Ростелеком
Солар

Программный комплекс «Solar Dozor»

Модуль «Dozor Endpoint Agent» (Linux)

Версия 4.2

Руководство по установке, обновлению и удалению (ОС Альт)

Москва, 2024

Содержание

Список иллюстраций

Список таблиц

Перечень сокращений

АРМ	Автоматизированное рабочее место
БД	База данных
ВМ	Виртуальная машина
ИБ	Информационная безопасность
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
EWS	Exchange Web Services – специальный протокол, разработанный Microsoft, и предназначенный для управления почтой и другими компонентами, составляющими Microsoft Exchange
HTML	HyperText Markup Language – язык гипертекстовой разметки
HTTP	HyperText Transfer Protocol – протокол передачи гипертекста
HTTPS	HyperText Transfer Protocol Secure – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
ICAP	Internet Content Adaptation Protocol – протокол адаптируемого интернет-содержимого
ICAPS	Internet Content Adaptation Protocol Secure – расширение протокола ICAP для поддержки шифрования в целях повышения безопасности
ID	Identifier – идентификатор
IMAP	Internet Message Access Protocol – протокол прикладного уровня для доступа к электронной почте
POP3	Post Office Protocol Version 3 – стандартный интернет-протокол прикладного уровня, используемый клиентами электронной почты для получения почты с удалённого сервера по TCP-соединению
SMB	Server Message Block – сетевой протокол прикладного уровня для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия
SMTP	Simple Mail Transfer Protocol – простой протокол передачи почты
SSH	Secure Shell – сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP–соединений (например, для передачи файлов)
URL	Uniform Resource Locator – стандартизированная форма записи адресов в Интернет
USB	Universal Serial Bus – последовательный интерфейс для подключения периферийных устройств к вычислительной технике
VDI	Virtual Desktop Infrastructure – инфраструктура управления виртуальными рабочими столами пользователей, которая предполагает, что каждому сотруднику выделяется виртуальная рабочая станция (виртуальная машина, ВМ) с определенным набором программ, документов и других данных, хранящихся на сервере
XML	eXtensible Markup Language – расширяемый язык разметки

Термины и определения

Агент / Endpoint Agent	Модуль контроля действий пользователей рабочих станций «Dozor Endpoint Agent»
Политика	Правила обработки, хранения и передачи информации Агентом
Конфигурация	Технические параметры работы агента
Endpoint-сервер / Сервер агентов	Сервер, предназначенный для хранения и передачи Агентам их конфигурации и политики, а также для сбора информации о состоянии Агентов
Рабочая станция	Компьютер сотрудника компании
GNOME	Свободная среда рабочего стола для UNIX-подобных операционных систем
PulseAudio	Звуковой сервер, который предоставляет возможность управлять и контролировать источники и выходы звука в системах Linux
Wayland	Протокол для организации графического сервера в Linux и других UNIX-подобных операционных системах
X.org	Свободная реализация оконной системы X с открытым исходным кодом

1. Введение

1.1. Назначение документа

Данный документ представляет собой руководство администратора и предназначен для пользователей Программного комплекса «Solar Dozor» (далее – Solar Dozor). В документе описаны требования к программному и аппаратному обеспечению, процесс подготовки рабочих станций к развертыванию модуля контроля действий пользователей рабочих станций «Dozor Endpoint Agent для ОС Linux» (далее – Endpoint Agent, EAL или Агент), а также способы установки, обновления и удаления модуля.

1.2. Комплект документации

В комплект документации на Endpoint Agent также входит документ *ПК Solar Dozor. Модуль контроля действий пользователей рабочих станций «Dozor Endpoint Agent». Руководство администратора*, который содержит подробную информацию по использованию модуля Endpoint Agent.

1.3. Уровень подготовки пользователя

Для установки, настройки и применения Агента требуются знания и навыки администрирования ОС семейства Linux, навыки администрирования Solar Dozor и умение реализовывать с его помощью корпоративную политику безопасности в части, относящейся к информационному обмену.

2. О модуле Endpoint Agent

Модуль Endpoint Agent предназначен для использования на рабочих станциях сотрудников компании с целью своевременного выявления и защиты компании от утечек конфиденциальной информации.

Агент позволяет записывать звук с микрофона и запускать видеотрансляцию экрана рабочей станции интересующей персоны; контролировать отправку сообщений и вложений по протоколу EWS, операции с буфером обмена, печать документов, копирование файлов на съемные носители и сетевые ресурсы и подключение USB-устройств на рабочих станциях пользователей.

EAL может перехватывать:

- сетевой трафик, передаваемый в соответствии с протоколом HTTP/HTTPS (так контролируются веб-почта, поисковые запросы, операции отправки файлов в облачные хранилища и на другие веб-ресурсы);
- сетевой трафик, передаваемый в соответствии с протоколами SMTP, POP3 и IMAP (контролируется входящая и исходящая переписка в клиентских приложениях электронной почты);
- мгновенные сообщения и файлы, передаваемые через мессенджеры Telegram и WhatsApp Web;
- данные, которые вводятся при помощи клавиатуры на рабочих станциях.

Агент также может собирать статистику по действиям пользователей в приложениях и сети Интернет для функции мониторинга рабочего времени.

Кроме того, можно задать политику, при которой EAL будет формировать снимки экрана рабочей станции.

3. Условия эксплуатации

3.1. Требования к аппаратному обеспечению

Для установки и эффективной работы Агента версии 4.2.0 рекомендуется следующая конфигурация рабочих станций:

- CPU – не менее 2 ядер;
- ОЗУ – не менее 4 ГБ;
- свободное место на системном разделе жесткого диска – не менее 50 ГБ.

3.2. Требования к программному обеспечению

3.2.1. Требования к ОС

Модуль Endpoint Agent представляет собой набор исполняемых и вспомогательных файлов, обеспечивающих контроль действий пользователя на рабочей станции под управлением ОС семейства Linux и информирование серверной части системы о действиях пользователей. Агент версии 4.2.0 функционирует под управлением ОС Альт Рабочая станция 10.2/К 10.2.

3.2.2. Требования к зависимостям пакета linux-agent

Для успешного развертывания Endpoint Agent на рабочей станции в системе должны быть установлены необходимые пакеты. Получить информацию об их версиях можно, выполнив соответствующие команды (см. **Табл.3.1**).

Внимание!

При отсутствии зависимостей или наличии зависимостей с устаревшими версиями установка Агента завершится с ошибками.

Табл. 3.1. Зависимости пакета linux-agent

ОС	Пример команды для вывода версий зависимостей	Список пакетов, необходимых для успешной установки Агента
Альт 10.2/К 10.2	~ rpm -qpR ./linux-agent-4.2.0.60.alt10.rpm	`ca-certificates fontconfig glib2 glibc-core glibc-pthread iptables lame libasound2 libblkid libcrypto10 libcups libcurl libevent2 libfreetype libgcc1 libgio libgtk+2 libjpeg libmagic libpcre3 libpng12 libssl10 libstdc++6 libudev1 libX11 libxcb libXdamage libXext libXfixes libXi libxml2 libXrandr logrotate net-tools NetworkManag er libnetfilter_queue nss-utils sh systemd zip zlib`

3.2.3. Требования к антивирусному ПО

Модуль Endpoint Agent совместим с модулями антивирусов, контролирующих веб-трафик – Kaspersky Endpoint Security for Linux (версия 11.2 и выше) и Dr.Web (версия 11.1 и выше).

3.3. Требования к используемым портам

Агент использует для своей работы порты 10025, 10080, 10110, 10139, 10143, 10443, 10445, 10465, 10587, 10993, 10995, 11010, 11080, 12270, 12443, 13128, 15900 и 18080.

3.4. Требования к версии Solar Dozor

Endpoint Agent версии 4.2.0 должен использоваться совместно с Solar Dozor версии 7.4 или выше.

4. Настройка взаимодействия Endpoint Agent с Solar Dozor

Основными компонентами, обеспечивающими взаимодействие EAL с Solar Dozor, являются сервер управления и сервер(ы) агентов. В обработке информации от Агентов принимают участие сервер фильтрации, сервер архивирования, почтовый фильтр, сервер архива и медиа-сервер.

Сервер агентов предназначен для хранения и передачи Агентам их настроек (конфигурации) и политик, а также для сбора информации о состоянии Агентов. Эти данные сервер агентов получает от сервера управления Solar Dozor.

Агент, установленный на рабочую станцию пользователя, соединяется с сервером агентов (по адресу, указанному при установке) и получает свои параметры настроек и политику, в соответствии с которыми во время своей работы он будет обрабатывать и отсылать перехваченные данные на сервер агентов. Сервер агентов, в свою очередь, будет передавать эти данные в виде сообщений на сервер фильтрации.

Сервер фильтрации определяет тип сообщения и передает сообщение на сервер архивирования. Сервер архивирования отправляет сообщения на сервер архива и в файловое хранилище. Состав отправляемой информации зависит от используемого профиля архивирования (подробнее о профилях архивирования описано в документе *Программный комплекс «Solar Dozor». Руководство пользователя*).

Для настройки взаимодействия Endpoint Agent с Solar Dozor необходимо выполнить следующие действия:

- назначить роль **Сервер агентов** узлу, на котором будет выполняться управление Агентами (раздел **4.1**);
- если планируется добавлять рабочие станции в группу, выбирая их из структуры каталогов 389 Directory Server, и автоматически установить на них Endpoint Agent, настроить синхронизацию с FreeIPA (раздел **4.2**);
- подготовить группу станций с конфигурацией, настройками перехвата и политикой информационной безопасности (раздел **4.3**);
- при необходимости:
  - изменить настройки конфигурации, заданные по умолчанию (раздел **4.4**);
  - создать собственный набор настроек перехвата или отредактировать существующий (раздел **4.5**);
  - создать собственный набор правил политики ИБ или отредактировать существующий (раздел **4.6**);
- связать логин учетной записи пользователя ОС Linux с карточкой персоны для удобства оперативной идентификации сотрудника в системе по ФИО (раздел **4.7**).

Примечание

Шаг не обязателен к исполнению.

4.1. Назначение роли «Сервер агентов»

Перед установкой Endpoint Agent необходимо назначить роль **Сервер агентов** узлу, на котором будет выполняться управление модулями Endpoint Agent, установленными на рабочих станциях пользователей (подробнее о назначении ролей см. в документе *Программный комплекс «Solar Dozor». Руководство по развёртыванию и установке*). Узлы с этой ролью выполняют обмен данными с Агентами по протоколу HTTPS и отправку собранных данных на почтовый шлюз Solar Dozor по протоколу SMTP.

Для корректной работы Агентов в подкластере роль **Сервер агентов** должна быть назначена одному из узлов этого подкластера. Вне подкластеров (на общих ресурсах) такая роль нужна, если Агенты функционируют на узлах, которые являются общими для компании.

Для назначения роли следует выполнить действия:

1. Перейти в раздел интерфейса **Система >Узлы и роли** (Рис.4.1).
2. В строке с нужным узлом щелкнуть мышью в поле **Роли узла** и выбрать в раскрывающемся списке роль **Сервер агентов**.
3. Применить изменения, нажав кнопку **Применить**.

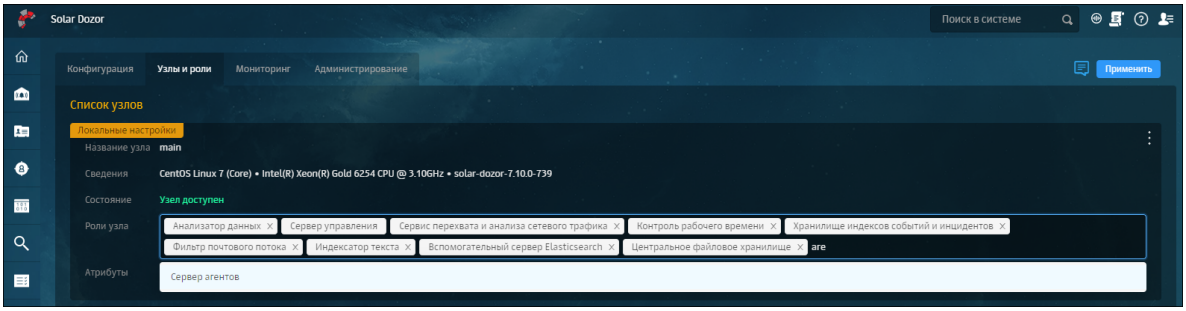

Рис. 4.1. Узлы и роли: назначение узлу роли Сервер Агентов

Если роли **Фильтр почтового потока** и **Сервер агентов** назначены разным узлам, в интерфейсе Solar Dozor следует выполнить настройку соединения с сервисом **mailfilter**. Для этого перейти в секцию **Настройки серверов Endpoint Agent** раздела **Система > Конфигурация > Расширенные настройки > Endpoint Agent** и установить значение параметра **Соединения с сервисом фильтрации сообщений** равным **Задать в виде списка**. Кроме того, для параметра **Сетевой адрес** (Рис.4.2) необходимо указать IP-адрес или имя узла с сервисом **mailfilter**.

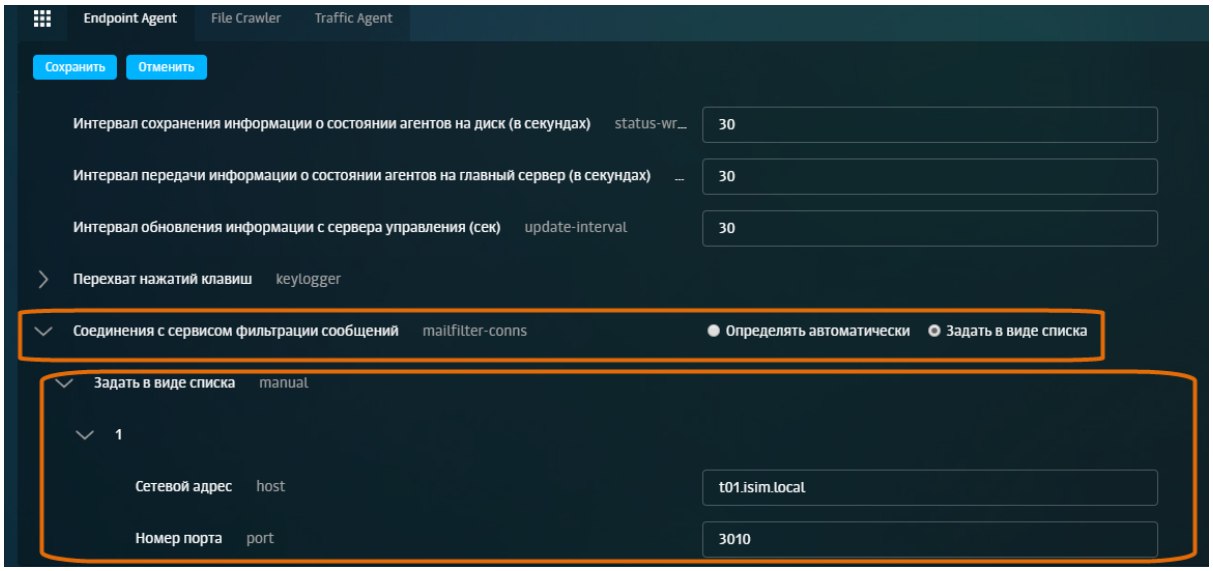

Рис. 4.2. Настройка соединений с сервисом mailfilter

4.2. Синхронизация с FreeIPA

В Solar Dozor, начиная с версии 7.9, реализована поддержка LDAP-сервера со свободной лицензией и открытым программным кодом – FreeIPA (389 Directory Server). Если планируется добавлять рабочие станции в группу, выбирая их из структуры каталогов 389 Directory Server, необходимо перейти в раздел **Система > Конфигурации > Расширенные настройки > Endpoint Agent** и в секции **Сервер управления Endpoint Agent** задать следующие параметры (Рис.4.3):

- **URL LDAP-сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например – **ldap://ldap.organization.local:389**).
- **DN пользователя** – DN учётной записи с правами чтения каталога 389 Directory Server.
- **Пароль пользователя** – пароль учётной записи, указанной в предыдущем параметре.
- **Базовый DN для поиска** – база поиска. Следует указать значение в соответствии со структурой каталогов организации.

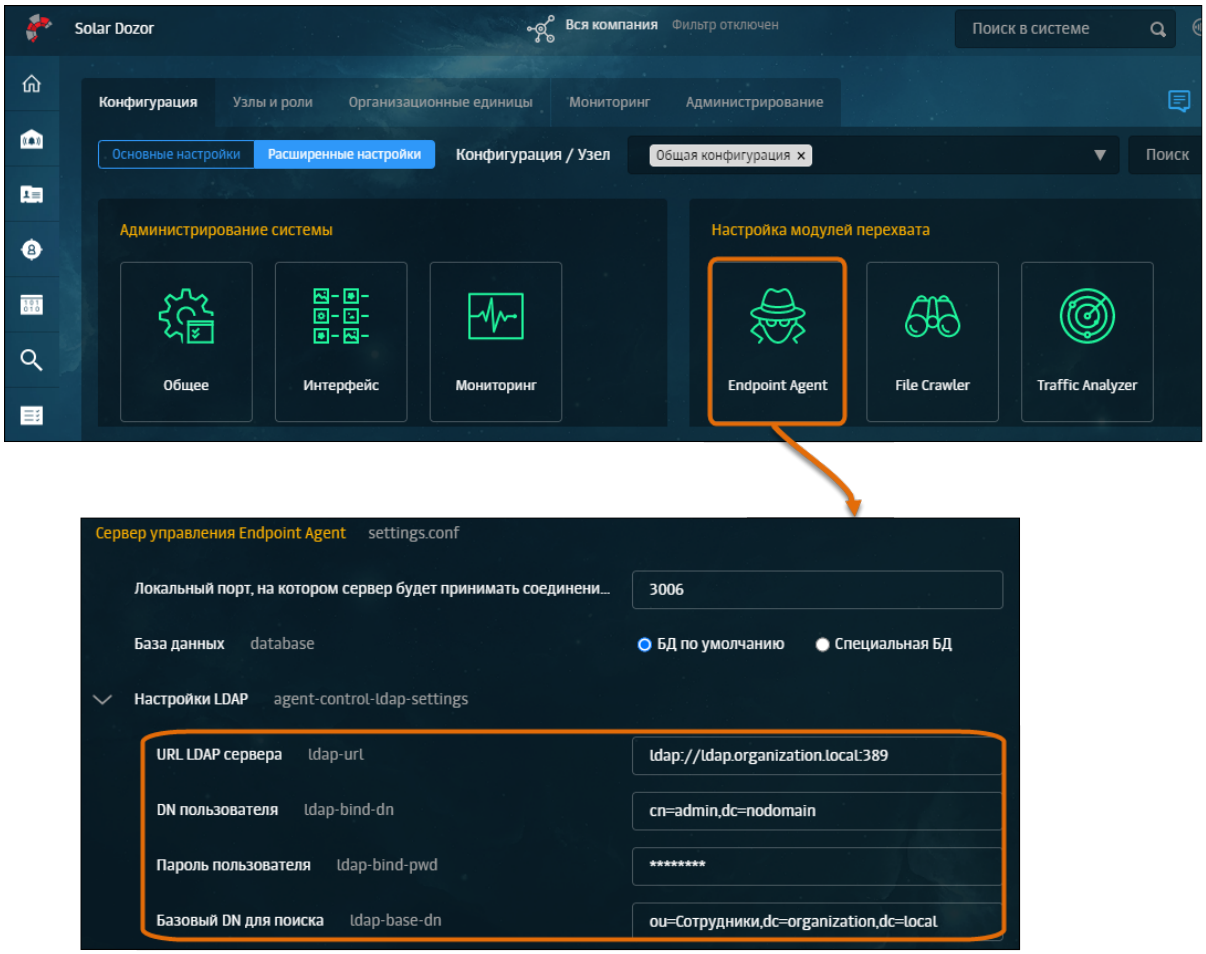

Рис. 4.3. Настройка «Сервера управления» для работы с каталогом 389 Directory Server

4.3. Подготовка группы станций

При необходимости можно создать группу станций на основе уже существующей – то есть скопировать все заданные для группы параметры и настройки. Для этого необходимо выполнить следующие действия:

1. В меню действий с разделом **Endpoint Agents > Станции > Группы станций > <Название группы станций>** выбрать пункт **Копировать**.

2. В отобразившемся окне указать название новой группы и/или выбрать другой раздел.

3. Нажать кнопку **Копировать**.

Подробную информацию о создании, копировании и удалении группы см. в документе *ПК Solar Dozor. Модуль контроля действий пользователей рабочих станций «Dozor Endpoint Agent». Руководство администратора*.

Развертывание Endpoint Agent на рабочей станции выполняется в соответствии с параметрами группы, в которой эта станция состоит. Параметры группы станций включают в себя учетные данные для аутентификации на станции, набор дистрибутивов, дату и время развертывания Агента на станциях, набор правил политики безопасности, настройки перехвата и конфигурацию.

Задание параметров выполняется в разделе **Endpoint Agents > Станции > Группы станций > <Название группы станций>**, на вкладке **Параметры**.

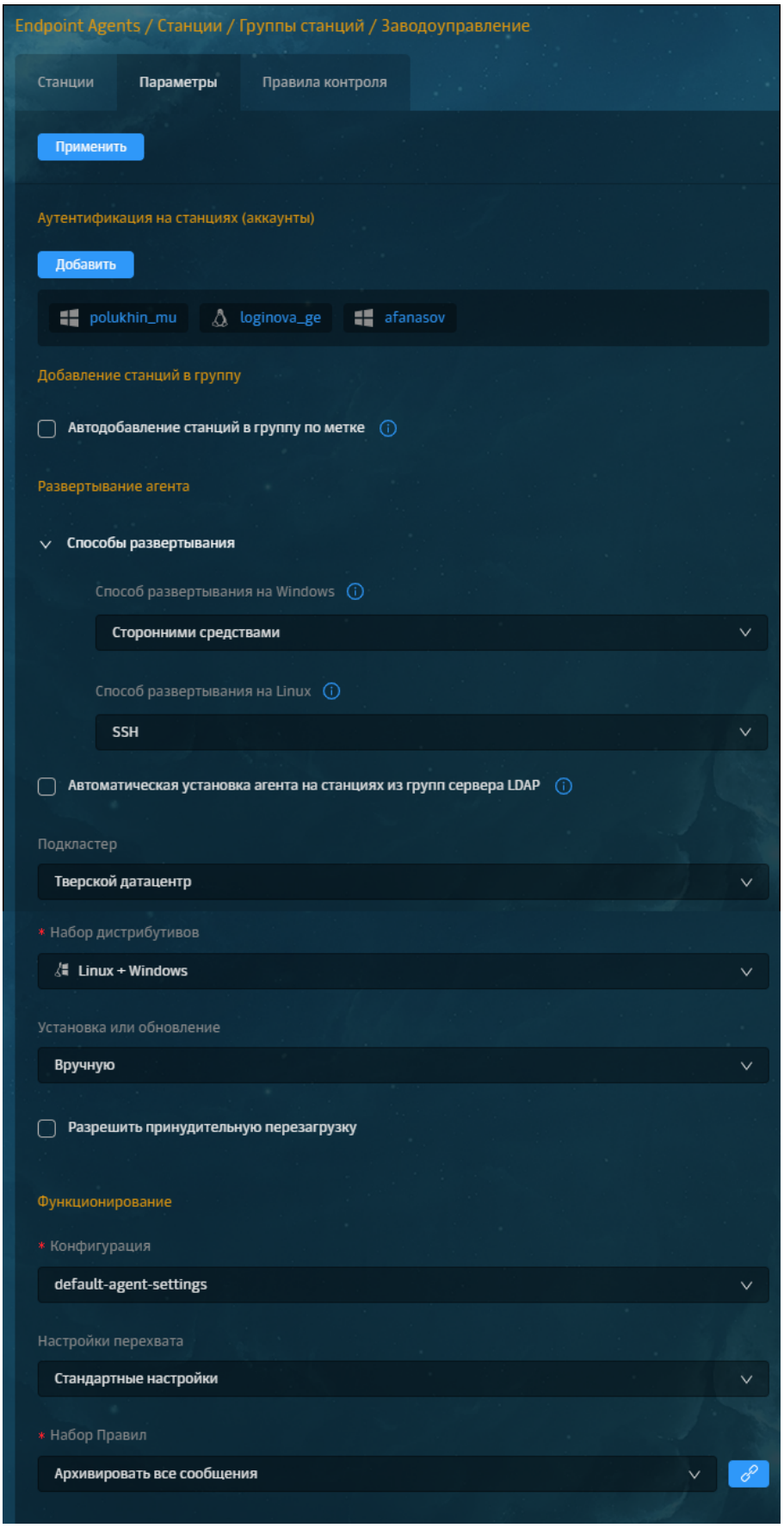

Рис. 4.4. Параметры группы станций

В секции **Аутентификация на станциях (аккаунты)** можно добавить учетную запись локального администратора с правами выполнения команды **sudo** для аутентификации на рабочей станции. Для этого:

1. Нажать кнопку **Добавить**.
2. Ввести логин/пароль учетной записи, а в поле **OS** выбрать **Linux**.
3. Нажать кнопку **Сохранить**.

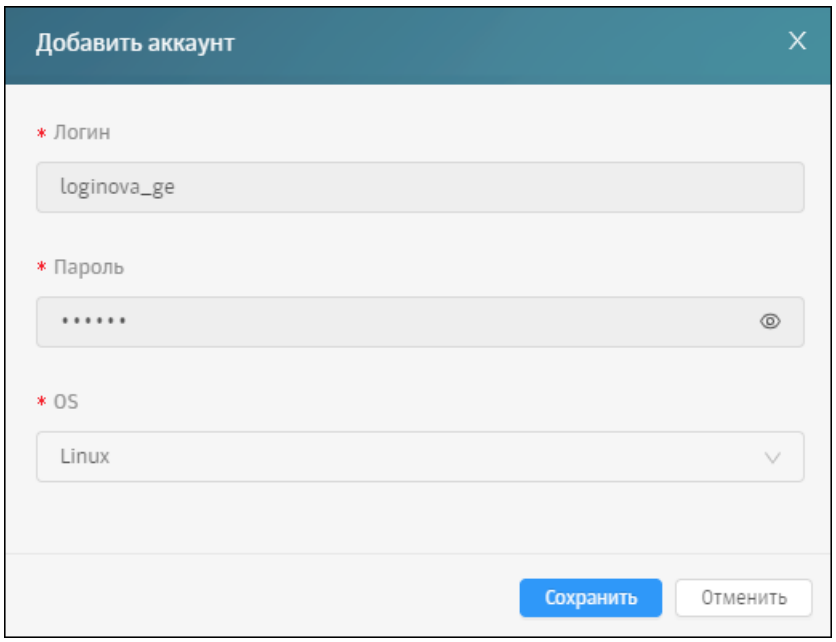

Рис. 4.5. Окно добавления учетных записей

В секции **Добавление станций в группу** расположен флажок **Автодобавление станций в группу по метке**, который включает автоматическое добавление в группу рабочих станций, на которых агент установлен сторонними средствами, например, из образа Master Image. В этом случае при подготовке Master Image устанавливается агент, ему присваивается метка (при установленном флажке доступно поле **Метка**), по которой рабочие станции, полученные из этого образа, будут автоматически добавлены в данную группу.

Примечание

При наведении курсора мыши на значок информации, расположенный справа от названия параметра, можно просмотреть подсказку с описанием функционала.

В секции **Развертывание агента** можно задать способы развертывания Агента; параметры автоматической установки на станциях из групп сервера LDAP; выбрать набор дистрибутивов для развертывания на всех станциях в группе; настроить установку и обновление Агентов по расписанию или вручную.

Раскрывающийся список **Способы развертывания** содержит параметры **Способ развертывания на Windows** и **Способ развертывания на Linux**.

Параметр **Способ развертывания на Linux** принимает значения:

- **Сторонними средствами** – функционал развертывания Агентов средствами Solar Dozor не используется. В этом случае установка Агента на рабочих станциях может быть выполнена только сторонними средствами, рекомендованными вендором.

- **SSH** – развертывание Агента из графического интерфейса Solar Dozor выполняется с использованием протокола SSH. Используется в качестве значения по умолчанию.

При территориально-распределенном режиме работы Solar Dozor в настройках группы станций отображается параметр **Подкластер**. Следует выбрать значение из списка, если Агенты должны быть развернуты на ресурсах подкластера. При развертывании Агентов на общих ресурсах значение не указывается.

Флажок **Автоматическая установка агента на станциях из групп сервера LDAP** включает автоматическое добавление станций из групп сервера LDAP (FreeIPA) в группу станций Solar Dozor. После установки флажка необходимо в открывшемся окне выбрать группы сервера LDAP, контролируемые Solar Dozor, и нажать на кнопку **Применить**. При выполнении синхронизации все станции выбранных групп LDAP будут добавляться в группу станций Solar Dozor. На всех добавленных станциях будет выполнена однократная попытка установки Агента способом, указанным в значении параметра **Способ развертывания**. При этом будет использован дистрибутив Endpoint Agent, заданный в значении параметра **Набор дистрибутивов**.

Примечание

При наведении курсора мыши на значок информации, расположенный справа от названия параметра, можно просмотреть подсказку с описанием функционала.

Примечание

При необходимости повторной установки модуля Endpoint Agent, например, в случае недоступности станции в момент установки, рекомендуется воспользоваться параметром Установка или обновление с расписанием.

Примечание

Ошибки добавления станций в группу записываются в журнал сервиса управления агентами. Ошибки установки Агента отображаются в столбцах Статус и Подстатус карточки рабочей станции.

Примечание

Период синхронизации Solar Dozor с сервером LDAP задается в часах и регулируется параметром Периодичность синхронизации списка станций, значение которого можно отредактировать в секции Сервер управления Endpoint Agent раздела Система > Конфигурация > Расширенные настройки > Настройка модулей перехвата > Endpoint Agent.

В секции **Функционирование** можно выбрать конфигурацию, настройки перехвата и набор правил политики безопасности.

Примечание

Как правило, используется конфигурация, заданная в системе по умолчанию (default-agent-settings), но при необходимости можно добавить новую конфигурацию или отредактировать настройки по умолчанию в разделе Система > Конфигурация > Расширенные настройки > Настройка модулей перехвата > Endpoint Agent, в секции Конфигурации Endpoint Agent.

4.4. Управление настройками конфигурации Endpoint Agent

Перед установкой Endpoint Agent следует проверить настройки агентов по умолчанию в интерфейсе Solar Dozor в разделе **Система > Конфигурация > Расширенные настройки > Настройка модулей перехвата > Endpoint Agent** и при необходимости скорректировать их.

Рабочая станция, планируемая для развертывания Агента через веб-интерфейс Solar Dozor, должна ожидать SSH-соединения на порту с номером 22. Если соединения принимаются на порту с другим номером, необходимо указать соответствующее значение параметра **Порт для подключения SSH-клиента**, расположенного в секции **Центр приложений Endpoint Agent**.

Внимание!

Для применения нового способа развертывания требуется Solar Dozor, начиная с версии 7.9.

Примечание

Подробное описание расширенных настроек приведено в документе ПК «Solar Dozor». Руководство системного администратора.

4.5. Управление настройками перехвата

4.5.1. Общие принципы

Наборы настроек перехвата задаются в разделе **Endpoint Agents > Настройки перехвата**.

По умолчанию в системе создаются следующие наборы настроек перехвата:

- **Настройки без перехвата** – предназначен для групп станций, на которых требуется временно остановить работу Агента. При необходимости набор можно удалить, переименовать или изменить для него настройки перехвата.

Примечание

Настройки без перехвата в интерфейсе Solar Dozor являются эталонными и неизменяемыми, и доступны только для копирования.

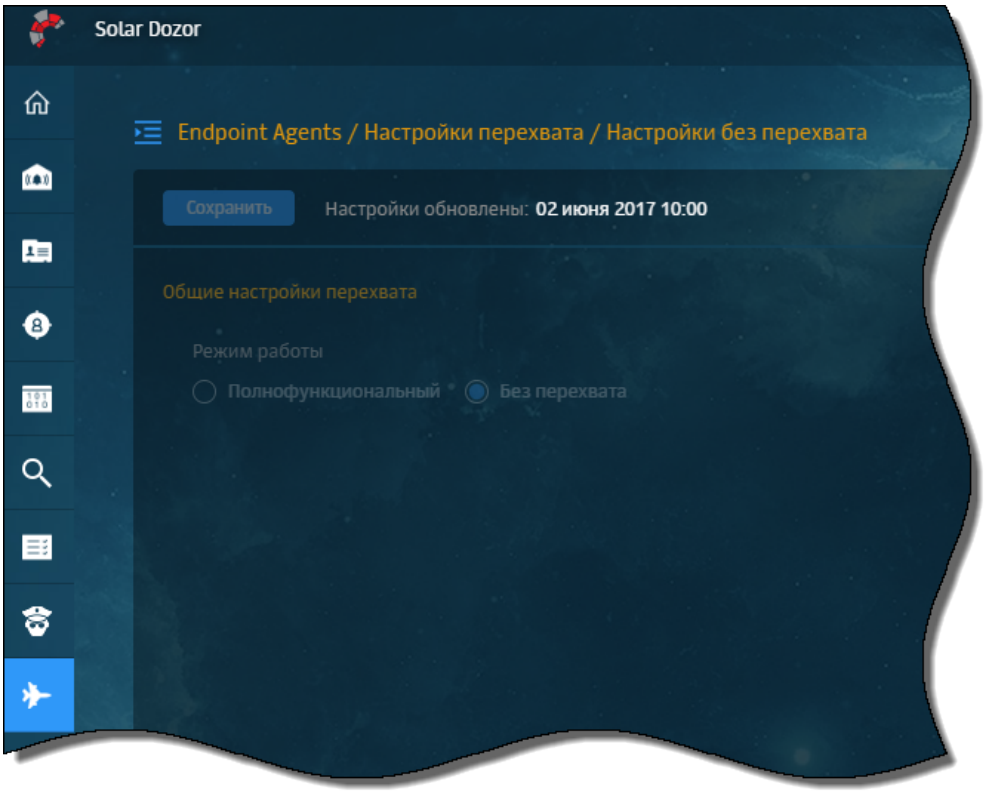

Рис. 4.6. Настройки без перехвата

- **Стандартные настройки** – включает в себя наиболее часто используемые настройки и предназначен для групп Агентов с полной функциональностью.

Примечание

Стандартные настройки перехвата Endpoint Agent в интерфейсе Solar Dozor являются эталонными и неизменяемыми, и доступны только для копирования.

Используя шаблон со стандартными настройками перехвата, можно создать новый профиль настроек, в котором задать, что и как перехватывать: установить нужные флажки и при необходимости изменить списки ресурсов, приложений и т.п. (списки поставляются вместе с системой, подробное описание справочников приведено в документе Программный комплекс«Solar Dozor». Руководство пользователя). Так, например, при установке флажков Каналы перехвата > HTTP / HTTPS / EWS Агент будет перехватывать сообщения и файлы, переданные с помощью веб-ресурсов, указанных в списке контролируемых.

Рис. 4.7. Стандартные настройки перехвата

Для создания и копирования набора настроек перехвата следует воспользоваться соответствующим пунктом меню действий в интерфейсе Solar Dozor. (**Рис.4.8**).

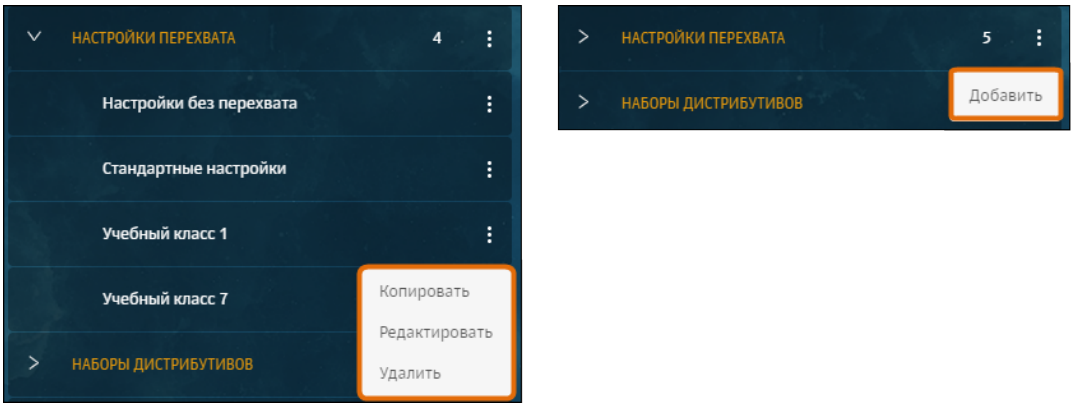

Рис. 4.8. Настройки перехвата: меню действий

Для создания нового набора настроек перехвата необходимо:

1. В меню действий с разделом **Endpoint Agents > Настройки перехвата** выбрать пункт **Добавить**.

2. В открывшемся окне указать название группы и нажать кнопку **Сохранить**.

При необходимости можно создать профиль настроек на основе уже существующего – то есть скопировать все параметры и настройки. Для этого следует:

1. В меню действий с разделом **Endpoint Agents > Настройки перехвата > <Название набора настроек>** выбрать пункт **Копировать** (см. Рис.4.8).

2. В отобразившемся окне указать название нового профиля настроек и нажать кнопку **Копировать**.

4.5.2. Описание параметров, отвечающих за перехват данных

При настройке модуля Endpoint Agent необходимо учитывать следующие параметры:

- **Список приложений, исключаемых из контроля** – приложения, у которых сетевой трафик, буфер обмена, нажатия клавиш, копирование (на съемные устройства и сетевые ресурсы) должны быть исключены из анализа и контроля. Задаются через справочник приложений.

- **Список путей и файлов, которые не требуется контролировать** – имена файлов и/или каталогов, операции с которыми/в которых не требуется контролировать. Можно указать несколько таких файлов (при необходимости - и пути к ним) и/или каталогов, разделяя их символом «|». Также можно задавать шаблоны (wildcard-маски) файлов/каталогов.

Примечание

Можно указать несколько таких файлов (при необходимости - и пути к ним) и/или каталогов, разделяя их символом «|». Также можно задавать шаблоны (wildcard-маски) файлов/каталогов. Примеры масок:

**.tmp - все файлы с расширением "tmp";*

\$|*.tmp - все служебные каталоги или все tmp-файлы.*

Рекомендованное значение:

```
*/run/user/1001/media/by-uuid-48A9-3FD4/*, *отпуск*
```

- **Контроль сетевых ресурсов** – при установленном флажке Агент фиксирует факты копирования/перемещения (по протоколу SMB) файлов на сетевые ресурсы.
- **Перехват копирования файлов на съемные носители (включая мобильные устройства)** – при установленном флажке Агент фиксирует факты копирования/перемещения файлов на съемные носители (включая мобильные устройства, только Android), а также факты считывания файлов приложениями с локального диска.

Примечание

В текущей реализации не фиксируются факты копирования на мобильные устройства, работающие по протоколу MTP. Ограничить доступ к таким устройствам можно с помощью параметра "Мобильные телефоны, смартфоны, планшеты, подключаемые по USB" в секции "Контроль подключения USB-устройств".

- **Перехват буфера обмена** – при установленном флажке Агент перехватывает все копируемые в буфер обмена данные.

Примечание:

Примечание

При наличии соответствующих правил политики можно контролировать операции с этими данными: например, заблокировать их вставку из буфера обмена.

Можно выбрать приложения, операции с которыми будут контролироваться Агентом по каналу перехвата **Буфер обмена**. Допустимые значения:

- **Все** – при выборе этого параметра Агент контролирует все приложения.
- **Все, кроме** – при выборе этого параметра Агент контролирует все приложения, кроме указанных в списке.
- **Только выбранные** – при выборе этого параметра Агент контролирует только указанные в списке приложения.

При выборе параметра **Все, кроме** или **Только выбранные** отобразится строка для ввода категории или названия приложения. Можно выбрать значение в списке или начать вводить название, при этом система выполнит поиск по справочнику.

- **Язык уведомлений пользователя** – При формировании правил для действия Агента **блокировать с уведомлением пользователя** может быть задан текст уведомления.

В данном параметре задается, на каком языке (русском или английском) пользователь получает сообщения.

- **Ограничение размера передаваемой и обрабатываемой информации** – параметры, ограничивающие передачу/обработку файлов в зависимости от их размера.

  Примечание

  Можно организовать работу так, чтобы при превышении размера вложения сообщение не передавалось в Solar Dozor, но сохранялась информация о нем. Таким образом, можно сократить нагрузку на систему.

  Секция включает параметры:

  - **Максимальный размер сообщений, передаваемых на endpoint-сервер** – определяет, будут ли проверенные по политике файлы приложены к сообщению о перехвате, которое Агент отправляет в Solar Dozor. Если суммарный размер всех проверенных файлов превышает установленное значение параметра, то к сообщению о перехвате будут прикреплены несколько файлов, которые будут проверены первыми и чей суммарный размер не больше заданного. Остальные файлы будут обозначены в сообщении о перехвате названиями.

  - **Максимальный размер сканируемых файлов** – на основании значения параметра определяется, будет ли файл обработан Агентом по правилам политики безопасности. Если размер файла больше установленного значения параметра, он не будет проверен. При значении, равном 0, ограничение отсутствует.

- **Получение структуры каталогов со съемных носителей** – при установленном переключателе Агент считывает структуру каталогов со съемных носителей информации (флеш-накопителей, карт памяти и внешних жестких дисков), подключаемых через USB-порт к рабочим станциям пользователей.

  Параметры секции:

  - **Максимальное количество файлов** – максимальное количество файлов, считываемых Агентом с одного съемного носителя. Значение по умолчанию: 100. Максимальное значение: 20000.

    Примечание

    При превышении количества файлов, указанного в данном параметре, оставшиеся файлы не считываются Агентом (например, при значении "100" 101-ый и последующие файлы не будут считываться). Если съемных носителей несколько, то ограничение по количеству считываемых файлов применяется к каждому носителю.

  - **Максимальный уровень вложенности каталогов** – максимальный уровень вложенности каталогов на съемных носителях, который будет считан Агентом. Значение по умолчанию: 5.

- **Контроль подключения USB-устройств** – при переводе переключателя **Состояние** в положение **Включено** Агент контролирует подключение USB-устройств к рабочим

станциям. Идентификаторы VID, PID и серийный номер обнаруженного Агентом устройства проверяются на соответствие записям из списков устройств. Если Агент находит USB в списках экземпляров, подключение такого устройства разрешается или блокируется в зависимости от значения параметра, и на этом проверка по спискам завершается. Если устройство не упоминается в списке экземпляров или параметр **Списки экземпляров устройств** принимает значение **Не контролировать**, Агент проверяет список моделей и т.д. Если после проверки списков производителей соответствие все еще не обнаружено, решение принимается по категории устройства.

Принимает значения:

- **Подключение экземпляров устройств** – определяет разрешения на подключение экземпляров USB-устройств к рабочим станциям.

  Принимает значения:

  - **Разрешено** – будет разрешено подключение экземпляров устройств из указанных списков экземпляров.
  - **Запрещено** – будет запрещено подключение экземпляров устройств из указанных списков экземпляров.
  - **Не контролировать** – разрешения/запреты на подключение различных экземпляров USB-устройств к рабочим станциям через списки экземпляров контролироваться не будут.

- **Подключение моделей устройств** – определяет разрешения на подключение моделей USB-устройств к рабочим станциям.

  Принимает значения:

  - **Разрешено** – будет разрешено подключение моделей устройств из указанных списков моделей.
  - **Запрещено** – будет запрещено подключение моделей устройств из указанных списков моделей.
  - **Не контролировать** – разрешения/запреты на подключение различных моделей USB-устройств к рабочим станциям через списки моделей контролироваться не будут.

- **Подключение устройств производителей** – определяет разрешения на подключение USB-устройств различных производителей к рабочим станциям.

  Принимает значения:

  - **Разрешено** – будет разрешено подключение устройств производителей из указанных списков производителей.
  - **Запрещено** – будет запрещено подключение устройств производителей из указанных списков производителей.
  - **Не контролировать** – разрешения/запреты на подключение USB-устройств различных производителей к рабочим станциям через списки производителей контролироваться не будут.

- **Подключение устройств по категориям** – при выбранном параметре можно предоставить/запретить (значения **Разрешено** и **Запрещено**) доступ к следующим категориям USB-устройств:
  - **USB флеш-накопители и картридеры**,
  - **USB внешние жесткие диски и док-станции**,
  - **USB оптические приводы (CD/DVD/BD)**,
  - **USB токены**,
  - **Сканеры, web-камеры, цифровые фотоаппараты, подключаемые по USB**,
  - **Мобильные телефоны, смартфоны, планшеты, подключаемые по USB**,
  - **Прочие USB**

- **Каналы перехвата** – при переводе переключателя **Состояние** в положение **Включено** Агент перехватывает данные на уровне базовых сетевых протоколов, в том числе с шифрованием SSL. Включенный параметр обеспечивает перехват по протоколам: HTTP(S)/Exchange Web Services/SMTP/POP3/IMAP. Для выбора конкретных протоколов, по которым требуется перехват данных, переведите переключатель **Состояние** в положение **Включено** и установите флажки рядом с названиями этих протоколов.

  При установленном флажке **HTTP/HTTPS/EWS** доступен выбор следующих параметров:

  - **Список контролируемых веб-ресурсов** – список веб-ресурсов, контролируемых Агентом.
  - **Список исключаемых процессов, трафик которых не требуется расшифровывать** – список исключаемых процессов, трафик которых не будет расшифровываться Агентом. Может содержать wildcard-выражения.
  - **Список исключаемых веб-ресурсов, трафик которых не требуется расшифровывать** – список исключаемых веб-ресурсов, трафик которых не будет расшифровываться Агентом. Может содержать wildcard-выражения.

  Внимание!

  Удаление значений по умолчанию может привести к возникновению проблем при работе приложений или нарушению доступа к отдельным веб-ресурсам.

- **Перехват печати на принтере** – при переводе переключателя **Состояние** в положение **Включено**Агент перехватывает печать на принтере. Доступен выбор параметров:
  - **Контролировать приложения** – выбор приложений, которые будут контролироваться Агентом при перехвате печати. Принимает значения:
    - **Все, кроме исключаемых из контроля** – при выборе этого значения Агент контролирует все приложения, кроме указанных в параметре **Список приложений, исключаемых из контроля**.

- **Только выбранные** – Агент контролирует только указанные в списке приложения. При выборе этого параметра отобразится строка для ввода категории или названия приложения. Можно выбрать значение в списке или начать вводить название, при этом система выполнит поиск по справочнику.

- **Прикладывать исходный файл, отправленный на печать** – включает/отключает отправку исходного файла в Solar Dozor. Допустимые значения: установлен флажок, не установлен флажок.

- **Печатать водяной знак на каждой странице** – включает/отключает печать информации о документе на каждой странице. Допустимые значения: установлен флажок, не установлен флажок.

- **Водяной знак, выводимый на печатаемую страницу** – строка текста водяного знака, выводимого на печатаемую страницу. Возможные подстановки: **${Date}** – текущая дата в формате dd.MM.yyyy; **${Time}** – текущее время в формате HH:mm:ss; **${DomainName}** – имя домена; **${HostName}** – имя рабочей станции; **${UserName}** – имя пользователя.

  Пример:

  ```
  ${Date} ${Time} Host: ${DomainName} ${HostName} User: ${UserName}
  ```

- **Прикладывать изображения напечатанных страниц** – включает/отключает запись образов напечатанных страниц.

- **Перехват мгновенных сообщений**:

  - **Перехват Instant Messaging** – включает/отключает перехват служб мгновенных сообщений. Допустимые значения: установлен флажок, не установлен флажок.

  - **Перехват звука в аудио- и видеозвонках** – включает/отключает запись звука. Допустимые значения: установлен флажок, не установлен флажок. Если флажок не установлен, то информация о факте совершенного звонка приходить не будет.

- **Мониторинг рабочего времени**:

  - **Сбор данных об активности пользователя** – включает/отключает сбор и сохранение информации об активности пользователей на рабочих станциях. Отслеживаются действия в приложениях и на вкладках браузера.

- **Создание снимков экрана** – при переводе переключателя **Состояние** в положение **Включено** Агент формирует снимки экрана через заданный интервал времени или по заданному событию (по активации окна приложения, по нажатию пользователем клавиши **Enter** в активном окне).

  - **Интервал записи снимков экрана (максимум 24 часа)** – интервал снятия снимков экрана. Рекомендованное значение: **1ч.**

  - **Запись снимков при активации окна пользователем** – включает/отключает формирование снимков при активации окна. Допустимые значения: установлен флажок, не установлен флажок.

- **Запись снимков экрана при нажатии пользователем клавиши "Ввод" в активном окне** – включает/отключает создание снимков экрана при нажатии на клавишу **Enter** в активном окне. Допустимые значения: установлен флажок, не установлен флажок.

- **Интервал снятия снимка экрана при нажатии клавиши "Ввод" (от 1 сек. до 60 сек.)** – интервал снятия снимка экрана при нажатии клавиши **Enter**. Рекомендованное значение: **3с.** Указываются значения в диапазоне от 1 до 60 с.

- **Выполнять сжатие снимков экрана** – включает/отключает сжатие снимков экрана. Допустимые значения: установлен флажок, не установлен флажок.

- **Отслеживать нажатия клавиш** – при переводе переключателя **Состояние** в положение **Включено** Агент перехватывает нажатия клавиш сотрудниками компании на рабочих станциях. Фиксируются следующие действия пользователя: ввод с клавиатуры (нажатия клавиш физической клавиатуры и экранной клавиатуры Windows, включая функциональные клавиши и их сочетание); нажатия клавиш мыши; факт снятия снимка экрана.

  - **Отслеживать приложения** – выбор приложений, которые будут контролироваться Агентом при перехвате нажатий клавиш. При выборе параметра **Все, кроме** или **Только выбранные** отобразится строка для ввода категории или названия приложения. Можно выбрать значение в списке или начать вводить название, при этом система выполнит поиск по справочнику.

  - **Контролировать действия** – выбор действий, которые будут контролироваться Агентом при перехвате нажатий клавиш:

    - **Ввод пароля архива, файла, листа** – включает/отключает перехват паролей архивов, файлов, листов документов формата **xls**.

    - **Создание снимков экрана** – включает/отключает определение попытки снятия снимка экрана.

  - **Время неактивности, после которого начнется новая запись в журнал нажатий клавиш (мин, максимум 30)** – период в минутах с момента нажатия последней клавиши, по истечении которого сформированный блок перехваченных нажатий клавиш будет отправлен в систему и начат новый блок перехватов.

- **Отправка данных по ICAP** – при переводе переключателя **Состояние** в положение **Включено** Агент преобразует данные и передает их на ICAP-сервер модуля перехвата и анализа сетевого трафика Traffic Analyzer, который используется для корректного, углубленного и более производительного анализа HTTP(S)-сессий. Таким образом, можно получить больше информации о совершенном действии, например, не только факт загрузки неправильного файла, но и псевдоним пользователя.

  - **URL для подключения по ICAP** – строка для ввода протокола, адреса и порта для подключения по ICAP. Адрес должен указываться в формате **<протокол>://<hostname или ip-адрес>:<порт>** (например, *icap://abc.solar.local:1344, icap://192.168.1.100:1344*).

4.6. Настройка политики Endpoint Agent

Для работы Endpoint Agent необходимо создать соответствующую политику в интерфейсе Solar Dozor в разделе **Политики > Политика**, т.е. задать условия и наборы правил, описывающих реакцию системы на поведение пользователей на рабочих станциях с установ-

ленным Агентом, и действий, необходимых при выполнении заданных условий (см. документ *Программный комплекс «Solar Dozor». Руководство пользователя*).

Пример набора условий и правил политики Агента приведен на **Рис.4.9**. После сохранения добавленных условий и правил необходимо применить изменения в политике безопасности, нажав кнопку **Применить политику** на вкладке редактирования любого объекта политики.

Если сообщение отвечает заданным условиям проверки, над ним могут быть выполнены следующие действия:

- **Агент: блокировать с уведомлением пользователя** – действие пользователя блокируется.
- **Агент: разрешить действие** – действие пользователя будет разрешено, а информация об событии будет отправлена на сервер. Сообщение пользователю о факте возникновения утечки данных не отображается.

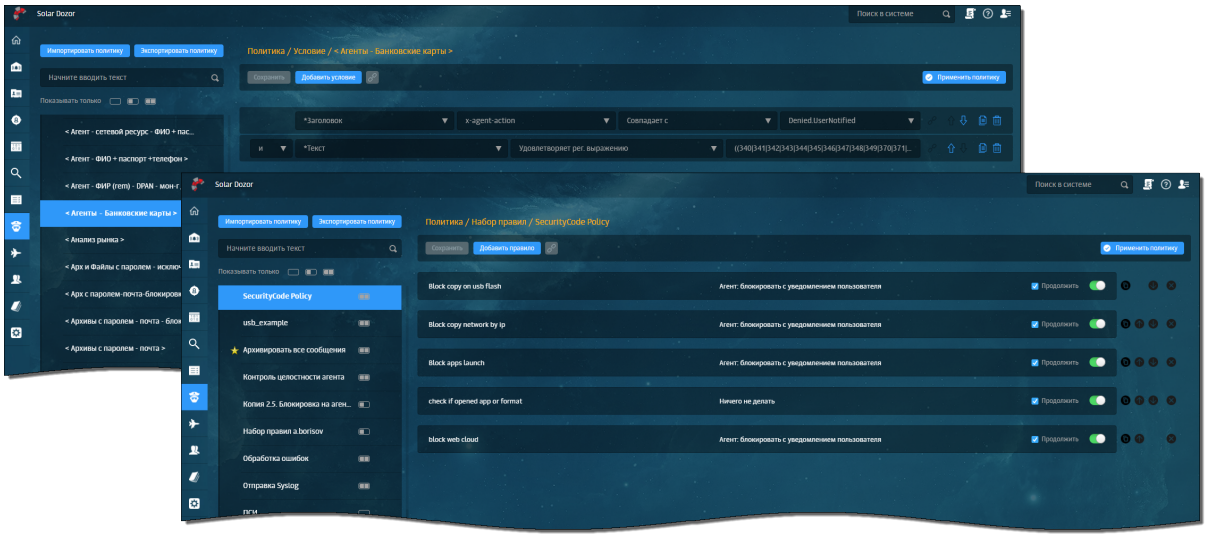

Рис. 4.9. Создание политики для агентов

4.7. Регистрация пользователя станции в Solar Dozor

Чтобы вместо логина учетной записи пользователя ОС Linux в карточке сообщения с данными перехвата отображалось ФИО сотрудника компании, следует добавить неизвестные системе данные пользователя в существующую карточку персоны, указав для атрибута **Login** имя учетной записи, под которой пользователь вошел на рабочую станцию (или создать новую карточку).

Примечание

Подробное описание создания/редактирования персоны приведено в документе ПК Solar Dozor. Руководство пользователя.

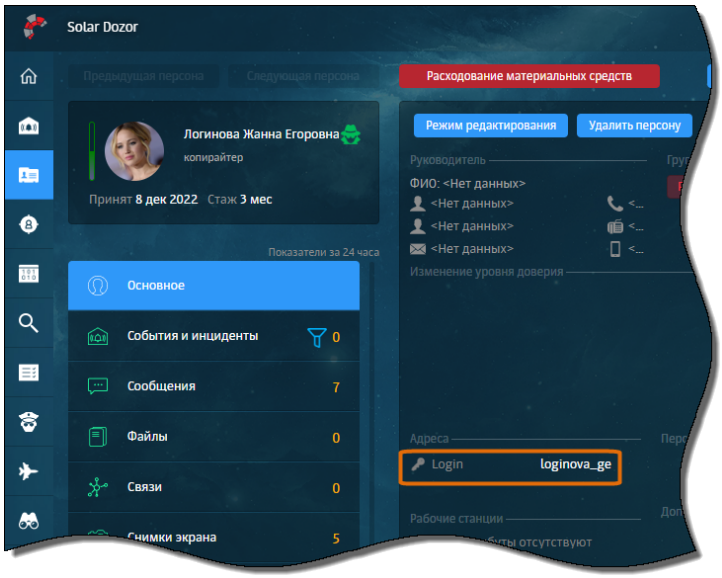

Рис. 4.10. Карточка персоны: заполненный атрибут Login

5. Установка, обновление и удаление Endpoint Agent

5.1. Сценарии установки: рекомендации

EAL может быть установлен:

- Вручную на отдельную станцию (раздел **5.3.1**) – установка выполняется с помощью пакетного менеджера.
- Централизованно из веб-интерфейса Solar Dozor, начиная с версии 7.9 (раздел **5.3.2**).

Внимание!

Установку из веб-интерфейса Solar Dozor выполнять в ОС:

- *при включенных stable-репозиториях на рабочей станции – любой минорной версии;*
- *при отключенных stable-репозиториях или включенных frozen-репозиториях (архивных) на рабочей станции – только поддерживаемой минорной версии (см. раздел 3.2.1).*

Полнофункциональная и стабильная работа Агента гарантируется только при работе пользователя АРМ в графической системе X Window System.

Примечание

Установку Агента необходимо выполнять от имени учетной записи пользователя с полномочиями администратора системы с высоким уровнем целостности. Учетные записи должны находиться в группе sudo.

Сценарии установки Endpoint Agent приведены в **Табл.5.1**.

Табл. 5.1. Способы установки Endpoint Agent: контрольный лист действий

Способ установки	Действия и ссылки на разделы
Установка с помощью пакетного менеджера	1. Выключить систему принудительного контроля доступа – раздел **5.2.1**. 2. Настроить переменную среды на станции – раздел **5.2.5**. 3. Установить Endpoint Agent – раздел **5.3.1**.
Установка с помощью веб-интерфейса Solar Dozor, начиная с версии 7.9	1. Выключить систему принудительного контроля доступа – раздел **5.2.1**. 2. Отключить вывод приветствия при доступе к станции по протоколу SSH – раздел **5.2.2**. 3. Установить lsb_release – раздел **5.2.3**. 4. Сформировать дистрибутив Агента – раздел **5.2.4**. 5. Установить Endpoint Agent – раздел **5.3.2**.

5.2. Подготовка к установке Endpoint Agent

5.2.1. 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.

Примечание

При отсутствии SELinux на рабочей станции шаги пропускаются.

5.2.2. Настройка вывода приветствия при доступе к станции по протоколу SSH

Необходимо отключить вывод приветственных сообщений при доступе к станции по протоколу SSH. Для этого следует открыть файл **/etc/bash.bashrc** и добавить в самое начало строки:

```
if    [ -z "$PS1" ]; then
    return
fi
```

После этого необходимо сохранить и закрыть файл, а затем перезапустить ОС.

5.2.3. Установка lsb_release

Необходимо проверить наличие утилиты **lsb_release** на рабочих станциях, планируемых для установки Агента. Для этого от имени пользователя **root** следует выполнить команду:

```
# lsb_release -a
```

Если в выводе присутствует информация о том, что команда не найдена, необходимо установить эту утилиту.

Внимание!

Установка утилиты обязательна. Если этого не сделать, развертывание EAL будет завершено с ошибками. При этом в истории состояний Агента появятся статусы:

```
Установка - Ошибка SSH
Установка - Ошибка загрузки дистрибутива
```

Подробное описание статусов Агента приведено в документе ПК Solar Dozor. Модуль контроля действий пользователей рабочих станций «Dozor Endpoint Agent». Руководство администратора.

5.2.3.1. Установка в ОС Альт

Для установки утилиты **lsb_release** в ОС Альт следует выполнить действия:

1. Проверить наличие доступа к стандартным репозиториям ОС, выполнив команду:

```
# apt-get update
```

2. Установить пакет утилиты **lsb_release**, выполнив команду:

```
# apt-get install /usr/bin/lsb_release
```

3. Удостовериться, что пакет установлен в системе, выполнив команду:

```
# lsb_release -a
```

5.2.4. Работа с наборами дистрибутивов

Для развертывания Endpoint Agent на рабочих станциях необходимо загрузить архив с дистрибутивом/дистрибутивами в Solar Dozor.

Дистрибутив включает в себя:

- пакеты установки Агента и их зависимости, оптимизированные под разные ОС платформы Linux;
- файл с контрольной суммой md5;
- файл **metadata.json** с указанием каталогов, в которых расположены пакеты установки Агента и их зависимости.

Для удобства развертывания и обновления Агентов в группе станций все дистрибутивы объединяются в наборы. Состав и назначение набора дистрибутивов определяется администратором по своему усмотрению. Например, можно назначить набор дистрибутивов группе станций, на которых требуется переустановить Агента при нарушении целостности его компонентов.

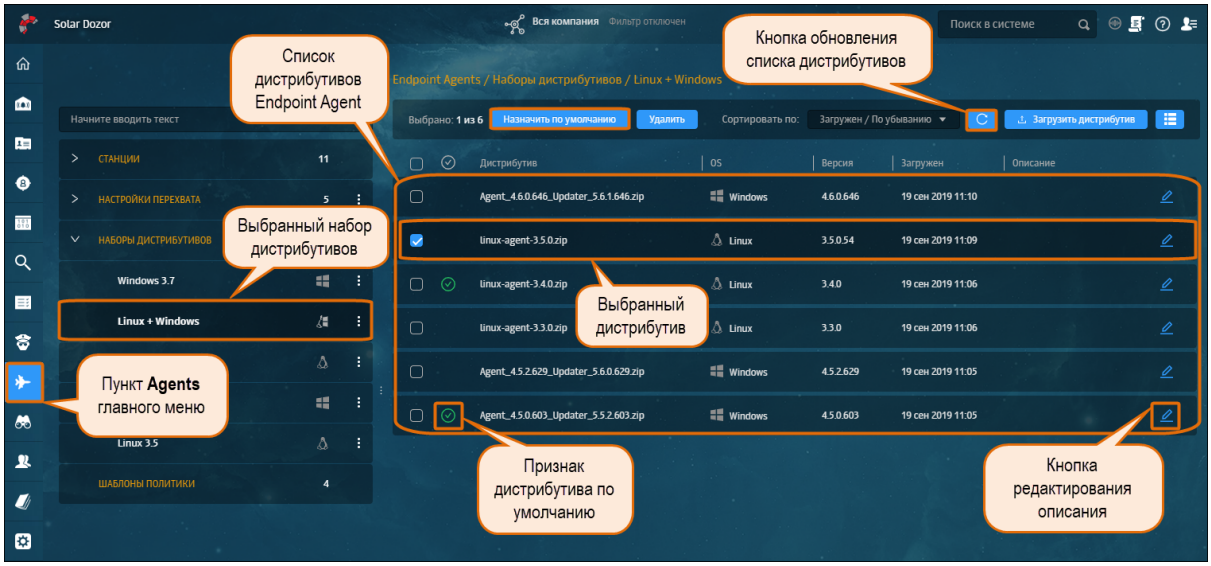

Рис. 5.1. Веб-интерфейс Solar Dozor: работа с наборами дистрибутивов

При переходе в раздел конкретного набора дистрибутивов отобразится таблица со следующими столбцами:

- столбец, в котором отображается признак дистрибутива, по умолчанию предназначенного для развертывания Агентов в группе рабочих станций. Первый загруженный в набор дистрибутив автоматически назначается дистрибутивом по умолчанию, рядом с его названием отображается значок . Если в набор добавлено несколько дистрибутивов, можно указать, какой из них будет использоваться по умолчанию. Для этого следует установить флажок в строке с названием дистрибутива и нажать **Назначить по умолчанию**.

  Примечание

  Для каждого типа ОС может быть только 1 дистрибутив по умолчанию.

- **OS** – тип ОС, на которой функционирует Агент. Допустимые значения: **Linux** и **Windows**.
- **Версия** – версия Агента в составе дистрибутива.
- **Загружен** – дата и время загрузки дистрибутива в систему.
- **Описание** – дополнительная информация о наборе, например, задачи, для решения которых был настроен набор.

Можно выбрать отображаемые столбцы таблицы. Для этого необходимо нажать кнопку , установить флажки рядом с требуемыми столбцами и нажать кнопку **Сохранить**.

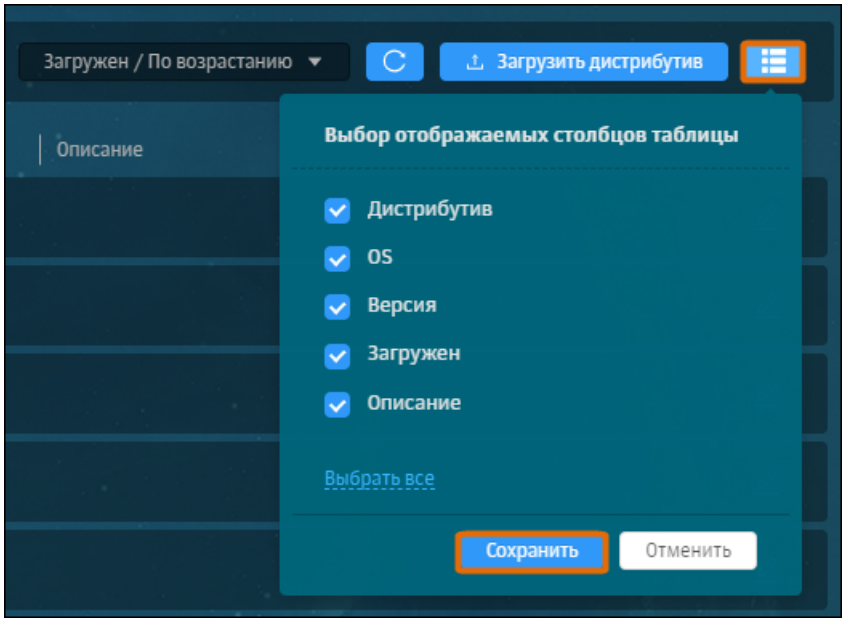

Рис. 5.2. Выбор отображаемых столбцов таблицы

Список дистрибутивов можно отсортировать по возрастанию/убыванию версии дистрибутива или даты и времени загрузки дистрибутива в систему. Для этого в раскрывающемся списке **Сортировать по** следует выбрать требуемое значение.

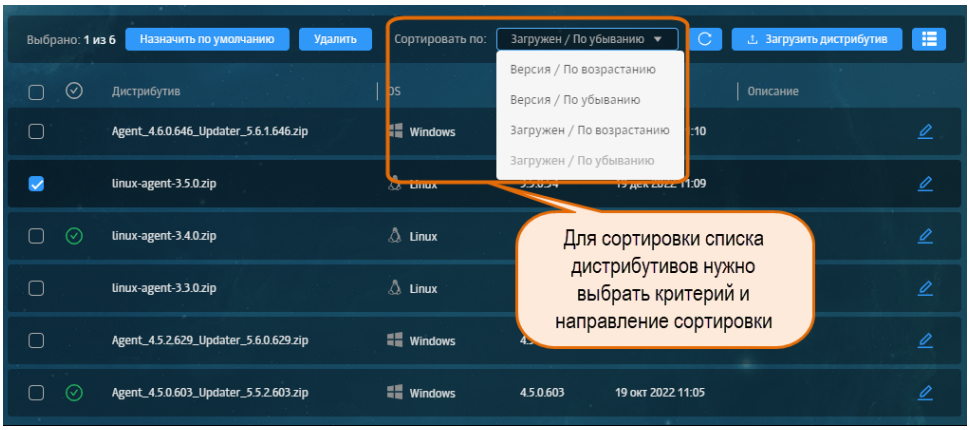

Рис. 5.3. Сортировка списка дистрибутивов

После загрузки дистрибутивов в набор система автоматически проверяет его состав и определяет тип ОС. По результатам проверки в строке отображается индикатор типа ОС:

- Windows ( );
- Linux ( );
- Linux и Windows ( ).

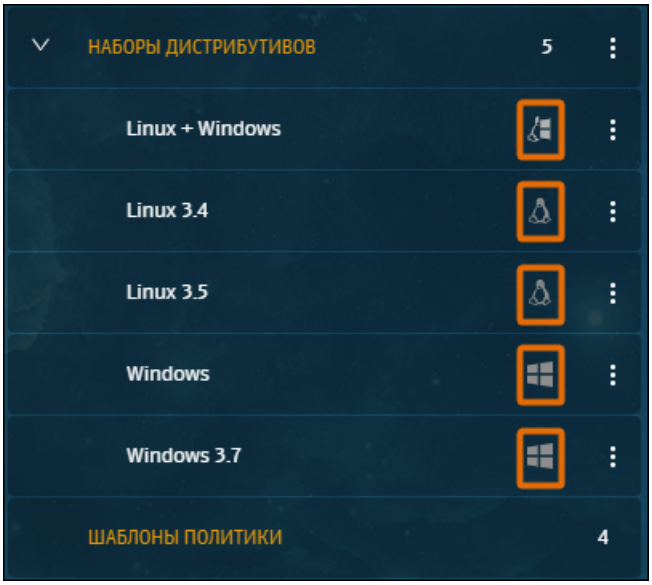

Рис. 5.4. Виды индикаторов, обозначающих типы ОС

Для добавления/переименования/удаления набора дистрибутивов можно воспользоваться соответствующим пунктом меню действий с требуемым объектом.

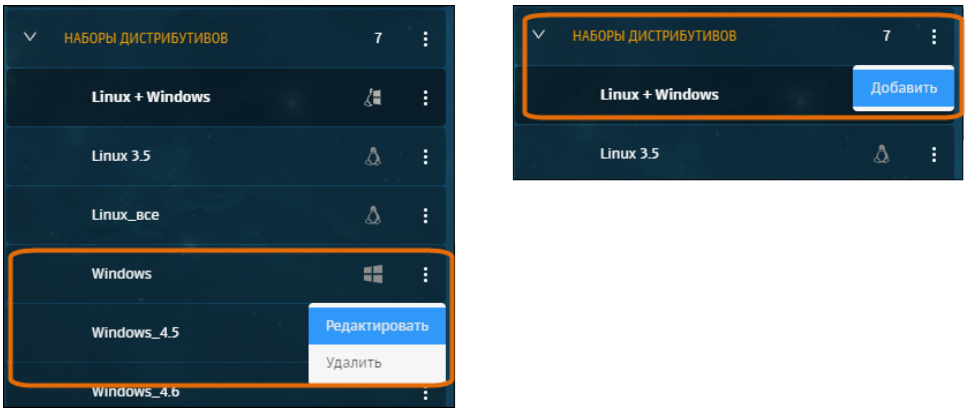

Рис. 5.5. Меню действий с наборами дистрибутивов

Для добавления нового набора дистрибутивов следует выполнить действия:

1. В меню действий с разделом **Endpoint Agents > Наборы дистрибутивов** выбрать пункт **Добавить**.

2. В открывшемся диалоговом окне указать название нового набора и нажать кнопку **Сохранить**.

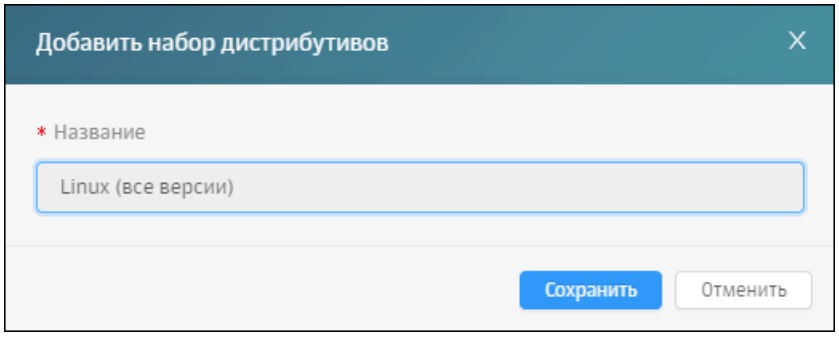

Рис. 5.6. Окно добавления набора дистрибутивов

Чтобы загрузить дистрибутив в набор, необходимо выбрать требуемый набор, нажать кнопку **Загрузить дистрибутив** и в открывшемся стандартном диалоговом окне выбрать ZIP-архив с дистрибутивом Агента.

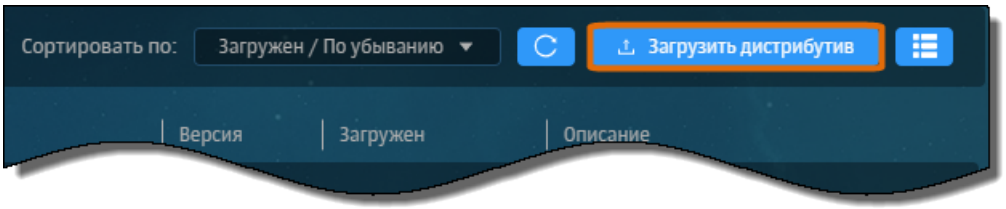

Рис. 5.7. Кнопка загрузки дистрибутива в набор

Для переименования набора дистрибутивов:

1. В меню действий с разделом **Endpoint Agents > Наборы дистрибутивов > <Имя набора>** выбрать пункт **Редактировать**.

2. В открывшемся диалоговом окне указать новое название и нажать кнопку **Сохранить**.

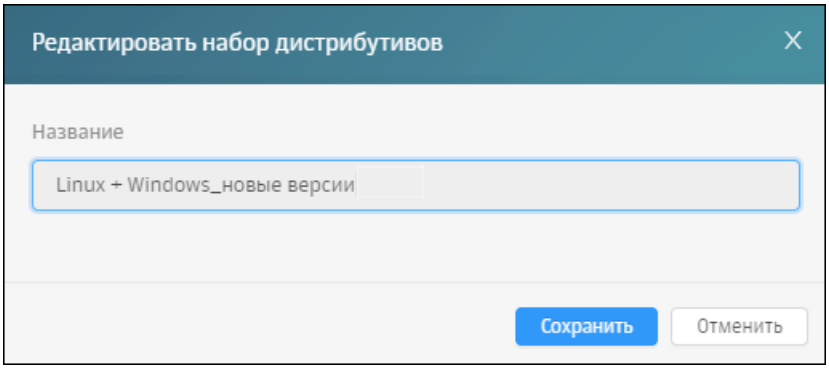

Рис. 5.8. Окно редактирования набора дистрибутивов

Для удаления набора дистрибутивов:

1. В меню действий с разделом **Endpoint Agents > Наборы дистрибутивов > <Имя набора>** выбрать пункт **Удалить**.

2. В открывшемся окне подтвердить операцию, нажав кнопку **Да**.

5.2.5. Подготовка к установке с помощью пакетного менеджера

Перед установкой Агента на отдельную станцию с помощью пакетного менеджера необходимо скопировать установочный пакет Агента на рабочую станцию пользователя и определить переменную среды **AGENT_SERVER_HOSTS**, указав в ней адрес/адреса одного/нескольких серверов Агентов, которые потребуются в процессе установки. Переменная среды задается следующей командой:

```
~$ export AGENT_SERVER_HOSTS=https://<сервер>:<порт>
```
– в случае одного сервера Агентов

или

```
~$ export AGENT_SERVER_HOSTS=https://<сервер1>:<порт>, https://<сервер2>:<порт> ... https://<серверN>:<порт>
```
– в случае нескольких серверов Агентов

Примеры:

```
~$ export AGENT_SERVER_HOSTS=https://123.4.5.6:4444,
https://123.4.5.7:4444
```

Внимание!

Если планируется создание "золотого образа" системы с установленным Агентом (Master Image) в инфраструктуре VDI, после определения переменной AGENT_SERVER_HOSTS выполнить команду:

```
~$ export AGENT_VM_FLAG=true && export
AGENT_GROUP_HINT="GROUP_HINT_VAL"
```

где GROUP_HINT_VAL – значение метки. Пример:

```
LeVT7UFCC9uIYUo9DVq2CO5W-8PvbEftWYNccF
```

5.3. Установка Endpoint Agent

5.3.1. Установка с помощью пакетного менеджера

Для установки Агента с помощью пакетного менеджера используются команды, описанные в Табл.5.2. В зависимости от операционной системы команды установки и имена пакетов Агента могут отличаться.

Табл. 5.2. Команды установки Агента

ОС	Пример команды
Альт РС 10.2/К 10.2	~$ sudo -E apt-get install /tmp/eal/linux-agent-4.2.0.60.alt10.rpm

5.3.2. Централизованная установка Endpoint Agent из веб-интерфейса Solar Dozor

Для установки Endpoint Agent из веб-интерфейса ПК «Solar Dozor» необходимо выполнить следующие шаги:

1. В разделе **Endpoint Agents > Наборы дистрибутивов** создать новый набор дистрибутивов и загрузить архив с дистрибутивом (см. раздел 5.2.4).

2. Перейти в раздел **Endpoint Agents > Группы станций** и создать новую группу станций (см. раздел 4.3). Добавить в группу станции, на которые требуется установить Endpoint Agent.

3. Задать параметры для созданной группы станций. Для этого выбрать группу станций, перейти на вкладку **Параметры** и выполнить действия:

   a. В секции **Аутентификация на станциях (аккаунты)** задать параметры аутентификации на рабочей станции.

   b. Проверить, что в секции **Развертывание агента** для параметра **Способ развертывания на Linux** задано значение **SSH**. Оставить снятым флажок **Разрешить автодобавление станций в группу**. Выбрать набор дистрибутивов для развертывания на всех станциях, добавленных в группу. Указать параметры обновления, задать дату и время, согласно которым будет выполняться автоматическое обновление Агентов.

   c. В секции **Функционирование** выбрать конфигурацию (как правило, **default-agent-settings**), набор настроек перехвата и политику.

   d. Нажать кнопку **Применить**.

4. Применить настройки политики безопасности, нажав кнопку **Применить политику** на вкладке редактирования любого объекта политики фильтрации (Рис.5.9).

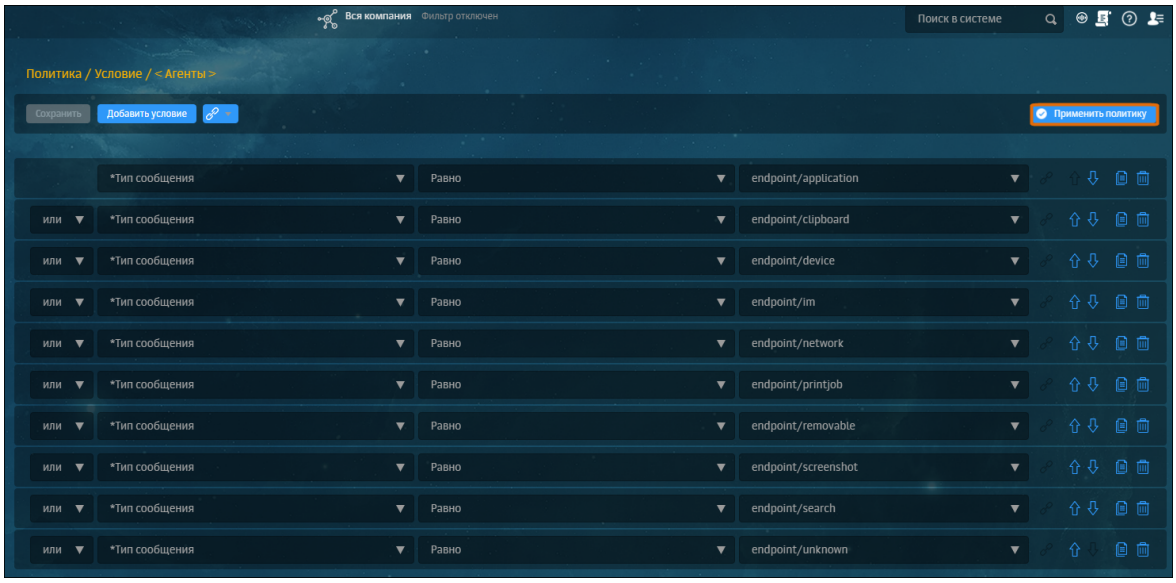

Рис. 5.9. Применение политики

После этого каждый агент в группе будет получать конфигурацию и набор правил, соответствующие группе.

5. Если в параметрах группы было задано развертывание вручную, перейти в группу станций, отметить флажком требуемые станции и нажать **Установить/Обновить** (**Рис.5.10**).

6. В появившемся окне подтвердить операцию, нажав кнопку **Да**.

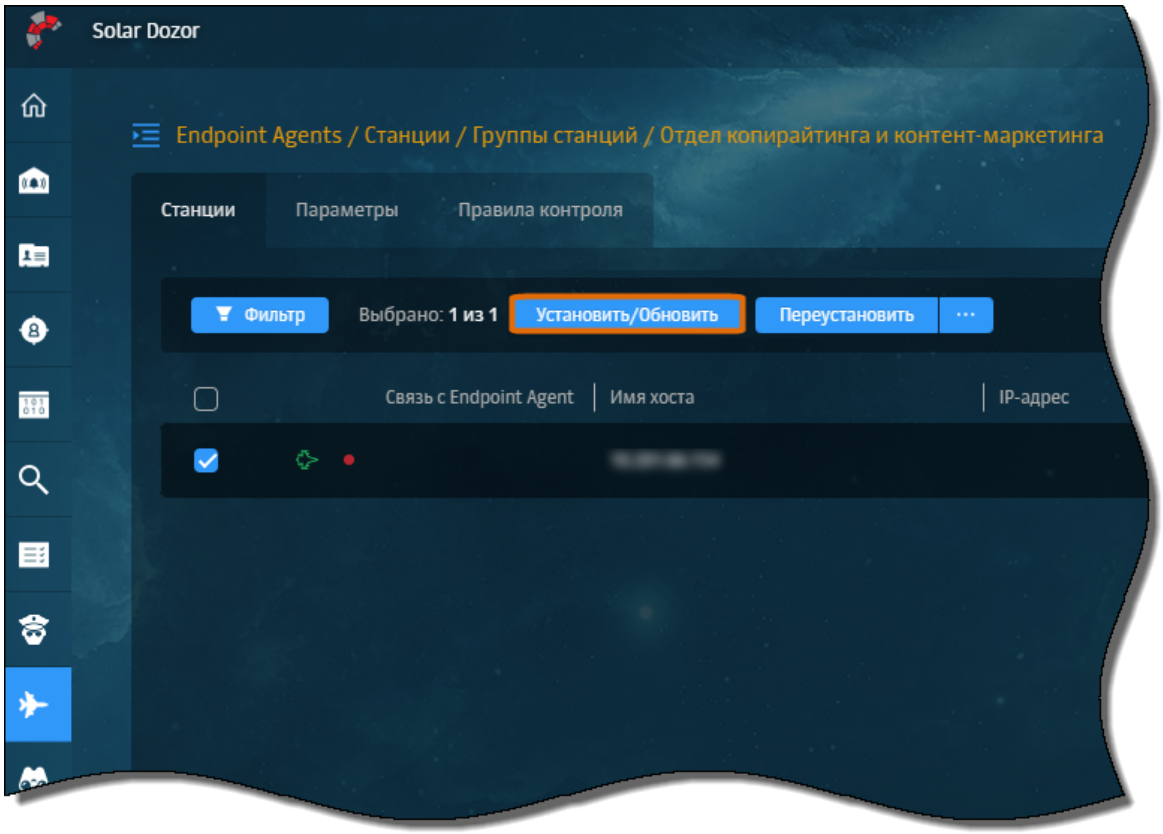

Рис. 5.10. Пример запуска развертывания Endpoint Agent в Solar Dozor

После выполненных действий начнется процедура развертывания Агента, на экране появится сообщение: **Выполняется подготовка к развертыванию Endpoint Agent. Это может занять некоторое время**.

5.4. Обновление Endpoint Agent

Необходимо выполнять обновление только тем способом, которым был установлен модуль Endpoint Agent.

Сценарии обновления Endpoint Agent приведены в Табл.5.3.

Табл. 5.3. Способы обновления Endpoint Agent: контрольный лист действий

Способ установки	Действия и ссылки на разделы
Обновление с помощью пакетного менеджера	1. Удалить Endpoint Agent предыдущей версии – раздел 5.5.1. 2. Настроить переменную среды на станции – раздел 5.2.5. 3. Установить Endpoint Agent актуальной версии – раздел 5.3.1.
Обновление с помощью веб-интерфейса Solar Dozor	1. Подготовить рабочую станцию к установке Агента – раздел 5.2.3. 2. Обновить Endpoint Agent – раздел 5.4.1

5.4.1. Обновление Endpoint Agent с помощью веб-интерфейса Solar Dozor

Для обновления Endpoint Agent с предыдущих версий следует выполнить действия:

1. В интерфейсе Solar Dozor в разделе **Endpoint Agents > Группы станций** выбрать группу станций для обновления.

2. Загрузить дистрибутив с новой версией Агента в набор, заданный для выбранной группы станций, назначить его дистрибутивом по умолчанию (подробнее о наборах дистрибутивов см. раздел 5.2.4).

3. Если в параметрах группы станций было задано развертывание вручную, перейти в группу станций, отметить флажком нужные станции и в меню действий выбрать пункт **Переустановить** (Рис.5.11).

4. Подтвердить операцию, нажав кнопку **Да**.

   После выполненных действий начнется процедура развертывания Агента, на экране появится сообщение: **Выполняется подготовка к развертыванию Endpoint Agent. Это может занять некоторое время.**

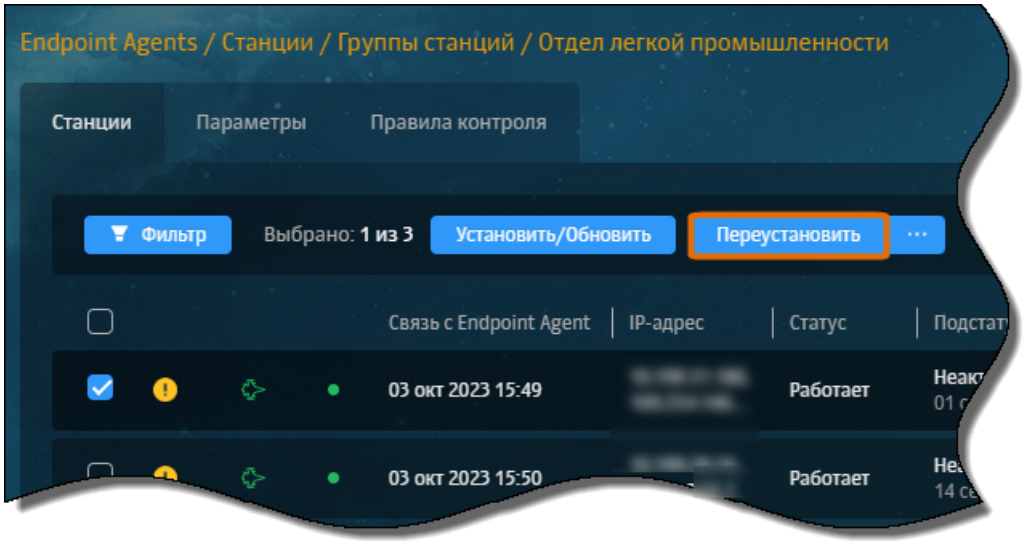

Рис. 5.11. Пример запуска обновления Endpoint Agent в Solar Dozor

Если в параметрах группы станций было задано развертывание по расписанию, Агент будет обновлен на всех станциях автоматически согласно расписанию.

5.5. Удаление Endpoint Agent

Необходимо выполнять удаление только тем способом, которым был установлен модуль Endpoint Agent.

5.5.1. Удаление с помощью пакетного менеджера

Для удаления Агента с помощью пакетного менеджера предназначены команды из Табл.5.4.

Табл. 5.4. Команды удаления Агента

ОС	Команда
Альт	~$ sudo apt-get remove linux-agent

5.5.2. Удаление Endpoint Agent с помощью веб-интерфейса Solar Dozor

Для удаления Endpoint Agent необходимо выполнить следующие действия:

1. Перейти в раздел **Endpoint Agents > Станции**, отметить флажком требуемую станцию с Агентом и в меню действий выбрать пункт **Деинсталлировать**.

2. Подтвердить операцию, нажав кнопку **Да**.

После выполненных действий начнется процедура развертывания Агента, на экране появится сообщение: **Выполняется подготовка к удалению Endpoint Agent. Это может занять некоторое время.**

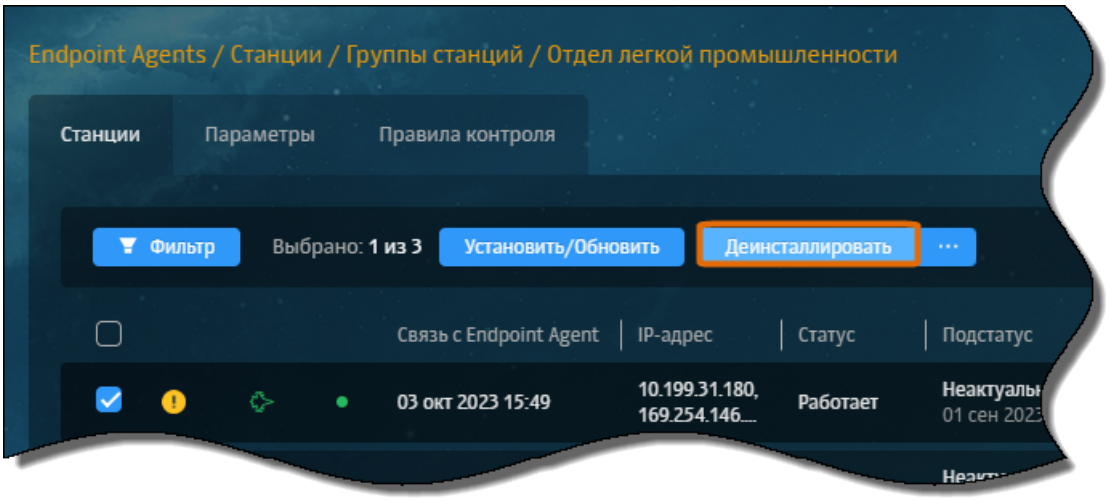

Рис. 5.12. Удаление Агента в Solar Dozor

Лист контроля версий

25/04/2024-13:58