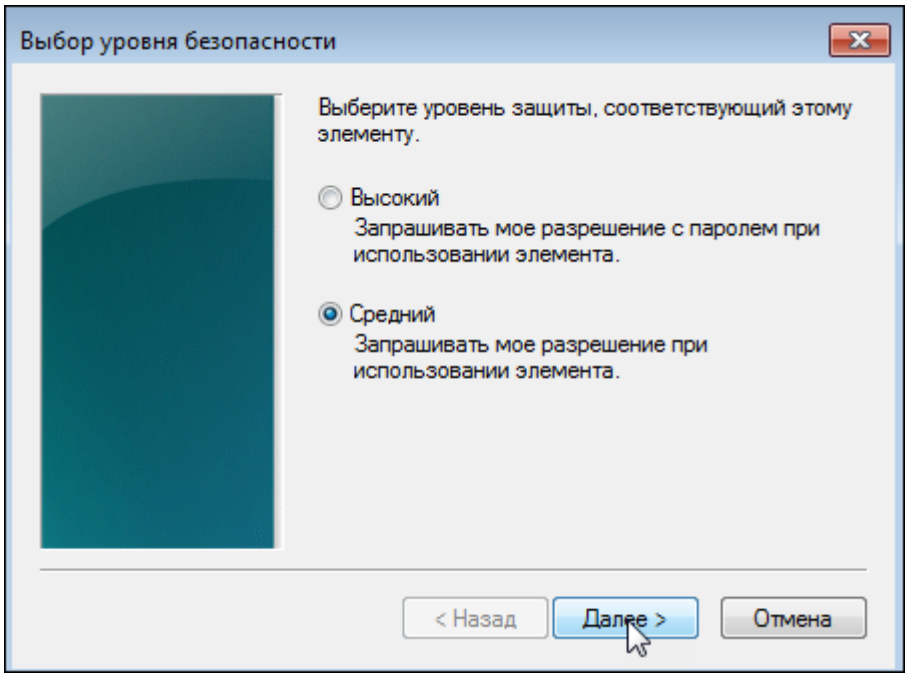


Рис. 9.8. Выбор уровня защиты

10. Откроется окно с сообщением об установке уровня безопасности (Рис.9.9). Для закрытия окна и завершения настройки Microsoft Outlook на работу с ключом шифрования следует нажать кнопку **Готово**:

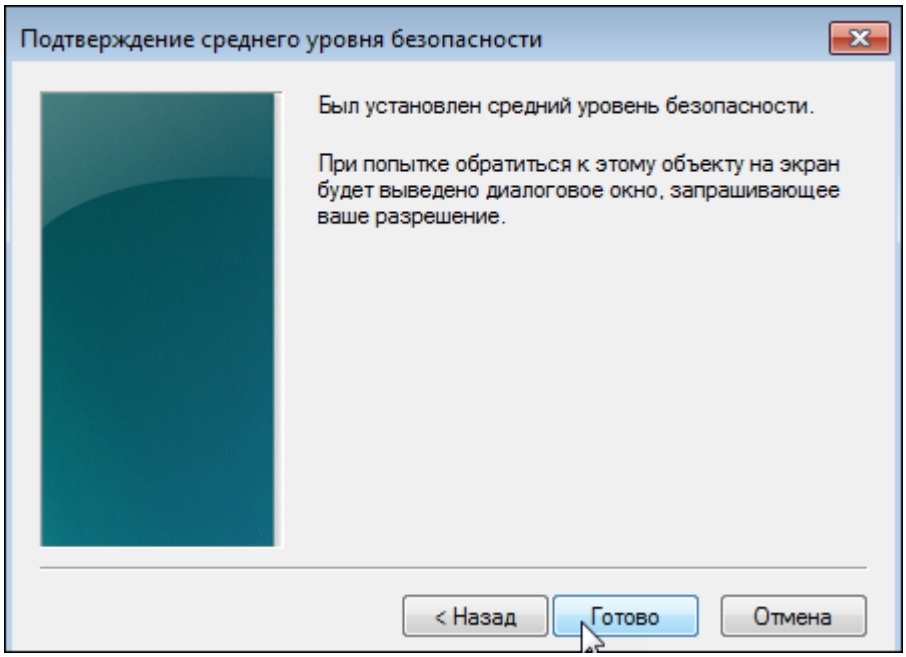


Рис. 9.9. Завершение импорта закрытого ключа

9.3.2. Настройка Mozilla Thunderbird

Для импорта ключа шифрования и настройки почтового клиента Mozilla Thunderbird на работу с зашифрованными сообщениями необходимо выполнить следующие действия:

1. Выбрать раздел **Учетные записи> Просмотр параметров этой учетной записи** (Рис.9.10).

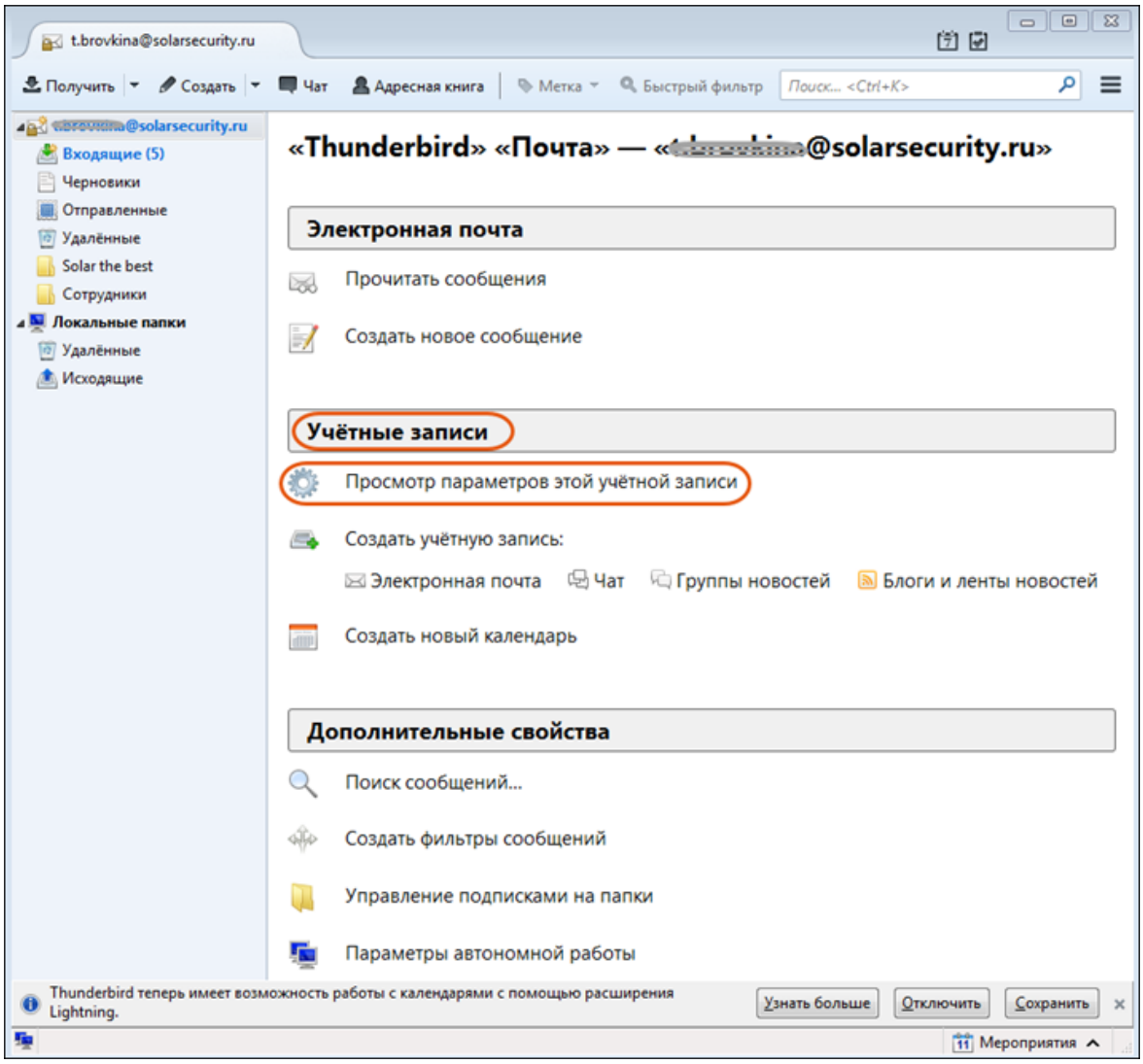


Рис. 9.10. Просмотр параметров учетной записи

2. В открывшемся окне **Параметры учетной записи** в списке параметров выбрать пункт **Защита** (Рис.9.11).

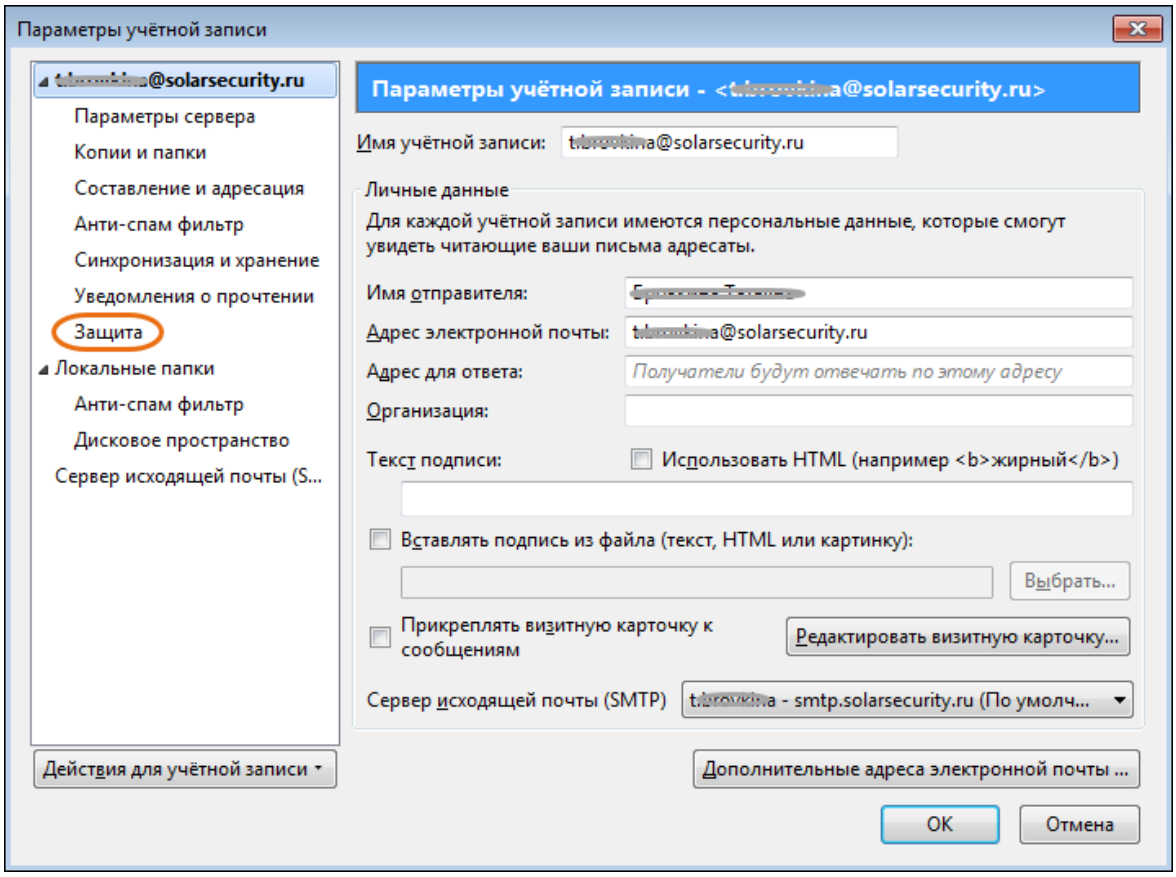


Рис. 9.11. Окно Параметры учетной записи

3. В правой части окна отобразятся параметры настройки шифрования и работы с зашифрованными сообщениями (Рис.9.12). Операция импорта сертификата должна быть подтверждена вводом мастер-пароля. Если он уже был создан ранее, то можно пропустить следующие шаги и переходить к пункту 6. Если мастер-пароль еще не создан, то необходимо в окне **Параметры учетной записи > Защита** нажать кнопку **Устройства защиты**.

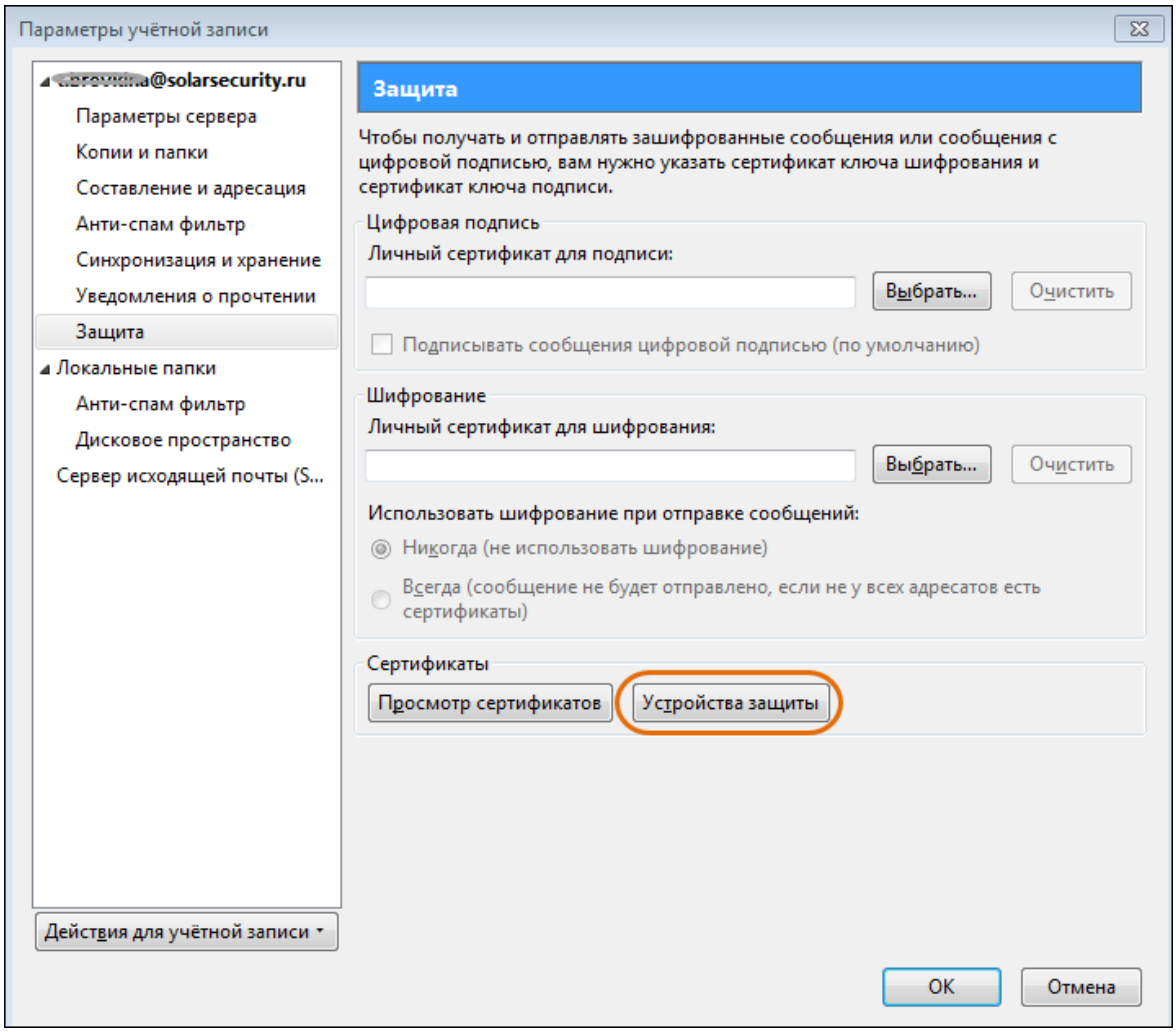


Рис. 9.12. Параметры настройки шифрования и работы с зашифрованными сообщениями

4. В открывшемся окне **Управление устройствами** в списке **Модули и устройства защиты** выбрать пункт **Модуль защиты** и нажать кнопку **Сменить пароль** (Рис.9.13):

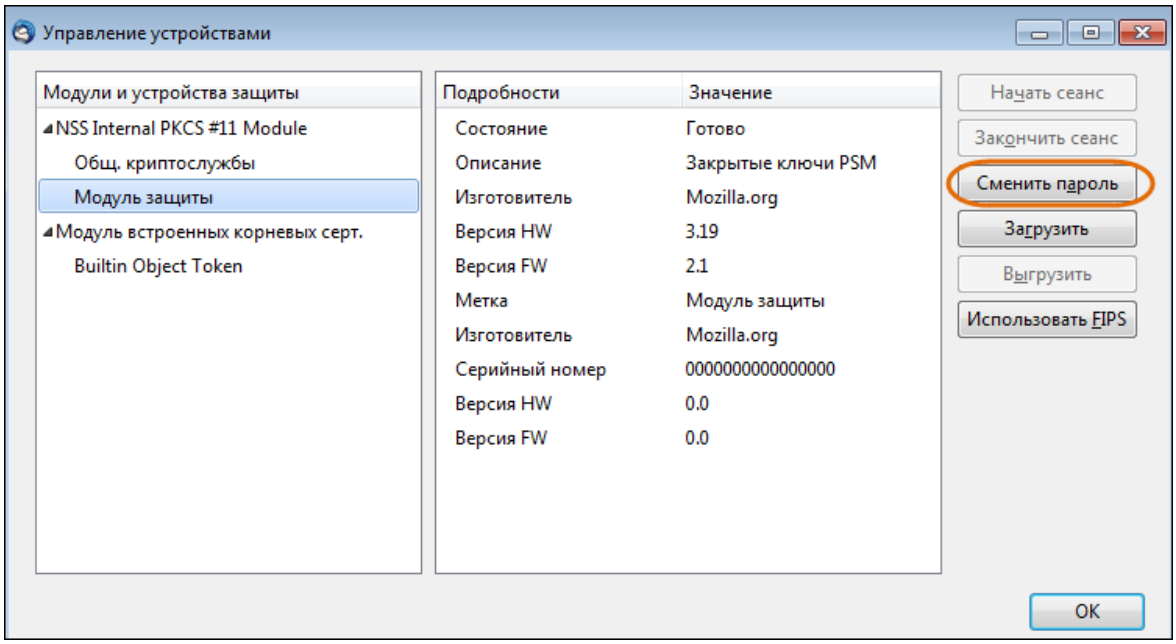


Рис. 9.13. Окно Управление устройствами

5. В открывшемся окне (Рис.9.14) следует ввести мастер-пароль (и подтвердить его, указав повторно) и нажать кнопку **OK**:

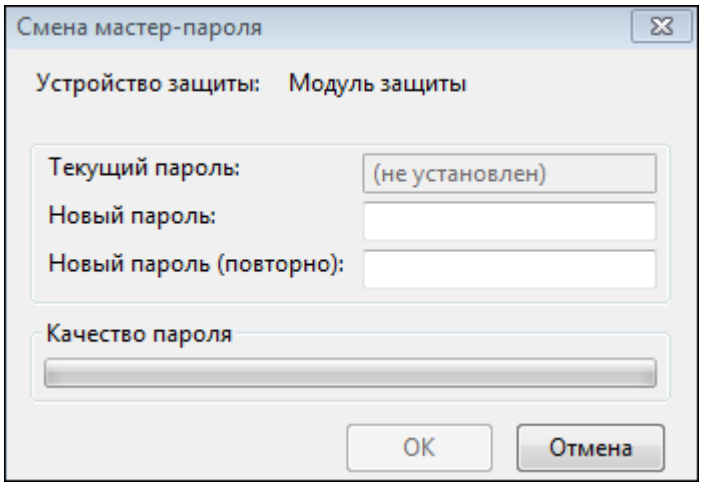


Рис. 9.14. Окно создания мастер-пароля

6. После того, как мастер-пароль создан, в окне **Параметры учетной записи** необходимо нажать кнопку **Просмотр сертификатов** (Рис.9.12). Откроется окно **Управление сертификатами** (Рис.9.15):

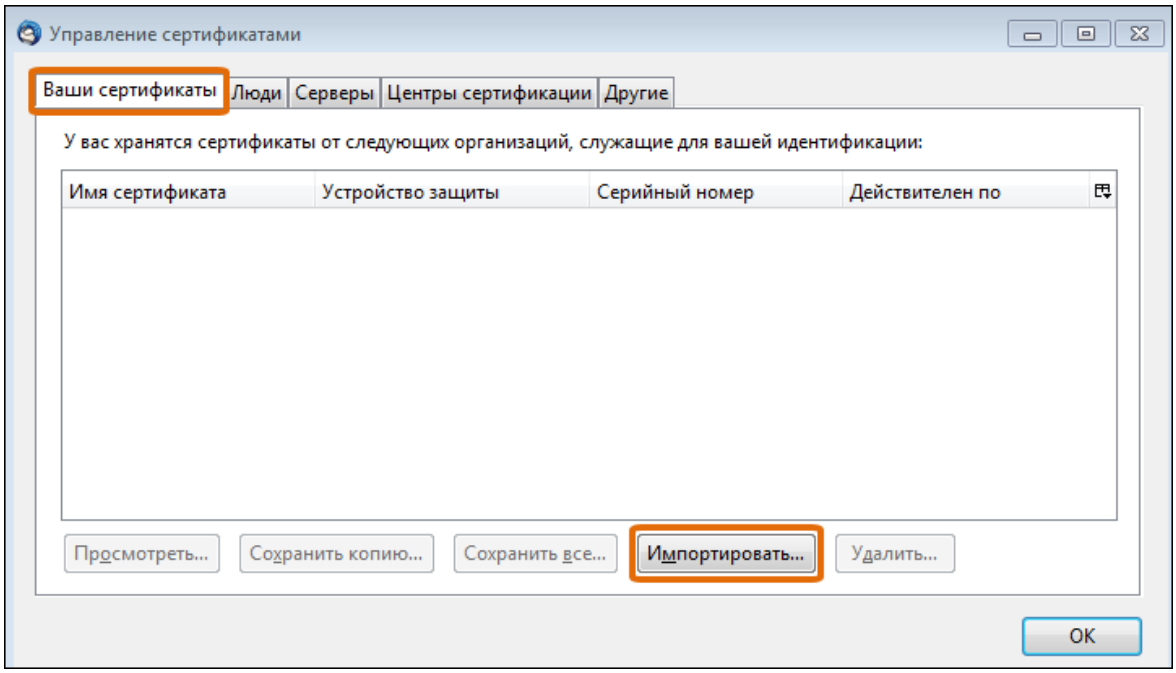


Рис. 9.15. Окно менеджера сертификатов

7. В окне **Управление сертификатами** перейти на вкладку **Ваши сертификаты**, нажать кнопку **Импортировать** и в открывшемся окне Проводника найти на жестком диске компьютера файл с сертификатом в формате **.p12**, созданный ранее. Выбрав файл, нажать кнопку **Открыть**:

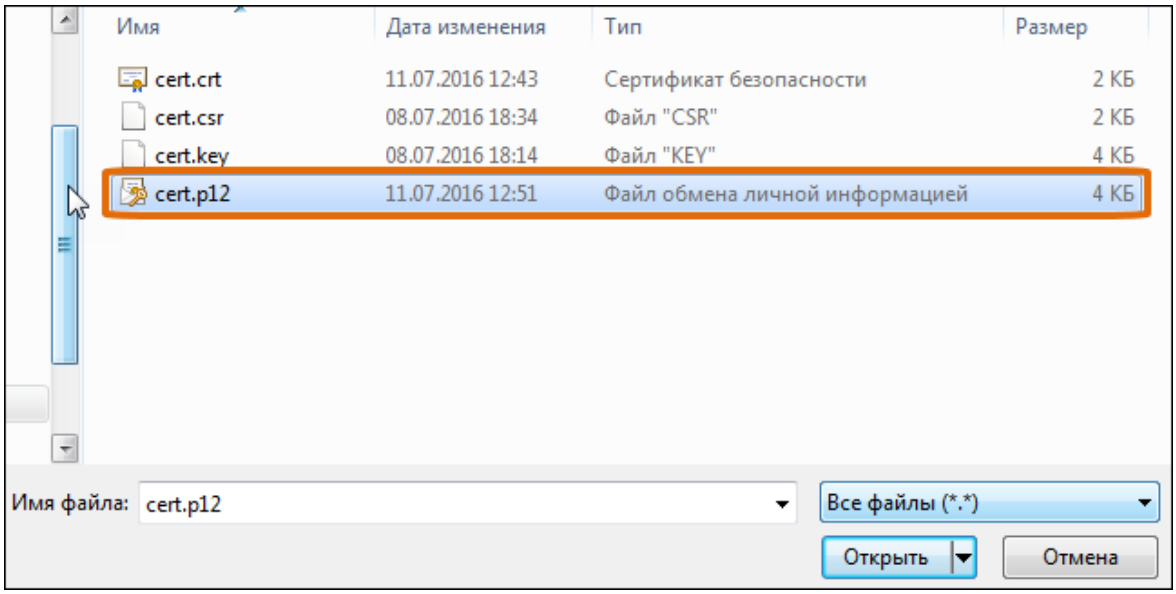


Рис. 9.16. Выбор файла сертификата

8. Для подтверждения импорта файла сертификата ввести мастер-пароль и нажать кнопку **ОК** (см. Рис.9.17):

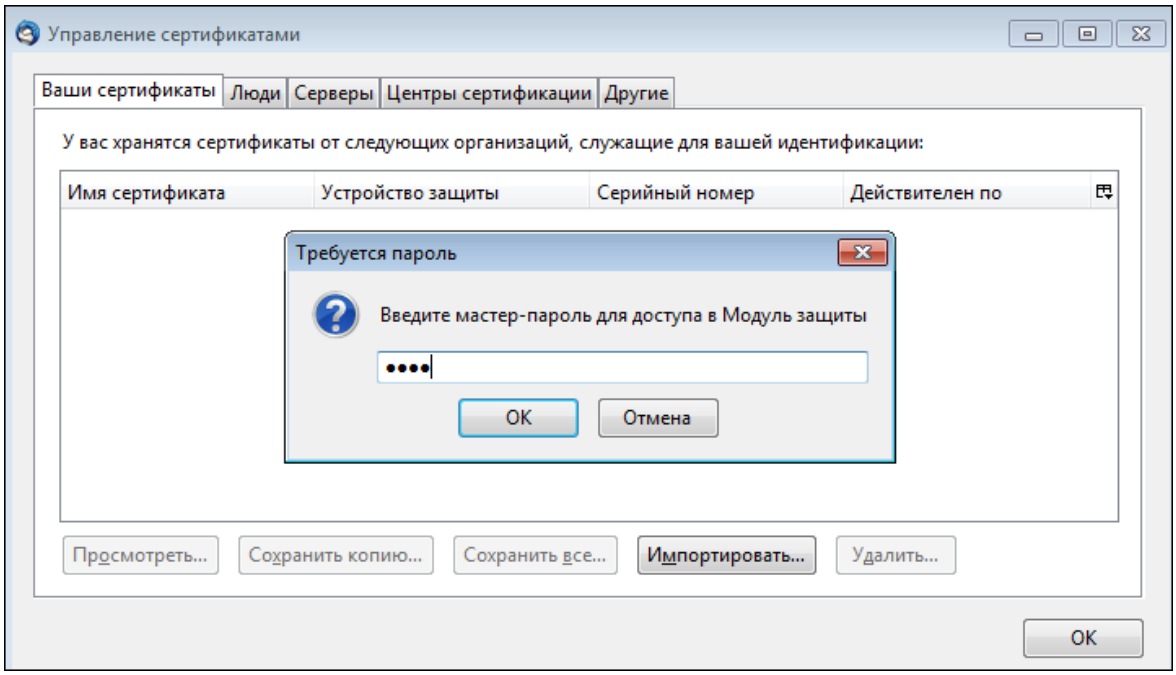


Рис. 9.17. Ввод мастер-пароля

9. Далее в окне **Ввод пароля** (см. Рис.9.18) указать пароль для экспорта, заданный на шаге 6 в процессе генерации сертификата. Нажать кнопку **ОК**:

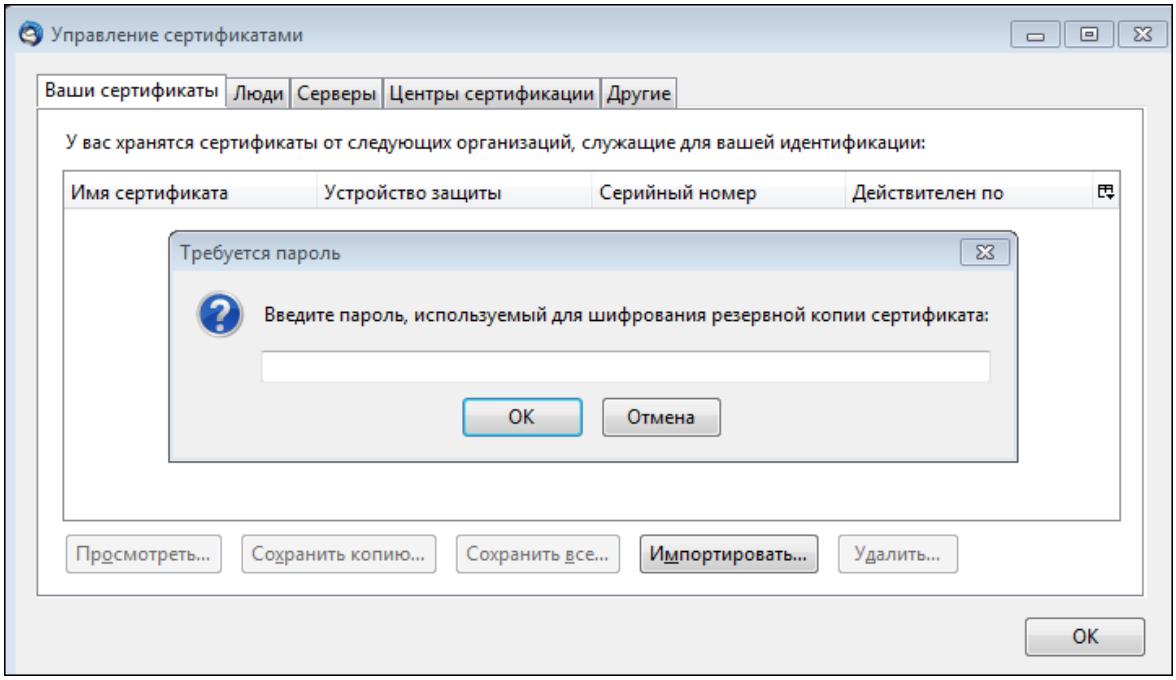


Рис. 9.18. Ввод пароля для экспорта сертификата

10. В открывшемся окне с сообщением об успешном завершении операции нажать кнопку **ОК**.

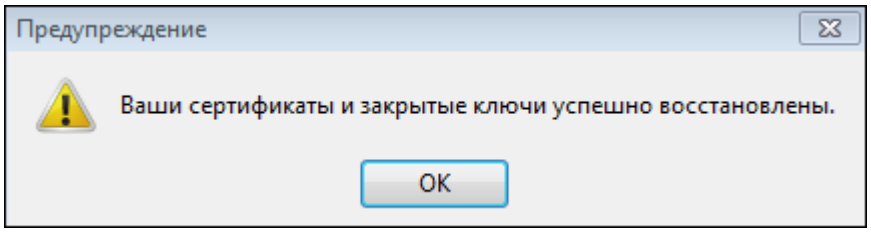


Рис. 9.19. Сообщение об успешном завершении операции

11. В окне **Управление сертификатами** будет добавлена запись с сертификатом пользователя (см. Рис.9.20). Нажать кнопку **ОК**:

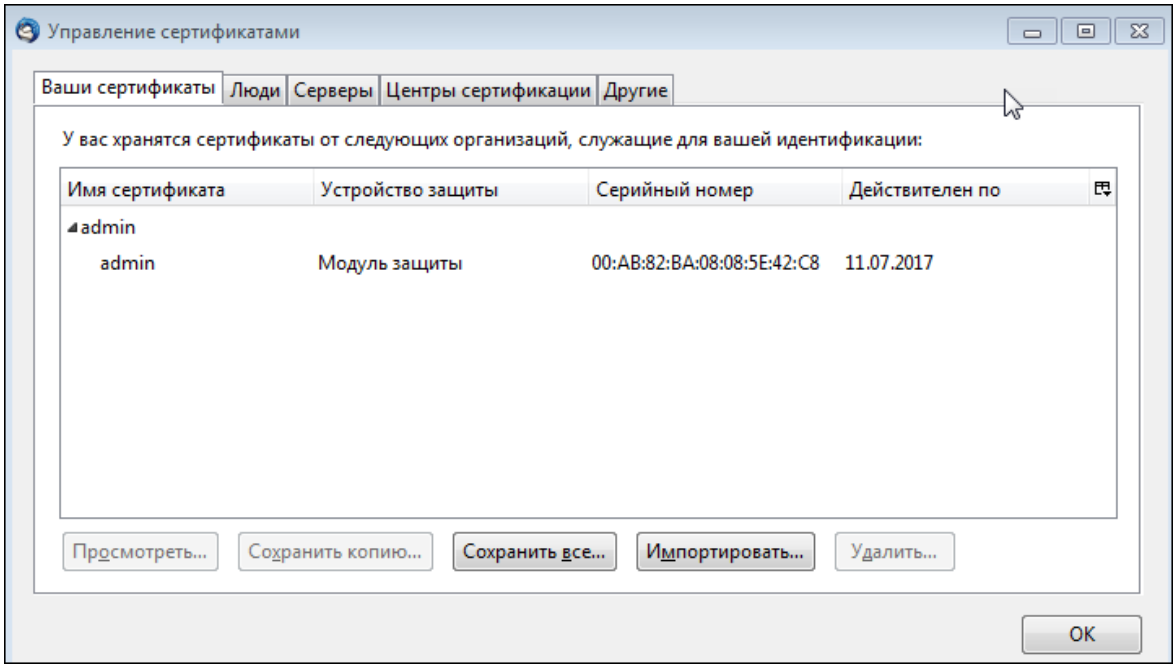


Рис. 9.20. Импортированный сертификат пользователя

12 В окне **Параметры учетной записи > Защита** (см. Рис.9.11) в разделе **Цифровая подпись** нажать кнопку **Выбрать**. В открывшемся окне **Выбор сертификата** (Рис.9.21) в раскрывающемся списке **Сертификат** выбрать импортированный ранее сертификат. В поле **Подробности о выбранном сертификате** необходимо проверить данные сертификата: главное, чтобы в качестве значения **Кому выдан** был указан правильный адрес электронной почты. Для подтверждения выбора сертификата нажать кнопку **ОК**:

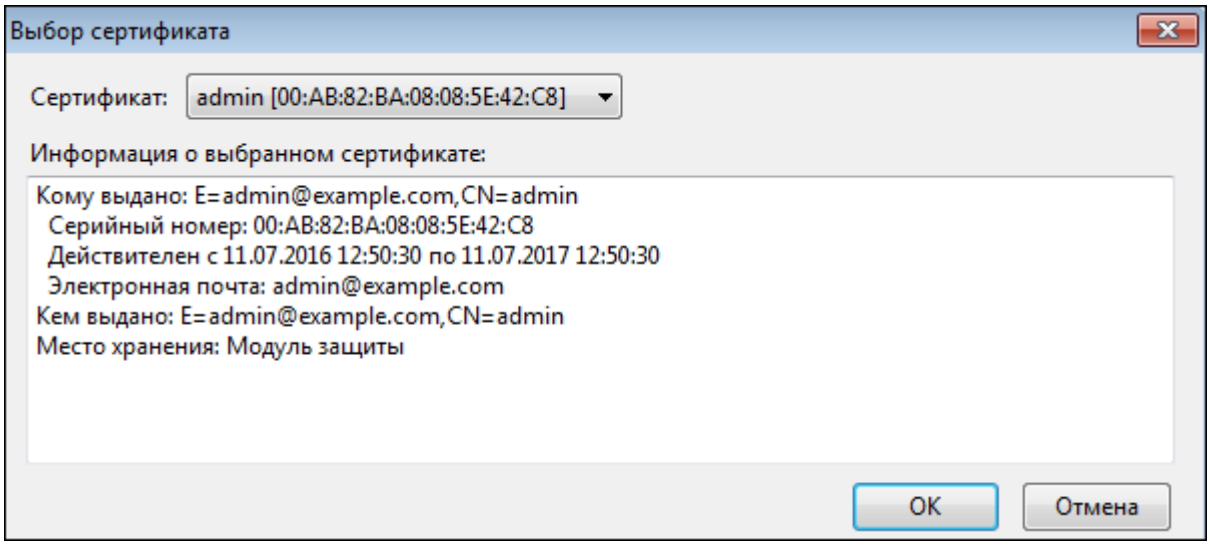


Рис. 9.21. Выбор сертификата для шифрования почтовых сообщений

13. В открывшемся окне с предложением использовать один и тот же сертификат как для шифрования, так и для расшифровки сообщений нажать кнопку **Да** (Рис.9.22).

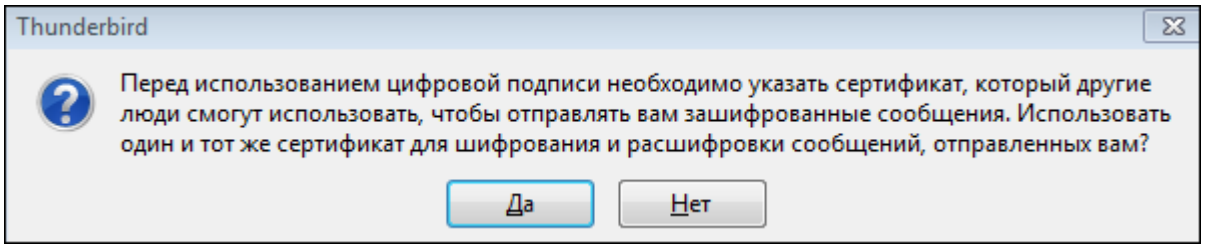


Рис. 9.22. Выбор сертификата для шифрования почтовых сообщений

14. В окне **Параметры учетной записи** будет указан выбранный сертификат для цифровой подписи и шифрования сообщений (Рис.9.23). Теперь появилась возможность получать сообщения, зашифрованные ключом, соответствующим импортированному сертификату. При этом для отправляемых сообщений шифрование по умолчанию не используется. При необходимости можно установить флажки, чтобы шифровать отправляемые сообщения или вставлять в сообщения цифровую подпись. Закрыть окно **Параметры учетной записи**, нажав кнопку **ОК**:

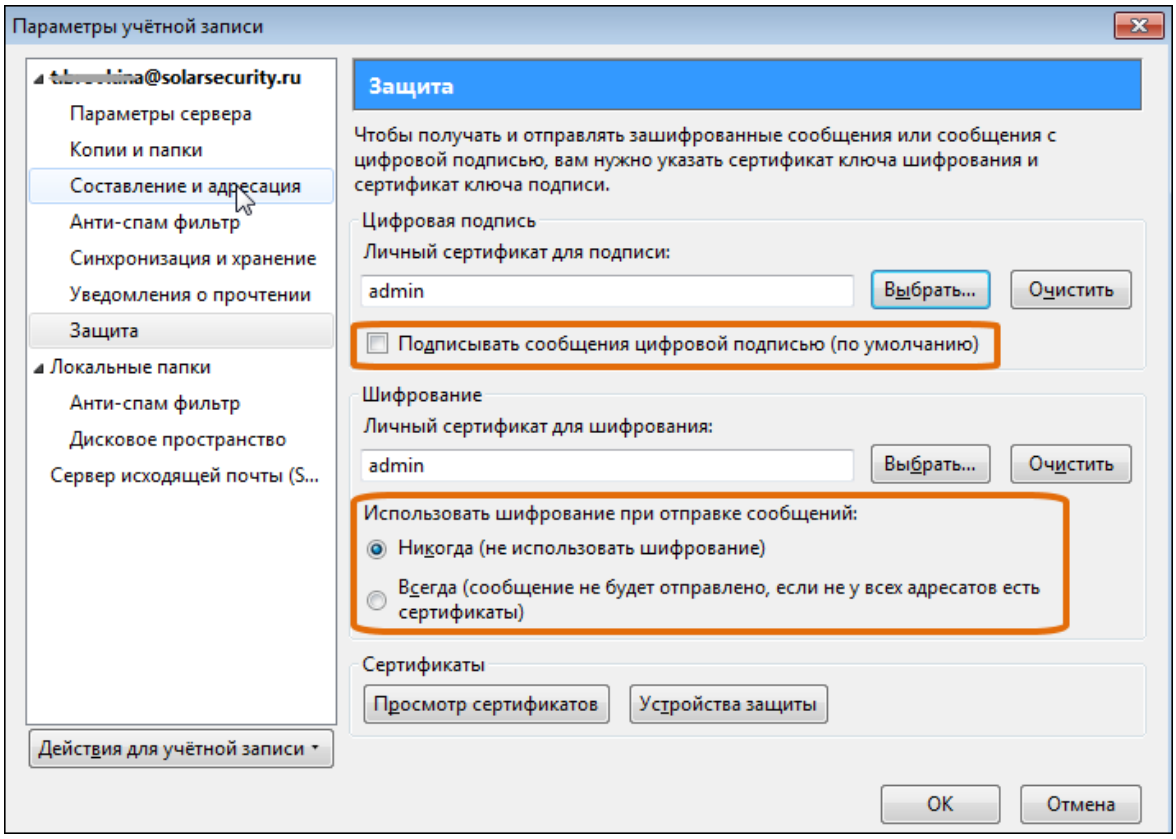


Рис. 9.23. Завершение настройки личных сертификатов

10. Настройка системы подтверждения отправки сообщений

Система подтверждения отправки сообщений даёт возможность отправителю подтвердить или отменить отправку сообщения, задержанного на почтовом фильтре в соответствии с политикой безопасности Solar Dozor.

Операции по подтверждению или отмене отправки сообщения регистрируются в журнальном файле **/opt/dozor/smap/log/confirm.log**. Также регистрируются попытки неавторизованного доступа к сообщениям.

Просмотр и подтверждение/отмена отправки сообщения разрешается пользователю, если почтовый ящик в SMTP-заголовке MAIL FROM совпадает с именем пользователя, а домен в SMTP-заголовке MAIL FROM совпадает со значением параметра **Локальный почтовый домен** в файле конфигурации.

Работоспособность системы не зависит от механизма аутентификации пользователя, так как на веб-сервере используется подключаемый модуль аутентификации, что позволяет подключать различные схемы аутентификации без модификации системы.

10.1. Настройка аутентификации пользователей

Система подтверждения отправки сообщений позволяет настроить аутентификацию пользователей через LDAP или PAM (Pluggable Authentication Modules, подключаемый модуль аутентификации). Рекомендуется использовать LDAP-аутентификацию.

10.1.1. Настройка LDAP-аутентификации пользователей

В интерфейсе системы подтверждения отправки пользователю необходимо ввести имя учётной записи и пароль. Вид учётной записи зависит от используемой схемы LDAP. В общем случае он содержит имя пользователя и домен в виде **user@domain**. В случае использования AD имя учётной записи указывается пользователем в виде **netbios-domain\user** или **domain\user**. На основе учётной записи по определенным правилам строится **Bind DN**. В конфигурации **Bind DN** указывается в виде шаблона с подстановочными параметрами:

- **%l** – полное имя учётной записи пользователя: **user@domain**
- **%u** – имя пользователя: **user**
- **%d** – домен пользователя: **domain**
- **%c** – домен, разбитый на уровни. При этом для каждого уровня повторяется подстрока от предшествующей запятой до **%c**. То есть если домен имеет вид **xxx.yyy.ru**, то **dc=%c** заменяется на **dc=xxx, dc=yyy, dc=ru**. Например, шаблон **cn=%l, dc=%c** для **user@example.solarsecurity.ru** заменяется на **cn=user@example.solarsecurity.ru, dc=example, dc=solarsecurity, dc=ru**.

Примеры Bind DN: **AD, CGP: %l**; **OpenLDAP: uid=%u, dc=%c**.

Поиск учетной записи пользователя ведется по атрибуту, имя и значение для которого указываются в конфигурации. Например:

- для AD: имя **sAMAccountName**, значение **%u** или имя **userPrincipalName**, значение **%l**;
- для CGP: имя **uid**, значение **%u** или имя **mail**, значение **%l**.

Из найденной записи автоматически извлекаются все атрибуты, содержащие email-адреса (при этом таких атрибутов в записи может быть несколько и в каждом атрибуте может содержаться несколько адресов). Имея полный список email-адресов пользователя, можно получить список всех сообщений этого пользователя, ожидающих подтверждения отправки.

Для настройки LDAP-аутентификации пользователей необходимо перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Администрирование системы > Вспомогательные сервисы** и в секции **Модуль подтверждения отправки** определить значения следующих параметров (**Рис.10.1**) :

Локальный почтовый домен	Локальный почтовый домен.
Список ldap-Серверов ldap://host:port	Список LDAP-серверов (каждый сервер должен быть указан в формате **ldap://host:port**). Могут быть указаны адреса основного и резервного (на случай недоступности основного) серверов. Адреса серверов указываются через пробел.
Шаблон bind-dn	Шаблон bind-dn: строка, в которой последовательности **%l**, **%u**, **%d** заменяются на значения **user@domain**, **user** и **domain** соответственно.
Шаблон base-dn	Шаблон base-dn: строка, в которой последовательности **%l**, **%u**, **%d** заменяются на значения **user@domain**, **user** и **domain** соответственно.
Шаблон фильтра	Шаблон фильтра для поиска объектов в LDAP, из которых извлекаются данные о почтовых адресах.
Атрибуты с адресами	Атрибуты записи, в которых содержатся email-адреса. Список атрибутов указывается через пробел. Например: **mail proxyAddresses**.
Глубина поиска в LDAP	Глубина поиска в LDAP.
Опции LDAP	Дополнительные опции LDAP. Например, версия протокола LDAP (рекомендуется указать **version=3**).
Таблица трансляции доменов NETBIOS	Таблица трансляции доменов NETBIOS (таблица соответствия имен доменов для AD). Указывается список пар через пробел. Например: **NETBIOS1=FQDN1 NETBIOS2=FQDN2**.
Вывод отладочной информации	Включение отладочного режима журналирования сообщений системы подтверждения отправки. Если флажок **Вывод отладочной информации** снят, то в журнал записываются только сообщения о действиях пользователей и событиях, связанных с безопасностью. Например: Message ... confirmed by user Message ... canEntryed by user Access to message ... denied for user Authentication for user ... failed User ... logged User ... logged out.

	Если флажок **Вывод отладочной информации** установлен, то, помимо сообщений о действиях пользователя и событиях, связанных с безопасностью, в журнал записываются сообщения о свойствах найденных объектов (к объектам относятся, например, списки адресов), параметрах сформированного запроса в LDAP и состоянии сессии. Формат этих сообщений может меняться в зависимости от версии Solar Dozor.
Почтовый домен для вывода в окне авторизации	Почтовый домен для вывода в окне авторизации.

Примечание

*В случае LDAP-аутентификации значение параметра **Локальный почтовый домен** (локальный почтовый домен, пользователям которого разрешено подтверждать отправку сообщений) не задается.*

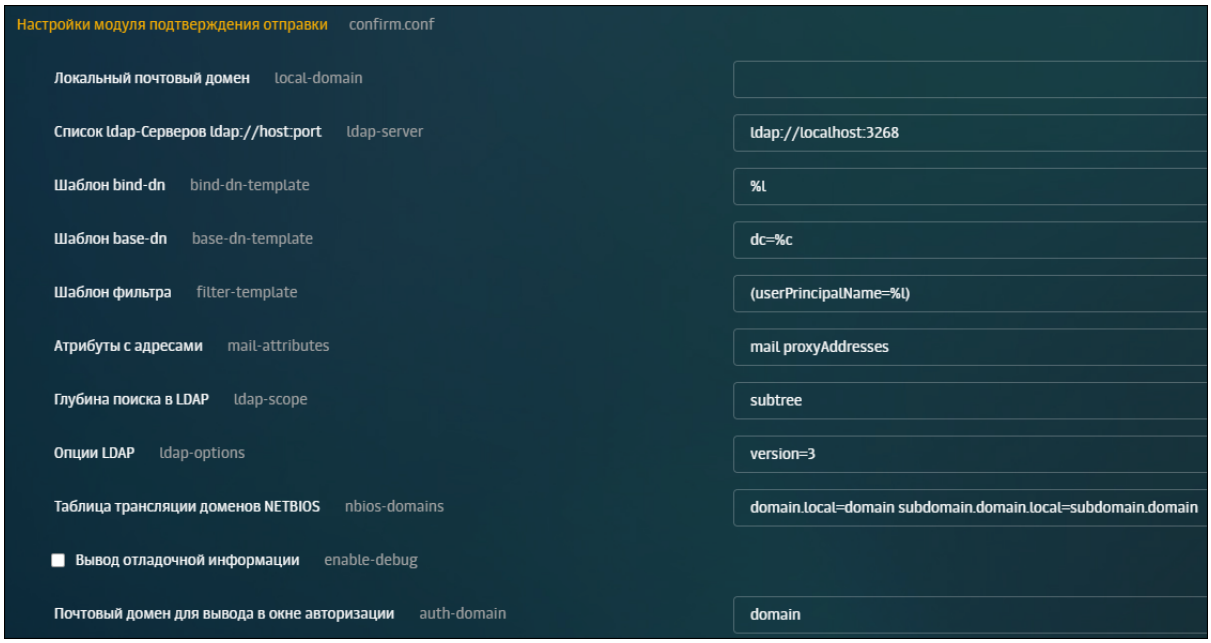


Рис. 10.1. Настройки модуля подтверждения отправки сообщений

После изменения параметров конфигурации необходимо нажать кнопки **Сохранить** и **Применить**.

Далее приведены примеры настроек LDAP-аутентификации для различных случаев (приведенные примеры являются работоспособными для определенной конфигурации сети, оптимальная же настройка в каждом конкретном случае выполняется администратором в соответствии с сетевой инфраструктурой):

1. Домен LDAP

```
local-domain = ""
auth-type = "ldap"
ldap-server = "ldap://10.31.6.105:389"
bind-dn-template = "cn=%u,dc=%c"
```

```
base-dn-template = "dc=domain,dc=ru"
filter-template = "(cn=%u)"
mail-attributes = "mail"
ldap-scope = "subtree"
ldap-options = "version=3"
nbios-domains = "domain=domain.ru"
```

В параметре **Список ldap-Серверов ldap://host:port** указывается IP адрес или имя узла, на котором развернут сервер LDAP.

2. Домен AD

```
local-domain = ""
auth-type = "ldap"
ldap-server = "ldap://10.31.7.16:389"
bind-dn-template = "%l"
base-dn-template = "dc=domain,dc=local"
filter-template ="(userPrincipalName=%l)"
mail-attributes = "mail proxyAddresses"
ldap-scope = "subtree"
ldap-options = "version=3"
nbios-domains = "domain=domain.local"
```

В параметре **Список ldap-Серверов ldap://host:port** указывается IP адрес или имя узла, являющегося контроллером домена.

3. Домен AD с дочерним доменом

```
local-domain = ""
auth-type = "ldap"
ldap-server = "ldap://10.31.5.113:3268"
bind-dn-template = "%l"
base-dn-template = "dc=domain,dc=local"
filter-template = "(userPrincipalName=%l)"
mail-attributes = "mail proxyAddresses"
ldap-scope = "subtree"
ldap-options = "version=3"
nbios-domains = "domain=domain.local subdomain.domain=subdomain.domain.local"
```

В параметре **Список ldap-Серверов ldap://host:port** указывается IP адрес или имя узла, на котором развернут глобальный каталог (включая порт глобального каталога – 3268).

4. Пример настроек для работы модуля подтверждения отправки с CommuniGatePro (CGP)

```
local-domain = ""
auth-type = "ldap"
ldap-server = "ldap://vm40.solar.local:389"
bind-dn-template = "%l"
base-dn-template = "cn=%d"
filter-template = "(uid=%u)"
mail-attributes = "mail"
ldap-scope = "subtree"
ldap-options = "version=3"
nbios-domains = "vm40=vm40.solar.local"
```

В параметре **Список ldap-Серверов ldap://host:port** указывается IP адрес или имя узла, на котором развернут CommuniGatePro.

10.2. Проверка работоспособности подсистемы подтверждения отправки сообщений

Пример: необходимо выявлять случаи отправки сообщений, например, со словом **Приказ** в теме на адреса, которые не входят в группу легитимных получателей подобных сообщений.

Для выявления таких случаев следует:

1. Идентифицировать в потоке сообщений файлы, содержащие в теме слово **Приказ**.
2. Определить, входит ли получатель такого сообщения в группу легитимных получателей сообщений, содержащих приказы.
3. В том случае, если получатель сообщения, содержащего слово **Приказ** в теме сообщения, не входит в группу легитимных получателей, поместить это сообщение в архив с пометкой **Ожидается подтверждение отправки** и отправить автору сообщения уведомление (используя заранее созданный шаблон уведомления) о возможном нарушении политики безопасности с запросом на подтверждение отправки сообщения или на ее отмену.

Чтобы реализовать вышеуказанное, необходимо в интерфейсе Solar Dozor выполнить следующие действия:

1. В меню действий с разделом GUI **Политика > Шаблоны и профили > Шаблоны уведомлений** выбрать пункт **Добавить** (Рис.10.2).
2. В открывшемся окне ввести название шаблона уведомления и нажать кнопку **Сохранить** (Рис.10.2).

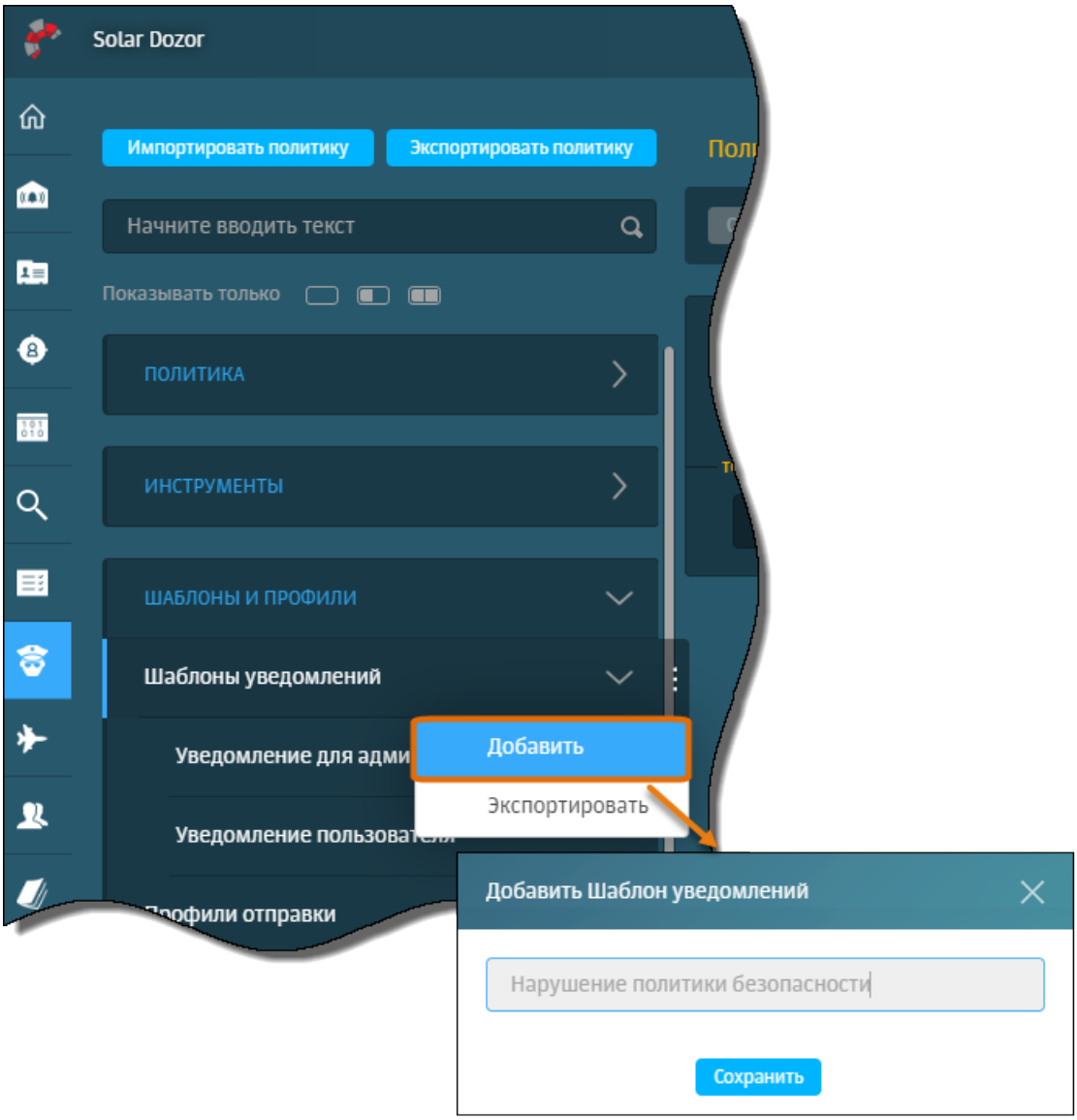


Рис. 10.2. Создание шаблона уведомления «Нарушение политики безопасности»

3. В правой части экрана ввести следующие значения полей (Рис.10.3):
   - **От** – адрес администратора.
   - **Кому** – адрес отправителя.
   - **Тема** – например, **Нарушение политики безопасности**.
   - **Название заголовка** – например, **subject**.
   - **Значение заголовка** – например, **Приказ**.
   - **Текст сообщения** – шаблон сообщения, в котором должна содержаться ссылка на интерфейс подтверждения отправки (URL интерфейса подтверждения).
4. Нажать кнопку **Сохранить**.

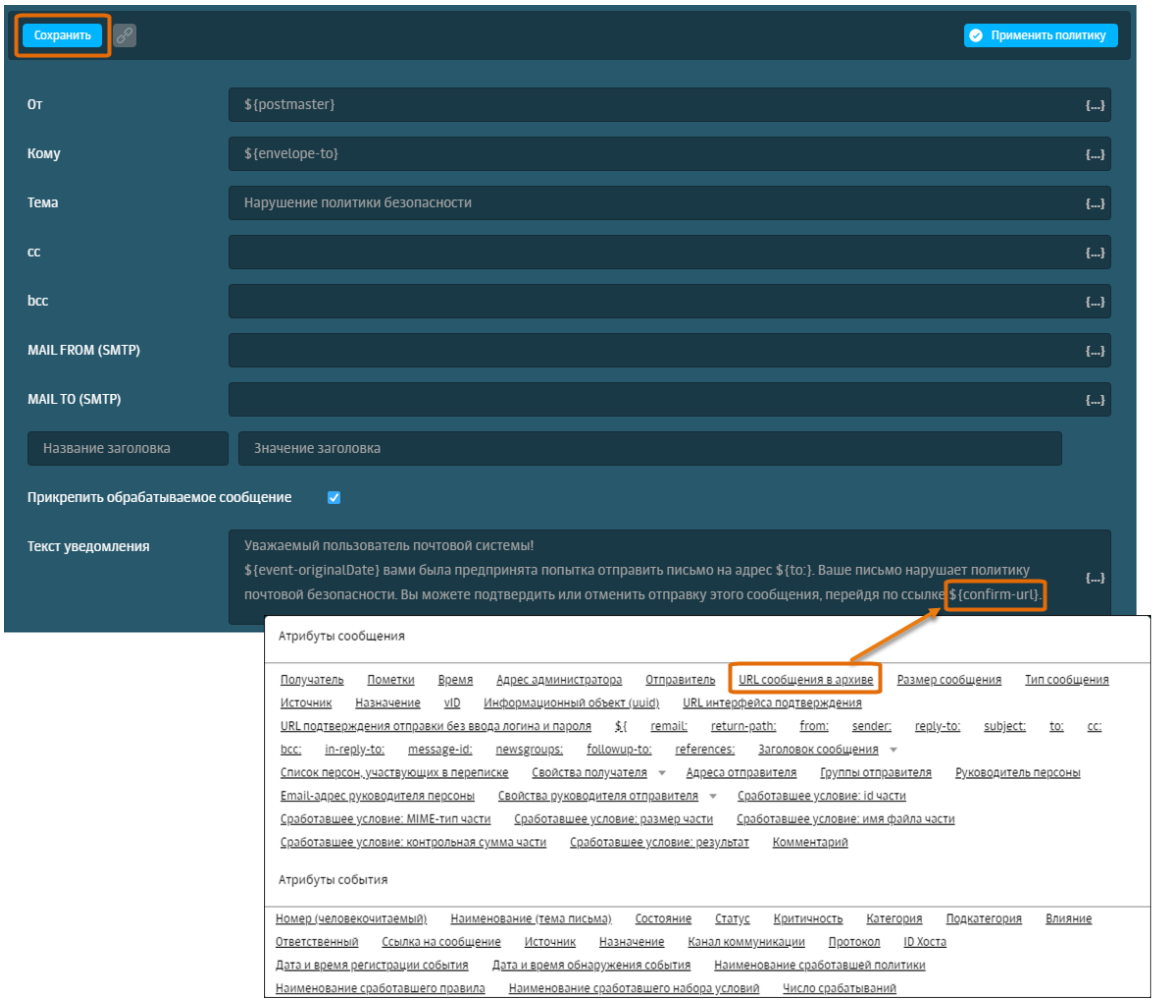


Рис. 10.3. Заполнение полей шаблона уведомления «Нарушение политики безопасности»

5. В меню действий с разделом GUI **Политика > Политика > Условия** выбрать пункт **Добавить** (Рис.10.4).

6. В открывшемся окне ввести название условия и нажать кнопку **Сохранить** (Рис.10.4).

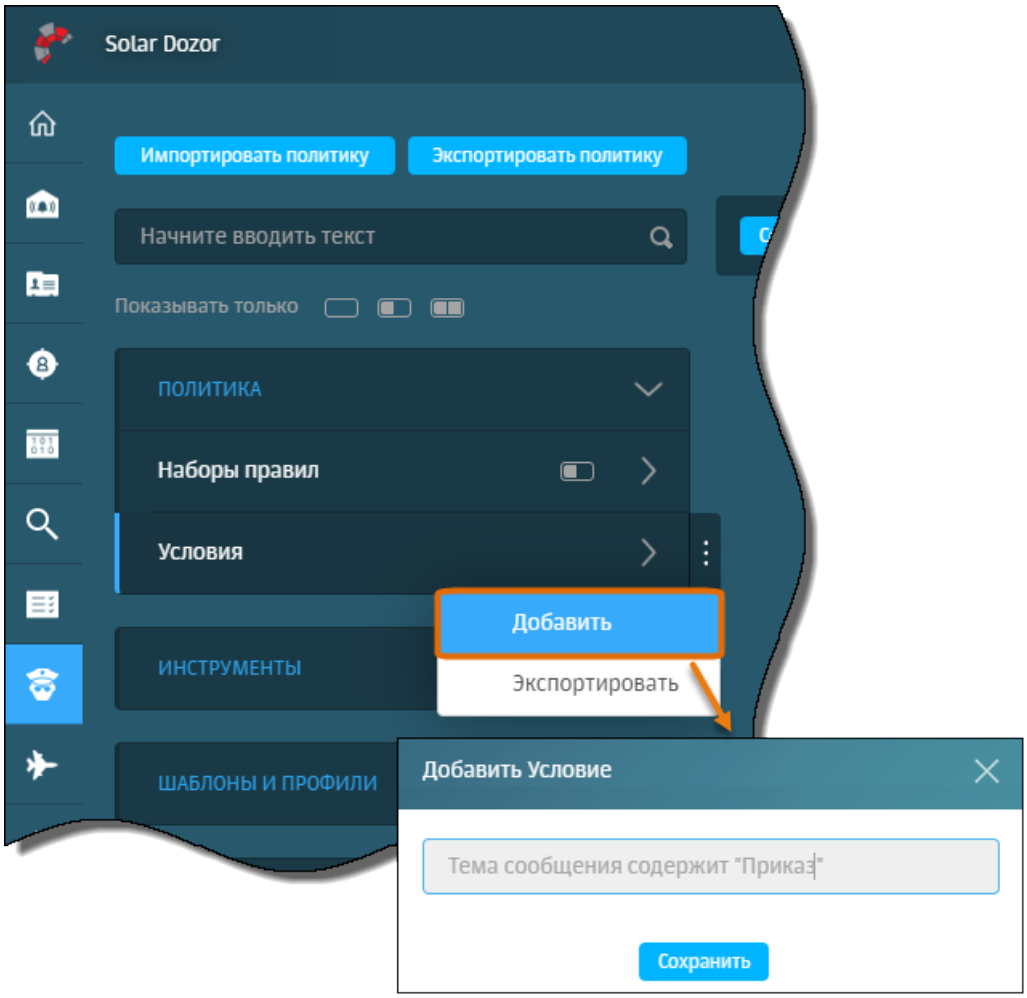


Рис. 10.4. Создание условия

7. В правой части экрана указать (выбрать из раскрывающихся списков) следующие элементы первого условия (Рис.10.5):
   - ***Заголовок**
   - **subject**
   - **Содержит**
   - **Приказ**
8. Нажать кнопку **Добавить условие** и указать следующие элементы второго условия (Рис.10.5):
   - **Получатель**
   - **Содержит**
   - **user2@company.ru**
9. Нажать кнопку **Сохранить** (Рис.10.5).

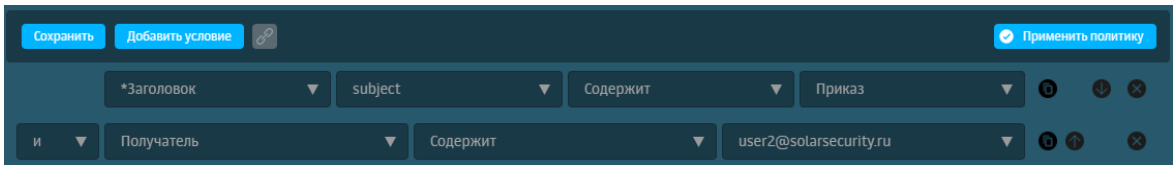


Рис. 10.5. Настройка условия

10. В меню действий с разделом GUI **Политика > Политика > Наборы правил** выбрать пункт **Добавить** (Рис.10.6).

11. В открывшемся окне ввести название набора правил (например, **Уведомление пользователей**) и нажать кнопку **Сохранить** (Рис.10.6).

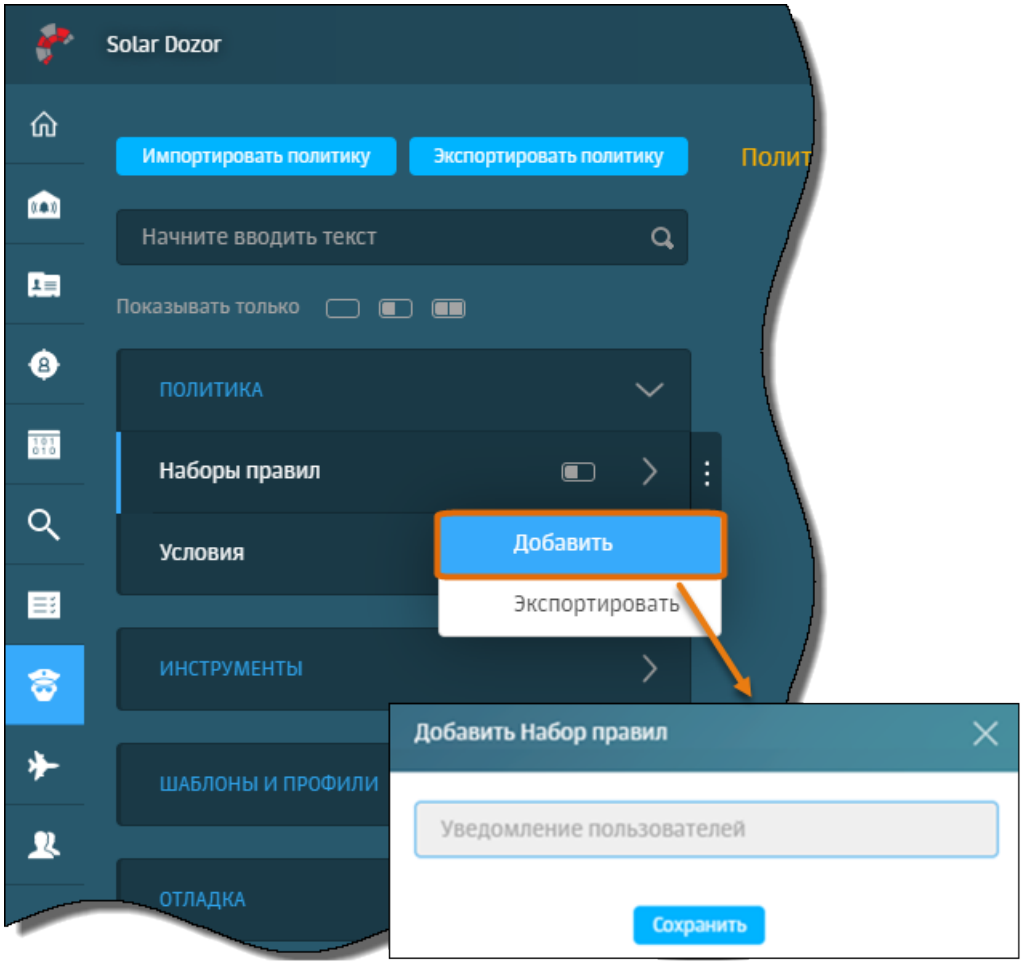


Рис. 10.6. Создание набора правил «Уведомление пользователей»

12. В правой части экрана указать элементы правила (Рис.10.7):

- Название правила: **Уведомление пользователей**
- Если: **Тема сообщения содержит «Приказ»**
- то: **Отправить с подтверждением** / **Профиль1** / **Выполнить**

И

Отправить уведомление / Нарушение политики безопасности / Профиль1 / Выполнить

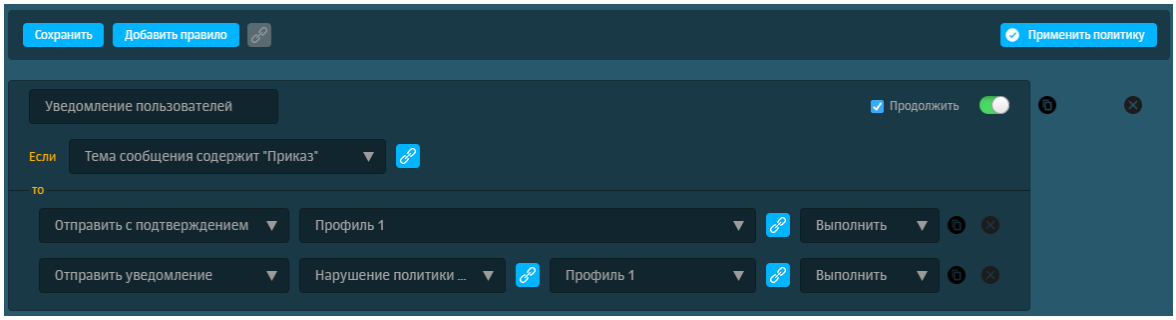
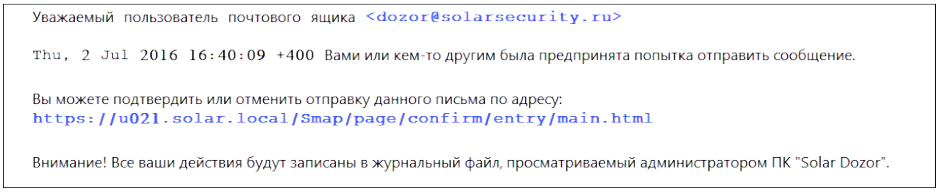


Рис. 10.7. Настройка набора правил «Уведомление пользователей»

13. Нажать кнопки **Сохранить** и **Применить политику**.

14. Отправить через Solar Dozor на соответствующий адрес несколько сообщений с указанием слова **Приказ** в теме каждого сообщения. После отправки каждого сообщения на адрес, с которого отправлялись сообщения, должно прийти уведомление о нарушении политики безопасности, шаблон которого был сформирован ранее. Уведомление имеет следующий вид (Рис.10.8):


Уважаемый пользователь почтового ящика <dozor@solarsecurity.ru>

Thu, 2 Jul 2016 16:40:09 +400 Вами или кем-то другим была предпринята попытка отправить сообщение.

Вы можете подтвердить или отменить отправку данного письма по адресу:
https://u021.solar.local/Smap/page/confirm/entry/main.html

Внимание! Все ваши действия будут записаны в журнальный файл, просматриваемый администратором ПК "Solar Dozor".

Рис. 10.8. Уведомление о нарушении политики безопасности

15. Перейти по ссылке, указанной в уведомлении, в появившемся диалоговом окне аутентификации ввести имя пользователя и пароль своей учетной записи в БД, используемой PAM. После входа в интерфейс подтверждения отправки сообщений на экране появится таблица с данными о сообщениях, ожидающих подтверждения отправки (Рис.10.9).

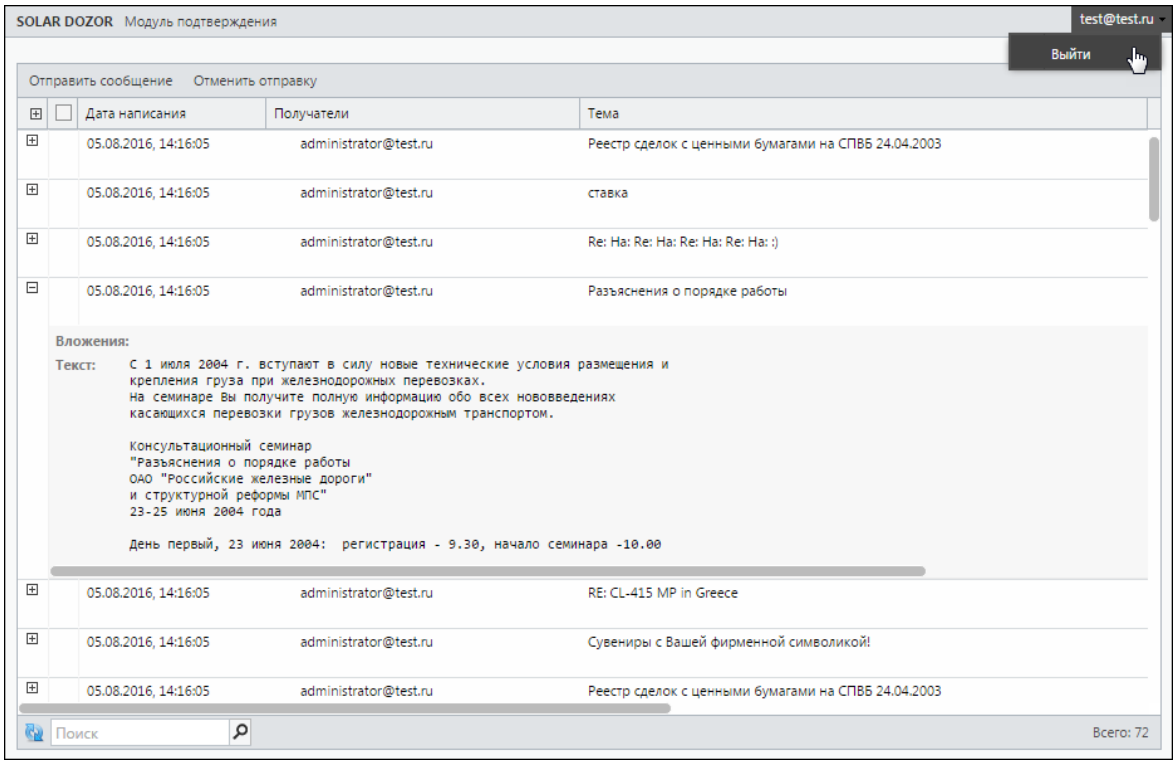


Рис. 10.9. Таблица с данными сообщений, ожидающих подтверждения отправки

16. Выбрать несколько сообщений, установив флажок в соответствующих строках таблицы, и выполнить действие **Отправить сообщение** или **Отменить отправку**. Убедиться, что данные сообщений, к которым были применены эти действия, не отображаются в таблице.

17. Выйти из интерфейса подтверждения отправки.

18. В разделе **Поиск** выполнить запрос на просмотр всех сообщений. Убедиться, что в архиве находятся сообщения с пометками, соответствующими действиям **Отправка сообщения подтверждена** и **Отправка сообщения отменена**, которые были выполнены над этими сообщениями.

11. Установка модуля OCR

Модуль OCR предназначен для распознавания текста изображений, пересылаемых в сообщениях электронной почты. В Solar Dozor поддерживаются два движка системы распознавания текста изображений: ContentReader Engine и Tesseract.

Перед установкой и настройкой какого-либо движка необходимо проверить настройку семафоров. Для этого на каждом узле Solar Dozor следует выполнить следующие действия:

1. Выполнить следующую команду:

   # cat /etc/sysctl.conf

2. Если в выводе файла **/etc/sysctl.conf** будут отсутствовать следующие строки, то их необходимо добавить в конец этого файла:

```
kernel.msgmni = 1024
kernel.sem = 250 256000 32 1024
```

Библиотеки распознавания текстов изображений Tesseract и пакеты ContentReader Engine поставляются вместе с Solar Dozor и не нуждаются в установке. Для настройки необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Работа системы** и в секции **Сервис распознавания текста изображений** для параметра **Используемый движок** выбрать значение **Tesseract** или **ContentReader Engine 12**.

2. Перейти в раздел **Расширенные настройки > Обработка сообщений** и в секции **Сервис фильтрации сообщений** установить флажок **Использовать OCR**.

3. Нажать **Сохранить** и **Применить**.

4. Назначить роль **Распознавание текста изображений** всем узлам, ресурсами которых предполагается осуществлять распознавание текстов изображений (см. раздел 8.2).

Описание работы с модулем приведено в документе *Руководство по работе с модулем OCR*.

12. Установка модуля Dozor File Crawler

Модуль Dozor File Crawler устанавливается в процессе установки Solar Dozor.

После установки необходимо назначить роль **Сервер управления Краулером** одному узлу, и роль **Краулер: файловые ресурсы и IMAP** всем узлам, на которых планируется использование краулера. Для этого следует открыть в GUI Solar Dozor раздел **Система**, перейти на вкладку **Узлы и роли** и выбрать соответствующий пункт в списке для нужных узлов.

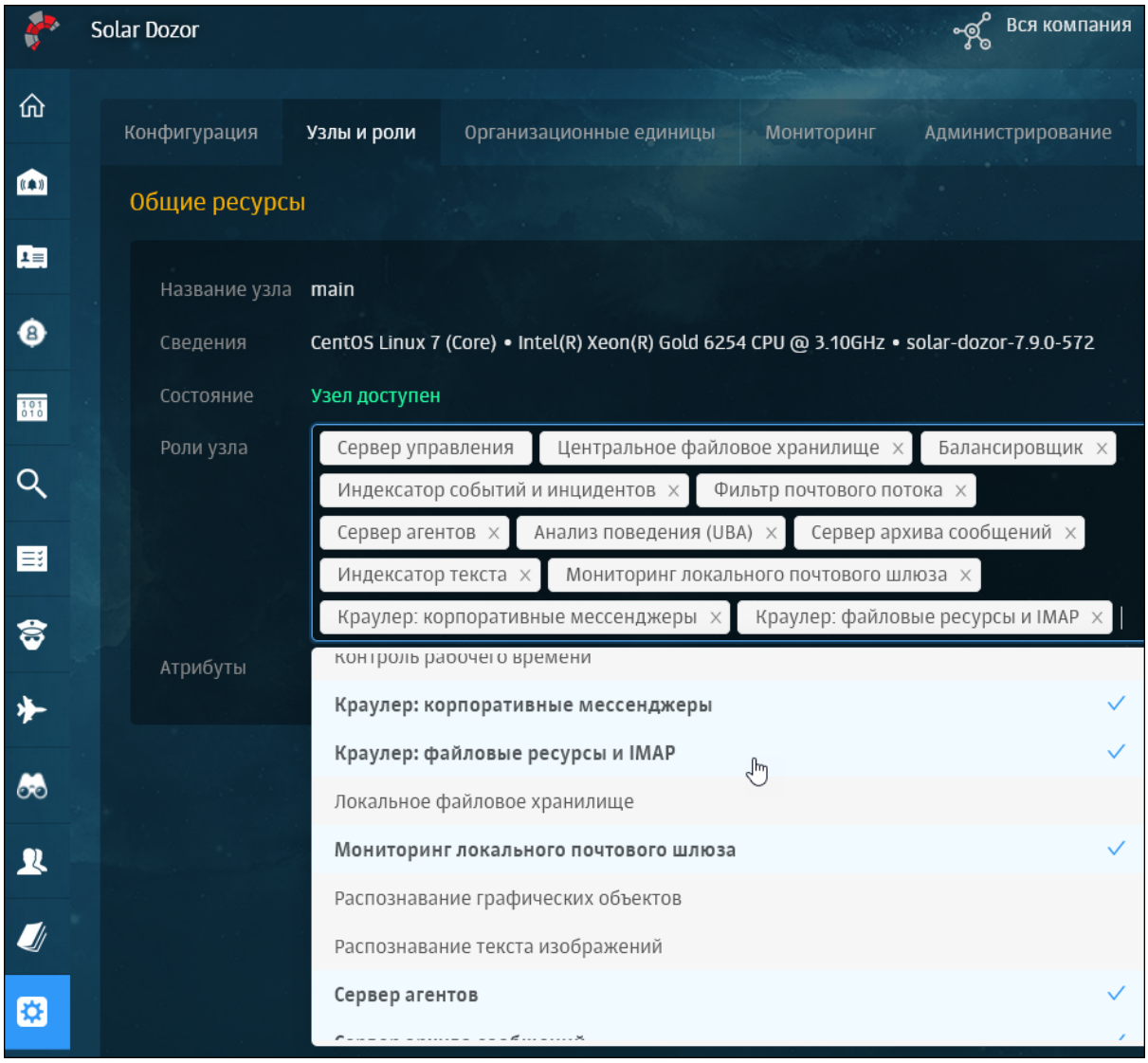


Рис. 12.1. Назначение узлу роли Краулер

После назначения узлу роли **Сервер управления Краулером** следует явно указать IP-адреса узлов кластера Solar Dozor с ролью **Фильтр почтового потока**. Для этого следует выполнить действия:

1. Перейти в раздел настроек **Система > Конфигурация > Расширенные настройки > Настройка модулей перехвата > File Crawler**.

2. В секции **Сервис обработки данных File Crawler** переключить параметр **Настройки mailfilter** в значение **Задать вручную**.

3. Раскрыть список **Настройки mailfilter** и задать значения следующих параметров:

   - **Хост** – тип адреса (IP или FQDN) узла с ролью **Фильтр почтового потока**, ожидающего соединения. В зависимости от выбранного значения появляется подчиненный параметр **IP-адрес** или **Сетевой адрес**, в котором нужно указать соответствующее значение.

   - **Порт** – порт, на котором узел с ролью **Фильтр почтового потока** ожидает соединения.

4. Нажать **Сохранить**, **Применить**.

Управление модулем осуществляется с помощью разделов **File Crawler > Задачи** и **File Crawler > Карта сети** (Рис.12.2).

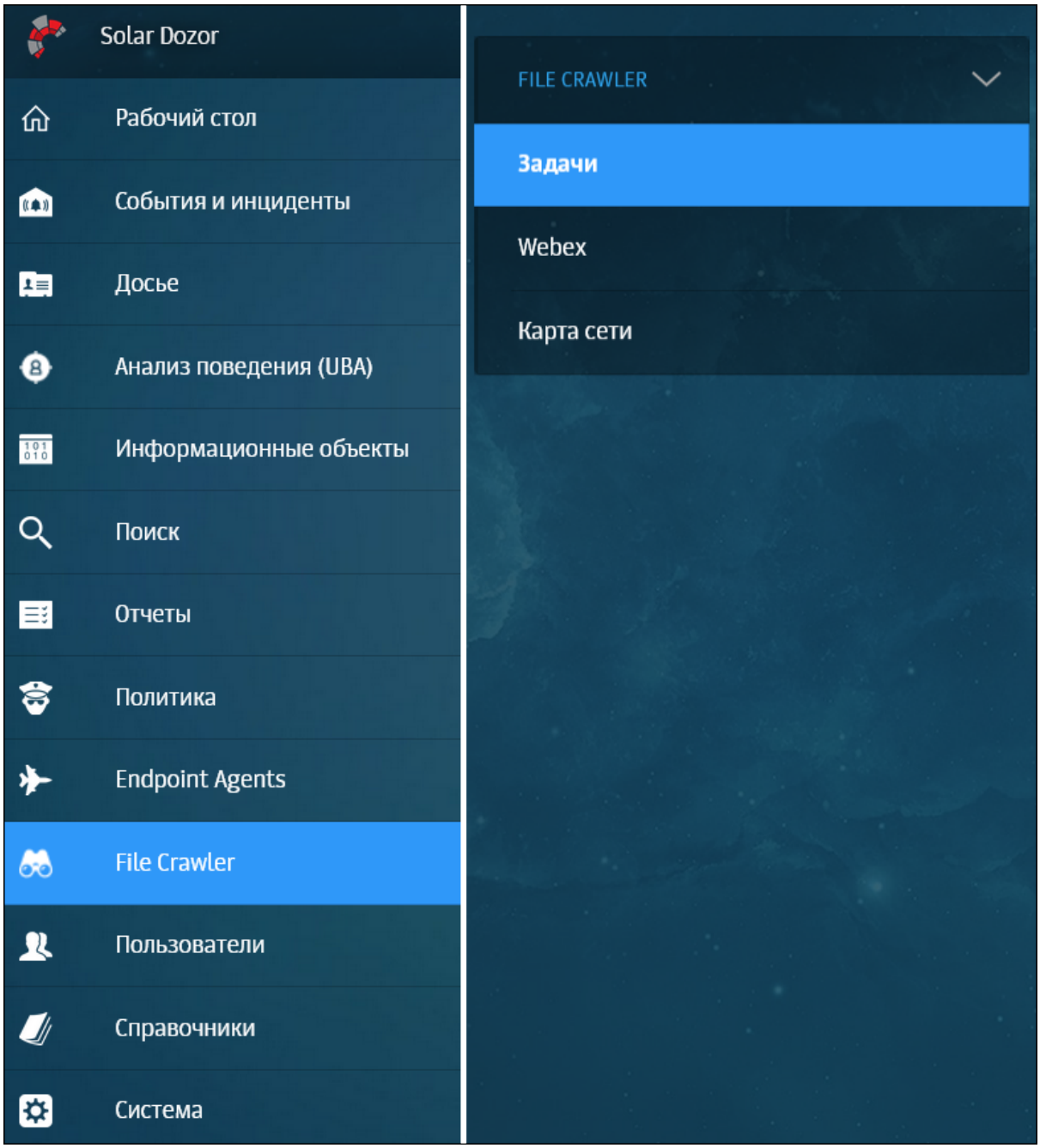


Рис. 12.2. Раздел File Crawler

Описание работы с модулем приведено в документе *Руководство по работе с модулем инвентаризации файловых хранилищ «Dozor File Crawler»*.

13. Установка модуля Traffic Analyzer

Дистрибутив Traffic Analyzer поставляется в составе дистрибутива Solar Dozor, и его установка выполняется в процессе установки Solar Dozor.

Дальнейшую настройку следует выполнять согласно документу *Модуль перехвата и анализа сетевого трафика «Traffic Analyzer». Руководство системного администратора*. После окончания настройки модуля следует перейти в GUI Solar Dozor и в разделе **Система > Узлы и роли** выбрать роль **Сервер перехвата и анализа сетевого трафика**.

14. Установка агентов

Процедура установки и настройки агентов подробна описана в следующих документах:

- *Модуль «Dozor Endpoint Agent». Руководство по установке и настройке*.
- *Модуль «Dozor Endpoint Agent». Руководство администратора*.

15. Настройка антивируса

В Solar Dozor имеется возможность использования антивируса, функционирующего на внешнем ICAP-сервере. Внешний антивирус используется для обнаружения и устранения вирусов, передаваемых по электронной почте и совершающих действия, результатом которых является частичная или полная потеря данных, остановка работы сотрудников, сбои в работе электронной почты и ПО, используемого в компании.

В ряде случаев исполняемый вредоносный или другой тип вложения сообщений может быть умышленно или случайно обфусцирован (замаскирован) под простой текст. Solar Dozor не учитывает всех возможных вариантов обфускации содержимого, поэтому для определения вредоносного содержимого рекомендуется использовать внешний антивирус.

15.1. Подключение Kaspersky

Для подключения внешнего антивируса Kaspersky необходимо выполнить следующие действия:

1. Перейти в раздел GUI **Система > Конфигурация > Расширенные настройки > Обработка сообщений** и в секции **Сервис фильтрации сообщений** в группе **Проверка сообщений с помощью антивируса** задать следующие параметры:
   - **Включить проверку с помощью антивируса** – установить флажок.
   - **Действие Антивируса** – **Сканировать**.
   - **Имя хоста** – IP-адрес ICAP-сервера антивируса Kaspersky.
   - **URL** – **/av/respmod**
   - **Порт** – 1344
2. Нажать **Сохранить** и **Применить**.
3. Перейти в CLI сервера антивируса Kaspersky, открыть для редактирования файл конфигурации **/etc/opt/kaspersky/kav4proxy.conf** и задать значения следующих параметров:
   - **AnswerMode=complete**
   - **SendAVScanResult=true**
   - **Timeout=60**
4. Сохранить и закрыть файл. Выполнить следующую команду:

   # systemctl restart kav4proxy.service

15.2. Использование локального антивируса

В Solar Dozor имеется возможность использования антивируса, установленного на одном из серверов кластера. Использование такой возможности **настоятельно не рекомендуется** ввиду непредсказуемых рисков и отрицательного влияния на производительность системы, однако не запрещается. При установке и настройке локального антивируса придерживайтесь следующих рекомендаций:

- Внести в исключения контроля антивирусом все каталоги с файлами, имеющими отношение к работе Solar Dozor, по умолчанию следующие:
  - **/data**
  - **/opt/dozor**
  - **/var/log/journal**
  - **/tmp**

  Более тонкая настройка исключений высылается по запросу в службу технической поддержки.

  Внимание!

  Антивирусная проверка каталогов с полученными сообщениями приводит к значительному замедлению работы фильтрации из-за многократных повторных проверок сохраняемых данных (тел сообщений и извлеченных данных) и блокировки доступа к файлам.

- Отключить контроль сетевых соединений и веб-трафика кластера Solar Dozor и межкомпонентного взаимодействия ПО Solar Dozor для модулей антивирусного ПО, выполняющих функции защиты от сетевых угроз.
- С осторожностью использовать модуль анализа поведения (**KESL Behavior_Detection** и аналогичные ему). При нарушениях работы сервисов Solar Dozor рекомендуется отключить использование такого модуля.

Не рекомендуется развертывать серверные компоненты других средств защиты информации на серверах Solar Dozor. Невыполнение рекомендаций может привести к значительному снижению производительности системы вплоть до полной её остановки, нарушениям работоспособности и потере данных.

Приложение А. Настройка проверки пароля пользователя для подключения к БД

Для повышения уровня безопасности можно включить принудительный ввод пароля пользователя **dozor** при подключении к следующим БД, использующимся в Solar Dozor:

- БД политики фильтрации.
- БД событий и инцидентов ИБ.
- БД модуля Dozor File Crawler.
- БД архива сообщений под управлением СУБД PostgreSQL.

Для этого необходимо выполнить следующие действия:

1. Подключиться по протоколу SSH к узлу, на котором функционирует выбранная БД:
   - БД политики фильтрации – master-узел.
   - БД событий и инцидентов ИБ, БД архива сообщений под управлением СУБД PostgreSQL – тот узел, на котором была создана схема этой БД. Это значение указано в параметре **Сетевое имя сервера базы данных** в разделе GUI **Система > Конфигурация > Основные настройки > Доступ к данным** в секции **Схемы соединений с БД** для соответствующей записи схемы соединения.
   - БД модуля Dozor File Crawler – все узлы, которым назначены роли **Сервер управления Краулером** и/или **Краулер: файловые ресурсы и IMAP**.
2. Подключиться к БД, выполнив следующую команду:

   # psql -U dozor -h localhost -p <port>

   где **<port>** – порт, на котором БД ожидает соединения:
   - БД политики фильтрации – 5434.
   - БД модуля Dozor File Crawler – порт по умолчанию 5439. Актуальное значение указано в параметре **Порт для сервиса БД Краулера** в разделе GUI **Система > Конфигурация > Расширенные настройки > File Crawler** в секции **Подключение к БД File Crawler**.
   - БД событий и инцидентов ИБ, БД архива сообщений под управлением СУБД PostgreSQL – значение порта указано в параметре **Сетевой порт сервера базы данных** в разделе GUI **Конфигурации > Основные настройки > Доступ к данным** в секции **Схемы соединений с БД** для соответствующей записи схемы соединения.
3. Задать новый пароль пользователя БД, выполнив команду:

   # alter user dozor with password '<password>';

   где **<password>** – новый пароль пользователя БД, например:

   # alter user dozor with password 'q1';

4. Перейти в каталог БД:

   - БД политики фильтрации – **/data/base/dozor/pgsql**
   - БД модуля Dozor File Crawler – **/data/base/crawler/pgsql/**
   - БД событий и инцидентов ИБ, БД архива сообщений под управлением СУБД PostgreSQL – путь к каталогу можно узнать, выполнив команду:

     # ps ax | grep <port>

     где **<port>** – порт, на котором выбранная БД ожидает соединения. В результате выполнения команды на экран будет выведена информация следующего вида:

     ```
     # ps ax | grep 5435
     10440 ?        S      3:25 /usr/pgsql-9.6/bin/postmaster -p 5435 -D /data/base/smap-archive
     31078 pts/0    S+     0:00 grep 5435
     ```

     Путь **/data/base/smap-archive** в данном примере является путем к каталогу БД.

5. Открыть файл **pg_hba.conf** для редактирования и найти строки следующего вида:

   ```
   # IPv4 local connections:
   host    all             all             <IP>/<mask>             trust
   ```

   Убедиться, что в качестве значений **<IP>/<mask>** установлены правильные значения доверенной подсети и маски. Заменить слово **trust** на **password**, сохранить и закрыть файл.

6. Задать пароль пользователя БД в параметрах конфигурации Solar Dozor:

   - БД политики, БД событий и инцидентов ИБ, БД архива сообщений под управлением СУБД PostgreSQL – параметр **Пароль пользователя базы данных** в разделе GUI **Система > Конфигурация > Основные настройки > Доступ к данным** в секции **Схемы соединений с БД** для соответствующей записи схемы соединения.
   - БД модуля Dozor File Crawler – параметр **Пароль пользователя БД с метазаданиями**, раздел GUI **Конфигурации** > **Расширенные настройки** > **File Crawler**, секции:
     - **Центр управления File Crawler**
     - **Прокси центра управления File Crawler**
     - **Сервис отпечатков File Crawler**

7. Если приведённые выше шаги выполнялись для БД событий и инцидентов ИБ или БД архива сообщений под управлением СУБД PostgreSQL, перезапустить БД, выполнив команду следующего вида:

   # systemctl restart <db-script-name>.service

   где **<db-script-name>** – имя скрипта автозапуска БД, который был создан при создании схемы этой БД. Если имя этого скрипта по каким-либо причинам не может быть установлено, следует выполнить следующие команды:

   ~$ sudo su - dozor

$ pg_ctl stop -D /data/base/<db-name>

$ pg_ctl start -D /data/base/<db-name>

где **<db-name>** – имя каталога БД (например, в шаге 4 – **smap-archive**).

8. Перезагрузить процессы Solar Dozor, выполнив следующую команду:

   # /opt/dozor/bin/dsctl restart

Приложение B. Ответвление сообщений с почтовых серверов

Схемы подключения при работе в пассивном режиме зависят от используемого почтового сервера (MTA). Блокировка сообщений при ответвлении невозможна, поскольку обработка по политике ИБ ведется только для копий сообщений. Ниже описаны способы ответвления почтового потока для наиболее распространённых почтовых серверов.

B.1. Ответвление почтового потока с сервера Yandex

Для настройки ответвления почтового потока с сервера Yandex 360 необходимо выполнить следующие действия:

1. Зарегистрировать приложение в сервисе Яндекс OAuth (раздел B.1.1);
2. Добавить правила обработки писем (раздел B.1.2);
3. Настроить Dozor File Crawler для сбора писем (раздел B.1.3).

B.1.1. Регистрация приложения

Для создания и регистрации приложения в сервисе Яндекс OAuth необходимо выполнить следующие действия:

1. Для создания приложения с особыми правами доступа перейти по ссылке https://oauth.yandex.ru/client/new/, и заполнить название приложения в открывшейся форме.
2. В разделе **Платформы приложения** выбрать **Веб-сервисы**, и в появившемся поле **Redirect URL** ввести **https://oauth.yandex.ru/verification_code** или нажать **Подставить URL для отладки** во всплывающем окне.
3. В разделе **Доступ к данным** добавить особые права доступа для работы с правилами:
   - **ya360_admin:mail_write_routing_rules** – управление правилами обработки почты для домена (просмотр и изменение);
   - **ya360_admin:mail_read_routing_rules** – чтение правил обработки почты для домена (просмотр).
4. Скопировать и сохранить для дальнейшего использования данные из поля **ClientID**. Пример: **26d2d876b59445b6a97d2a4cf4b47eb8**.

   Примечание

   Этот идентификатор становится недействительным через один год.

5. Получить отладочный токен, перейдя по ссылке вида https://oauth.yandex.ru/authorize?response_type=token&client_id=<ClientID>, где **<ClientID>** – идентификатор, полученный в предыдущем шаге. В ответе будет содержаться отладочный токен, например:

y0_AgAAAABwZwdkAAqE8wAAAADtEOEqyCSm4UqQQ_2fQKVnGwdeEmtJF-A.

При возникновении затруднений следует обратиться к документации по адресу https://yandex.ru/dev/id/doc/ru/register-client.

B.1.2. Добавление правил обработки писем

Для создания правил обработки писем необходим идентификатор организации. Его можно узнать, перейдя по адресу https://admin.yandex.ru и открыв вкладку **Профиль организации** (поле **ID**). Пример идентификатора: 7949520.

URL для запросов чтения и записи правил обработки писем имеет следующий вид:

https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules

где **<id>** – идентификатор организации.

Для чтения и записи правил обработки писем используется утилита командной строки **curl**.

Внимание!

*Из-за технических ограничений невозможна пересылка скрытых копий сообщений (**bcc**).*

B.1.2.1. Чтение правил

Для вывода на экран текущих правил обработки писем в формате JSON следует выполнить команду следующего вида:

**curl -H "Authorization: OAuth <oauth_token>" -v -k **
https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules

где **<oauth_token>** – отладочный токен, полученный в разделе B.1.1, **<id>** – идентификатор организации.

Для записи в файл текущих правил обработки писем в формате JSON следует выполнить команду следующего вида:

```
curl -H "Authorization: OAuth <oauth_token>" -v -k \
https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules \
-o <output_filename>
```

где **<oauth_token>** – отладочный токен, полученный в разделе B.1.1, **<id>** – идентификатор организации, **<output_filename>** – имя файла для записи правил.

B.1.2.2. Запись правил

Внимание!

При выполнении любой команды записи правил все текущие правила для данной организации будут перезаписаны правилами, указанными в этой команде. Если необходимо обновить текущие правила – следует их получить как показано в предыдущем разделе, объединить

с новыми правилами и записать. Для удобства рекомендуется использовать запись правил из файла.

Пример команды для записи правила пересылки входящих писем на заданный адрес в формате JSON из командной строки:

```
curl -H "Authorization: OAuth <oauth_token>" -v -k -X PUT \
https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules \
-d '{
  "rules": [
    {
      "terminal": false,
      "condition": {},
      "actions": [
        {
          "data": {
            "email": "dlp@organization.ru"
          },
          "action": "forward"
        }
      ],
      "scope": {
        "direction": "inbound"
      }
    }
  ]
}'
```

где **<oauth_token>** – отладочный токен, полученный в разделе B.1.1, **<id>** – идентификатор организации, **dlp@organization.ru** – почтовый адрес для приёма пересылаемых писем.

Пример команды для записи правила в формате JSON из файла:

```
curl -H "Authorization: OAuth <oauth_token>" -g -i -v -k -X PUT \
https://api360.yandex.net/admin/v1/mail/routing/org/<id>/rules \
--databinary @input.json
```

где **<oauth_token>** – отладочный токен, полученный в разделе B.1.1, **<id>** – идентификатор организации, **input.json** – имя файла, содержащего правило.

Пример правила пересылки входящих и исходящих писем на заданный адрес в формате JSON для использования в командах записи:

```
{
  "rules": [
    {
      "terminal": false,
      "condition": {},
      "actions": [
        {
          "data": {
            "email": "dlp@organization.ru"
          },
          "action": "forward"
```

```
      }
    ],
    "scope": {
      "direction": "inbound"
    }
  },
  {
    "terminal": false,
    "condition": {},
    "actions": [
      {
        "data": {
          "email": "dlp@organization.ru"
        },
        "action": "forward"
      }
    ],
    "scope": {
      "direction": "outbound"
    }
  }
```

Пример правила пересылки входящих и исходящих писем одного пользователя на заданный адрес в формате JSON для использования в командах записи:

```
{
  "rules": [
    {
      "scope": {
        "direction": "outbound"
      },
      "actions": [
        {
          "data": {
            "email": "dlp@solardozor.ru"
          },
          "action": "forward"
        }
      ],
      "terminal": false,
      "condition": {
        "$or": [
          {
            "from": {
              "$eq": "a.petrov@solardozor.ru"
            }
          },
          {
            "to": {
              "$eq": "a.petrov@solardozor.ru"
            }
          }
        ]
      }
    },
    {
      "scope": {
        "direction": "inbound"
```

```
    },
    "terminal": false,
    "actions": [
     {
      "data": {
       "email": "dlp@solardozor.ru"
      },
      "action": "forward"
     }
    ],
    "condition": {
     "$or": [
      {
       "from": {
        "$eq": "a.petrov@solardozor.ru"
       }
      },
      {
       "to": {
        "$eq": "a.petrov@solardozor.ru"
       }
      }
     ]
    }
   }
 ]
}
```

Пример правила пересылки входящих и исходящих писем двух пользователей на заданный адрес в формате JSON для использования в командах записи:

```
{
 "rules": [
  {
   "scope": {
    "direction": "outbound"
   },
   "actions": [
    {
     "data": {
      "email": "dlp@solardozor.ru"
     },
     "action": "forward"
    }
   ],
   "terminal": false,
   "condition": {
    "$or": [
     {
      "from": {
       "$eq": "a.petrov@solardozor.ru"
      }
     },
     {
      "to": {
       "$eq": "a.petrov@solardozor.ru"
      }
     }
```

```
    ]
  },
},
{
  "scope": {
    "direction": "inbound"
  },
  "terminal": false,
  "actions": [
    {
      "data": {
        "email": "dlp@solardozor.ru"
      },
      "action": "forward"
    }
  ],
  "condition": {
    "$or": [
      {
        "from": {
          "$eq": "a.petrov@solardozor.ru"
        }
      },
      {
        "to": {
          "$eq": "a.petrov@solardozor.ru"
        }
      }
    ]
  }
},
{
  "scope": {
    "direction": "outbound"
  },
  "actions": [
    {
      "data": {
        "email": "dlp@solardozor.ru"
      },
      "action": "forward"
    }
  ],
  "terminal": false,
  "condition": {
    "$or": [
      {
        "from": {
          "$eq": "n.serov@solardozor.ru"
        }
      },
      {
        "to": {
          "$eq": "n.serov@solardozor.ru"
        }
      }
    ]
  },
```

```
  },
  {
    "scope": {
      "direction": "inbound"
    },
    "terminal": false,
    "actions": [
      {
        "data": {
          "email": "dlp@solardozor.ru"
        },
        "action": "forward"
      }
    ],
    "condition": {
      "$or": [
        {
          "from": {
            "$eq": "n.serov@solardozor.ru"
          }
        },
        {
          "to": {
            "$eq": "n.serov@solardozor.ru"
          }
        }
      ]
    }
  }
 ]
}
```

B.1.3. Настройка Dozor File Crawler для сбора писем

Для настройки сбора писем в Solar Dozor следует настроить доступ к почтовому ящику, на который выполняется пересылка писем, и создать соответствующую задачу в Dozor File Crawler.

B.1.3.1. Настройка доступа к почтовому ящику

Для настройки доступа к почтовому ящику необходимо выполнить следующие действия:

1. Перейти на адрес **https://mail.yandex.ru** и выполнить вход с учетной записью почтового ящика, на который выполняется пересылка писем (в данном примере – dlp@organization.ru).

2. Перейти в раздел **Настройки > Все настройки > Почтовые программы** и установить флажки:

   - **С сервера imap.yandex.ru по протоколу IMAP**
   - **Пароли приложений и OAuth-токены**

3. Сохранить настройки.

4. Перейти в раздел **Настройки > Все настройки > Безопасность** и нажать на ссылку **Пароли приложений**. В открывшемся разделе **Создать пароль приложения** выбрать данные, к которым необходимо предоставить доступ (тип приложения).

5. Ввести название пароля, с которым он будет отображаться в списке. В качестве названия можно указать название приложения, для которого создается пароль. Нажать **Далее**.

6. В новом окне на экран будет выведен пароль приложения. Следует сохранить этот пароль для дальнейшего использования.

Внимание!

Созданный пароль можно увидеть только один раз. Если пароль был утрачен – следует удалить его и создать заново.

Примечание

Для начала работы пароля требуется некоторое время: Яндекс предупреждает о 2–3 часах, хотя обычно это занимает несколько минут.

B.1.3.2. Настройка задачи в Dozor File Crawler

Для настройки задачи в Dozor File Crawler для сбора писем следует создать задачу со следующими параметрами:

- **Почтовый сервер** – **imap.yandex.ru**
- **Порт** – **993**
- **Использовать SSL-соединение** – включить
- **Почтовый ящик** – указать почтовый ящик, для которого выполнялась настройка (в данном примере – dlp@organization.ru)
- **Пароль** – пароль, созданный в предыдущем разделе
- **Входящие** и **Письма с вложениями** – включить
- **Уведомлять при завершении задачи с ошибками** – рекомендуется включить

Также рекомендуется самостоятельно отслеживать результаты работы задачи в разделе **Результат**. После успешной проверки выполнения задачи следует настроить расписание для неё.

B.1.3.3. Возможные проблемы

При пересылке на единый адрес (в данном примере – dlp@organization.ru) письма могут попадать в папку **Спам**. Следует вручную указать, что рассылки с данного адреса не являются спамом.

B.1.4. Идентификация сообщений

Для поиска сообщений Yandex 360 политикой фильтрации следует использовать два условия, объединенных логическим оператором **И**:

- **Заголовок x-dar-host Совпадает с imap.yandex.ru**
- **Тип сообщения Равно exchange**

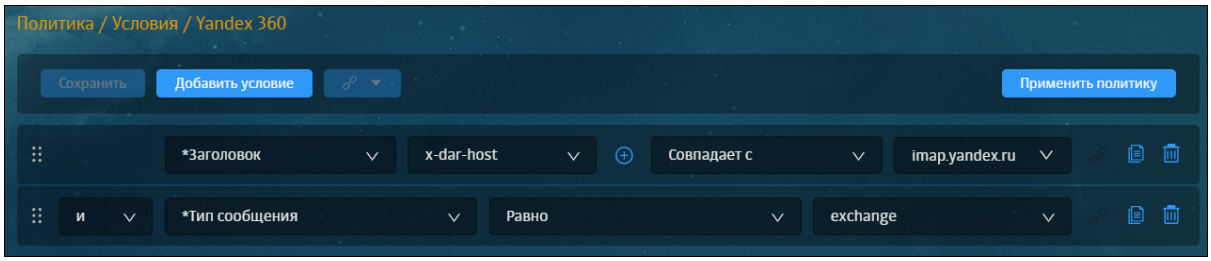


Рис. B.1. Условие для поиска сообщений Yandex 360

B.2. Ответвление почтового потока с сервера «МойОфис Почта»

Для настройки ответвления почтового потока с сервера «МойОфис Почта» необходимо выполнить на этом сервере следующие действия:

1. Создать резервную копию конфигурационного файла **/opt/poseidon/postfix/main.cf**, выполнив команды:

   cd /opt/poseidon/postfix

   cp main.cf main.cf.bak

2. Открыть для редактирования файл **main.cf** и добавить в него следующие строки:

   ```
   always_bcc = <m_address>
   transport_maps = lmdb:/etc/postfix/transport_map
   ```

   где **<m_address>** – почтовый адрес для отправки скрытых копий в Solar Dozor, например: **dozor@dozor.solar.local**. Сохранить и закрыть файл.

3. Создать файл **/opt/poseidon/postfix/transport_map**, выполнив команду:

   touch /opt/poseidon/postfix/transport_map

4. Открыть созданный файл и записать в него содержимое следующего вида:

   ```
   <m_address> smtp:[<filter_address>]:<filter_port>
   ```

   где:

   - **<m_address>** – почтовый адрес для отправки скрытых копий в Solar Dozor;
   - **<filter_address>** – адрес сервера Solar Dozor, имеющего роль **Фильтр почтового потока**;
   - **<filter_port>** – номер порта, на котором этот сервер ожидает входящие сообщения.

Пример:

```
dozor@dozor.solar.local smtp:[10.201.31.2]:1025
```

5. Создать файл **/usr/local/bin/postfix_to_dozor_fix.sh**, выполнив команду:

   touch /usr/local/bin/postfix_to_dozor_fix.sh

6. Открыть созданный файл и записать в него следующее содержимое:

```
#!/bin/bash

docker service update psn-mail_postfix --force --with-registry-auth
container_id=$(docker ps | grep postfix | awk '{print $1}')

echo "Container_id is $container_id"
docker cp /opt/poseidon/postfix/transport_map $container_id:/etc/postfix/
docker exec -it $container_id postmap -v /etc/postfix/transport_map
```

   Сохранить и закрыть файл.

7. Создать файл **/usr/local/bin/postfix_to_dozor_fix_cron.sh**, выполнив команду:

   touch /usr/local/bin/postfix_to_dozor_fix_cron.sh

8. Открыть созданный файл и записать в него следующее содержимое:

```
#!/bin/bash
container_id=$(docker ps | grep postfix | awk '{print $1}')
docker cp /opt/poseidon/postfix/transport_map $container_id:/etc/postfix/
docker exec -it $container_id postmap -v /etc/postfix/transport_map
```

   Сохранить и закрыть файл.

9. Открыть расписание планировщика, выполнив команду:

   crontab -e

10. Добавить в расписание следующие строки:

```
@reboot root /usr/local/bin/postfix_to_dozor_fix_cron.sh
*/1 * * * * root /usr/local/bin/postfix_to_dozor_fix_cron.sh
```

11. Перезапустить службу планировщика, выполнив команду:

    systemctl restart crond.service

B.3. Ответвление почтового потока с сервера Microsoft Exchange

Действия по ответвлению почтового потока с сервера Microsoft Exchange отличаются для Microsoft Exchange разных версий. Описание процесса ответвления для версии Microsoft Exchange 2000 приведено ниже. Руководства по ответвлению почтовых потоков для версий Microsoft Exchange 2003 и 2007 приведены в приложениях B.5 и B.6. В документации по Microsoft Exchange для процесса ответвления почтового потока используется термин «журналирование».

Внимание!

*При использовании данного метода пропадает оригинальное значение заголовка **mail from**, которое заменяется значением, указанным при настройке ответвления.*

B.3.1. Microsoft Exchange 2000

Для включения журналирования необходимо выполнить следующие действия:[1]

1. Создать новую учетную запись пользователя в **Active Directory Users and Computers**. При создании необходимо снять флажок **Create Exchange Mailbox**.
2. После создания пользователя в свойствах объекта пользователя (вызывается щелчком правой кнопкой мыши) следует выбрать пункт **Exchange Tasks** и в появившемся окне выбрать пункт **Establish E-mail Address**. Затем в открывшемся окне нужно ввести произвольный адрес пользователя на компьютере, где установлен Solar Dozor (например, dozor@server.domain, где server.domain – имя сервера, на котором установлен Solar Dozor).
3. В **Exchange System Manager** перейти на вкладку **Servers**.
4. Выбрать **Storage Group**, щелкнуть правой кнопкой мыши на списке хранилищ и выбрать пункт **Properties**.
5. На вкладке **General** выбрать пункт **Archive all messages sent or received by mailboxes on this store** и нажать кнопку **Browse** для выбора записи, на которую будут пересылаться скопированные сообщения (т.е. учетной записи получателя, созданного на первом шаге).

Эти действия необходимо проделать для каждого из хранилищ.

B.3.2. Преобразование журнальных сообщений Exchange в оригинальные SMTP-сообщения

При обработке журнальных сообщений, поступающих от сервера Exchange, Solar Dozor может преобразовать их в оригинальные SMTP-сообщения. Соответствующие модули поставляются в составе стандартной конфигурации. Модули встраиваются в точку разбора файлов в спуле и позволяют обрабатывать смешанный поток сообщений (журнальные и не журнальные сообщения в одном входящем потоке), при этом можно применять разные политики обработки к сообщениям журнальной подсистемы и обычным сообщениям. То есть включение обработки журнальных сообщений не влияет на обработку обычных сообщений.

Модуль поддержки Exchange отвечает за обработку журнальных сообщений с серверов Exchange любых версий. Возможность распознавания сообщений **Exchange** определяется параметром **Определять тип сообщений Exchange** в секции **Сервис фильтрации сообщений** (раздел GUI **Система > Конфигурация > Основные настройки > Работа системы**). Журнальные сообщения определяются по наличию любого из заголовков:

- **"X-MS-Exchange-Organization-Journal-Report"**

[1] По материалам Microsoft.com

- **"X-MS-Journal-Report"**
- **"X-MS-Exchange-Organization-Processed-By-Journaling"**

а также двух вложенных частей типа **text/plain** и **message/rfc2822**.

Адреса действительных отправителя и получателей сообщения определяются в ходе разбора полей журналирования (добавляемых сервером Exchange) в части сообщения **text/plain**. Текст оригинального сообщения берется из части типа **message/rfc2822**.

Модуль поддержки Exchange 2003 определяет обработку журнальных сообщений с сервера Exchange 2003, отличных по своей структуре. Для таких сообщений, полученных с адресов, определенных параметром **Значения RCPT TO для журнальных сообщений Exchange 2003** (раздел GUI **Система > Конфигурация > Основные настройки > Работа системы**, секция **Сервис фильтрации сообщений**), адреса отправителя и получателей определяются не в ходе разбора полей журналирования, а из заголовков самого сообщения: **Sender** или **From** – для отправителя, **To**, **CC** и **Bcc** – для получателей.

Примечание

*Параметром **Значения RCPT TO для журнальных сообщений Exchange 2003** определяются почтовые адреса - коннекторы, соответствующие специальным учетным записям на сервере Exchange 2003, которые обеспечивают пересылку журнальных сообщений с сервера Exchange на сервер Solar Dozor. Поэтому эти адреса не соответствуют реальным адресам отправителей и получателей из оригинальных сообщений. Для таких сообщений и осуществляется подстановка адресов из заголовков оригинального сообщения. Подробнее см. B.5.*

На сообщения типа Email, полученные в результате преобразования журнальных сообщений Exchange, ставится соответствующая пометка: **«Преобразовано из журнала Exchange»** – в случае, если сообщение было обработано модулем разбора Exchange, или **«Преобразовано из журнала Exchange: Exchange 2003»** в случае, если сообщение было обработано модулем разбора Exchange 2003.

B.4. Ответвление почтового потока с сервера Exim

В зависимости от версии Exim настройки файла конфигурации несколько различаются. Для Exim версии 3.x необходимо в начало раздела **ROUTERS CONFIGURATION** конфигурационного файла вписать следующие строки (в примере предполагается, что сервер, на котором установлен Solar Dozor, имеет имя **dozor.example.ru**):

```
smaphost1:
driver = domainlist
transport = remote_SMTP
route_list = "* dozor.example.ru bydns_a"
unseen
```

Для Exim версии 4.x строки будут следующими:

```
smaphost1:
driver = manualroute
transport = remote_SMTP
route_list = "* dozor.example.ru"
unseen
```

B.5. Ответвление сообщений с сервера Microsoft Exchange 2003

B.5.1. Общая последовательность действий

Для журналирования сообщений с сервера Microsoft Exchange 2003 необходимо выполнить следующие действия:

1. Создать объект типа «контакт» в службе Active Directory. В качестве почтового адреса для данного объекта указать почтовый адрес, для которого в доменной части прописать DNS-имя сервера, где функционирует Solar Dozor.

2. Создать учетную запись пользователя, имеющего почтовый адрес на сервере Exchange, с которого будет осуществляться ответвление почтового потока. Весь почтовый поток будет дублироваться в почтовом ящике этого пользователя и далее пересылаться на сервер, где функционирует Solar Dozor.

3. Провести дополнительную настройку, если Solar Dozor работает не через стандартный SMTP-порт (25).

4. Включить стандартное журналирование на сервере Exchange, с которого будет происходить ответвление почтового потока на Solar Dozor.

5. Включить BCC-журналирование на сервере Exchange, с которого будет происходить ответвление почтового потока на Solar Dozor.

B.5.2. Создание объекта типа «контакт» в Active Directory

В Active Directory требуется создать объект типа «contact». Для этого необходимо выполнить следующие действия:

1. Открыть консоль управления **Microsoft Management Console**, перейти к оснастке **Active Directory Users and Computers**, щелкнуть правой кнопкой мыши и в контекстном меню выбрать пункт **New > Contact**.

2. В открывшемся диалоговом окне создания нового контакта заполнить формы ввода, указав значения **First Name** и **Last Name**. Например, в поле **First Name** ввести значение «**To**», а в поле **Last Name** значение «**Dozor**». Нажать кнопку **Next**.

3. В следующем открывшемся окне создания нового контакта нажать кнопку **Modify**.

4. В окне **New E-mail Address** установить флажок **SMTP Address** и нажать кнопку **OK**.

5. В окне **Internet Address Properties** перейти на вкладку **General** и ввести почтовый адрес **copyforarchive@<DNS-имя сервера Solar Dozor>**. Нажать кнопку **Next**.

Внимание!

Почтовый адрес обязательно должен начинаться с copyforarchive@.

В результате описанных действий на экране должна отобразиться форма **New Object > Contact** следующего вида (см. Рис.B.2). Для завершения создания нового контакта следует нажать кнопку **Next** и далее кнопку **Finish**:

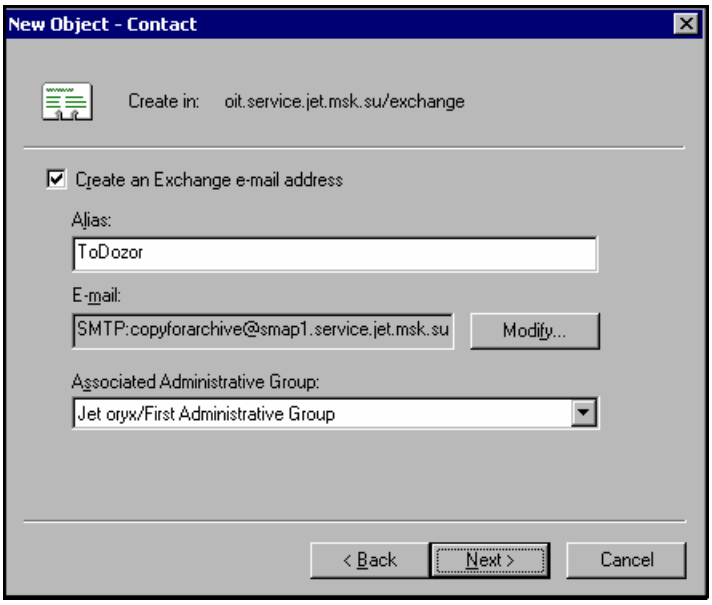


Рис. B.2. Форма New Object > Contact

B.5.3. Создание учетной записи пользователя

Далее требуется создать учетную запись нового пользователя, на почтовый адрес которого будут отправляться архивные сообщения. Для этого необходимо выполнить следующие действия:

1. В Active Directory создать объект типа **user** с любым именем (например, **user1**) с почтовым адресом на сервере Exchange. С этого адреса будет происходить ответвление почтового потока.

2. После создания пользователя **user1** необходимо скрыть его почтовый адрес в досье. Для этого следует открыть окно **Properties** для пользователя **user1**, перейти на вкладку **Exchange Advanced**, где установить флажок **Hide from Exchange Address lists** (см. Рис.B.3):

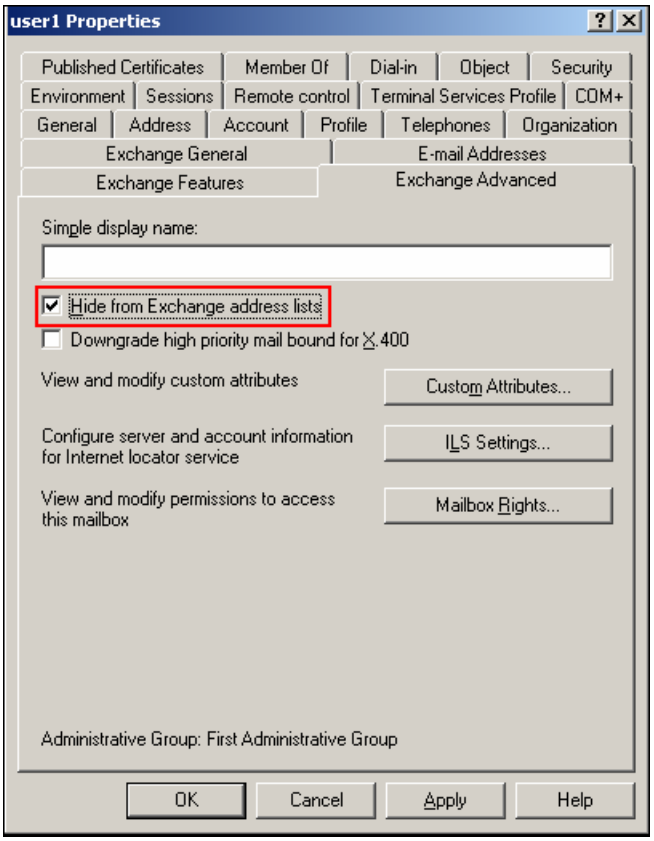


Рис. B.3. Сокрытие адреса пользователя в досье

Примечание

*Если в свойствах пользователя не отображается вкладка **Exchange Advanced**, то нужно выбрать пункт меню **View** в консоли **Active Directory Users and Computers** и установить параметр **Advanced Features**.*

3. Далее необходимо настроить пересылку всей почты с ящика пользователя **user1** на созданный ранее контакт. Для этого следует перейти на вкладку **Exchange General** в окне свойств пользователя и нажать кнопку **Delivery Options** (см. Рис.B.4):

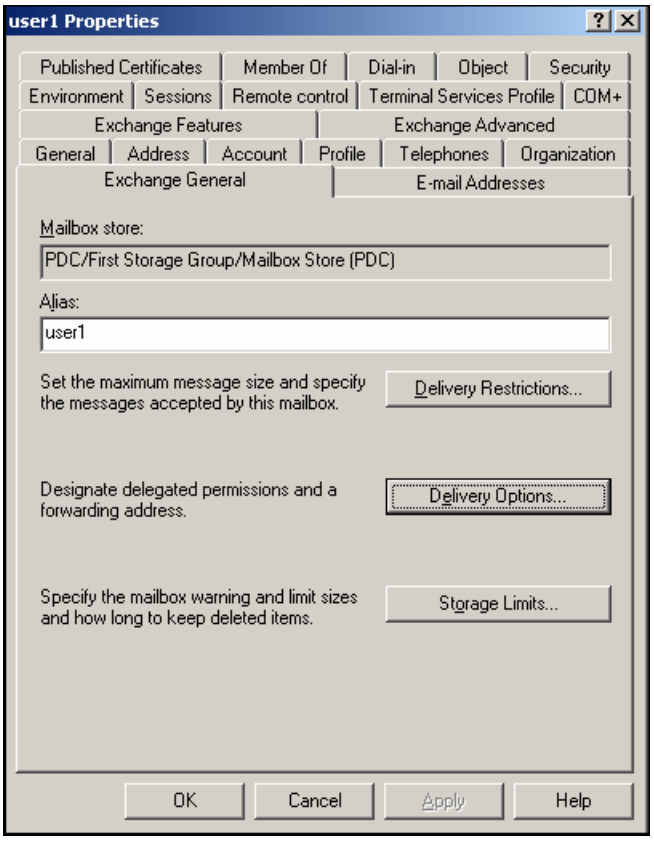


Рис. В.4. Свойства пользователя, вкладка Exchange General

4. В открывшемся окне **Delivery Options** для параметра **Forwarding Address** установить значение **Forward to** и нажать кнопку **Modify** (см. Рис.В.5). В появившемся окне необходимо ввести имя созданного контакта и нажать кнопку **OK**:

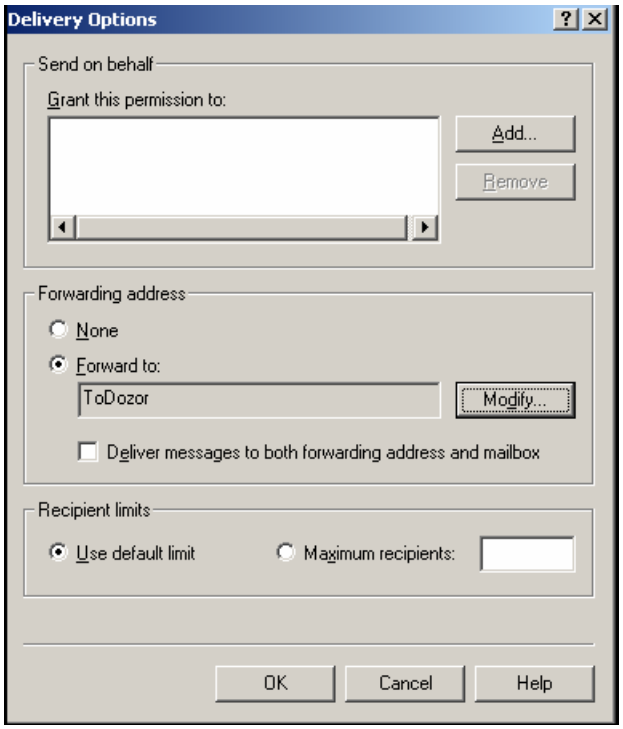


Рис. B.5. Окно Delivery Options

5. В окне **Delivery Options** нажать кнопку **ОК**. Создание учетной записи пользователя завершено.

B.5.4. Дополнительная настройка

Примечание

*Если Solar Dozor работает в режиме архивирования сообщений типа Email, то в этом случае важно знать, какой порт использует процесс **SMTP_GW**. Если **SMTP_GW** использует 25 порт, то SMTP-коннектор в Microsoft Exchange создавать не нужно. Важно только, чтобы был правильно настроен DNS, и Exchange-сервер отправлял сообщения на сервер, где функционирует Solar Dozor. Если процесс **SMTP_GW** использует порт, отличный от 25, то необходимо произвести дополнительную настройку сервера Exchange.*

Если процесс **SMTP_GW** использует нестандартный порт (отличный от 25), то для настройки сервера Exchange необходимо выполнить следующие действия:

- Создать второй **SMTP Virtual Server**.
- Создать два SMTP-коннектора, один из которых будет доставлять почту в обычном режиме через **Default SMTP Virtual Server**, а второй через **Dozor SMTP Virtual Server** будет пересылать на Solar Dozor все архивные сообщения.

Для создания **SMTP Virtual Server** необходимо выполнить следующие действия:

1. Открыть оснастку **Exchange System Manager** и в раскрывающемся дереве слева выбрать пункт **Servers > Name Exchange > Protocols > SMTP**, щелкнув на нем правой

кнопкой мыши. В открывшемся контекстном меню необходимо выбрать пункт **New SMTP Virtual Server**.

2. Указать для нового SMTP-сервера имя **Dozor**.

3. Щелкнуть правой кнопкой мыши на имени сервера **Dozor** и в контекстном меню выбрать пункт **Properties**.

4. В окне свойств сервера перейти на вкладку **Delivery** (см. Рис.В.6) и нажать кнопку **Outbound connections**:

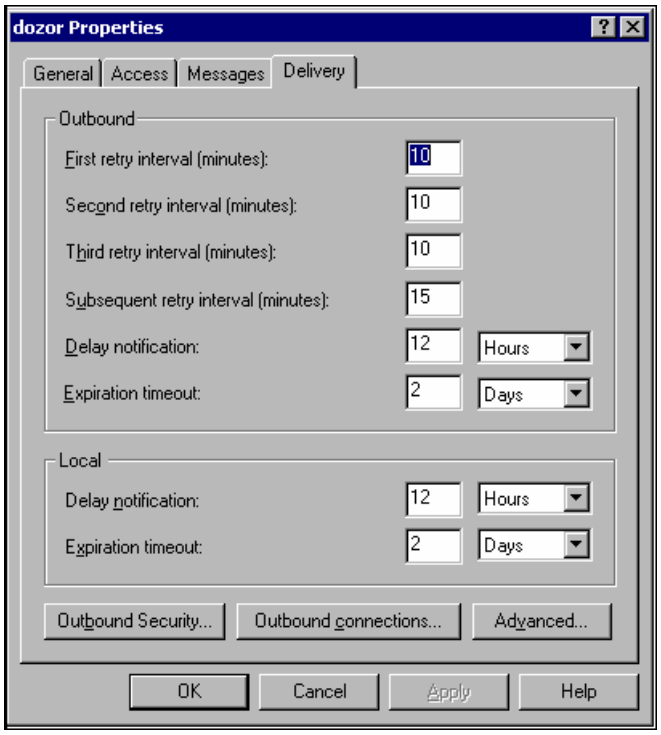


Рис. В.6. Свойства виртуального сервера SMTP

5. В открывшемся окне в поле **TCP port** необходимо ввести номер порта, по которому работает процесс **SMTP_GW** в Solar Dozor, например 1025.

6. Для завершения создания **SMTP Virtual Server** необходимо нажать кнопку **OK** во всех окнах.

Для создания коннектора для работы через **Default SMTP Virtual Server** необходимо выполнить следующие действия:

1. Открыть оснастку **Exchange System Manager > Connectors** (либо **Exchange System Manager > Routing Groups > First Routing Group > Connectors** – в зависимости от настройки Exchange).

2. Создать новый SMTP-коннектор. На кладке **General** ввести название для созданного коннектора и установить флажок **Use DNS to route to each address space on this connector** (если Exchange сам производит рассылку поступающей из внешних источников почты).

3. На той же вкладке **General** в разделе **Local bridgeheads** необходимо добавить сервер **Default SMTP virtual server**.

4. Перейти на вкладку **Address Space** и добавить адресное пространство типа SMTP с почтовым доменом, в качестве которого выступает сервер Solar Dozor. Для этого на вкладке **Address Space** нажать кнопку **Add** и в открывшемся окне ввести в поле **E-mail domain** символ «*», в поле **Cost** ввести значение **1**.

Для создания коннектора для работы через **Dozor SMTP Virtual Server** необходимо выполнить следующие действия:

1. Открыть оснастку **Exchange System Manager > Connectors** (либо **Exchange System Manager > Routing Groups > First Routing Group > Connectors** - в зависимости от настройки Exchange).

2. Создать новый SMTP-коннектор. На вкладке **General** ввести название коннектора, установить переключатель **Forward all mail through this connector to the following smart hosts** и ввести DNS-имя сервера, где функционирует Solar Dozor.

3. На той же вкладке **General** в разделе **Local bridgeheads** добавить сервер **Dozor SMTP virtual server**.

4. На вкладке **Address Space** указать в поле **Type** значение **Other**, а затем в открывшемся окне ввести следующие значения (см. **Рис.В.7**):

   - в поле **Type** ввести **SMTP**;
   - в поле **Cost** ввести **1**;
   - в поле **Address** ввести почтовый адрес **copyforarchive@<DNS-имя сервера Solar Dozor>**.

5. Для завершения создания **Dozor SMTP Virtual Server** нажать кнопку **OK** во всех окнах:

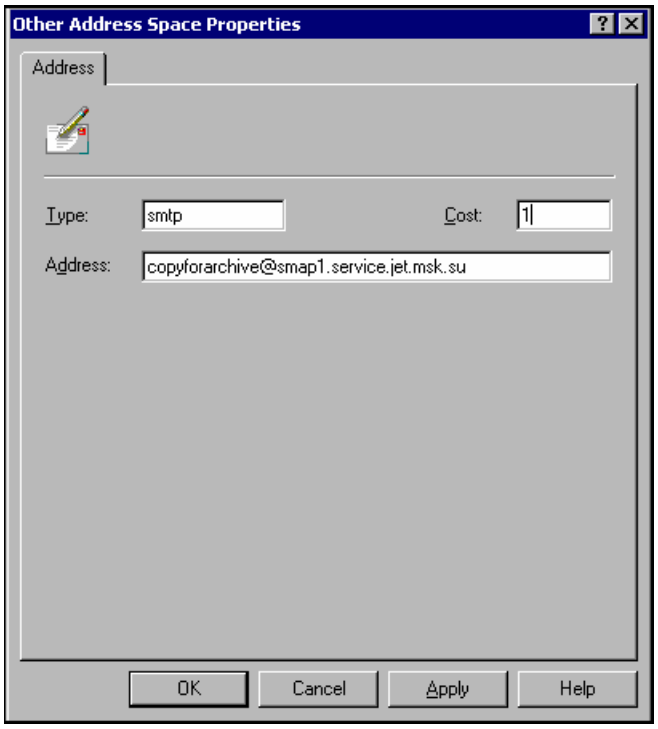


Рис. B.7. Создание коннектора. Вкладка Address

B.5.5. Включение стандартного журналирования

Если изначально использовался режим расширенного журналирования, то его можно отключить, для чего используется специальная программа настройки журналирования **Exejcfg**, доступную для загрузки с официального сайта компании Microsoft. Для отключения режима расширенного журналирования необходимо в командной строке Windows выполнить команду:

Exejcfg.exe -d

где:

- **Exejcfg.exe** – исполняемый файл программы настройки журналирования;
- **-d** – параметр, означающий отключение режима расширенного журналирования.

После этого необходимо включить стандартное журналирование, выполнив следующие действия:

1. Открыть оснастку **Exchange System Manager**, щелкнуть правой кнопкой мыши в области того хранилища (**Information Store**), применительно к которому требуется включить стандартное журналирование, и в появившемся контекстном меню выбрать пункт **Properties**.

2. В открывшемся окне свойств хранилища перейти на вкладку **General** и установить флажок **Archive all messages sent or received by mailboxes on this store** (см. Рис.B.8):

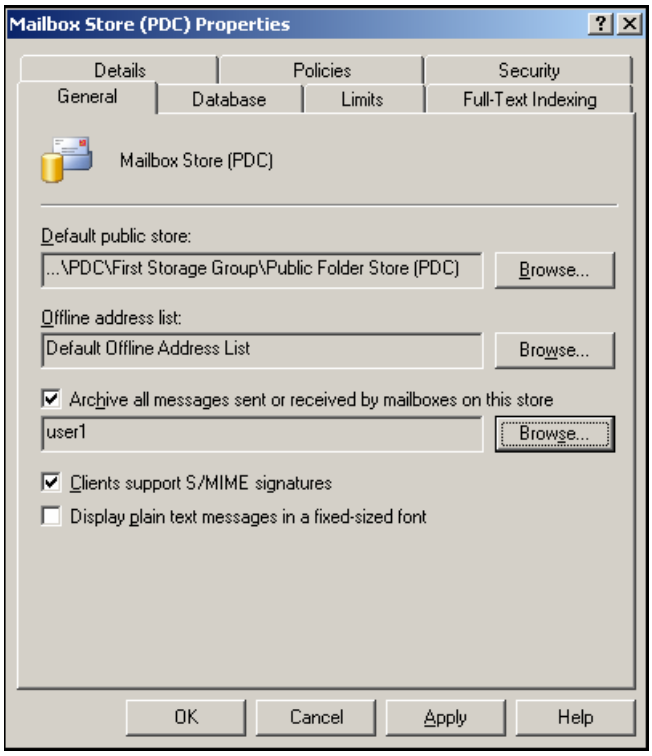


Рис. B.8. Установка архивирования всех сообщений из хранилища

3. Нажать кнопку **Browse** рядом с данным флажком и в открывшемся окне выбрать созданную ранее учетную запись пользователя **user1** (см. B.5.3). Нажать кнопку **OK**.

B.5.6. Включение BCC-журналирования

Для включения журналирования BCC необходимо выполнить следующие действия:

1. Запустить редактор реестра. Для этого открыть пункт меню **Пуск > Выполнить**. И в командой строке выполнить команду запуска реестра. Формат команды для запуска следующий:

   regedit

2. В открывшемся окне реестра найти ключ **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeTransport\Parameters**. Для данного ключа создать новый параметр типа **D_WORD** с именем **JournalBCC** и присвоить этому параметру значение **1** (см. Рис.B.9). После чего закрыть редактор реестра:

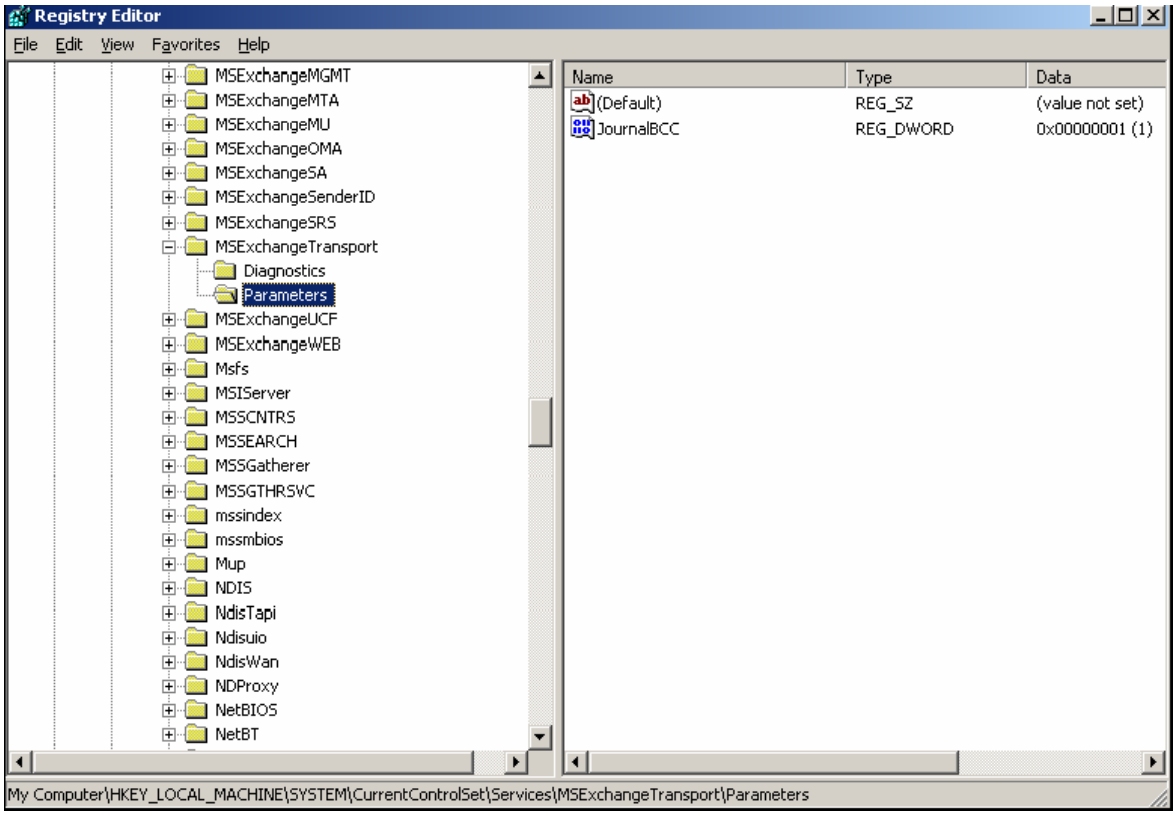


Рис. B.9. Редактирование реестра для включения BCC-журналирования

3. Запустить оснастку **Services**, в которой перезапустить службу SMTP, выполнив соответствующую команду контекстного меню (см. Рис.B.10):

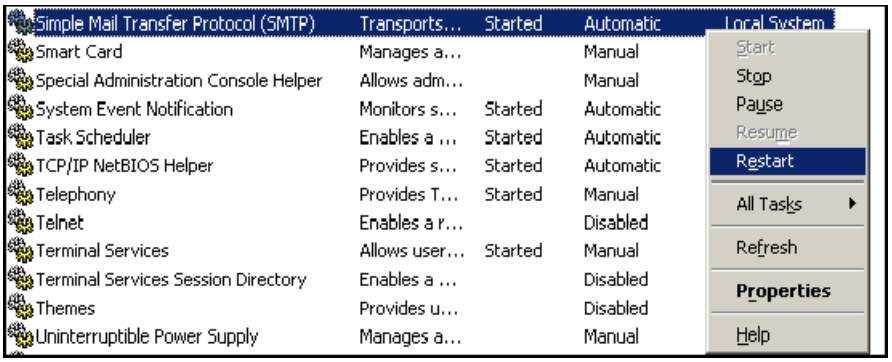


Рис. B.10. Перезапуск службы SMTP

B.5.7. Откат изменений

Под начальным состоянием понимается отсутствие на сервере Exchange какого-либо ответвления почтового потока на сервер Solar Dozor. Для отката изменений и возврата к начальному состоянию необходимо выполнить следующие действия:

1. Удалить созданный ключ реестра (см. B.5.6 , пункт 1 списка действий).

2. Деактивировать стандартное журналирование путем снятия флажка **Archive all messages sent or received by mailboxes on this store** в свойствах выбранного хранилища **Information Store** (см. B.5.5, пункт 2 списка действий).

3. Перезапустить службу SMTP (см. B.5.6 , пункт 3 списка действий).

B.6. Ответвление сообщений с сервера Microsoft Exchange 2007

На рисунке ниже (см. Рис.B.11) показана типовая схема ответвления почтового потока с использованием журналирования Exchange 2007. Все сообщения, отправляемые и принимаемые пользователями, обрабатываются сервером - транспортировщиком почтовых сообщений. На каждом таком сервере функционирует специальный агент, который осуществляет журналирование почтовых сообщений согласно заданной политике журналирования.

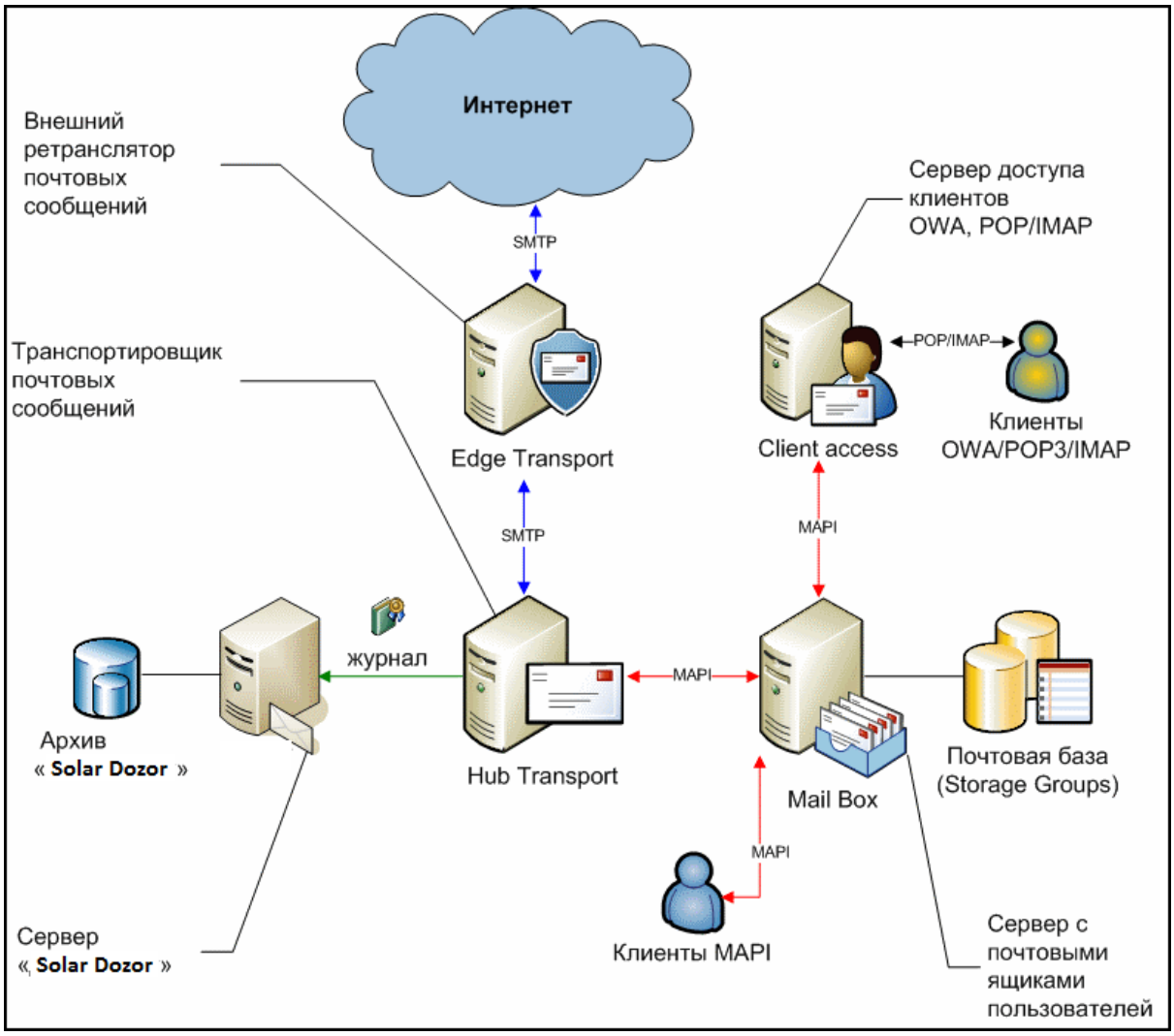


Рис. B.11. Схема ответвления почтового потока

В Microsoft Exchange Server 2007 используется два типа журналирования:

1. Стандартное журналирование. Обеспечивает журналирование всех почтовых сообщений, отправленных и принятых пользователями с учетными записями на определенном

почтовом хранилище. Данный тип журналирования аналогичен журналированию, используемому в MS Exchange Server 2000/2003.

2. Расширенное журналирование. Обеспечивает использование правил журналирования, которые могут быть настроены для обеспечения потребностей организации.

При использовании расширенного журналирования в среде Exchange 2007 объектами журналирования могут являться:

- Внутренняя переписка (Internal). В данную категорию входят сообщения, в которых получатель и отправитель являются пользователями, принадлежащими одной организации Exchange и имеющими учетные записи в домене Active Directory, в котором развернута данная организация Exchange.
- Внешняя переписка (External). В данную категорию входят сообщения, в которых получатель или отправитель являются внешними пользователями по отношению к организации Exchange.
- Общая переписка (Global). В данную категорию входят все почтовые сообщения как внешних пользователей, так и пользователей, находящихся в организации Exchange.
- Почтовый ящик, Группа или Все пользователи. Правила расширенного журналирования могут применяться к одному почтовому ящику, одной или нескольким группам, ко всем пользователям организации.

Процесс журналирования подразумевает своей конечной целью отправку журнала на сторонний SMTP-адрес (приемник журнальных данных). Под журналом понимается почтовое сообщение, содержащее служебную информацию и оригинал исходного сообщения. В качестве стороннего SMTP-адреса могут использоваться следующие объекты:

- организация Exchange;
- сторонний почтовый сервис.

В данном случае приемником журнальных данных является сервер Solar Dozor, осуществляющий архивирование поступающего почтового потока. В независимости от типа приемника журнальных данных в домене Active Directory должен присутствовать объект получателя для этих журнальных данных. Объектом может являться конкретный почтовый ящик Exchange 2007, контакт или список рассылки.

Для отправки журнальных данных на сервер Solar Dozor объектом получателя является контакт Active Directory, в котором прописан почтовый адрес с доменной частью, для которой настроен соответствующий коннектор Exchange. Данный коннектор осуществляет маршрутизацию почтовых сообщений, содержащих журнальные данные, на сервер Solar Dozor.

B.6.1. Общая последовательность действий

Для журналирования почтовых сообщений с сервера Microsoft Exchange 2007 необходимо выполнить следующие действия:

1. Создать объект типа «контакт» в Active Directory. В качестве почтового адреса для данного объекта указать почтовый адрес, для которого в доменной части прописать DNS-имя сервера, где функционирует Solar Dozor.

2. Настроить коннектор для пересылки сообщений, содержащих журнальные данные, на сервер Solar Dozor.

3. Включить журналирования для групп хранения (Storage Groups), почтовые сообщения которых необходимо журналировать.

4. Проверить корректность работы механизма ответвления.

B.6.2. Создание объекта типа «контакт» в MS Exchange server 2007

Для создания объекта типа «контакт» необходимо выполнить следующие действия:

1. Открыть оснастку **Exchange Management Console**. Открыть раскрывающийся список **Настройка получателей (Recipient Configuration)**, в котором выбрать пункт **Почтовые контакты (Mail Contact)**. Выбрать пункт меню **Действия (Action) > Новый Почтовый Контакт (New Mail Contact)**.

2. В открывшемся окне редактирования свойств контакта (см. Рис.B.12) в списке слева выбрать пункт **Новый контакт (New Mail contact)** и в полях ввода **First name**, **Name**, **Alias** ввести **Dozor**. В поле ввода **External e-mail address**: указать почтовый ящик в формате **dozor@<полное DNS имя сервера Solar Dozor>**. Нажать кнопку **Далее (Next)**:

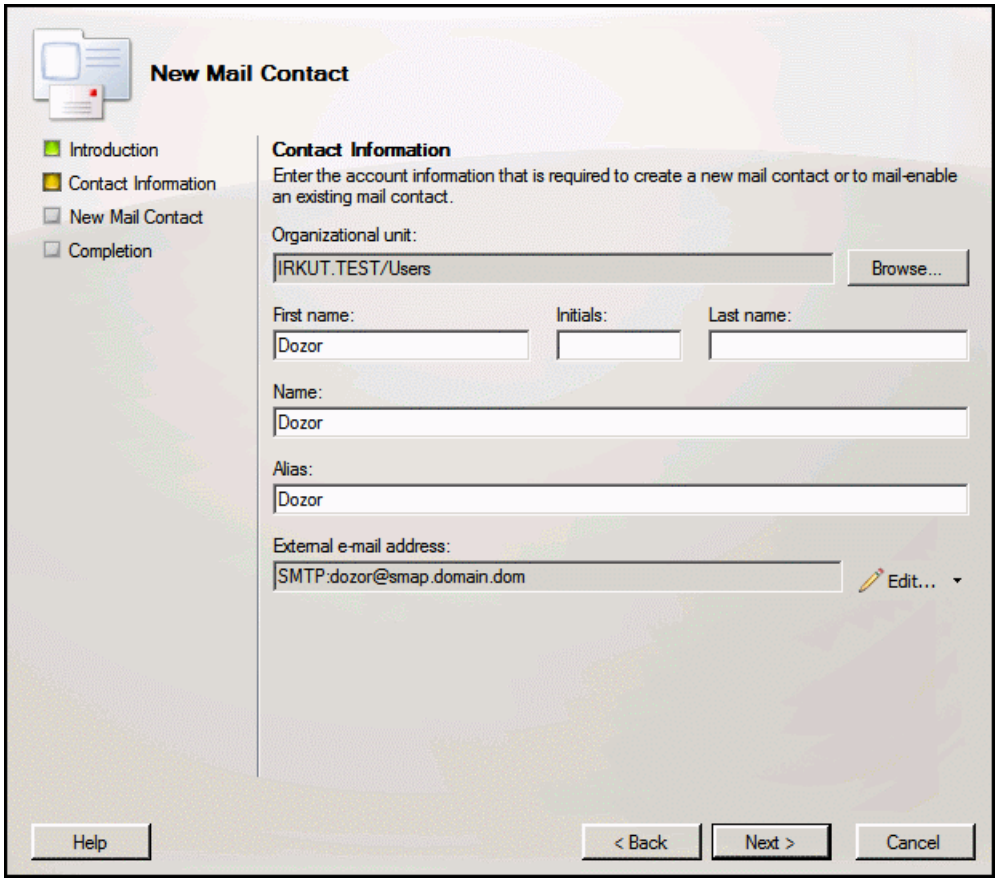


Рис. B.12. Окно редактирования свойств контакта в MS Exchange 2007

3. Далее для завершения создания нового контакта нажать кнопку **OK** во всех окнах.

B.6.3. Настройка коннектора для пересылки сообщений на сервер SMAP

Для настройки коннектора необходимо выполнить соответствующую команду в окне консоли **Exchange Management Shell**. Для запуска **Exchange Management Shell** следует открыть пункт меню **Пуск > Программы > Microsoft Exchange Server 2007 > Exchange Management Shell**. Откроется окно консоли для выполнения команд. Формат команды для выполнения настройки коннектора:

New-SendConnector -Name Dozor -AddressSpaces smap.dozor.dom -SmartHosts 192.168.11.136 -Port 1025 -SourceTransportServers cas1.irkut.test,cas2.irkut.test

где:

- **Name** – формальное имя коннектора;
- **AddressSpaces** – полное DNS-имя сервера SMAP;
- **SmartHosts** – ip-адрес сервера SMAP;
- **Port** – порт, на котором сервер SMAP ожидает приема почтовых сообщений;
- **SourceTransportServers** – серверы Exchange с ролью Hub Transport.

В результате в окне консоли должны отобразиться данные следующего вида:

```
Identity AddressSpaces          Enabled
-------- -------------          -------
Dozor    {smtp:smap.dozor.dom;1} True:
```

B.6.4. Включение журналирования

Стандартное журналирование.

На данном этапе необходимо указать для каких групп хранения будет использоваться журналирование. Для этого необходимо выполнить следующие действия:

1. Запустить оснастку **Exchange Management Console**, выполнив команду **Пуск > Программы > Microsoft Exchange Server 2007 > Exchange Management Console**.
2. В дереве элементов в левой части окна выбрать пункт **Server Configuration > Mailbox**. При работе с этим пунктом меню основное окно **Exchange Management Console** разделено на две области, верхнюю и нижнюю. В верхней области представлена таблица со списком созданных кластеров Exchange. В нижней области показаны характеристики выбранного кластера.
3. В верхней области необходимо выбрать мышью соответствующий кластер Exchange. В нижней области следует перейти на вкладку **Database Management** и выбрать нужную группу хранения, а в ней - нужную базу данных. Щелкнув правой кнопкой мыши на имя базы данных, выбрать в контекстном меню пункт **Properties**.
4. В окне **Properties** с параметрами выбранной базы данных следует прейти на вкладку **General** (см. Рис.B.13) и установить флажок **Journal Recipient**. После чего нажать кнопку **Browse** и в открывшемся окне выбора контактов **Select Recipient** выбрать созданный контакт **Dozor**:

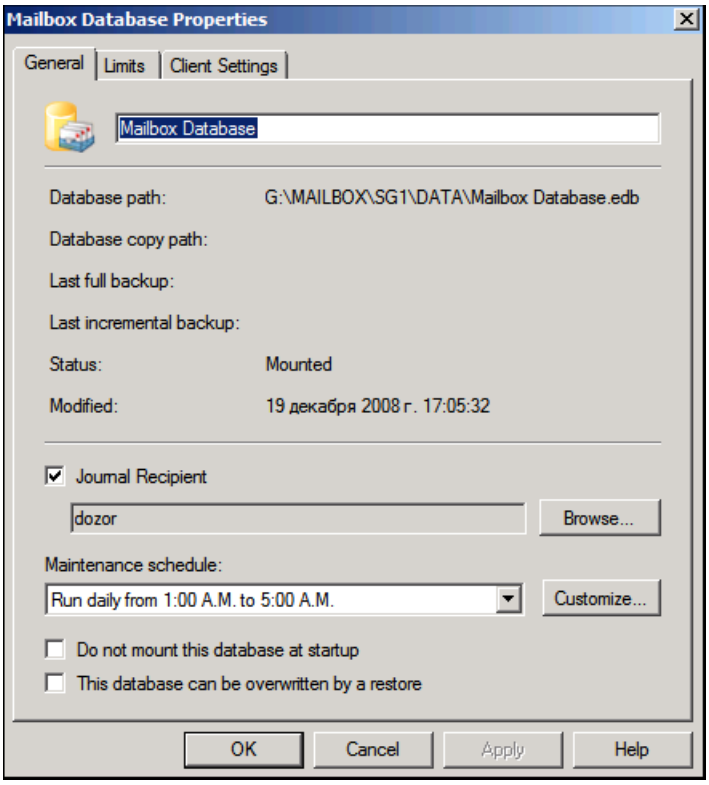


Рис. B.13. Окно свойств почтовой базы Exchange

5. Для завершения настройки журналирования необходимо нажать кнопку **ОК** в окне свойств базы данных.

Расширенное журналирование.

Чтобы включить расширенное журналирование, необходимо создать правило журналирования. Для этого следует выполнить следующие действия:

1. Запустить оснастку **Exchange Management Console**, выполнив команду **Пуск > Программы > Microsoft Exchange Server 2007 > Exchange Management Console**.

2. В дереве элементов в левой части окна выбрать пункт **Organization Configuration > Hub Transport** и перейти на вкладку **Journalling** в правой части окна.

3. В столбце действий **Actions** в правой части окна выбрать пункт **New Journal Rule** для создания нового правила журналирования. В открывшемся окне в поле **Rule Name** необходимо ввести имя для нового правила – **Dozor**, и установить для параметра **Scope** значение **Global -all messages**. В этом же окне необходимо установить флажок **Enable Rule**. Для завершения создания правила необходимо нажать кнопку **New**.

4. В таблице **Hub Transport** в окне **Exchange Management Console** должна появиться новая запись с именем **Dozor**. Если дважды щелкнуть мышью на строку с записью **Dozor** откроется окно со свойствами созданного правила журналирования (см. Рис.B.14):

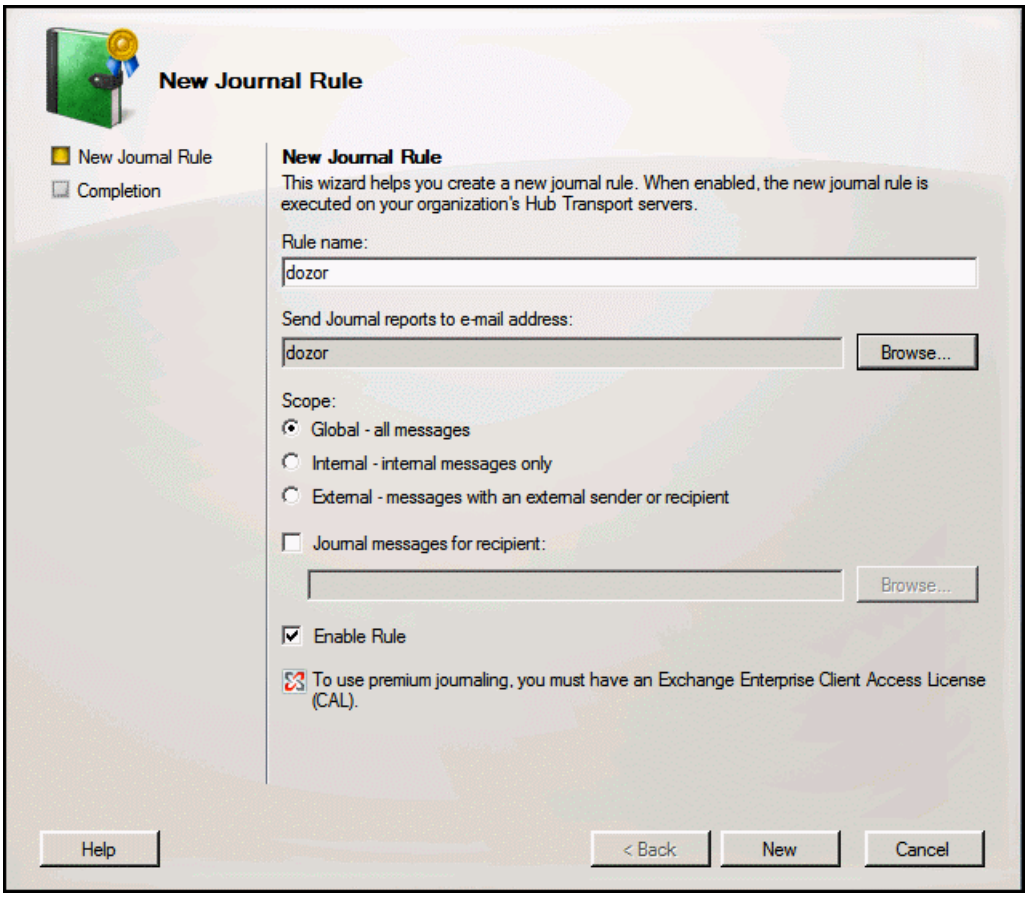


Рис. B.14. Создание правила журналирования

B.6.5. Проверка правильности работы журналирования

Для проверки правильности работы журналирования необходимо отправить тестовое сообщение на тестовый почтовый адрес в Exchange и проверить путь прохождения сообщения при помощи журнальных файлов утилиты **Exchange Message Tracking Tool**, входящей в состав ПО Microsoft Exchange 2007.

До начала просмотра журнальных файлов необходимо убедиться, что включен режим отслеживания сообщений. Для этого необходимо выполнить соответствующую команду, используя **Exchange Management Shell** (**Пуск > Программы > Microsoft Exchange Server 2007 > Exchange Management Shell**). Формат команды для выполнения проверки следующий:

Get-MailboxServer SERVERNAME | fl *messagetracking*

где **SERVERNAME** – имя кластера Exchange.

В результате в окне консоли должны отобразиться данные следующего вида:

```
MessageTrackingLogEnabled              :True
MessageTrackingLogMaxAge               :30.00:00:00
MessageTrackingLogMaxDirectorySize     :250MB
MessageTrackingLogMaxFileSize          :10MB
MessageTrackingLogPatch                :C:\Programm Files\Microsoft\Exchange
```

```
Server\TransportRoles\Logs\MessageTracking
MessageTrackingLogSubjectLoggingEnabled    :True
```

Значение переменной **MessagTrackingLogEnabled** должно быть **True**, а в переменной **MessagTrackingLogPath** должен быть указан путь к журнальным файлам утилиты. Если это не так, необходимо включить режим отслеживания сообщений. Для этого следует выполнить соответствующую команду в окне **Exchange Management Shell**.

Формат команды для включения режима отслеживания сообщений:

Set-TransportServer SERVERNAME –MessageTrackingLogEnabled $true

где **SERVERNAME** – имя сервера Exchange (или нескольких серверов, перечисленных через запятую), выполняющего роль **Hub Transport**.

Далее необходимо отправить тестовое сообщение с одного внутреннего почтового адреса Exchange на другой внутренний адрес. После отправки сообщения необходимо открыть файл, указанный в переменной **MessagTrackingLogPath** (см. листинг выполнения команды **Get-MailboxServer** выше) и убедиться, что в этом файле присутствуют строки (выделены полужирным шрифтом), свидетельствующие об отправке журнальных файлов на сервер SMAP:

```
#Software: Microsoft Exchange Server
#Version: 8.0.0.0
#Log-type: Message Tracking Log
#Date: 2008-12-19T14:59:22.558Z
#Fields: date-time,client-ip, client-hostname, server-ip, server-hostname, source-context, connector-id,
 source, event-id, internal-message-id, message-id, recipient-address, recipient-status, total-bytes,
recipient-count, related-recipient-address, reference, message-subject, sender-address, return-path,
message-info
2008-12-19T14:59:22.558Z, fe80::5c1a:d1de:8b91:5d24,
irkutbox.IRKUT.TEST,::1,CAS2,,,STOREDRIVER, RECEIVE, 4, <
F1926216EC7B4F48A45E9225AF49A4376466401764@IRKUTBOX.IRKUT.TEST>, ivanov@irkut.test;
 test@irkut.test; Administrator@irkut.test,,7684,3,,,FW: test message for
dozor,Administrator@irkut.test,Administrator@irkut.test,04I:
2008-12-19T14:59:23.777Z,,,,CAS2, Journaling,,AGENT, RECEIVE, 5,
<16bd3f92-f763-486d-ba61-55492d4b8f20@journal.report.generator>, dozor@domain.dom;
dozor@irkut.test,,9066,2,,4,FW: test message for dozor,
MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@IRKUT.TEST, <>,
2008-12-19T14:59:23.855Z,,,,CAS2,,,ROUTING, RESOLVE,
5,<16bd3f92-f763-486d-ba61-55492d4b8f20@journal.report.generator>, dozor@domain.dom,,9066,
 1, dozor@irkut.test,,FW: test message for dozor,
MicrosoftExchange329e71ec88ae4615bbc36ab6ce41109e@IRKUT.TEST,<>,
```

После этого необходимо убедиться, что отправленное сообщение попало в архив Solar Dozor.

B.7. Ответвление сообщений с сервера Microsoft Exchange 2013

B.7.1. Общая последовательность действий

Для журналирования почтовых сообщений с сервера Microsoft Exchange 2013 необходимо выполнить следующие действия:

1. Создать объект типа «контакт» в Active Directory. В качестве почтового адреса для данного объекта указать адрес, для которого в доменной части прописать имя сервера, на котором функционирует «Solar Dozor».

2. Настроить коннектор для пересылки сообщений, содержащих журнальные данные, на сервер «Solar Dozor».

3. Включить журналирование на сервере Exchange, с которого будет происходить ответвление почтового потока на «Solar Dozor».

B.7.2. Создание объекта типа «контакт» в MS Exchange server 2013

Для создания объекта типа «контакт» необходимо выполнить следующие действия:

1. Открыть сетевую консоль **Центр администрирования Exchange**.

2. Перейти в раздел **Получатели > Контакты**. Создать новый почтовый контакт (см. Рис.B.15):

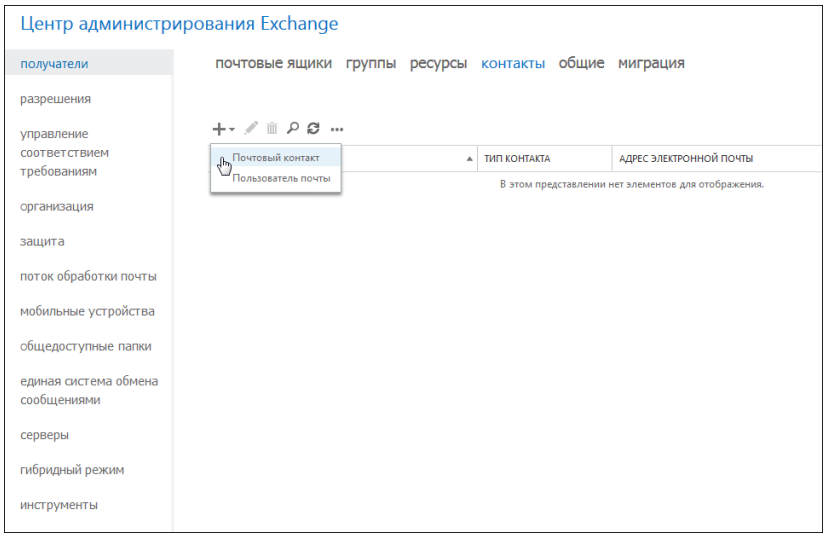


Рис. B.15. Центр администрирования Exchange

3. В открывшемся диалоговом окне создания нового контакта заполнить формы ввода, указав значения **Отображаемое имя**, **Имя**, **Псевдоним**, **Внешний почтовый ящик**. (см. Рис.B.16):

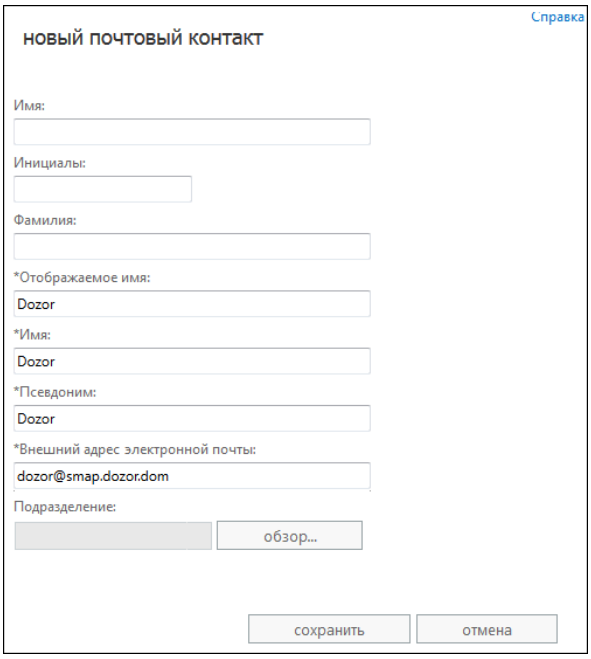


Рис. В.16. Создание почтового контакта

4. Для завершения создания нового контакта нажать кнопку **Сохранить**.

В.7.3. Настройка коннектора для пересылки сообщений на сервер Solar Dozor

Для настройки коннектора необходимо выполнить соответствующую команду в окне консоли **Exchange Management Shell**. Для запуска **Exchange Management Shell** следует открыть пункт меню **Пуск > Программы > Microsoft Exchange Server 2013 > Exchange Management Shell**. Откроется окно консоли для выполнения команд. Формат команды для выполнения настройки коннектора:

New-SendConnector -Name Dozor -AddressSpaces smap.dozor.dom -SmartHosts 10.199.29.209 -Port 1025 -SourceTransportServers a009.company.com.

где:

- **Name** – формальное имя коннектора;
- **AddressSpaces** – доменное имя сервера Solar Dozor;
- **SmartHosts** – ip-адрес сервера Solar Dozor;
- **Port** – порт, на котором сервер Solar Dozor ожидает приема почтовых сообщений;
- **SourceTransportServers** – сервер Exchange с ролью Hub Transport (если серверов несколько, их следует указывать через запятую).

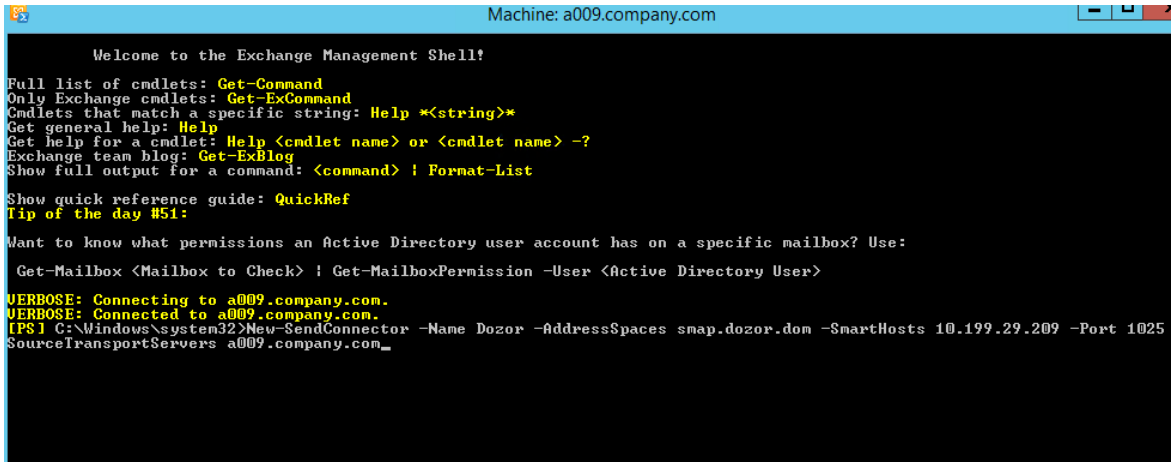


Рис. B.17. Консоль Exchange Management Shell

В результате в окне консоли должны отобразиться данные следующего вида:

```
Identity AddressSpaces          Enabled
-------- -------------          -------
Dozor    {smtp:smap.dozor.dom;1} True:
```

B.7.4. Включение журналирования

Чтобы включить журналирование, следует создать правило журналирования. Для этого необходимо выполнить следующие действия:

1. Открыть сетевую консоль **Центр администрирования Exchange**.
2. Перейти в раздел **Получатели > Группы**. Нажать кнопку **Создать+ > Группа рассылки**.

   В открывшемся диалоговом окне создания группы заполнить формы ввода, указав значения **Отображаемое имя**, **Псевдоним**, **Владельцы** (см. Рис.B.18).

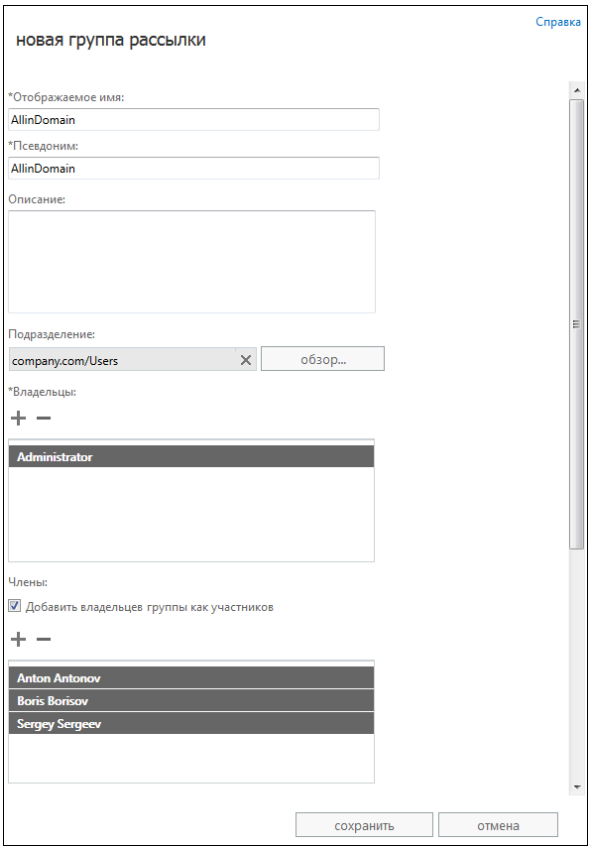


Рис. В.18. Создание группы рассылки

3. Для завершения создания новой группы нажать кнопку **Сохранить**

4. Перейти в раздел **Управление соответствием требованиям > Правила журнала**. Нажать кнопку **Добавить+**. В меню **Правило журнала** заполнить требуемые поля и нажать кнопку **Сохранить** (см. Рис.В.19).

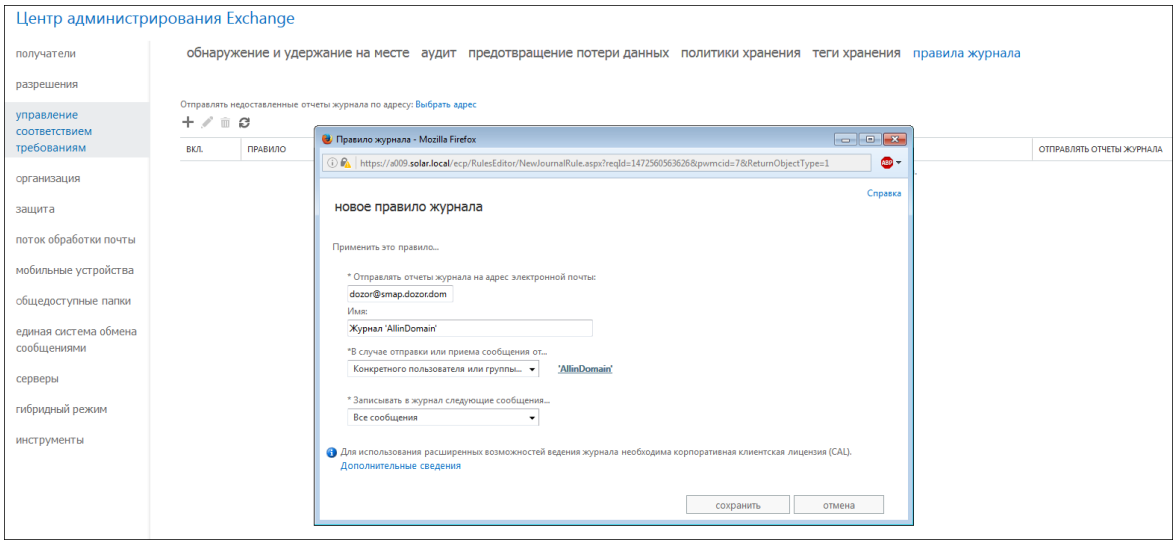


Рис. В.19. Создание правила журналирования

Приложение C. Описание ролей и сервисов

Ниже перечислены возможные роли узлов кластера Solar Dozor. Для каждой роли указано её назначение и состав сервисов, обеспечивающих её функционирование. Имена ролей указаны как они отображаются в GUI (раздел **Система > Узлы и роли**), а в скобках приведены имена ролей как они отображаются в CLI (скрипты **set-role**, **get-role** и **reg-slave**).

- Сервисы, которые по умолчанию запущены на всех узлах независимо от роли, обеспечивающие полноценное функционирование кластера Solar Dozor:
  - ds-bus-rc – сервис распределённого управления.
  - monitor-ng – сервис валидации параметров конфигурации.
  - smap-diag – виртуальный сервис регулярной отправки диагностических отчётов.
  - smap-settings – виртуальный сервис хранения общих для кластера настроек.
  - sender – сервис отправки почтовых сообщений.
  - internal-connectors – виртуальный внутренний сервис хранения метаинформации сервисов узла.
  - smap-redis – сервис хранения счётчиков, очередей сообщений для обработки и очередей действий над сообщениями.
  - monitor-agent – сервис мониторинга на узле.
- **Сервер управления** (**master**) – единая точка управления. Такую роль может иметь только один узел кластера (см. также описание роли **Все сервисы**). На узле с этой ролью запускается **Сервер архива сообщений** (см. ниже), веб-сервер для доступа к GUI, а также генерируется политика фильтрации, распространяемая на все остальные узлы кластера. Роль использует следующие сервисы:
  - database – сервис СУБД настроек, политики и Досье.
  - action-server-database – база данных сервера действий.
  - agent-control-ng – сервис управления модулем Dozor Endpoint Agent при помощи GUI.
  - software-center – сервис развёртывания агентов.
  - smap-agents – виртуальный сервис хранения настроек Агентов.
  - smap-address-book – виртуальный сервис, используемый скриптом **abook-sync**.
  - incident-daemon – сервис управления событиями и инцидентами информационной безопасности.
  - report-server – сервис построения отчётов.
  - smap-difi – сервис цифровых отпечатков.

- abook-daemon – сервис доступа к Досье.
- agent-media-server – сервис хранения медиаинформации, поступающей от агентов Dozor Endpoint Agent.
- license-server – сервис лицензирования.
- grafana – сервис построения графиков и диаграмм.
- monitor-server – сервис сбора данных мониторинга.
- monitor-httpd – сервис HTTP-интерфейса к системе мониторинга Zabbix. Обеспечивает работу пользовательского интерфейса мониторинга.
- archive-server – сервис доступа к сообщениям в архиве.
- action-server – сервис выполнения действий над сообщениями в архиве.
- webserver – сервис веб-сервера для доступа к GUI.
- smap-request-handler – сервис обработчика запросов из GUI.

- **Сервер архива сообщений** (**storage**) – роль, назначаемая slave-узлам для снижения нагрузки на master-узел при архивировании сообщений. Роль использует следующий сервис:
  - archive-server – сервис доступа к сообщениям в архиве.
- **Распознавание текста изображений** (**ocr**) – распознавание текстовых данных, находящихся в графических файлах вложений. Роль использует следующие сервисы:
  - ocr-server – сервис распознавания изображений, доступный для обращений клиентов. Производит обработку запросов, проверку и применение настроек распознавания, препроцессинг и постпроцессинг, выполняет распознавание текста изображений.
  - skvt-cassandra – сервис кэша результатов распознавания текста изображений.
  - ocr-crelic – сервис лицензирования движка ContentReader Engine.
- **Сервис распределённого хранения** (**cassandra**) – участие узла кластера Solar Dozor в кластере Cassandra. Назначение этой роли позволяет повысить производительность кластера Cassandra. Роль использует следующий сервис:
  - skvt-cassandra – сервис хранения индексов ФХ и кэша сервиса распознавания текстов изображений
- **Анализатор данных** (**analyzer**) – извлечение и анализ данных из тел сообщений и приложенных к сообщениям файлов. Роль использует следующие сервисы:
  - smap-difi – сервис работы с цифровыми отпечатками.
  - smap-idid – сервис контроля идентификаторов.
  - smap-tikaserver – сервис извлечения текстовых данных и определения кодировки.

- **Сервер интеграции** (**api-gateway**) – прием запросов к сервисам Solar Dozor от внешних клиентов. Роль использует следующий сервис:
  - api-gateway – сервис интеграции.
- **Сервис перехвата и анализа сетевого трафика** (**traffic-agent**) – перехват, фильтрация сетевого трафика и пересылка его на почтовый фильтр. Роль использует следующий сервис:
  - tragent – сервис перехвата, анализа и пересылки сетевого трафика.
- **Сервис репликации досье на подчинённых узлах** (**abook-slave**) – дублирование части данных Досье. Роль предназначена для повышения отказоустойчивости в ситуациях, когда связь с master-узлом (и хранящимся на нём Досье) временно отсутствует. Роль использует следующий сервис:
  - abook-daemon – сервис хранения и управления данными Досье.
- **Сервер агентов** (**agent-server**) – управление ПО Dozor Endpoint Agent, установленным на рабочих станциях пользователей. Узлы с этой ролью осуществляют обмен данными с Агентами по протоколу HTTPS и отправку собранных данных на почтовый шлюз Solar Dozor по протоколу SMTP. Роль использует следующий сервис:
  - agent-server – сервис взаимодействия с Агентами.
- **Центральное файловое хранилище** (**fsng-storage**) – долговременное хранение и ротация тел сообщений на файловой системе узла. Роль использует следующие сервисы:
  - filestorage-ng – сервис файлового хранилища.
  - skvt-cassandra – сервис хранения индексов файлового хранилища.
- **Локальное файловое хранилище** (**fsng-client**) – кратковременное хранение тел сообщений на файловой системе перед отправкой их в центральное файловое хранилище. Роль использует следующие сервисы:
  - filestorage-ng – сервис файлового хранилища.
  - skvt-cassandra – сервис хранения индексов файлового хранилища.

  Примечание

  *Назначение одному узлу ролей **Центральное файловое хранилище** и **Локальное файловое хранилище** эквивалентно назначению ему роли **Центральное файловое хранилище**.*
- **Индексатор текста** (**text-indexer**) – индексирование сообщений в оперативном архиве для полнотекстового поиска. Роль использует следующие сервисы:
  - indexer-ng – сервис индексации сообщений в архиве.
  - smap-elasticsearch – сервис текстовой индексации и поиска сообщений в архиве на основе Elasticsearch.

- **Вспомогательный сервис индексации текста** (**indexer-only**) – индексирование сообщений в оперативном архиве. Роль использует следующий сервис:
  - indexer-ng – сервис индексации сообщений в архиве.
- **Хранилище индексов событий и инцидентов** (**incident-indexer**) – хранение индексов оперативных событий и инцидентов информационной безопасности. Роль использует следующий сервис:
  - smap-elasticsearch – сервис текстовой индексации и поиска инцидентов на основе Elasticsearch.
- **Сервер управления событиями и инцидентами подкластера** (**local-incident-daemon**) – управление событиями и инцидентами ИБ в подкластере. Роль использует следующий сервис.
  - incident-daemon – сервис управления событиями и инцидентами информационной безопасности.
- **Вспомогательный сервер Elasticsearch** (**elasticsearch**) – осуществляет индексацию оперативных сообщений и инцидентов ИБ. Роль использует следующий сервис:
  - smap-elasticsearch – сервис поиска и индексации сообщений и инцидентов на основе поисковой машины Elasticsearch.
- **Хранилище индексов исторических событий и инцидентов** (**historic-incident-indexer**) – хранение исторических событий и инцидентов информационной безопасности. Роль использует следующий сервис:
  - smap-elasticsearch – сервис текстовой индексации и поиска инцидентов на основе Elasticsearch.
- **Индексатор исторических сообщений** (**historic-text-indexer**) – индексирование сообщений в историческом архиве для полнотекстового поиска. Роль использует следующие сервисы:
  - indexer-ng – сервис индексации сообщений в архиве.
  - smap-elasticsearch – сервис текстовой индексации и поиска сообщений в архиве на основе Elasticsearch.
- **Вспомогательный индексатор исторических сообщений** (**historic-indexer-only**) – индексирование сообщений в историческом архиве. Роль использует следующий сервис:
  - indexer-ng – сервис индексации сообщений в архиве.
- **Фильтр почтового потока** (**smtp-filter**) – приём, фильтрация и архивирование сообщений. Роль использует следующие сервисы:
  - smap-smtp-gw – сервис приёма почтовых сообщений.
  - mailfilter – сервис обработки почтовых сообщений согласно политике фильтрации.
  - archiver – сервис архивирования почтовых сообщений.

- smap-tikaserver – сервис извлечения текстовых данных и определения кодировки.
- smap-address-book – виртуальный сервис, используемый скриптом **abook-sync**.

- **Балансировщик** (**balancer**) – распределение трафика по серверам фильтрации Solar Dozor. Роль использует следующий сервис:
  - haproxy – сервис балансировщика HAProxy.
- **Вспомогательный сервер действий** (**action-server**) – работа с сообщениями в архиве: экспорт, удаление и отправка сообщений, добавление и удаление пометок, отправка уведомлений, перефильтрация сообщений. Роль использует следующий сервис:
  - action-server – сервис выполнения действий над сообщениями в архиве.

Внимание!

*Роль **Вспомогательный сервер действий** не может быть назначена одному узлу вместе с ролями **Сервер действий подкластера** и **Сервер управления**.*

- **Сервер действий подкластера** (**action-server-master**) – работа с сообщениями в архиве: экспорт, удаление и отправка сообщений, добавление и удаление пометок, отправка уведомлений, перефильтрация сообщений. Роль использует следующие сервисы:
  - action-server – сервис выполнения действий над сообщениями в архиве.
  - action-server-database – база данных сервера действий.

Внимание!

*Роль может быть назначена только узлу в подкластере. Роль **Сервер действий подкластера** не может быть назначена одному узлу вместе с ролями **Вспомогательный сервер действий** и **Сервер управления**.*

- **Сервер лицензирования подкластера** (**license-server**) – сервер лицензирования. Роль может быть назначена только узлу в подкластере. Роль использует следующий сервис:
  - license-server – сервер лицензирования.
- **Локальный веб-сервер** (**webserver-local**) – веб-сервер подкластера в территориально-распределенном режиме работы. Роль использует следующий сервис:
  - webserver-local – сервис GUI в подкластере.

Внимание!

*Узлу с ролью **Локальный веб-сервер** необходимо предварительно назначить одну или несколько из следующих ролей:*

- ***Индексатор текста***
- ***Хранилище индексов событий и инцидентов***
- ***Вспомогательный сервер Elasticsearch***

- **Сервер категорий** (**category-server**) – категоризация текстов вложений. Роль использует следующий сервис:
  - category-server – сервис категоризации.
- **Сервер обработки медиаданных** (**media-processor**) – распознавание текста медиаданных (например, снимков демонстрации экрана), полученных от агентов. Подкластер или общие ресурсы, в которых назначается эта роль, должны содержать узел с ролью **Сервер агентов**. Роль использует следующие сервисы:
  - ocr-crelic – сервис лицензирования движка ContentReader Engine.
  - media-processor-ocr-server – сервис распознавания текста изображений медиаданных.
  - media-processor-action-server – сервис выполнения действий по обработке медиаданных.
  - media-processor-action-server-database – БД сервиса выполнения действий по обработке медиаданных.
- **Сервер управления Краулером** (**crawler-x-master**) – управление экземплярами краулера. Роль использует следующие сервисы:
  - crawler-pccc – сервис координации между экземплярами краулера и веб-интерфейсом, сбор данных с экземпляров краулера.
  - crawler-database – сервис базы данных краулера.
- **Краулер: файловые ресурсы и IMAP** (**crawler-x**) – экземпляр краулера. Роль использует следующие сервисы:
  - crawler-ccc – сервис сбора статистики, телеметрии, журналов, управления заданиями, расписанием, передача информации на ProxyCCC.
  - crawler-database – сервис базы данных краулера.
  - smap-activemq – сервис управления очередью метазаданий.
  - crawler-snapshot – сервис, предоставляющий информацию о просканированных ранее объектах по запросу.
  - crawler-processor – сервис обработки результатов сканирования: применение политики к файлам, осуществление заданных действий над файлами.
  - crawler-scanner – сервис сканирования файловых данных.

- **Краулер: корпоративные мессенджеры** (**im-crawler**) – загрузка сообщений пользователей в корпоративных мессенджерах через официальный API. Роль использует следующий сервис:
  - im-crawler – сервис загрузки сообщений пользователей в корпоративных мессенджерах через официальный API.
- **Распознавание графических объектов** (**god-server**) – идентификация определённых графических объектов в файлах изображений (сканах), например, печатей или разворотов паспорта. Роль использует следующий сервис:
  - god-server – сервис распознавания графических объектов, доступный для обращений клиентов. Выполняет обработку запросов, проверку и применение настроек распознавания, выполняет распознавание графических объектов.
- **Контроль рабочего времени** (**time-control**) – сбор информации об активности пользователей. Роль необходима для работы раздела **Рабочее время** (при отсутствии в кластере Solar Dozor узла с ролью **Анализ поведения (UBA)**, см. ниже). Роль использует следующие сервисы:
  - clickhouse – сервис БД ClickHouse для хранения статистических данных.
- **Анализ поведения (UBA)** (**uba-server**) – сервер анализа поведения пользователей. Эта роль может быть только одна в кластере Solar Dozor и необходима для работы раздела **Поведение и аномалии** в большой карточке персоны. Роль также позволяет работать с разделом **Рабочее время**. Роль использует следующие сервисы:
  - uba-server – сервис сбора данных о поведении пользователей.
  - indexer-ng – сервис индексации сообщений в архиве.
  - clickhouse – сервис БД ClickHouse для хранения статистических данных.
- **Мониторинг локального почтового шлюза** (**mail-gw**) – при наличии роли на узле включается мониторинг почтовых серверов Postfix, указанных в наборах параметров отправки. Роль не содержит собственных сервисов.
- **Центр приложений** (**software-center**) – сервис удаленного управлением Агентами на станциях с ОС Windows. Роль использует следующий сервис:
  - software-center – центр приложений

Внимание!

Роль может быть назначена только узлу в подкластере. Не допускается назначение роли двум и более узлам в одном подкластере.

Приложение D. Описание файлового хранилища

D.1. Общая архитектура ФХ

В ФХ помещаются контейнеры, содержащие тела сообщений или медиаданные (аудиозаписи, видеозаписи, снимки экрана рабочего стола АРМ сотрудников и снимки демонстрируемого контента через средства ВКС), а атрибуты сообщений хранятся в БД архива. При выполнении запросов к архиву определяется местоположение сообщения в ФХ по его идентификатору, и тело сообщения извлекается из контейнера. Размещение тел сообщений на жёстком диске, а не в БД, даёт возможность хранить их в архивированном виде и таким образом уменьшить объем используемого дискового пространства.

Если используется распределённая конфигурация Solar Dozor, то можно настроить ФХ на нескольких узлах и создать распределённое ФХ. Для этого следует распределить роли **Центральное файловое хранилище** и **Локальное файловое хранилище** между узлами. Узлы с ролью **Фильтр почтового потока** обрабатывают поступающий поток сообщений и помещают информацию о структуре сообщений, проставленных пометках и прочее – в БД архива, а тела сообщений – в один из экземпляров ФХ:

- При наличии ФХ на локальном узле – в него;
- При отсутствии или недоступности ФХ на локальном узле – в любое доступное ФХ на других узлах.

Сообщения с узлов с ролью **Локальное файловое хранилище** перемещаются на узлы с ролью **Центральное файловое хранилище**. Локальные хранилища предназначены для быстрой обработки поступающего потока сообщений и их временного хранения, а центральное хранилище предназначено для постоянного хранения тел сообщений. Общая схема организации распределённого ФХ показана на рисунке **Рис.D.1**.

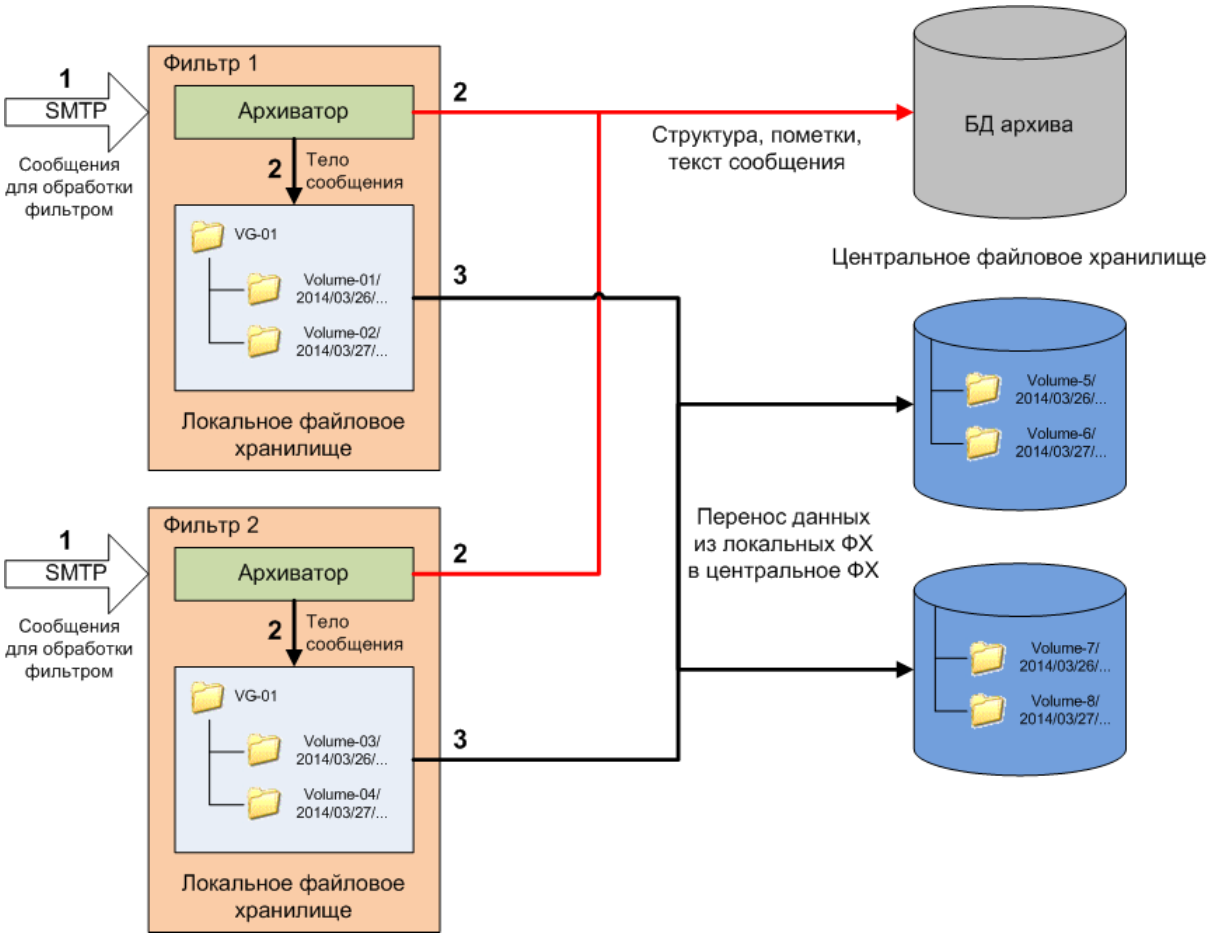


Рис. D.1. Общая схема организации распределённого файлового хранилища

ФХ имеет структуру каталогов следующего вида:

<path>/<год>/<месяц>/<число>/<час>/<минута>.

Каталоги иерархически организованы по времени (в зависимости от времени получения сообщений – эта информация хранится в метаданных сообщения). Здесь **<path>** – каталог с данными ФХ, который указан в настройках конфигурации.

На более низких уровнях вложенности располагаются контейнеры с объектами. Каждый контейнер в своём корневом каталоге содержит файл манифеста, в котором описывается содержимое контейнера в виде xml-структуры. Манифест описывает состояние контейнера с данными, тип данных (сообщение ПК, файл, другое), формат хранения (сжатый файл, дубликат и т. д.). Каждый такой контейнер имеет идентификатор vID, а также области данных и служебных данных. В подкаталоге **vid/data** хранится тело сообщения (файл **body** или **body.gz**, если включено сжатие).

Работа ФХ обеспечивается следующими сервисами:

- **filestorage-ng** – сообщает о наличии объектов в индексе ФХ. По запросу с идентификатором vID объекта проверяет наличие соответствующей записи в индексе БД **Cassandra** и возвращает URL объекта в ФХ, либо возвращает сообщение об ошибке, если объекта с указанным vID нет в индексе. Также используется для размещения в центральном ФХ контейнеров, сформированных на других узлах ФХ. Кроме того, выполняет функции web-сервера, который принимает по протоколу HTTPS запросы от

веб-интерфейса с URL контейнера с телом сообщения в ФХ, и передаёт тело сообщения на веб-интерфейс.

- **skvt-cassandra** – сервис управления распределённой БД индекса ФХ, в которой хранятся записи обо всех сообщениях, помещённых в ФХ. Такая запись содержит информацию, позволяющую сопоставить идентификатор vID сообщения и каталог ФХ с телом сообщения.

Примечание

БД индексов ФХ построена на основе продукта APACHE CASSANDRA, поэтому здесь далее БД индексов ФХ будет называться ***Cassandra****.*

D.2. Запись данных в файловое хранилище и базу данных Cassandra

Информация о размещении тела сообщения в ФХ записывается в **Cassandra**. В этой БД хранятся записи с данными о vID-идентификаторах сообщений и их расположении в иерархии каталогов ФХ. Зная идентификатор vID сообщения, можно получить ссылку на каталог с телом сообщения, обратившись к БД **Cassandra** .

Схема добавления записей в БД **Cassandra** показана на рисунке Рис.D.2.

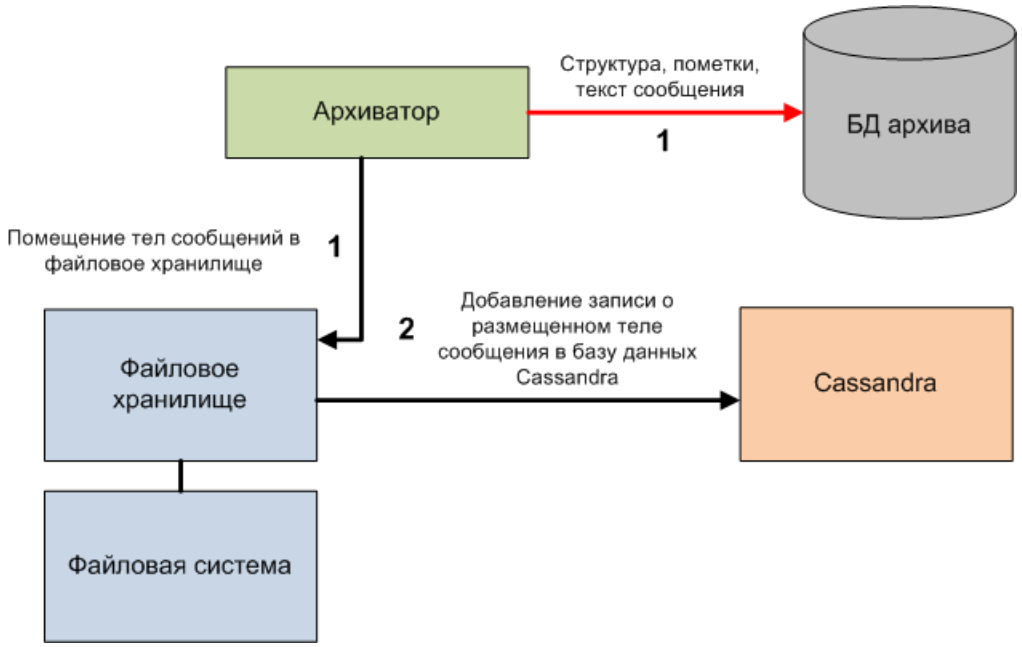


Рис. D.2. Добавление записей в базу данных Cassandra

D.3. Перемещение сообщений из локального ФХ в центральное

Локальное ФХ служит для временного хранения тел сообщений, прошедших фильтрацию. Центральное ФХ предназначено для долговременного хранения сообщений, поступающих со всех узлов фильтрации. Для этого периодически, через настроенные промежутки времени, выполняется перенос накопленных данных из локальных ФХ в центральное.

Схема и порядок перемещения сообщений из локального ФХ в центральное показана на рисунке Рис.D.3.

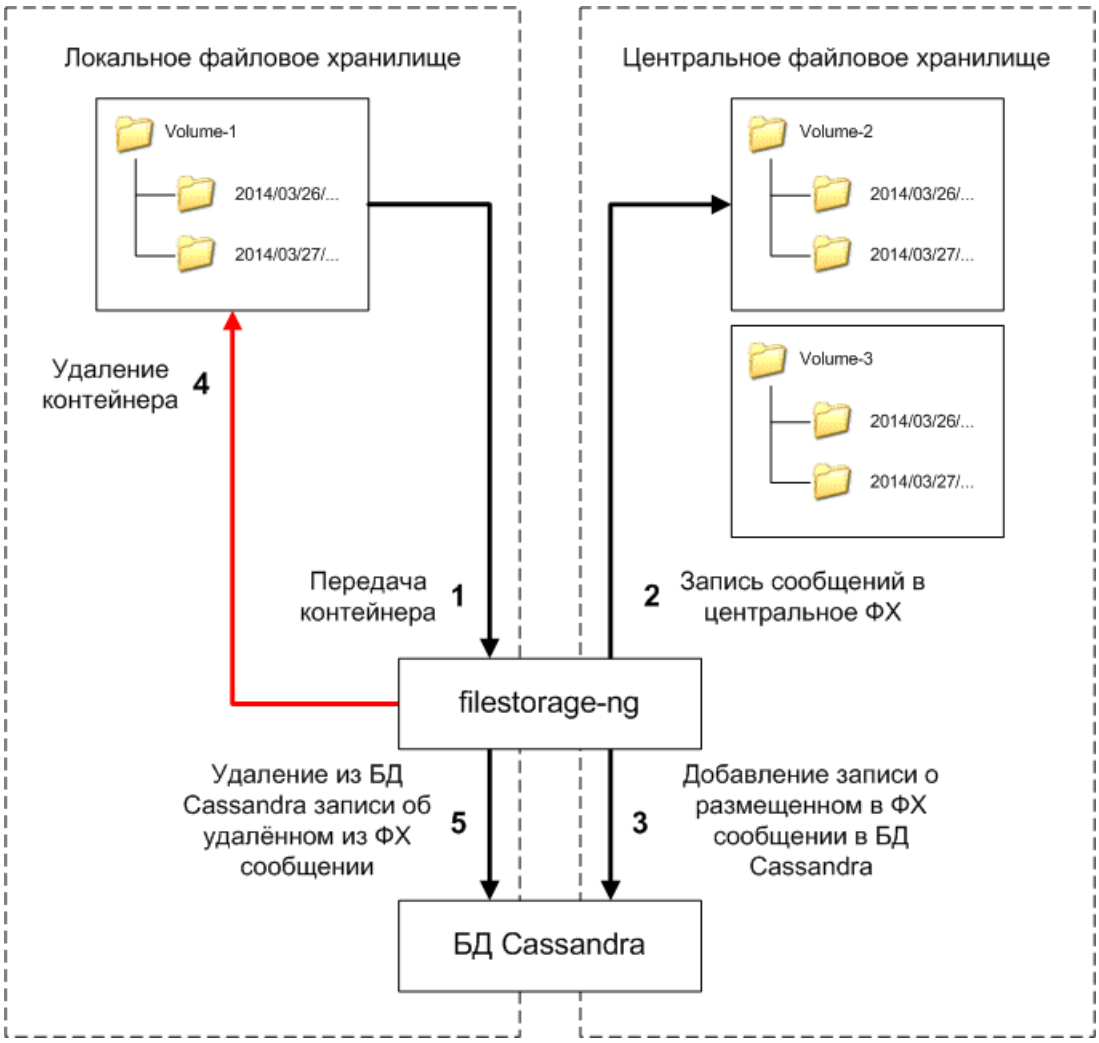


Рис. D.3. Перемещение сообщений из локального в центральное файловое хранилище

Перемещение контейнеров из локального ФХ в центральное осуществляется сервисом **filestorage-ng**, который размещает полученные из локального ФХ контейнеры с данными в центральном ФХ и добавляет записи о размещении контейнеров в базу данных **Cassandra**, после чего удаляет переданные контейнеры из локального ФХ, а затем удаляет соответствующую запись из БД **Cassandra**.

D.4. Извлечение сообщения из файлового хранилища

При обработке запроса на поиск сообщения в архиве, поступившего с АРМ администратора, происходит поиск этого сообщения в БД архива. Если выясняется, что тело сообщения хранится в ФХ, то БД архива возвращает vID искомого сообщения, после чего происходит обращение к сервису **filestorage-ng** для продолжения поиска сообщения сначала в БД **Cassandra**, а затем в ФХ.

Сервис **filestorage-ng** обращается к любому доступному узлу **Cassandra** для поиска информации о сообщении. Для этого передаётся идентификатор сообщения vID (см. Рис.D.4).

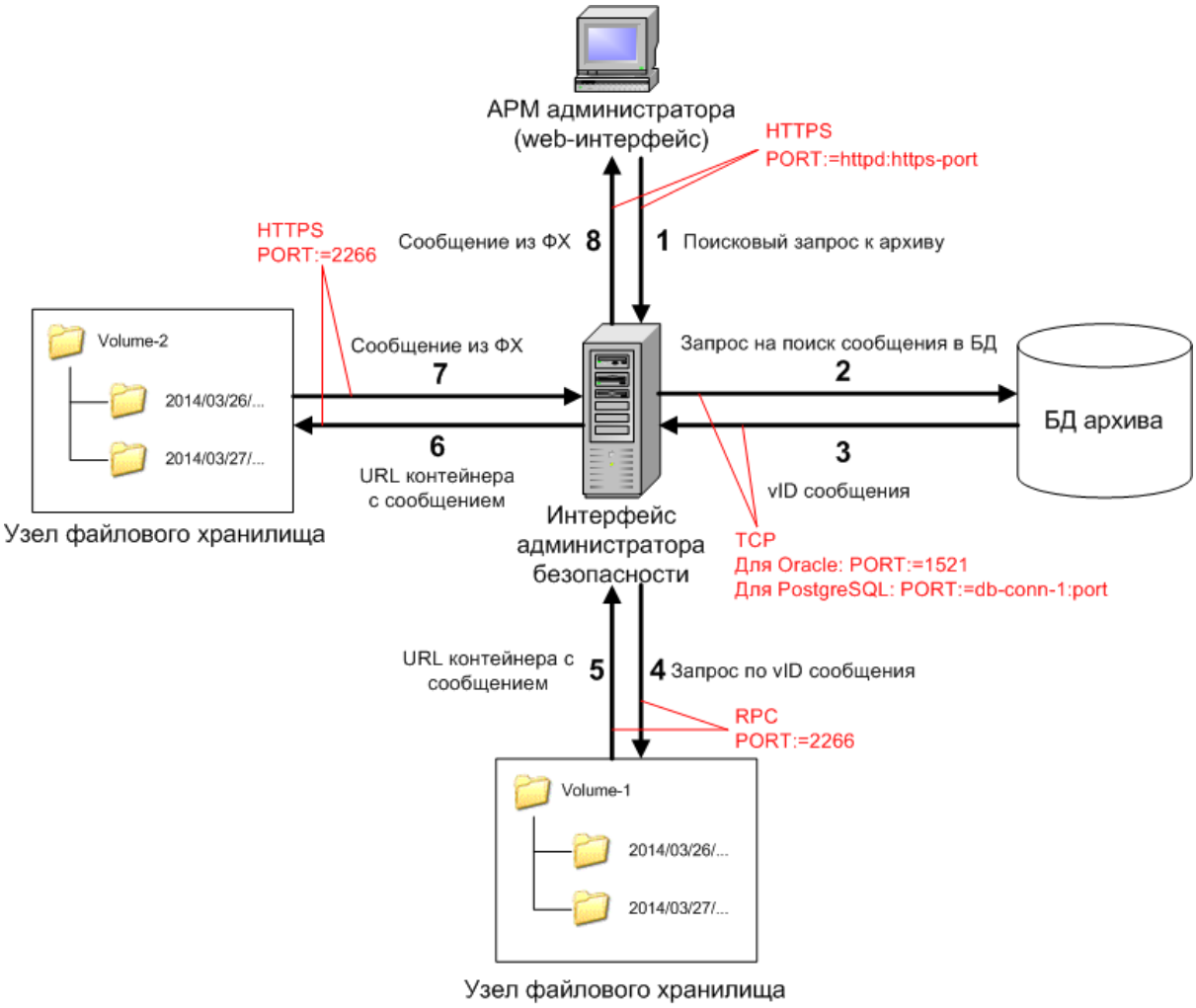


Рис. D.4. Извлечение сообщения из файлового хранилища

Если запись о сообщении не найдена, то **Cassandra** возвращает ошибку **Not found**. Если в **Cassandra** имеется запись с нужным vID, то сервису **filestorage-ng** возвращается URL контейнера с искомым сообщением. Сервис **filestorage-ng** передаёт эта данные веб-серверу.

После получения URL контейнера с телом сообщения выполняется запрос на получение файла, хранящегося по указанному URL, к сервису **filestorage-ng** на том узле, где было найдено сообщение. Сервис извлекает файл с телом сообщения и отправляет его веб-серверу. После этого веб-сервер формирует HTML-страницу с результатами поиска для просмотра найденного сообщения.

Приложение Е. Создание БД архива на удаленном сервере

Для создания БД архива на удаленном сервере следует выполнить действия:

1. Настроить схему соединения с БД архива на master-узле по инструкции в разделе 8.3.1.
2. Создать схему БД архива по инструкции в разделе 8.3.2.
3. Подключиться к БД, выполнив следующую команду:

   # psql -U dozor -h localhost -p <port>

   где **<port>** – порт, на котором БД ожидает соединения.
4. Проверить версию сервера БД PostgreSQL на master-узле. Для этого ввести следующий запрос:

   select version();

   Пример вывода команды:

   ```
   PostgreSQL 11.3 on x86_64-pc-linux-gnu, compiled by gcc (GCC) 4.8.5 20150623 (Red Hat 4.8.5-36),
    64-bit
   (1 строка)
   ```

   В данном примере сервер БД PostgreSQL имеет версию 11.3.
5. Подключиться к удаленному серверу по протоколу SSH.
6. Установить СУБД PostgreSQL версии, полученной на шаге 4.
7. Создать группу и учётную запись пользователя **dozor**, выполнив следующие команды:

   # groupadd dozor

   # useradd dozor
8. Назначить пользователю права на исполнение, выполнив команду:

   # chown dozor:dozor /data/ -R
9. Переключиться на пользователя **postgres**, выполнив команду:

   su - postgres
10. Создать учётную запись пользователя СУБД PostgreSQL. Для этого выполнить команду:

    createuser --interactive

    При появлении информации:

    ```
    Введите имя новой роли:
    ```

    ввести **dozor** и далее подтвердить полномочия суперпользователя, нажав клавишу **y**.

11. Переключиться на пользователя **root**, выполнив команды:

    $ exit

    $ su - root

12. Создать каталог, в котором будут размещаться файлы БД, например, **/data/base/remote**. Для этого выполнить команду:

    # mkdir -p /data/base/remote

13. Скопировать БД архива на удаленный сервер, выполнив команду:

    rsync -avze ssh --progress --human-readable <master>:<path> /data/base/remote

    где **<master>** – IP-адрес или FQDN master-узла, а **<path>** – каталог, в котором была создана БД (например, **/data/base/smap-archive/**).

14. Проверить наличие файлов БД архива. Для этого выполнить команду:

    # ls -la /data/base/remote

    Убедиться, что в выводе присутствует **dozor dozor**.

15. Запустить БД, выполнив команду:

    # su - dozor -c "pg_ctl -D /data/base/remote start"

16. Перейти в раздел GUI **Система > Конфигурация > Основные настройки > Доступ к данным > Схемы соединений с БД**.

17. В настройках соединения с БД изменить значение параметра **Сетевое имя сервера базы данных** на IP-адрес или FQDN удаленного сервера.

18. Проверить подключение к БД, нажав кнопку **Проверить**.

19. Нажать **Сохранить** и **Применить**.

Лист контроля версий

25/04/2024-17:27