



Программный комплекс «Solar webProxy»

Версия 4.3.1

Руководство по установке и настройке

Москва, 2025

Содержание

Перечень терминов и сокращений	10
Использование стилей	12
1. Введение	13
1.1. Область применения	13
1.2. Краткое описание возможностей	13
1.3. Уровень подготовки системного администратора	13
1.4. Перечень эксплуатационной документации для ознакомления	14
2. Назначение и возможности Solar webProxy	15
2.1. Назначение Solar webProxy	15
2.2. Состав Solar webProxy	15
2.3. Схемы подключения Solar webProxy	20
3. Требования к программному и аппаратному обеспечению	22
3.1. Требования к АРМ системного администратора	22
3.2. Требования к серверу	23
3.2.1. Алгоритм расчета сайзинга	23
3.2.2. Требования к программному обеспечению	29
3.2.3. Требования к конфигурации ОС	29
3.2.4. Рекомендации по разделению дисков в ОС при установке Solar webProxy	29
3.2.5. Рекомендации по размещению в сетевой инфраструктуре	29
3.2.6. Требования к паролю	29
4. Установка и удаление Solar webProxy	32
4.1. Установка ОС Astra 1.7.6, 1.7.7	32
4.2. Подготовка к установке Solar webProxy	57
4.2.1. Настройка DNS	57
4.2.2. Настройка синхронизации времени	58
4.2.3. Проверка и настройка БД Clickhouse (инструкции sse4_2)	59
4.3. Установка Solar webProxy	59
4.3.1. Отключение службы управления межсетевым экранированием	60
4.4. Обновление Solar webProxy	60
4.5. Удаление Solar webProxy	62
5. Первоначальная настройка Solar webProxy	63
5.1. Настройка кластера	63
5.2. Первый вход в систему и загрузка лицензии	64
5.3. Подключение к модулю MultiProxy	68
5.4. Управление настройками системы	69
5.5. Назначение ролей	75
5.5.1. Назначение ролей	75
5.5.2. Рекомендации по назначению ролей	78
5.6. Статическая маршрутизация	78
5.7. Настройка ротации журналов доступа	81
5.8. Настройка синхронизации Досье	81
5.8.1. Синхронизация с внешним источником	81
5.8.2. Синхронизация с внешним источником по протоколу LDAP	82
5.8.3. Синхронизация с внешним источником по протоколу LDAPS	85
5.8.4. Синхронизация с FreeIPA	90
5.8.5. Синхронизация с ALD Pro	92
5.8.6. Синхронизация со сторонним Досье	93
5.9. Настройка аутентификации	94
5.9.1. Общие сведения	94

5.9.2. Настройка аутентификации по IP-адресам	96
5.9.3. Настройка аутентификации Negotiate	96
5.9.4. Настройка NTLM-аутентификации	102
5.9.5. Настройка прозрачной аутентификации	104
5.9.6. Настройка basic-аутентификации	108
5.10. Настройка аутентификации SOCKS5	116
5.10.1. Настройка прокси-сервера SOCKS5 при Kerberos-аутентификации	116
5.10.2. Настройка прокси-сервера SOCKS5 при доступе без аутентификации	118
5.10.3. Настройка прокси-сервера SOCKS5 при парольной аутентификации	118
5.11. Настройка вскрытия SSL-трафика	119
5.11.1. Настройка вскрытия SSL-трафика (MITM, RSA)	119
5.11.2. Настройка вскрытия SSL-трафика (MITM, ECDSA)	125
5.12. Настройка вскрытия шифрованного трафика	131
5.13. Контентное кэширование	133
5.14. Настройка WCCP	135
5.14.1. Настройка оборудования Cisco	135
5.14.2. Настройка оборудования Solar webProxy	137
5.14.3. Проверка работоспособности WCCP	137
5.15. Настройка стороннего ICAP-прокси	138
5.16. Настройка баз категоризаторов	138
5.16.1. Используемые в системе категоризаторы	138
5.16.2. Настройка категоризатора webCAT	140
5.16.3. База Solar TI Feeds	141
5.16.4. База SkyDNS	142
5.16.5. База Blue Coat	146
6. Антивирус	148
6.1. Настройка антивируса	148
6.2. Формирование политики для работы антивируса	150
7. Отказоустойчивость и балансировка трафика	152
7.1. Общие сведения	152
7.2. Настройка балансировки подключений пользователей	152
7.3. Настройка балансировки антивируса	154
7.4. Настройка балансировки соединений по протоколу SOCKS5	156
7.5. Настройка отказоустойчивости (VRRP)	157
7.6. Отказоустойчивость сервиса балансировки	159
7.7. Настройка уведомлений от сервера мониторинга	160
8. Обратный прокси	161
8.1. Основные настройки	161
8.2. Создание сертификата для обратного прокси-сервера	164
8.2.1. Конвертация сертификатов в формат PEM	166
8.3. Просмотр статистики по работе обратного прокси	167
9. Дополнительные настройки Solar webProxy	168
9.1. Настройка сервиса skvt-wizor	168
9.2. Настройка журналирования сообщений сервисов skvt-wizor и skvt-play-server	168
9.2.1. Настройка журналирования сообщений сервиса skvt-wizor в файл syslog-ng	168
9.2.2. Настройка журналирования сообщений сервиса skvt-play-server в syslog-ng	171

9.2.3. Настройка журналирования сообщений сервисов skvt-wizor и skvt-play-server в файл	171
9.2.4. Остановка записи данных syslog в файл messages	172
9.3. Настройка принудительного использования HTTPS	172
9.4. Настройка сервиса igmproxy	173
10. Сопровождение Solar webProxy	175
10.1. Управление сервисами	175
10.2. Использование скриптов	176
10.2.1. Использование скриптов для получения информации о работе системы	176
10.2.2. Запуск скриптов из веб-интерфейса	177
10.2.3. Использование скрипта user-tool	178
10.3. Резервное копирование Solar webProxy	179
10.3.1. Общие сведения	179
10.3.2. Резервное копирование данных	180
10.3.3. Восстановление зарезервированных данных	181
10.3.4. Плановое резервное копирование	182
10.4. Просмотр журнальных файлов Solar webProxy	182
10.5. Настройки журналирования	184
10.6. Управление кластером	184
10.6.1. Регистрация узла в кластере	184
10.6.2. Управление структурой кластера	186
10.6.3. Диагностика кластера Cassandra	188
10.6.4. Удаление узла из кластера Cassandra	189
10.7. Изменение доменного имени	192
11. Настройка авторизации в веб-интерфейсе с учетной записью в домене	195
12. Выпуск сертификата организации для веб-интерфейса	196
13. Настройка передачи информации в пользовательский сервер Zabbix	202
14. Мониторинг системы	204
14.1. Состояние узлов кластера	204
14.2. Мониторинг показателей Solar webProxy	204
14.3. Мониторинг показателей аппаратного обеспечения	205
14.4. Подробные данные	206
14.5. Журналы событий: просмотр записей журнальных файлов в интерфейсе	207
14.6. Просмотр сетевых соединений	209
15. Проверка работоспособности настроенного Solar webProxy	211
16. Аварийные ситуации	212
16.1. БД Clickhouse	212
17. Получение технической поддержки	214
Приложение А. Коды фильтрации политики	215
Приложение В. Матрица МЭ Solar webProxy	216
Приложение С. Отчет об ошибках: утилита bug-report	219
Приложение D. Справочник MIME-типов	221
D.1. Краткое описание стандарта MIME	221
D.2. Описание MIME-типов	223
D.3. Язык описания регулярных выражений	235
Приложение Е. Аудит действий пользователей Solar webProxy	236
Приложение F. Описание назначения и форматов сообщений Solar webProxy	238
F.1. Файлы access-log	238
F.2. Файлы audit-log	241
Приложение G. API Solar webProxy	244

G.1. Конфигурирование API Solar webProxy	244
G.2. Работа со справочниками и объектами политик с помощью API Solar webProxy	244
Лист контроля версий	246

Список иллюстраций

2.1. Схема работы при подключении в разрыв потока	20
2.2. Схема работы при подключении в обратном режиме	21
3.1. Настройки сложности пароля	31
3.2. Настройка параметров входа в систему	31
4.1. Окно приветствия	32
4.2. Окно Лицензия	33
4.3. Настройка клавиатуры	33
4.4. Настройка сети	34
4.5. Окно Настройка учётных записей	34
4.6. Создание пароля для учетной записи администратора	35
4.7. Окно Разметка дисков	36
4.8. Выбор области для разметки	37
4.9. Создание таблицы разделов	37
4.10. Выбор пространства для создания разделов	38
4.11. Выбор варианта для создания раздела	38
4.12. Задание размера раздела	39
4.13. Выбор типа раздела	39
4.14. Выбор местоположения раздела	40
4.15. Параметры монтирования раздела	40
4.16. Выбор типа раздела	41
4.17. Выбор варианта использования раздела	42
4.18. Пункт настройки менеджера логических томов	42
4.19. Создание группы томов для LVM	43
4.20. Ввод имени группы томов	43
4.21. Выбор устройства для размещения группы томов	44
4.22. Задание имени логического тома root	44
4.23. Выделение размера для логического тома root	45
4.24. Разметка дисков для master-узла	46
4.25. Разметка дисков для slave-узла	46
4.26. Настройки тома root	47
4.27. Выбор файловой системы	48
4.28. Выбор точки монтирования	48
4.29. Заполненные настройки тома root	49
4.30. Заполненные настройки томов для master-узла	50
4.31. Заполненные настройки томов для slave-узла	50
4.32. Предупреждение об отсутствии разделов для пространства подкачки	51
4.33. Информация о разметке дисков	51
4.34. Выбор ядра	52
4.35. Выбор программного обеспечения	53
4.36. Выбор уровня защищенности	53
4.37. Дополнительные настройки ОС	54
5.1. Уведомление об отсутствии лицензии	65
5.2. Окно с информацией о лицензии	65
5.3. Вкладка «Настройки» раздела «Досье»	69
5.4. Вкладка «Настройки» раздела «Политика»	70
5.5. Раздел «Система > Основные настройки»	71
5.6. Раздел «Система > Расширенные настройки»	72
5.7. Поиск по конфигурации	72
5.8. Кнопки «Сохранить» и «Отменить»	72
5.9. Кнопка «Применить»	73

5.10. Подсказка с описанием параметра	73
5.11. Отображение подсказок	74
5.12. Выбор узла	74
5.13. Индикаторы индивидуальных настроек в списке узлов	75
5.14. Индикаторы индивидуальных настроек для выбранного узла	75
5.15. Использовать локальные настройки	75
5.16. Назначение и снятие ролей узла	76
5.17. Настройка синхронизации Досье	83
5.18. Управление шаблонами сертификатов	86
5.19. Создание копии шаблона сертификата	86
5.20. Переименование и публикация шаблона сертификата	87
5.21. Сохранение шаблона сертификата	87
5.22. Выбор сертификата для генерации	88
5.23. Выбор типа сертификата LDAPoverSSL	88
5.24. Запрос нового сертификата	89
5.25. Выпуск сертификата	89
5.26. Kerberos-аутентификация	99
5.27. Блокировка всего транзитного трафика	106
5.28. Параметры настройки веб-сервера	106
5.29. Настройка basic- + LDAP-аутентификации	109
5.30. Настройка basic- + LDAPS-аутентификации	110
5.31. Настройки basic-аутентификации с RADIUS-сервером	112
5.32. Настройки сервера Active Directory	113
5.33. Настройка аутентификации basic + IMAP	114
5.34. Настройка аутентификации basic + POP3	115
5.35. Экран приветствия УЦ Windows	121
5.36. Экран запроса сертификата	121
5.37. Экран особого запроса сертификата	121
5.38. Экран атрибутов сертификата	122
5.39. Экран выдачи сертификата	122
5.40. Экран приветствия УЦ Windows	123
5.41. Выбор центра сертификации	129
5.42. Создание правила в слое политики «Вскрытие HTTPS»	132
5.43. Добавление прокси-сервера	134
5.44. Добавление правила контентной фильтрации в слое "Маршрутизация соединений"	135
5.45. Настройки категоризатора веб-ресурсов и источника фидов	139
5.46. Схема подключения БД SkyDNS	142
6.1. Правило для перенаправления трафика антивирусу	151
7.1. Схема балансировки трафика Solar webProxy	152
7.2. Настройка балансировщика HAProxy	154
7.3. Гибкая настройка балансировки	154
7.4. Параметры настройки антивируса	155
7.5. Настройки ICAP-сервера для балансировки антивируса	155
7.6. Настройка балансировки трафика по протоколу SOCKS5	157
7.7. Схема работы Solar webProxy при использовании VRRP	158
7.8. Настройка отказоустойчивости	159
7.9. Настройка отказоустойчивости	159
7.10. Настройка отправки уведомлений от сервера мониторинга	160
8.1. Параметры настройки обратного прокси	162
8.2. Несколько публикуемых ресурсов	164
8.3. Статистика по работе обратного прокси на Рабочем столе	167

8.4. Мониторинг работы обратного прокси в Журнале запросов	167
9.1. Выбор формата записи журнала	169
9.2. Журналировать действия пользователей в messages	171
10.1. Запуск скриптов из веб-интерфейса	178
11.1. Настройки сервера Active Directory	195
12.1. Экран приветствия УЦ Windows	198
12.2. Экран запроса сертификата	198
12.3. Экран особого запроса сертификата	198
12.4. Экран атрибутов сертификата	199
12.5. Экран выдачи сертификата	199
12.6. Экран приветствия УЦ Windows	200
14.1. Вкладка «Состояние»	204
14.2. Вкладка «Подробные данные»	206
14.3. Выбор показателей для построения отчетов	207
14.4. Журнал событий	207
14.5. Фильтры журнала событий	208
14.6. Поиск по тексту в журнале событий	209
14.7. Таблица сетевых соединений	210
14.8. Фильтры таблицы сетевых соединений	210
16.1. Штатная работа БД Clickhouse	212
16.2. Работа БД Clickhouse с ошибками, указывающими на превышение лимита памяти	212

Список таблиц

2.1. Сервисы, используемые Solar webProxy	15
2.2. Дополнительные порты, используемые в работе Solar webProxy	19
3.1. Производительность ОС Astra Linux	23
3.2. Количество RPS по площадкам (HTTP)	24
3.3. Количество RPS по площадкам (HTTPS)	24
3.4. Количество пользователей по площадкам	25
3.5. Среднее количество запросов на пользователя в секунду (RPS)	25
3.6. RPS на систему в секунду	26
3.7. Итоговое количество серверов в базовом варианте	26
3.8. Итоговый сайзинг (виртуальные серверы)	27
3.9. Итоговый сайзинг (физические серверы)	28
5.1. Модули Solar webProxy в составе стандартной поставки	66
5.2. Дополнительные модули Solar webProxy	67
5.3. Группы основных настроек	70
5.4. Перечень ролей	76
5.5. Режимы аутентификации	95
9.1. Описание полей сообщений в формате access-log	169
9.2. Описание полей сообщений в формате siem-log	170
9.3. Описание полей сообщений в формате ip-translation-log	171
10.1. Команды для утилиты dsctl	175
10.2. Скрипты для сопровождения работы системы	176
10.3. Уровни детализации информации журнальных файлов	182
10.4. Уровни детализации информации	183
10.5. Перечень общих ключей	186
10.6. Перечень действий	187
14.1. Блоки данных вкладки "Показатели узлов"	205
14.2. Группа графиков выбранного узла	205
15.1. Проверки работоспособности системы	211
A.1. HTTP-коды фильтрации	215
B.1. Перечень сетей	216
B.2. Общая матрица доступов для explicit-прокси	216
C.1. Информация отчета об ошибках: bug-report	219
D.1. Типы содержимого	222
D.2. MIME-типы, относящиеся к типу файлов «Служебные файлы»	223
D.3. MIME-типы, относящиеся к типу файлов «Информационные технологии»	225
D.4. MIME-типы, относящиеся к типу файлов «Графика»	226
D.5. MIME-типы, относящиеся к типу файлов «Документы»	228
D.6. MIME-типы, относящиеся к типу файлов «Мультимедиа»	231
D.7. MIME-типы, относящиеся к типу файлов «Бизнес»	233
D.8. MIME-типы, относящиеся к типу файлов «Неопределенный тип файлов»	234
D.9. Описание метасимволов	235
E.1. Описание действий	236
F.1. Общие параметры файлов access-log	238
F.2. Общие параметры файлов audit.log	242
G.1. Методы при работе со словарями политики	245

Перечень терминов и сокращений

АРМ	Автоматизированное рабочее место
БД	База данных
ОС	Операционная система
ПО	Программное обеспечение
ПК	Программный комплекс
ИБ	Информационная безопасность
КА	Контентный анализ
Кластер	Совокупность серверов Solar webProxy, соединенных между собой управляющими связями
МЭ	Межсетевой экран
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр
ЭЦП	Электронная цифровая подпись
CLI	Command Line Interface — интерфейс командной строки
CSR	Certificate Signing Request — запрос на подпись сертификата
CRL	Certificate Revocation List — список отозванных сертификатов
DC	Domain controller — контроллер домена
DNAT	Destination Network Address Translation — скрытие IP-адреса назначения запроса пользователя путем преобразования адреса назначения в IP-заголовке пакета
FAQ	Frequently asked questions — «часто задаваемые вопросы», справка с полезной информацией
GUI	Graphical User Interface — графический интерфейс пользователя
FQDN	Fully Qualified Domain Name — полное имя домена (имя домена, не имеющее неоднозначностей в определении)
MIME	Multipurpose Internet Mail Extension — многоцелевое расширение интернет-почты
MITM	Man-In-The-Middle — атака «человек посередине», при которой злоумышленник тайно ретранслирует и при необходимости модифицирует данные между двумя сторонами
NAT	Network Address Translation — преобразование сетевых адресов
OWA	Outlook Web Access — веб-интерфейс почтового сервиса Microsoft Exchange
RFC	Request for Comments — спецификации и стандарты, применяемые в интернете
SMTP	Simple Mail Transfer Protocol — простой протокол передачи почты
SNAT	Source Network Address Translation — технология трансляции сетевых адресов, которая заключается в объединении компьютеров в мелкие локальные сети, каждой из которых присвоен единый IP-адрес

VRRP	Virtual Router Redundancy Protocol — сетевой протокол, предназначенный для увеличения доступности маршрутизаторов, выполняющих роль шлюза по умолчанию
ZIP	Формат архивации файлов и сжатия данных без потерь

Использование стилей

Шрифт без форматирования	Основной текст
Моноширинный шрифт	Пользовательский ввод
Рамка	Программный вывод на экран
<i>Курсивный шрифт</i>	Наименования документов
<u>Полужирный подчеркнутый фиолетовый шрифт</u>	Внутренняя ссылка
Полужирный шрифт	Наименование элементов интерфейса

1. Введение

1.1. Область применения

Программный комплекс Solar webProxy (далее – Solar webProxy) представляет собой систему анализа трафика, передаваемого по протоколам HTTP, HTTPS, FTP over HTTP, SOCKS5, и инспекцию пакетов на уровне L7 (DPI), с целью идентификации событий, которые могут свидетельствовать о нарушении правил информационного обмена. Для этого весь трафик должен проходить через Solar webProxy.

1.2. Краткое описание возможностей

Solar webProxy контролирует проходящий трафик для предотвращения доступа к запрещенным ресурсам и утечки важной информации. Solar webProxy обеспечивает следующие функциональные возможности:

- Анализ трафика по различным критериям. Объектом анализа является информация, передаваемая в запросах и ответах протоколов HTTP, HTTPS, FTP over HTTP и SOCKS5.
- Инспекция пакетов на уровне L7 (DPI).
- Выполнение заранее определенных действий над передаваемой информацией, соответствующей заданным критериям. Примерами действий могут быть блокировка доступа, явное разрешение доступа и разрешение доступа после подтверждения пользователем.
- Автоматизированное помещение в архив данных о передаваемой информации, отвечающей заданным критериям.
- Формирование отчетов о действиях пользователей в сети Интернет по различным критериям, таким как адрес сайта, время доставки информации, объем доставляемой информации.
- Предоставление администраторам безопасности, прошедшим процедуру аутентификации, возможности просмотра информации, собранной в процессе мониторинга.
- Предоставление администраторам безопасности, прошедшим процедуру аутентификации, возможности настройки функций безопасности.

1.3. Уровень подготовки системного администратора

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

К задачам системного администратора Solar webProxy относятся:

- установка и настройка компонентов Solar webProxy;
- мониторинг функционирования процессов системы;
- реагирование на служебные уведомления системы.

Системный администратор Solar webProxy должен:

- ориентироваться в особенностях работы Solar webProxy;
- понимать работу сетевых протоколов;
- обладать знаниями в области безопасности ОС класса UNIX.

В своей работе системные администраторы Solar webProxy должны использовать внутреннюю документацию и документацию по ОС Linux.

1.4. Перечень эксплуатационной документации для ознакомления

Системный администратор Solar webProxy должен ознакомиться с эксплуатационными документами:

- *Руководство по установке и настройке* (настоящий документ).
- *Руководство администратора безопасности*.

2. Назначение и возможности Solar webProxy

2.1. Назначение Solar webProxy

Solar webProxy предназначен для защиты корпоративных локальных вычислительных сетей от рисков, связанных с использованием веб-ресурсов. Защита обеспечивается комплексом мер, включая фильтрацию содержимого информационного обмена по протоколам HTTP, HTTPS, FTP over HTTP, SOCKS5, инспекцию пакетов на уровне L7 (DPI), авторизацию пользователей и протоколирование их действий.

2.2. Состав Solar webProxy

Solar webProxy имеет модульную структуру на основе сервисов, которые могут работать в распределенном режиме и обеспечивают решение конкретных задач (см. ниже).

Примечание

Большинство сервисов принимают соединение на сетевом интерфейсе 0.0.0.0.

Табл. 2.1. Сервисы, используемые Solar webProxy

Сервис	Решаемые задачи	Порт
Сервис Досье (abook-daemon)	Обеспечивает хранение и репликацию данных Досье: <ul style="list-style-type: none">поддержание основной БД адресной книги (создание и обновление схемы);синхронизация с внешними источниками (Active Directory) по протоколам LDAP (TCP/389), LDAPS (TCP/636).	2269 Обеспечивает внутреннюю коммуникацию между узлами (при необходимости порт можно изменить в настройках системы)
Антивирус (antivirus)	Управляет сервисами антивируса. Обеспечивает прием трафика по протоколу ICAP и его проверку по локальным антивирусным базам.	1344 Принимает запросы на поиск вирусов по протоколу ICAP от узлов с ролью Фильтр HTTP-трафика (при необходимости порт можно изменить в настройках системы)
Сервис хранения статистики пользователей (clickhouse)	Хранит запросы пользователей и извлекает данные для отчетов на основе сформированных запросов.	8123 Принимает данные от узлов с ролями Фильтр HTTP-трафика и Обратный прокси-сервер
Сервис хранения данных (database)	Сервис, который обеспечивает: <ul style="list-style-type: none">хранение политик для подсистемы фильтрации;хранение данных подсистемы мониторинга;хранение данных Досье;управление Solar webProxy.	5434

Сервис	Решаемые задачи	Порт
Сервис балансировки трафика (haproxy)	Обеспечивает распределение трафика между узлами в соответствии с настройками Solar webProxy.	2344, 1010 Принимает запросы от пользователей (при необходимости порт можно изменить в настройках системы)
Сервис пересылки широковещательных IGMP-пакетов (igmpproxy)	Обеспечивает пересылку IGMP-пакетов из одной сети в другую через прокси-сервер.	–
Сервис виртуального IP (keepalived)	Обеспечивает отказоустойчивость работы Solar webProxy, объединяя несколько узлов под одним виртуальным IP-адресом. Для автоматического переключения IP-адреса используется протокол VRRP (Virtual Router Redundancy Protocol).	–
Сервер лицензирования (license-server)	Проверяет состояние лицензии, лицензионных ограничений, а также предоставляет информацию о лицензии другим сервисам системы.	3004 Принимает соединения со всех узлов кластера
Сервис ретрансляции журнальных данных (log-streamer)	Обеспечивает взаимодействие с БД ClickHouse (отправка и архивация запросов): собирает журнальные файлы сервисов фильтрации, конвертирует их и переносит в БД сервиса хранения статистики пользователей ClickHouse. Некорректные журналы записываются в файл <code>/data/spool/skvt/access_log/invalid_log_entries</code> .	–
Сервис сбора данных о работоспособности системы (monitor-agent)	Сервис, который выполняет следующие функции: <ul style="list-style-type: none"> проверка состояния различных ресурсов Solar webProxy; запуск и остановка некоторых сервисов в зависимости от состояния проверяемых ресурсов. 	10050 При необходимости порт можно изменить в настройках системы
Сервис HTTP-интерфейса (monitor-httdp)	Сервис HTTP-интерфейса к системе мониторинга Zabbix. Обеспечивает работу пользовательского интерфейса мониторинга.	80
Сервис выполнения удаленных команд (monitor-nc)	Сервис, который обеспечивает: <ul style="list-style-type: none"> проверку задаваемых параметров конфигурации на соответствие диапазонам допустимых значений; выполнение удаленных команд; получение журналов сервисов. 	5555
Сервис анализа работоспособности системы (monitor-server)	Сервис, который выполняет следующие функции: <ul style="list-style-type: none"> накопление данных от сервиса сбора; сохранение информации о состоянии различных ресурсов Solar webProxy в БД; отправка уведомлений о проведении заданных проверок; выполнение действий в соответствии с заданными условиями. 	10051

Сервис	Решаемые задачи	Порт
Сервис управления сетевыми интерфейсами (network-config-agent)	<p>Сервис-агент, который обеспечивает:</p> <ul style="list-style-type: none"> настройку сетевой конфигурации узлов в соответствии с политикой Solar webProxy; распознание текущей сетевой конфигурации узлов; отправку информации о текущей сетевой конфигурации узлов на сервис skvt-play-server по протоколу SSE. 	5566
Сервис инспекции пакетов (ndpid)	Сервис собирает сетевой трафик и анализирует его на уровне L4 (TCP/UDP) и L7 (прикладной уровень), поддерживает классификацию протоколов и сбор метрик, обрабатывает потоки трафика и агрегирует данные о них.	5566
Сервис Basic-аутентификации (skvt-auth-server)	Обеспечивает вход в систему с предоставлением идентификационных данных: запрашивает и кэширует информацию о доменных пользователях с помощью Basic-аутентификации для источников LDAP (TCP/993), AD (TCP/995), IMAP (TCP/110), POP3 (TCP/143), RADIUS (TCP/1812).	2230 Skvt-auth-server ожидает запросы на аутентификацию от узлов фильтрации и/или управления (при необходимости порт можно изменить в настройках системы)
Сервис кэширования (skvt-cache)	<p>Служит для кэширования данных, получаемых от внешних веб-серверов, и выполняет следующие функции:</p> <ul style="list-style-type: none"> кэширование (временное локальное хранение) страниц сети Интернет, запрашиваемых по протоколу HTTP; выдача хранимых страниц из кэша по запросу пользователей рабочих станций; перенаправление запросов пользователей рабочих станций на ресурсы сети Интернет при отсутствии соответствующих страниц в кэше. <p>На данный момент кэшируется только HTTP-трафик.</p>	2228 Принимает и обрабатывает HTTP/FTP/HTTPS-запросы от локального skvt-wizor (при необходимости порт можно изменить в настройках системы)
Сервис масштабируемого хранилища данных Cassandra (skvt-cassandra)	<p>СУБД, которая хранит счетчики трафика, подтверждения, кэш привязки неаутентифицированного трафика к пользователям и кэш пользователей, получивших страницу загрузки сертификата вскрытия HTTPS.</p> <p>Сервис хранит:</p> <ul style="list-style-type: none"> идентификаторы аутентифицированных пользователей; идентификаторы пользователей с ошибкой вскрытия HTTPS; подтверждения открытия страниц; цепочки сертификатов; статистику по объему трафика; информацию о загруженных файлах. 	7199, 7000, 9042 При наличии нескольких экземпляров БД Cassandra они могут обмениваться данными также по любому порту

Сервис	Решаемые задачи	Порт
Сервис Kerberos-аутентификации (skvt-kerberos-server)	Сервис, необходимый для аутентификации пользователей рабочих станций по протоколу Kerberos (TCP/2226). Принимает запросы от узлов фильтрации (при необходимости порт можно изменить в настройках системы)	2226
Сервис NTLM-аутентификации (skvt-ntlm-server)	Сервис, необходимый для аутентификации пользователей рабочих станций по протоколу NTLM (TCP/2225). Принимает запросы от узлов фильтрации (при необходимости порт можно изменить в настройках системы)	2225
Веб-сервер (skvt-play-server)	Сервер управления выполняет следующие функции: <ul style="list-style-type: none"> ● функционирование интерфейса управления; ● аутентификация администраторов; ● контроль действий администраторов; ● передача данных и задач в другие подсистемы; ● получение данных из других подсистем; ● установление подлинности и действительности загруженной лицензии. Также сервер журналирует действия администраторов по изменению политик фильтрации и настроек конфигурации.	8443 Принимает запросы от браузеров администраторов
Сервис учета трафика (skvt-trafdaemon)	Сервис учета трафика, который обеспечивает накопление и хранение данных о количестве трафика между сервисом фильтрации и сервером назначения. Сервером назначения считается узел, с которым связывается сервис фильтрации – это может быть как узел сети Интернет, так и родительский прокси-сервер. Если система установлена на единственном узле, skvt-trafdaemon используется как библиотека сервиса фильтрации и хранит данные о трафике в файле. Если система функционирует в кластере, в сервис фильтрации встраивается клиентская часть skvt-trafdaemon, которая отправляет данные через TCP-соединение. В этом случае данные о трафике хранятся в БД Cassandra сервиса масштабируемого хранилища данных и передаются по протоколу TLS.	2299
Сервис интеграции с доменом (skvt-winbind)	Сервис, организующий взаимодействие с контроллером домена. Служит для предоставления доступа сервисам NSS (Name-Service Switch) к различным приложениям через PAM (Pluggable Authentication Modules – подключаемые модули аутентификации) и ntlm_auth (утилита NTLM-аутентификации), а также к Samba.	–
Сервис фильтрации (skvt-wizor)	Реализует политику безопасности для пользователей и на ее основе выполняет анализ данных, передаваемых в обоих направлениях. Сервис выполняет следующие функции:	Сервис принимает соединения на следующих портах (при необходимости порты можно изменить в настройках системы):

Сервис	Решаемые задачи	Порт
	<ul style="list-style-type: none"> применение политики фильтрации к запросам пользователей рабочих станций к ресурсам сети Интернет; аутентификация пользователей. <p>Сервис является ядром прокси-сервера и находится на пути потока данных между рабочими станциями пользователей и сетью Интернет. Он может функционировать на нескольких узлах Solar webProxy.</p>	<ul style="list-style-type: none"> 2270 – порт для принятия HTTP-запросов; 2278 – порт для принятия трафика от модуля балансировки; 2277 – порт для получения отладочной информации о модуле; 2281 (HTTP), 2282 (HTTPS) – порты для отображения таких внутренних ресурсов как страница подтверждения перехода, страница отложенной загрузки, страница аутентификации, страница проверки сертификата, страница инструкции по установке сертификата; 2272 – порт для принятия сообщений в формате ICAP; 2443 – порт для принятия HTTPS-запросов; 2444 – порт для принятия HTTPS-запросов в прозрачном режиме.
Сервис распаковки и конвертирования данных (smartikaserver)	<p>Сервис выполняет следующие функции:</p> <ul style="list-style-type: none"> извлечение текста и вложений из бинарных файлов; нормализация кодировки текстов из неизвестных источников. 	9998 Принимает запросы с фрагментами сообщений от узлов фильтрации (при необходимости порт можно изменить в настройках системы)
Сервис категоризации (url-checker-next)	Выполняет проверку URL на соответствие категориям. Определение соответствий происходит согласно настройкам Solar webProxy.	Сервис принимает соединения на следующих портах (при необходимости порты можно изменить в настройках системы): <ul style="list-style-type: none"> 9090 – порт gRPC-сервера; 8090 – порт REST-сервера

Также Solar webProxy использует дополнительные порты, представленные в таблице ниже.

Табл. 2.2. Дополнительные порты, используемые в работе Solar webProxy

Номер порта	Сервис	Назначение
Взаимодействие фильтра с внешними сервисами		
TCP/25 (можно изменить в настройках системы)	Отправка почты	<p>Сервис отправляет:</p> <ul style="list-style-type: none"> POST-запросы правил фильтрации на запись данных в архив;

Номер порта	Сервис	Назначение
		<ul style="list-style-type: none"> уведомления о срабатывании правил фильтрации; уведомления о проблемах сервера мониторинга
53 (UDP)	DNS	Обеспечивает взаимодействие с DNS-серверами
22	SSH	Предоставляет доступ для подключения по SSH
80, 443	internet	Организует доступ к внешним HTTP/HTTPS/FTP-серверам

Для управления системой используется графический интерфейс пользователя (далее – GUI).

2.3. Схемы подключения Solar webProxy

Для Solar webProxy предусмотрено несколько схем подключения к корпоративной сети:

- Система устанавливается в разрыв потока с *явным указанием настроек прокси у пользователя* и контролирует все данные, передаваемые между пользователями и ресурсами сети Интернет. Возможно подключение Active Directory.
- Система устанавливается в разрыв потока в *прозрачном режиме* и контролирует все данные, передаваемые между пользователями и ресурсами сети Интернет. Возможно подключение Active Directory.



Рис. 2.1. Схема работы при подключении в разрыв потока

- Система устанавливается для работы в обратном режиме, что позволяет публиковать внутренние ресурсы организации на внешние источники. Например, организация может предоставить своим сотрудникам доступ к корпоративной почте за пределами организации. При этом Solar webProxy проверяет и блокирует файлы с конфиденциальной информацией при попытке их выгрузить.

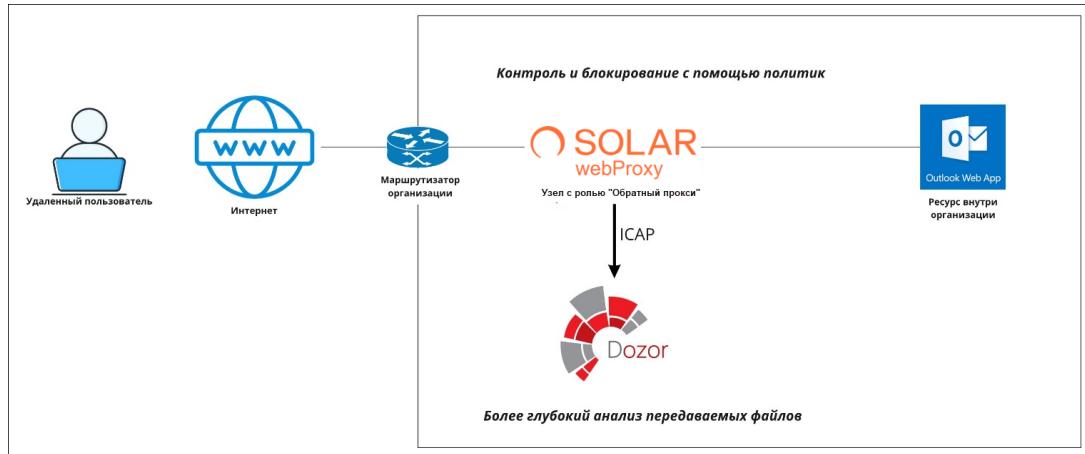


Рис. 2.2. Схема работы при подключении в обратном режиме

3. Требования к программному и аппаратному обеспечению

3.1. Требования к АРМ системного администратора

АРМ системного администратора Solar webProxy должно быть оборудовано персональным компьютером. Особых требований к аппаратному обеспечению нет. Рекомендуются следующие характеристики персонального компьютера:

- процессор P-IV с тактовой частотой не менее 2 ГГц;
- объем оперативной памяти не менее 4 ГБ;
- объем жесткого диска не менее 20 ГБ.

В состав программного обеспечения АРМ системного администратора Solar webProxy должен входить браузер. Рекомендуемые браузеры:

- Mozilla Firefox,
- Google Chrome.

Примечание

Браузеры на базе Chromium при работе с медиаданными некорректно используют прокси-сервер. Для решения проблемы:

- 1. В файле **etc/sysctl.conf** добавьте строку:*

```
export CHROMIUM_FLAGS="$CHROMIUM_FLAGS --proxy-server=XXX.XXX.XXX.XXX:XXXXXX"  
где XXX.XXX.XXX.XXX:XXXXXX – IP-адрес Solar webProxy вместе с портом.
```

- 2. Перезапустите браузер.*

Работа с управляющим интерфейсом Solar webProxy возможна в других браузерах, но в таком случае полноценная работоспособность Solar webProxy не гарантируется.

Для корректной работы Solar webProxy настоятельно рекомендуется разрешить выполнение JavaScript и сохранение cookies (настройка по умолчанию).

Внимание!

Если вручную увеличить размер шрифта в браузере, дизайн интерфейса Solar webProxy будет нарушен, и интерфейс станет непригодным к использованию.

3.2. Требования к серверу

3.2.1. Алгоритм расчета сайзинга

За базу для расчета берутся исходные данные по внутренним нагрузочным тестам с различными стартовыми характеристиками стендов и различными политиками. Основными параметрами, которые впоследствии соотносятся с требованиями заказчиков и определяют необходимый сайзинг, является RPS (количество запросов в секунду или пропускная способность) на одного пользователя и необходимое количество пользователей.

Рекомендуемые характеристики аппаратного обеспечения сервера для установки Solar webProxy в зависимости от пропускной способности и количества пользователей:

Табл. 3.1. Производительность ОС Astra Linux

Производительность	vCPU16	vCPU24	vCPU32	CPU 16 (железный стенд)	CPU 24 (железный стенд)	CPU 32 (железный стенд)	CPU 64 (железный стенд)
Пропускная способность вскрытия HTTPS, Мбит/сек (Сложность политики низкая. Политика оптимизирована: минимальное количество регулярных выражений и вложенных структур правил. Сокращенные справочники без дублей)	4850	8400	10080	6400	11090	13306	17960
Пропускная способность антивируса, Мбит/сек (Антивирусные проверки конкретных типов файлов (текстовые документы и бизнес файлы), корректировки по размерам отправляемых файлов)	1103	1253	1501	1454	1651	1979	2673
Вскрытие HTTPS, RPS	1559	2673	3208	2058	3527	4234	5716
Антивирус, RPS	403	490	588	531	649	777	1049
Рекомендовано пользователей при вскрытии HTTPS	5197	8910	10693	6860	11757	14113	19053
Рекомендовано пользователей при вскрытии и включенном антивирусе	1343	1633	1960	1770	2163	2590	3497

Например, у заказчика следующие данные:

Табл. 3.2. Количество RPS по площадкам (HTTP)

Площадка	Год 1	Год 2	Год 3	Год 4	Год 5
	Количество запросов в минуту (среднее за месяц)				
Москва (Ярославль)	90558	135837	203756	305633	458450
Офис	43200	64800	97200	145800	218700
VPN	40900	61350	92025	138038	207056
Wi-Fi	3968	5952	8928	13392	20088
Гостевая сеть 802.1x	390	585	878	1316	1974
Прокси для серверов	2100	3150	4725	7088	10631
Санкт-Петербург	2200	3300	4950	7425	11138
Ростов-на-Дону	2420	3630	5445	8168	12251
Офис	1990	2985	4478	6716	10074
Гостевая сеть 802.1x	430	645	968	1451	2177
Саратов	3640	5460	8190	12285	18428
Новосибирск	4229	6344	9515	14273	21409
Офис	1869	2804	4205	6308	9462
Гостевая сеть 802.1x	2360	3540	5310	7965	11948
Екатеринбург	14460	21690	32535	48803	73204
Хабаровск	687	1031	1546	2319	3478
Итого	124843	187265	280897	421345	632018

Табл. 3.3. Количество RPS по площадкам (HTTPS)

Площадка	Год 1	Год 2	Год 3	Год 4	Год 5
	Количество запросов в минуту (среднее за месяц)				
Москва (Ярославль)	309675	464513	696769	1045153	1567730
Офис	227500	341250	511875	767813	1151719
VPN	61770	92655	138983	208474	312711
Wi-Fi	3995	5993	8989	13483	20225
Гостевая сеть 802.1x	410	615	923	1384	2076
Прокси для серверов	16000	24000	36000	54000	81000
Санкт-Петербург	15730	23595	35393	53089	79633
Ростов-на-Дону	63383	95075	142612	213918	320876
Офис	62900	94350	141525	212288	318431
Гостевая сеть 802.1x	483	725	1087	1630	2445

Площадка	Год 1	Год 2	Год 3	Год 4	Год 5
	Количество запросов в минуту (среднее за месяц)				
Саратов	50600	75900	113850	170775	256163
Новосибирск	34283	51425	77137	115705	173558
Офис	30800	46200	69300	103950	155925
Гостевая сеть 802.1x	3483	5225	7837	11755	17633
Екатеринбург	49800	74700	112050	168075	252113
Хабаровск	15650	23475	35213	52819	79228
Итого	636787	955181	1432771	2149156	3223734

Табл. 3.4. Количество пользователей по площадкам

Наименование	Единица измерения	Год 1	Год 2	Год 3	Год 4	Год 5
Москва	чел.	26154	30077	34589	38048	43755
Москва (доступ с серверов в интернет)	серверы	4800	5520	6348	7300	8760
Северо-Западный регион	чел.	3162	3636	4182	4600	5290
Южный регион	чел.	5079	5841	6717	7389	8497
Приволжский регион	чел.	5209	5990	6889	7578	8714
Сибирский регион	чел.	2752	3165	3640	4003	4604
Уральский регион	чел.	3143	3614	4157	4572	5258
Дальневосточный регион	чел.	1315	1512	1739	1913	2200
Количество пользователей, которые будут использовать ПО, итого	чел.	51614	59356	68260	75085	86348

Среднее количество запросов на пользователя в секунду (RPS) считается по формуле:

Сумма запросов *HTTP* и *HTTPS* за минуту / (число пользователей*60 сек.)

Табл. 3.5. Среднее количество запросов на пользователя в секунду (RPS)

RPS (среднее количество запросов на пользователя в секунду)	Год 1	Год 2	Год 3	Год 4	Год 5
Москва	0,26	0,33	0,43	0,59	0,77
Москва (доступ с серверов в интернет)	0,06	0,08	0,11	0,14	0,17
Северо-Западный регион	0,09	0,12	0,16	0,22	0,29
Южный регион	0,22	0,28	0,37	0,5	0,65
Приволжский регион	0,17	0,23	0,3	0,4	0,53

RPS (среднее количество запросов на пользователя в секунду)	Год 1	Год 2	Год 3	Год 4	Год 5
Сибирский регион	0,23	0,3	0,4	0,54	0,71
Уральский регион	0,34	0,44	0,58	0,79	1,03
Дальневосточный регион	0,21	0,27	0,35	0,48	0,63

Итого RPS на систему в секунду считается по формуле:

Сумма запросов HTTP и HTTPS за минуту / 60 сек.

Табл. 3.6. RPS на систему в секунду

Итого RPS на всю систему	Год 1	Год 2	Год 3	Год 4	Год 5
Москва	6671	10006	15009	22513	33770
Москва (доступ с серверов в интернет)	302	453	679	1018	1527
Северо-Западный регион	299	448	672	1009	1513
Южный регион	1097	1645	2468	3701	5552
Приволжский регион	904	1356	2034	3051	4577
Сибирский регион	642	963	1444	2166	3249
Уральский регион	1071	1607	2410	3615	5422
Дальневосточный регион	272	408	613	919	1378

Расчет количества необходимых серверов проводится исходя из числа пользователей на площадке ([Табл.3.4](#)) и нагрузке на один сервер ([Табл.3.1](#)). Исходя из вводных для расчета данных брались значения для политики со вскрытием и включенным антивирусом. Значение RPS на пользователя в секунду по внутренней статистике вендора находятся в пределах 0,3. Данные Заказчика в первый и второй года внедрения соответствуют этому. Рост данного показателя в третий, четвертый и пятый года будет нивелирован повышением производительности решения, а также расширением возможностей кэширования. При этом риски для заказчика снимаются гарантийным письмом о допоставке серверных мощностей в случае превышения заявленных заказчиком значений RPS.

Примечание

Масштабирование решения при увеличении числа пользователей предполагает самостоятельную закупку заказчиком серверных мощностей.

Табл. 3.7. Итоговое количество серверов в базовом варианте

Кол-во серверов с 32 vCPU в зависимости от количества пользователей	Год 1	Год 2	Год 3	Год 4	Год 5
Москва	11	13	15	16	19

Кол-во серверов с 32 vCPU в зависимости от количества пользователей	Год 1	Год 2	Год 3	Год 4	Год 5
Москва (доступ с серверов в интернет)	2	3	3	3	4
Северо-Западный регион	1	2	2	2	2
Южный регион	2	3	3	3	4
Приволжский регион	2	3	3	3	4
Сибирский регион	1	1	2	2	2
Уральский регион	1	2	2	2	2
Дальневосточный регион	1	1	1	1	1

Табл. 3.8. Итоговый сайзинг (виртуальные серверы)

Площадка	Тип сервера	Год 1	Год 2	Год 3	Год 4	Год 5
Москва, пользовательский сегмент	Main	1	1	1	1	1
	Main-backup	1	1	1	1	1
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	16 (8)	18 (9)	20 (10)	22 (11)	24 (12)
Москва, серверный сегмент	Main	1	1	1	1	1
	Main-backup	1	1	1	1	1
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
Москва, гостевой сегмент	Main	1	1	1	1	1
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
Северо-Западный регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	4 (2)	4 (2)
Южный регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	4 (2)	4 (2)	4 (2)	4 (2)	6 (3)
	Main	1	1	1	1	1
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
Приволжский регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	4 (2)	4 (2)	4 (2)	4 (2)	6 (3)
Сибирский регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
	Main	1	1	1	1	1

Площадка	Тип сервера	Год 1	Год 2	Год 3	Год 4	Год 5
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	4 (2)
Уральский регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	4 (2)
Дальневосточный регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)

Табл. 3.9. Итоговый сайзинг (физические серверы)

Площадка	Тип сервера	Год 1	Год 2	Год 3	Год 4	Год 5
Москва, пользовательский сегмент	Main	1	1	1	1	1
	Main-backup	1	1	1	1	1
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	10 (5)	10 (5)	10 (5)	10 (5)	12 (6)
Москва, серверный сегмент	Main	1	1	1	1	1
	Main-backup	1	1	1	1	1
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
Москва, гостевой сегмент	Main	1	1	1	1	1
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
Северо-Западный регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	4 (2)	4 (2)
Южный регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	4 (2)	4 (2)	4 (2)	4 (2)	6 (3)
	Main	1	1	1	1	1
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
Приволжский регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	4 (2)	4 (2)	4 (2)	4 (2)	6 (3)
Сибирский регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
	Main	1	1	1	1	1
	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
Уральский регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)
Дальневосточный регион	Proxy-slave (фильтрация трафика + антивирус + балансировка)	2 (1)	2 (1)	2 (1)	2 (1)	2 (1)

3.2.2. Требования к программному обеспечению

Данная версия Solar webProxy функционирует под управлением ОС Astra Linux Special Edition версий 1.7.6 и 1.7.7 «Смоленск».

3.2.3. Требования к конфигурации ОС

Solar webProxy поддерживает работу только по протоколу IPv4. Использование ПО, работающего по протоколу IPv6, может приводить к ошибкам в работе Solar webProxy. Рекомендуется отключить использование IPv6 средствами операционной системы.

Кроме того, в процессе работы Solar webProxy необходим файл с региональными установками **ru_RU.UTF8** для корректного отображения пользовательского веб-интерфейса Solar webProxy.

Функционирование Solar webProxy зависит от наличия в ОС определенных программ и компонентов. Большинство из них являются стандартными динамическими библиотеками ОС. Набор необходимых компонентов задается в виде зависимостей в установочном пакете Solar webProxy.

В настройках ОС должны быть открыты сетевые порты, которые используются в работе Solar webProxy. Перечень портов указан в [Табл.2.1](#).

3.2.4. Рекомендации по разделению дисков в ОС при установке Solar webProxy

По умолчанию Solar webProxy для ОС Linux настроен на использование следующих логических разделов диска:

- **/opt** – раздел, в который производится установка компонентов Solar webProxy.
- **/data** – раздел для размещения накапливаемых данных Solar webProxy.

3.2.5. Рекомендации по размещению в сетевой инфраструктуре

Аппаратное и программное обеспечение сервера должно располагаться внутри защищенного периметра безопасности для исключения несанкционированного доступа.

3.2.6. Требования к паролю

Solar webProxy обеспечивает стойкость паролей для доступа в систему. При создании пользователей система проверяет качество паролей, которое определяется следующими параметрами:

1. Минимально разрешенная длина пароля.
2. Известная и задокументированная максимальная длина пароля.
3. Количество различных символов в пароле:
 - заглавные буквы латиницы;
 - строчные буквы латиницы;
 - цифры;

-
- служебные символы: ~ ! @ # \$ % ^ & * () + - = ` ' _ / \ | ".

При создании пароля система рассчитывает уровень его сложности (от 0 до 10). Система не позволит создать пароль, если он не соответствует заданному в настройках уровню сложности – например, если он содержит более двух символов подряд из одного набора. По умолчанию уровень сложности пароля должен быть не менее 6. Расчет уровня сложности пароля выполняется на основании следующих условий:

1. Если длина пароля равна или больше минимальной, прибавляется 1.
2. Если длина пароля максимальная, прибавляется 2.
3. Если пароль содержит символы из двух наборов, прибавляется 1.
4. Если пароль содержит символы из трех наборов, прибавляется 1.
5. Если пароль содержит символы из четырех наборов, прибавляется 1.
6. Если пароль не содержит более двух символов из одного набора подряд, прибавляется 1.
7. Если пароль не содержит более одного символа из одного набора подряд, прибавляется 2.
8. Если количество разных символов больше минимальной длины пароля, прибавляется 1.
9. Если пароль выполняет условия пунктов 1, 5, 7, 8, прибавляется 1.

Если сумма условий больше 10, уровень сложности пароля считается равным 10.

В настройках по умолчанию минимальная длина пароля равна 6, максимальная – 12, минимально допустимый уровень сложности пароля – 6. Таким образом, если уровень сложности пароля меньше 6, система не позволит создать его.

Настройки по умолчанию можно изменить, отредактировав в GUI следующие параметры (раздел **Система > Расширенные настройки > Интерфейс**, секция **Сервер веб-интерфейса**):

- **Мин. длина пароля;**
- **Макс. длина пароля;**
- **Уровень сложности пароля.**

Сервер веб-интерфейса skvt-play-server.conf

<input checked="" type="checkbox"/> Журналировать действия пользователей в syslog	audit-to-syslog		
<input checked="" type="checkbox"/> Перенаправление с 443 порта на 8443 порт	https-redirect		
SMTP-адрес почтового сервера	smtp-host	10.199.28.17	
SMTP-порт почтового сервера	smtp-port	143	
Мин. длина пароля	password-minlen	1	
Макс. длина пароля	password-maxlen	12	
Уровень сложности пароля	password-level	1	
Задержка с последнего обращения к серверу перед завершением сессии (с)		auth-inactive-timeout	3600

Рис. 3.1. Настройки сложности пароля

В системе реализована защита от взлома путем перебора учетных данных (брутфорс). После заданного количества неудачных попыток входа перед каждой следующей попыткой вводится временная задержка, которая увеличивается экспоненциально после каждой последующей неудачной попытки входа. Настройки защиты можно задать, используя следующие параметры конфигурации (раздел **Система > Расширенные настройки > Интерфейс**, секция **Сервер веб-интерфейса > Параметры входа в систему**):

- **Макс. количество неудачных попыток входа в систему до задержки;**
- **Начальное значение задержки для входа в систему (с);**
- **Макс. значение задержки для входа в систему (с).**

▽ Параметры входа в систему brute-force-protection

Макс. количество неудачных попыток входа в систему до задержки	max-failures	5
Начальное значение задержки для входа в систему (с)	initial-delay	10
Макс. значение задержки для входа в систему (с)	max-delay	300

Рис. 3.2. Настройка параметров входа в систему

При неправильном вводе пароля воспользуйтесь сервисом **user-tool** для его изменения (см. раздел [10.2.3](#)).

4. Установка и удаление Solar webProxy

Процедура обновления Solar webProxy описана в документе [Описание релиза](#).

4.1. Установка ОС Astra 1.7.6, 1.7.7

Для установки ОС Astra 1.7.6 или 1.7.7 запустите сервер с использованием установочного диска или USB-носителя «Astra 1.7.6» или «Astra 1.7.7» версии и выполните следующие действия:

1. В окне приветствия оставьте выбор параметров программы установки по умолчанию (**Графическая установка, Русский**) и нажмите **Enter**.

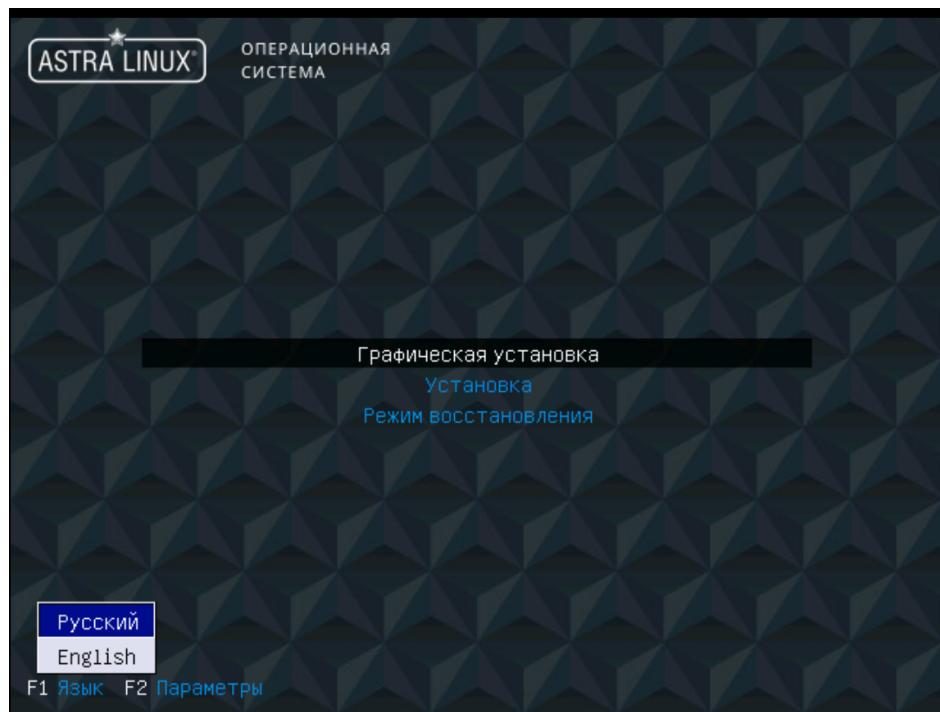


Рис. 4.1. Окно приветствия

2. В окне **Лицензия** нажмите **Продолжить**.

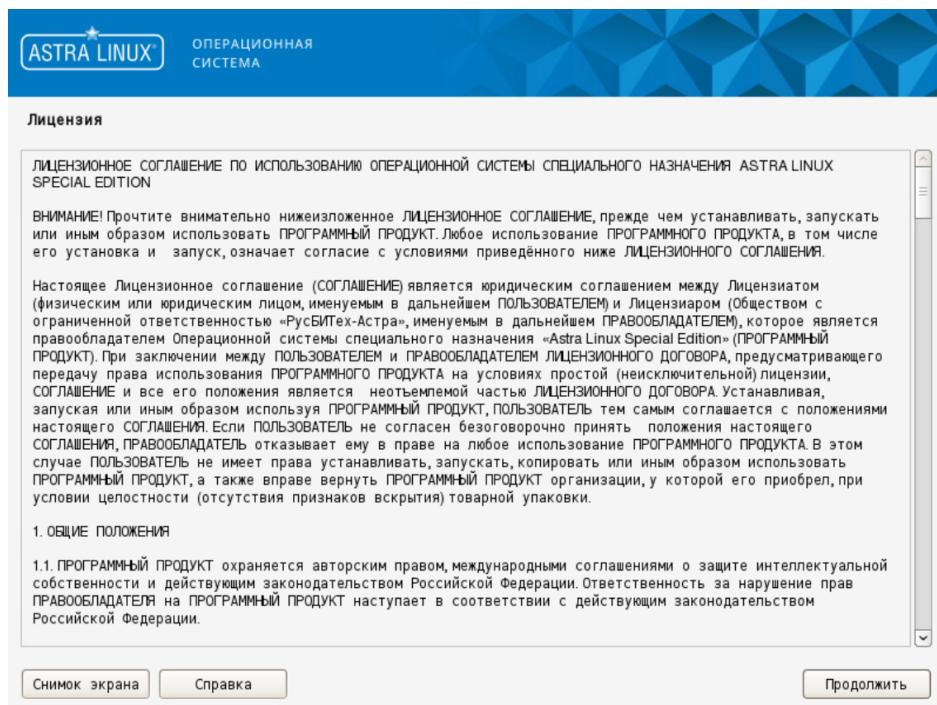


Рис. 4.2. Окно Лицензия

3. В окне **Настройка клавиатуры** выберите удобный способ переключения раскладки ввода с клавиатуры и нажмите **Продолжить**.

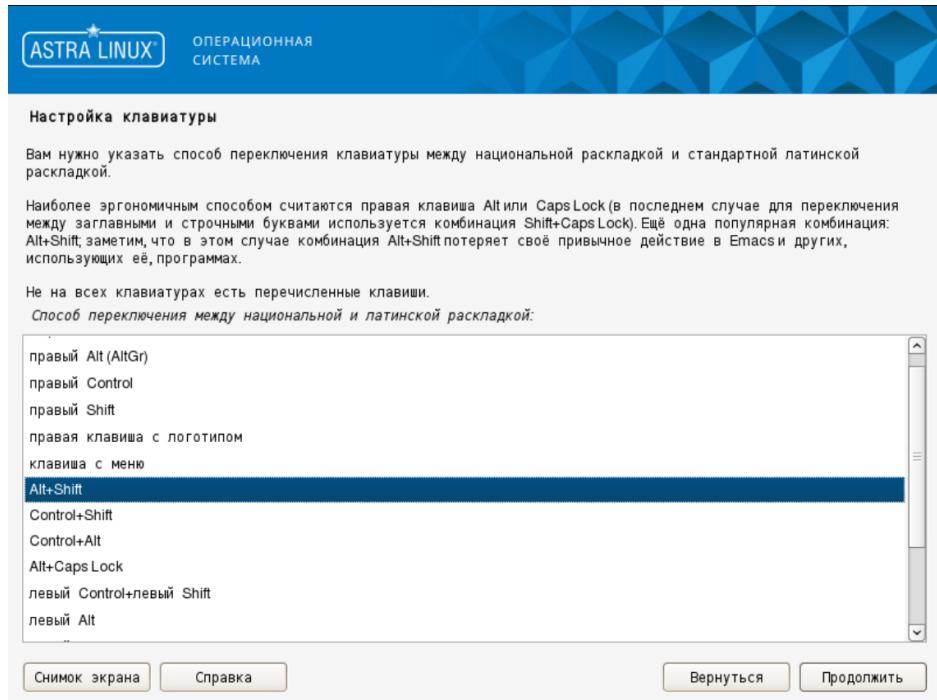


Рис. 4.3. Настройка клавиатуры

4. Дождитесь загрузки компонентов программы установки. В появившемся окне **Настройка сети** укажите краткое сетевое имя сервера.

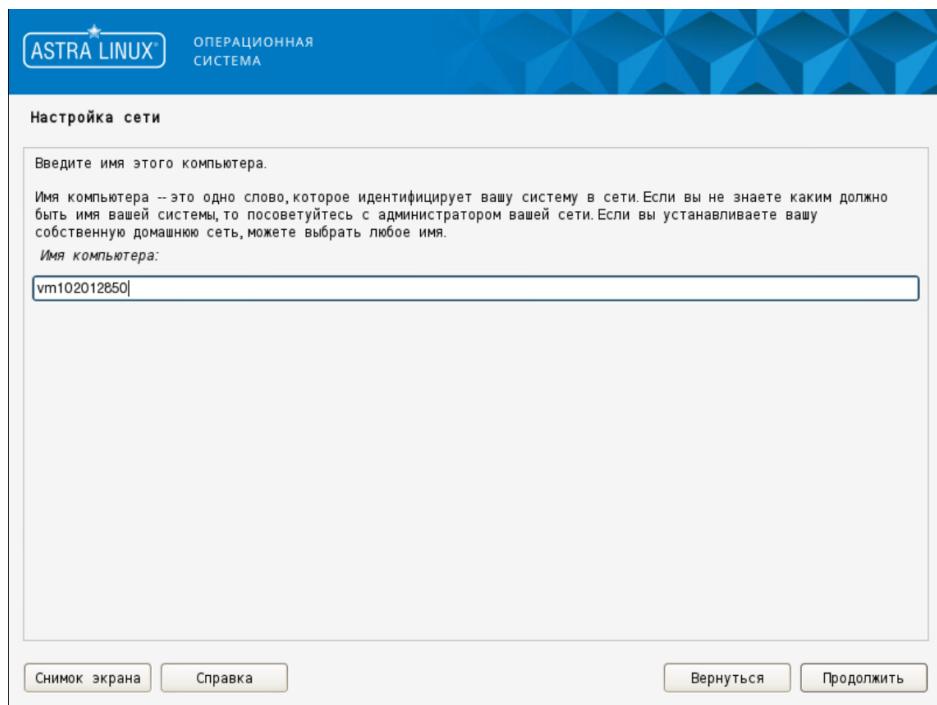


Рис. 4.4. Настройка сети

5. В окне **Настройка учётных записей пользователей и паролей** в поле **Имя учётной записи администратора** укажите произвольное имя и нажмите **Продолжить**. Не следует использовать имя **dozor**, поскольку оно зарезервировано в Solar webProxy.

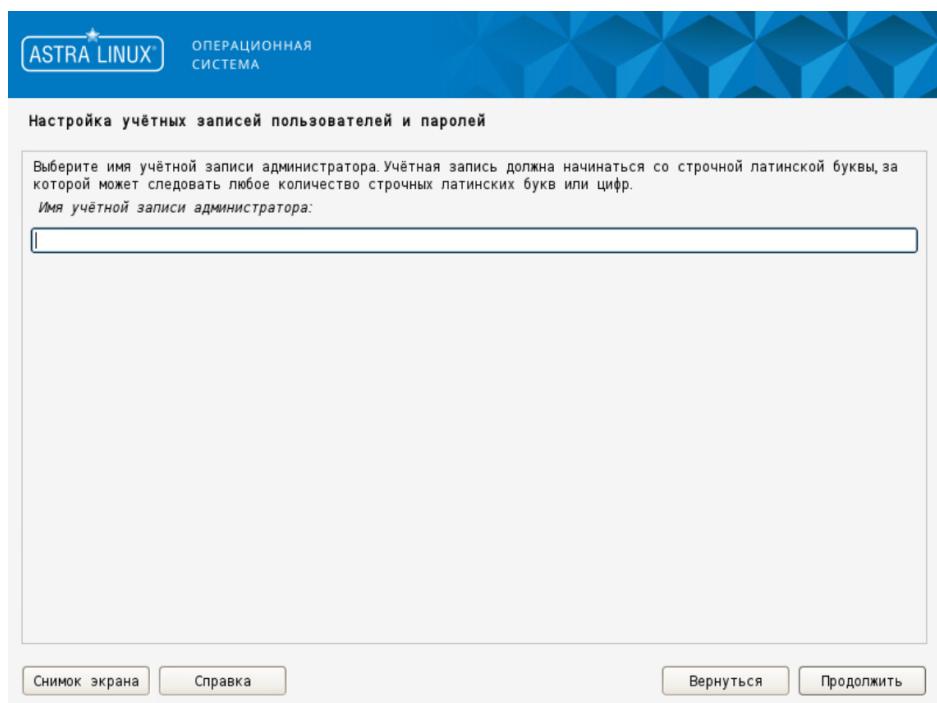


Рис. 4.5. Окно Настройка учётных записей

6. В появившемся окне задайте пароль для созданной учетной записи и подтвердите его. Нажмите **Продолжить**.

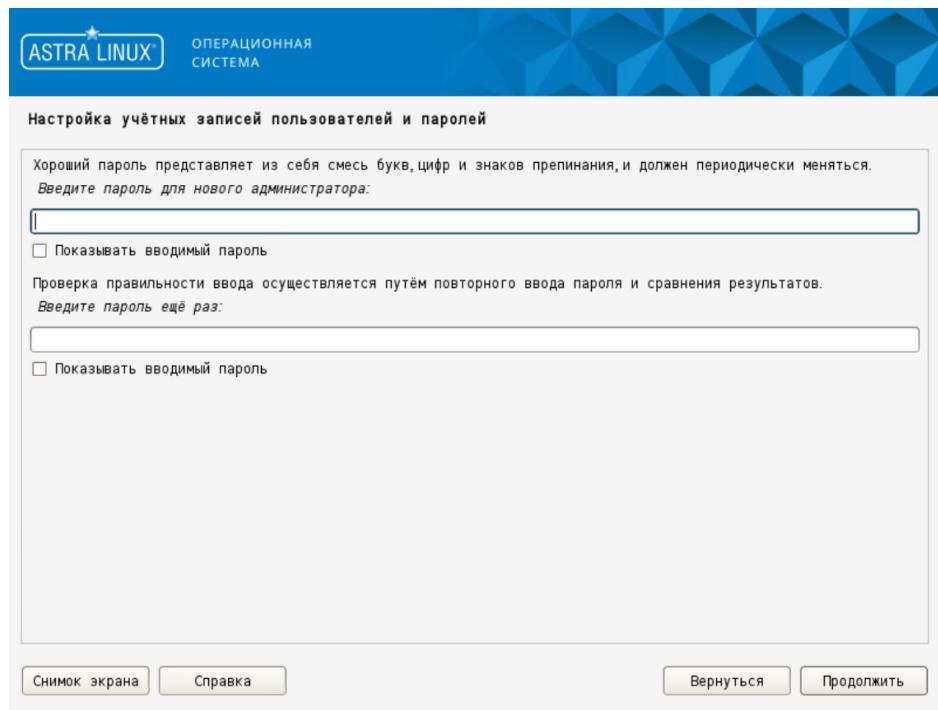
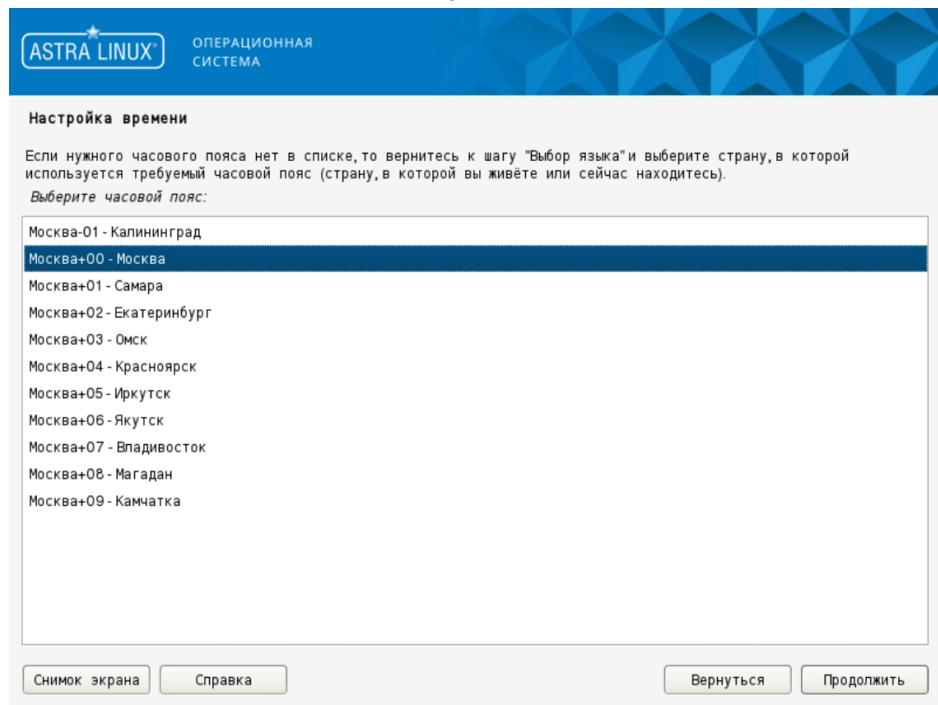


Рис. 4.6. Создание пароля для учетной записи администратора

7. В окне **Настройка времени** задайте требуемый часовой пояс и нажмите **Продолжить**.



8. В появившемся окне **Разметка дисков** выберите метод разметки **Вручную** и нажмите **Продолжить**.

Внимание!

При выборе любого другого метода разметки все данные на диске будут потеряны.

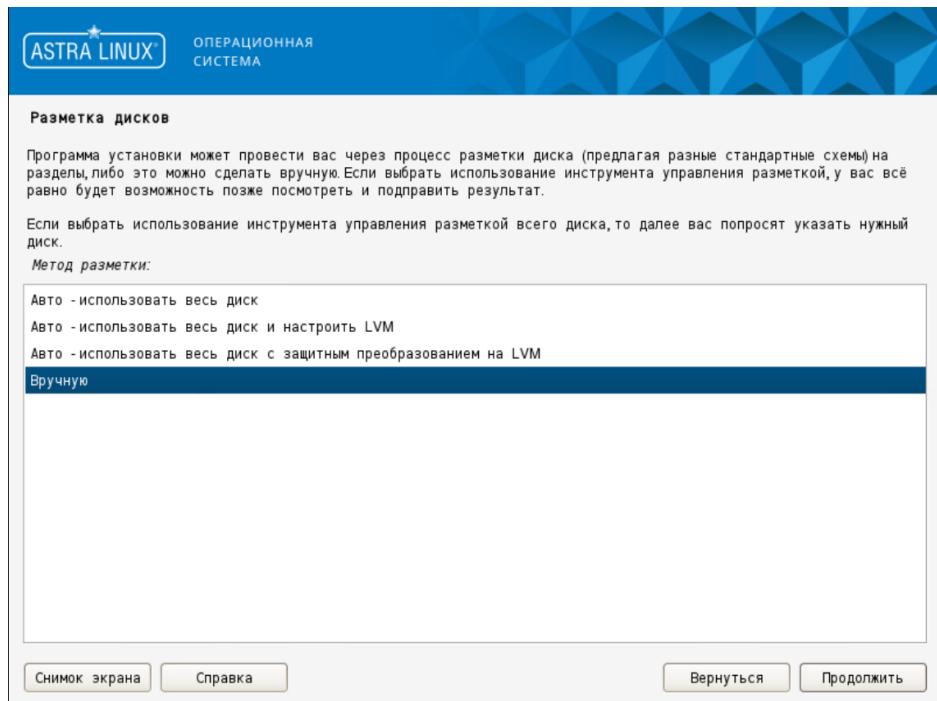


Рис. 4.7. Окно Разметка дисков

9. В появившемся окне выберите область для разметки, например, как показано ниже. Нажмите **Продолжить**.

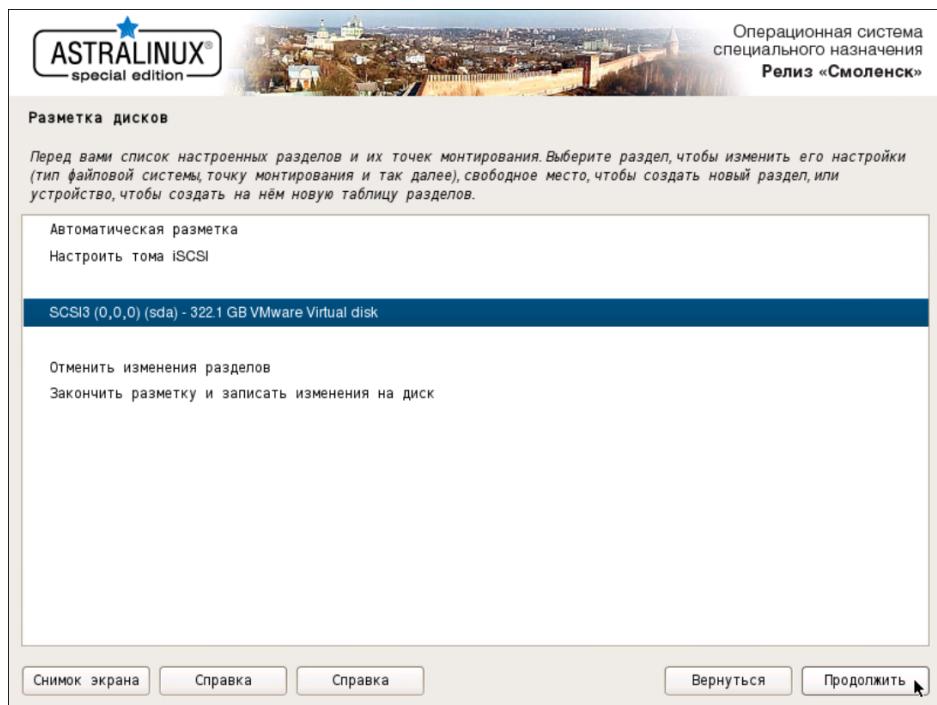


Рис. 4.8. Выбор области для разметки

10. В появившемся окне с запросом **Создать новую пустую таблицу разделов?** выберите вариант **Да**. Нажмите **Продолжить**.

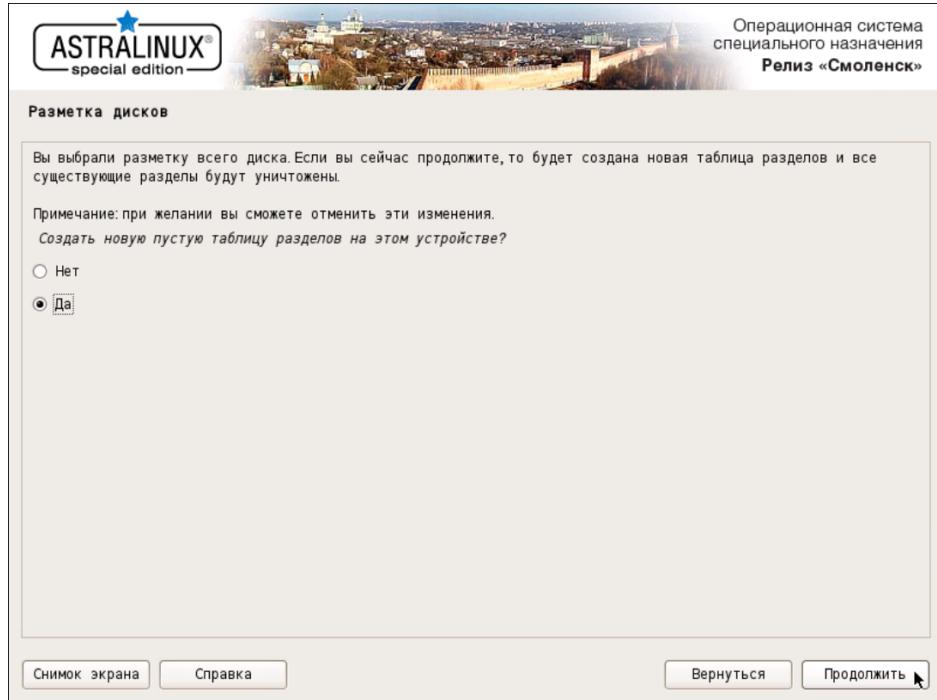


Рис. 4.9. Создание таблицы разделов

11. В появившемся окне выделите строку, помеченную как **СВОБОДНОЕ МЕСТО**, и нажмите **Продолжить**.

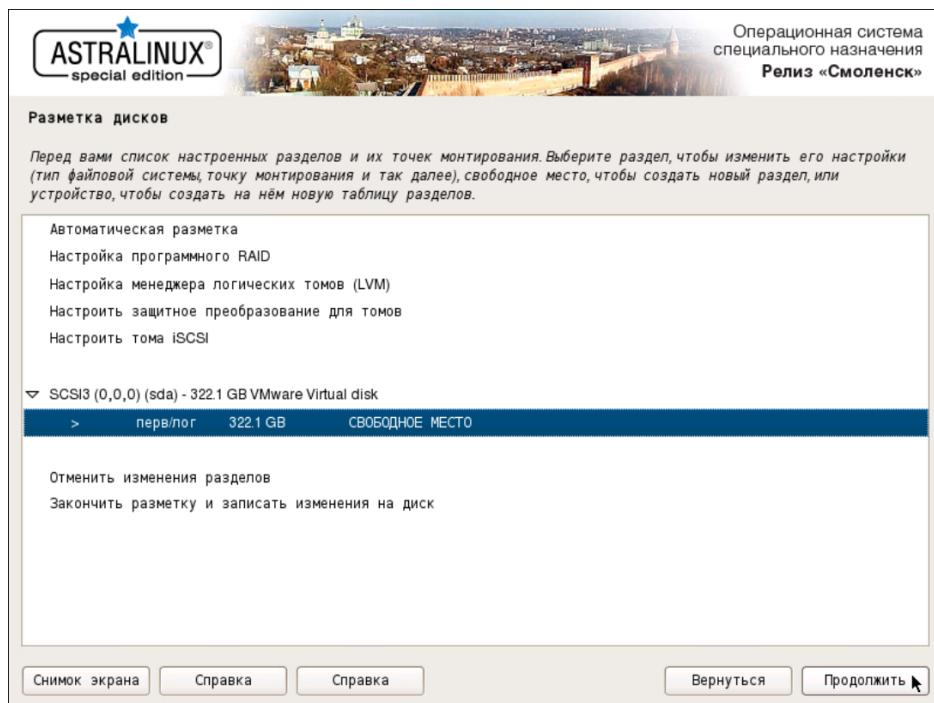


Рис. 4.10. Выбор пространства для создания разделов

12. В появившемся окне с запросом **Что делать со свободным пространством** выберите вариант **Создать новый раздел**. Нажмите **Продолжить**.

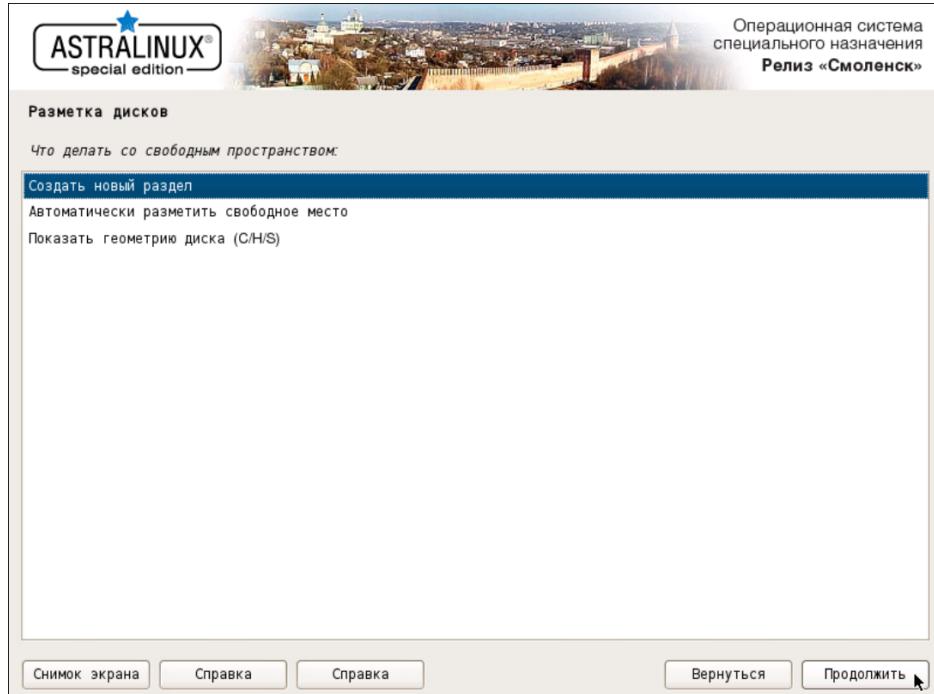


Рис. 4.11. Выбор варианта для создания раздела

13. В появившемся окне задайте размер диска **1 GB**. Нажмите **Продолжить**.

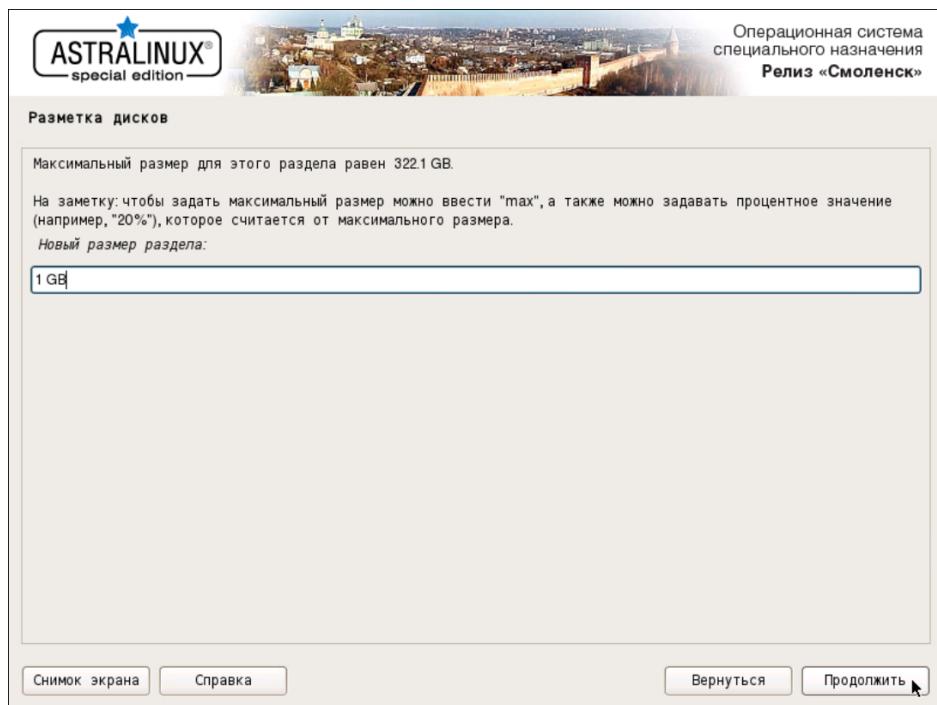


Рис. 4.12. Задание размера раздела

14. В появившемся окне выберите тип раздела **Первичный**. Нажмите **Продолжить**.

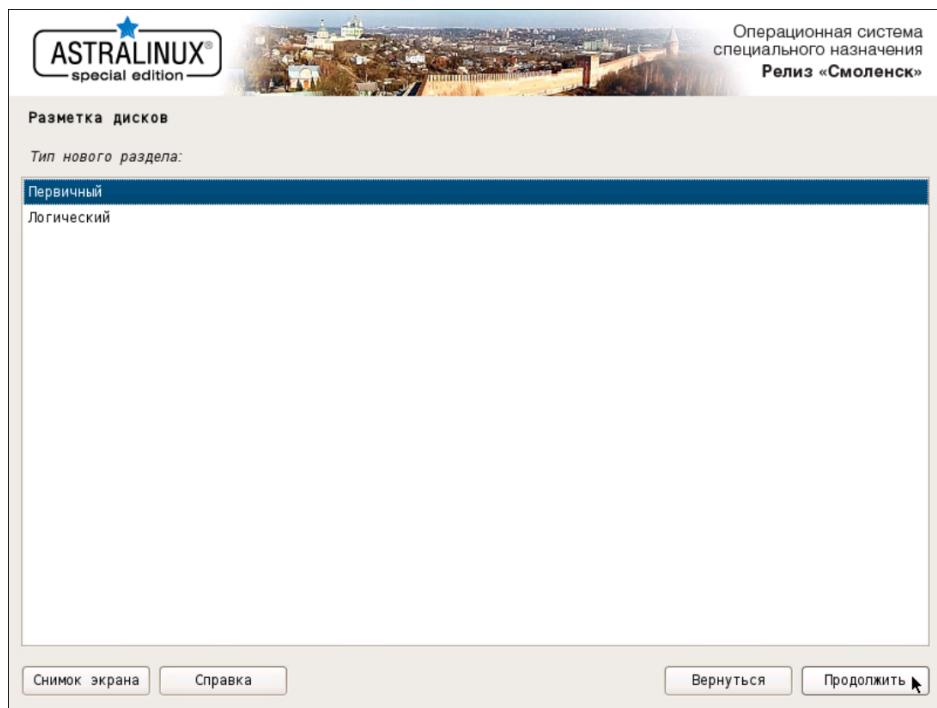


Рис. 4.13. Выбор типа раздела

15. В появившемся окне выберите расположение раздела **Начало**. Нажмите **Продолжить**.

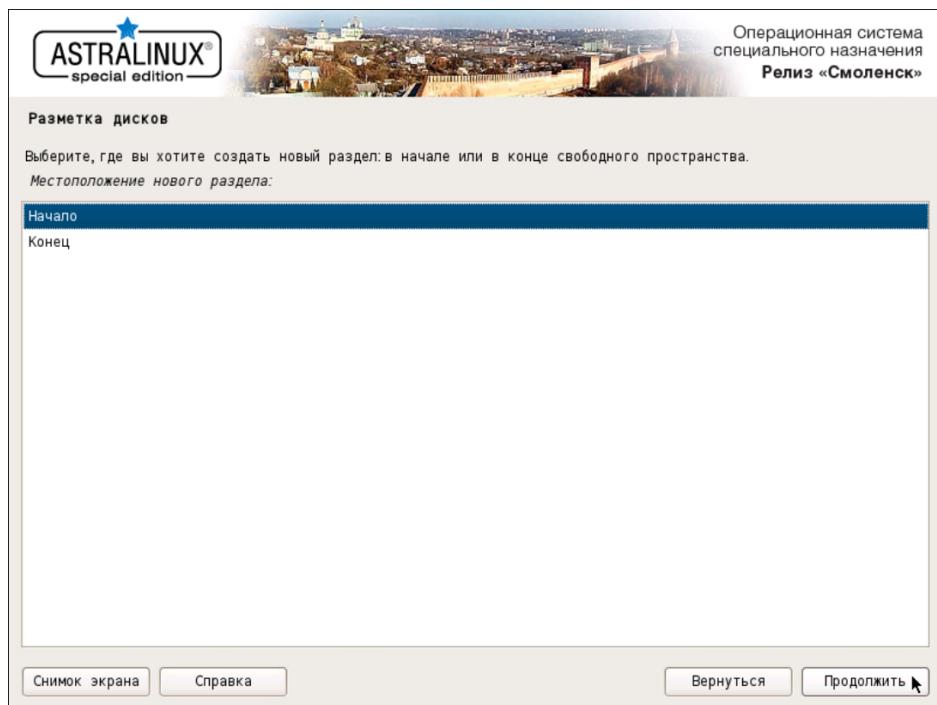


Рис. 4.14. Выбор местоположения раздела

16. Двойным щелчком мыши откроите параметры строки **Точка монтирования** и в появившемся окне выберите вариант **/boot**. Убедитесь, что на строке **Метка 'загрузочный'** выбрано значение **вкл**. Нажмите **Продолжить**.

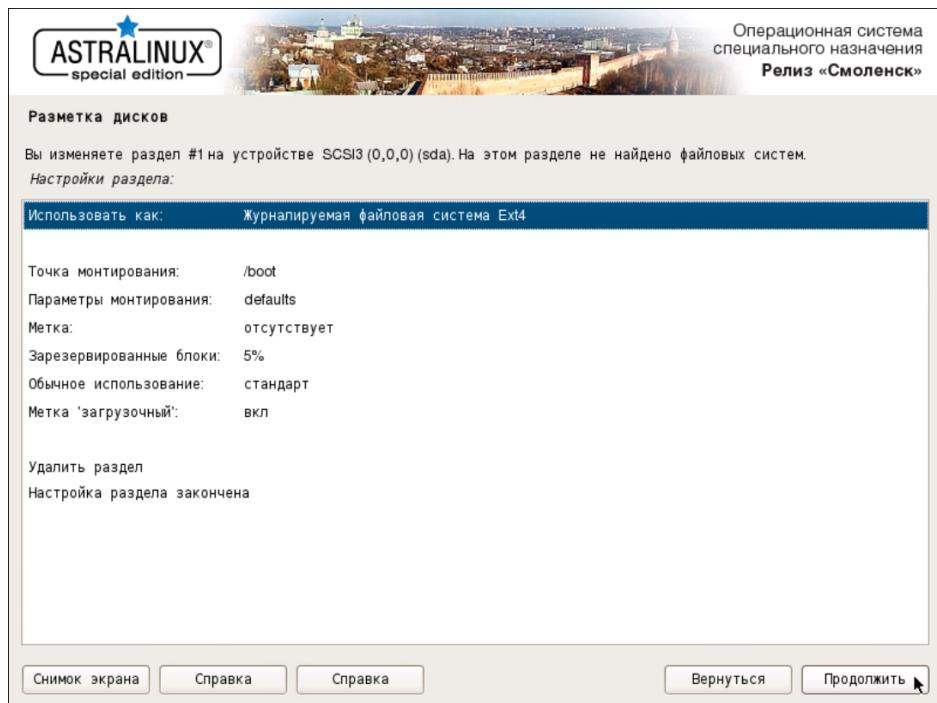


Рис. 4.15. Параметры монтирования раздела

17. Выделите строку **Настройка раздела закончена** и нажмите **Продолжить**.

-
18. Создайте новый раздел, выполнив шаги [11](#) и [12](#).
 19. В появившемся окне выбора размера раздела оставьте максимальное значение по умолчанию. Нажмите **Продолжить**.
 20. В появившемся окне выберите тип раздела **Логический**. Нажмите **Продолжить**.

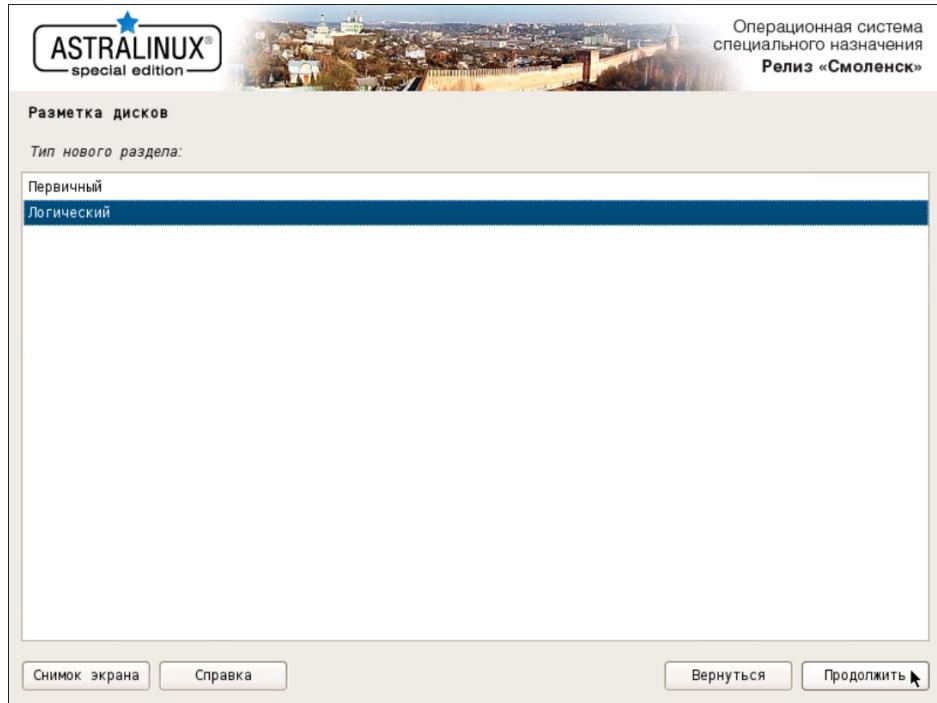


Рис. 4.16. Выбор типа раздела

21. В появившемся окне нажмите строку **Использовать как:**, выберите вариант **физический том для LVM** и нажмите **Продолжить**. Выделите строку **Настройка раздела закончена** и нажмите **Продолжить**.

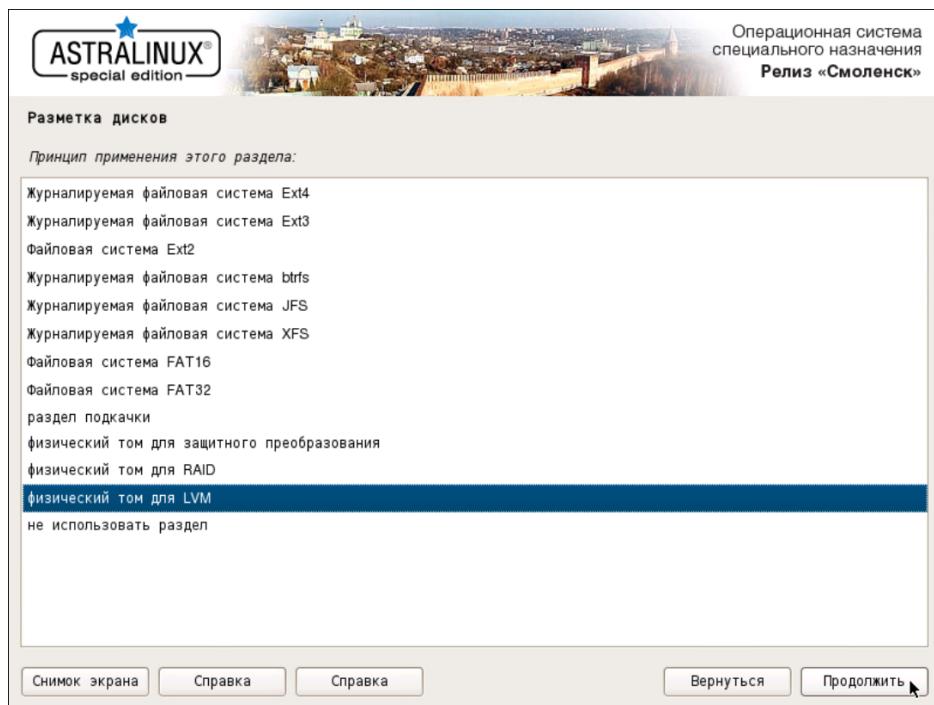


Рис. 4.17. Выбор варианта использования раздела

22. Двойным щелчком мыши откройте параметры строки **Настройка менеджера логических томов (LVM)** и в появившемся окне выберите **Да**. Нажмите **Продолжить**.

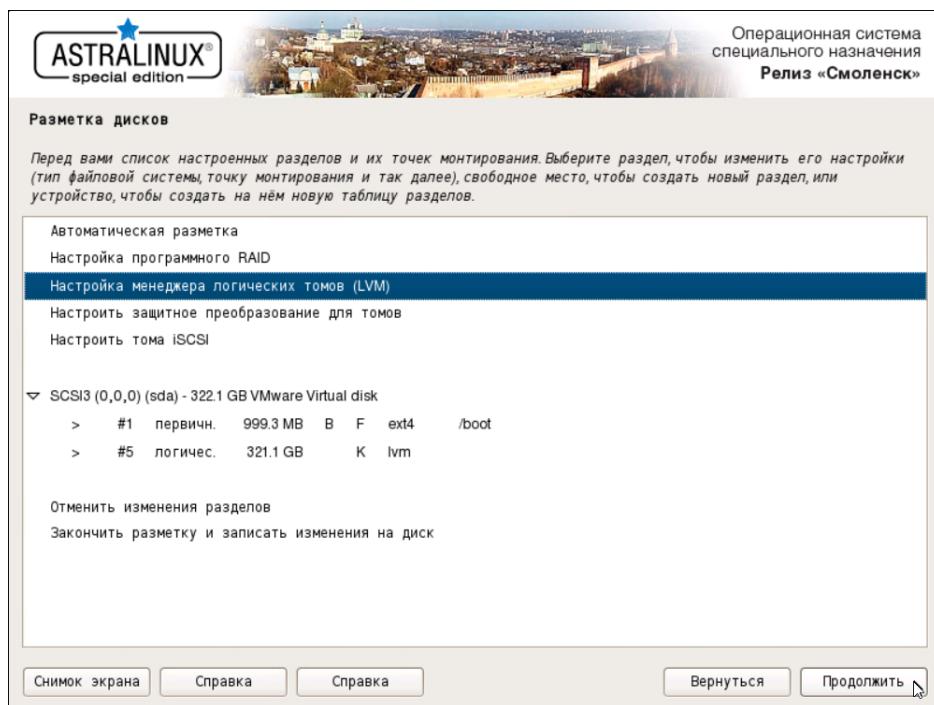


Рис. 4.18. Пункт настройки менеджера логических томов

23. В появившемся окне выберите вариант **Создать группу томов**. Нажмите **Продолжить**.

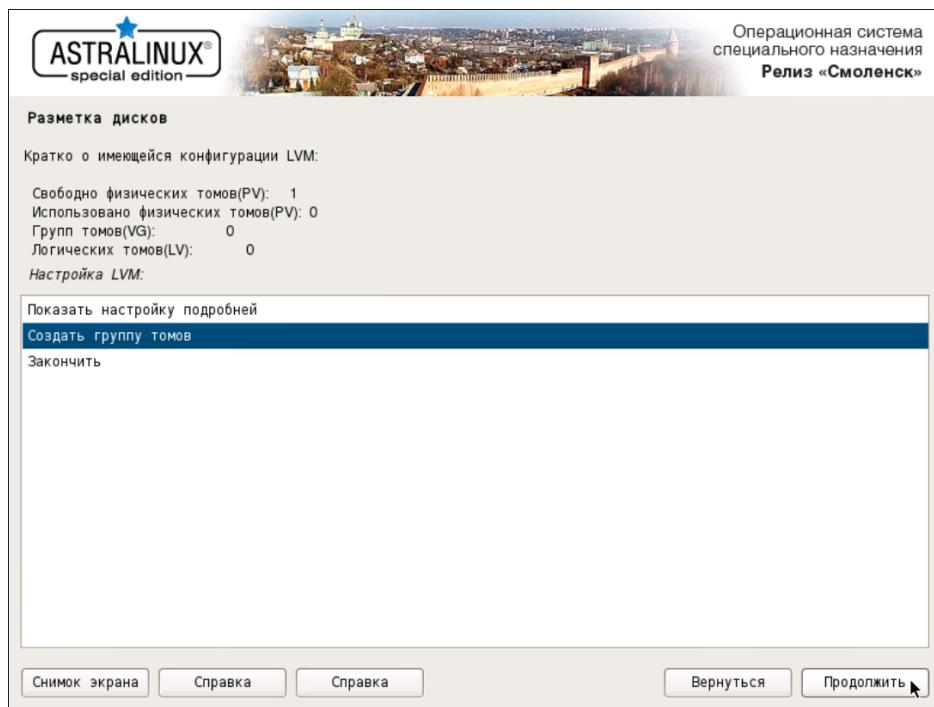


Рис. 4.19. Создание группы томов для LVM

24. В появившемся окне задайте название для группы томов, например, **webproxy**. Нажмите **Продолжить**.

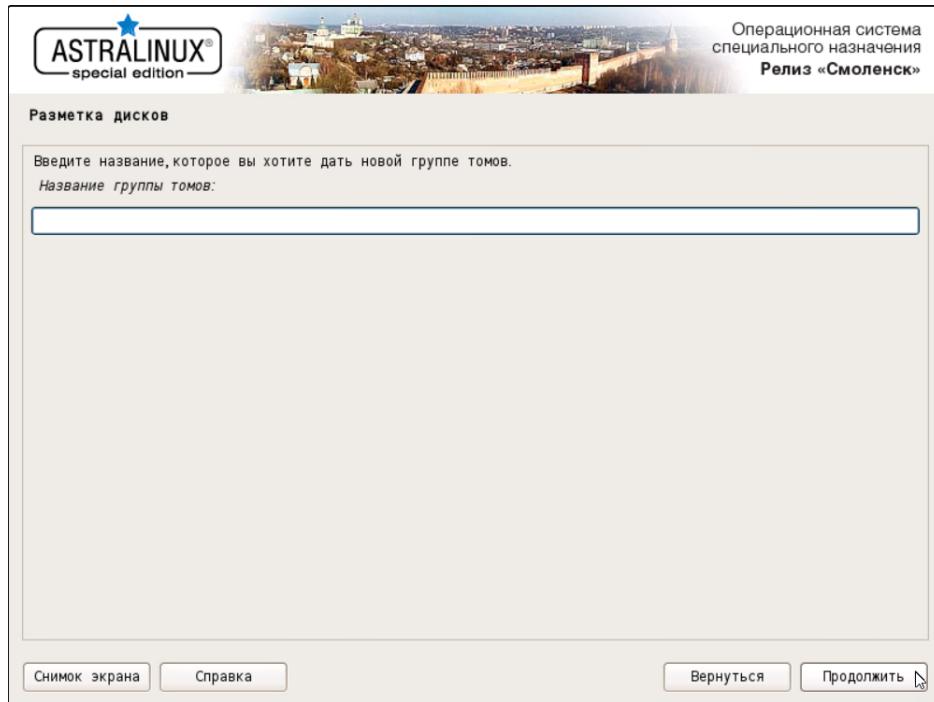


Рис. 4.20. Ввод имени группы томов

25. В появившемся окне выберите раздел, созданный на шаге [18](#). Нажмите **Продолжить**.

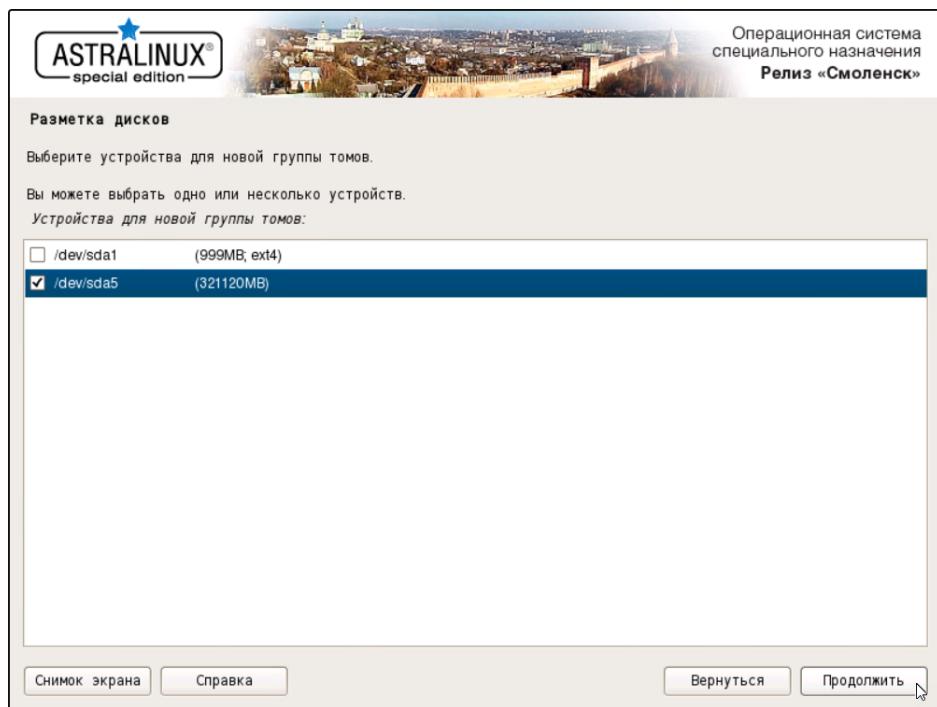


Рис. 4.21. Выбор устройства для размещения группы томов

26. В появившемся окне выберите вариант **Создать логический том**, нажмите **Продолжить** и укажите группу томов, созданную на шаге [23](#). Нажмите **Продолжить**.
27. В появившемся окне для нового логического тома задайте имя **root**. Нажмите **Продолжить**.

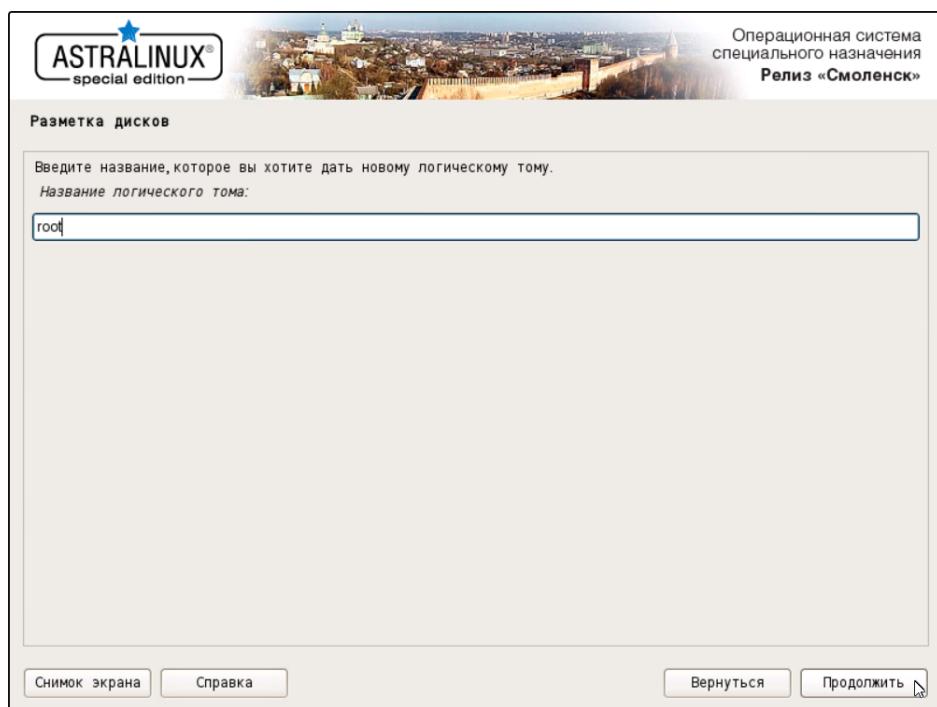


Рис. 4.22. Задание имени логического тома **root**

28. В следующем окне для нового логического тома задайте размер **25G**. Нажмите **Продолжить**.

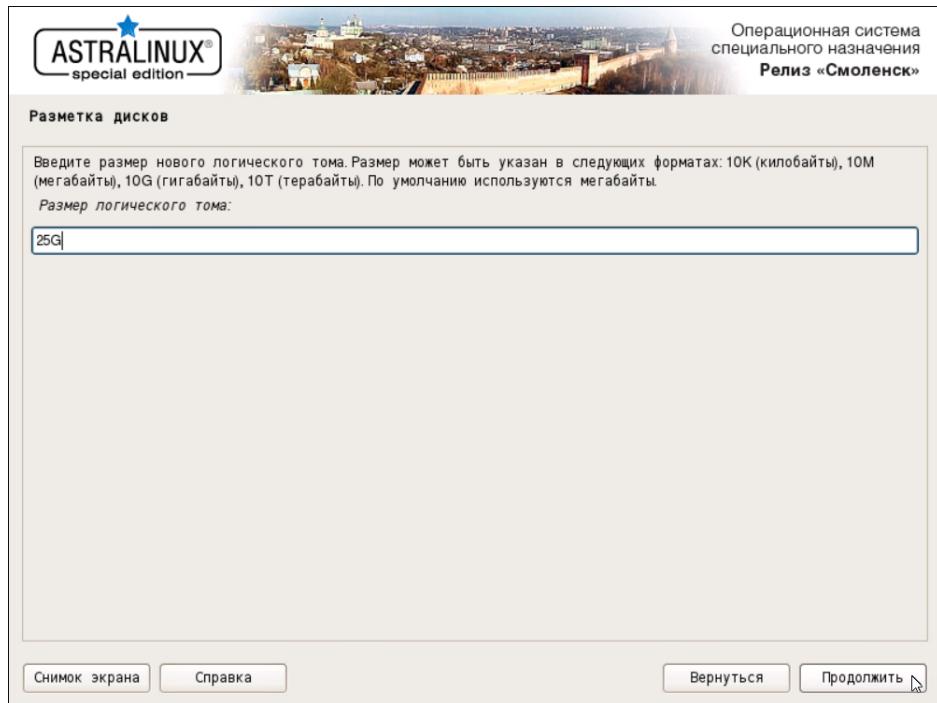


Рис. 4.23. Выделение размера для логического тома root

29. Создайте том с названием **var** и выделите для него 50 ГБ, выполняя действия шагов [26](#), [27](#) и [28](#).

30. Создайте тома, выполняя действия шагов [26](#), [27](#) и [28](#), в зависимости от назначения узла:

- При установке на master-узел – создайте тома **data** и **opt**. Для тома **data** выделите дисковое пространство в соответствии с требованиями к размеру хранилища. Рекомендуется выделить не менее 100 ГБ дискового пространства.

Внимание!

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

- При установке на slave-узел – создайте тома **opt** и **data**. Для тома **opt** выделите не менее 130 ГБ дискового пространства, а для тома **data** – все оставшееся дисковое пространство.

31. В появившемся окне **Настройка LVM** выберите вариант **Закончить**. Нажмите **Продолжить**.

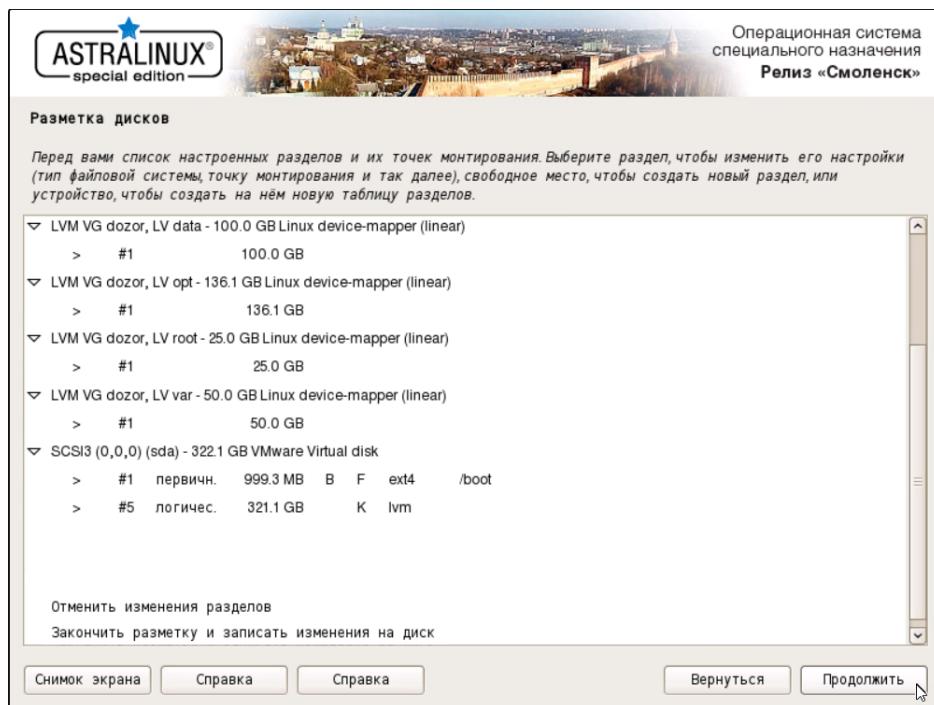


Рис. 4.24. Разметка дисков для master-узла

Примечание

На master-узле размер тома **opt** можно уменьшить до 50 ГБ.

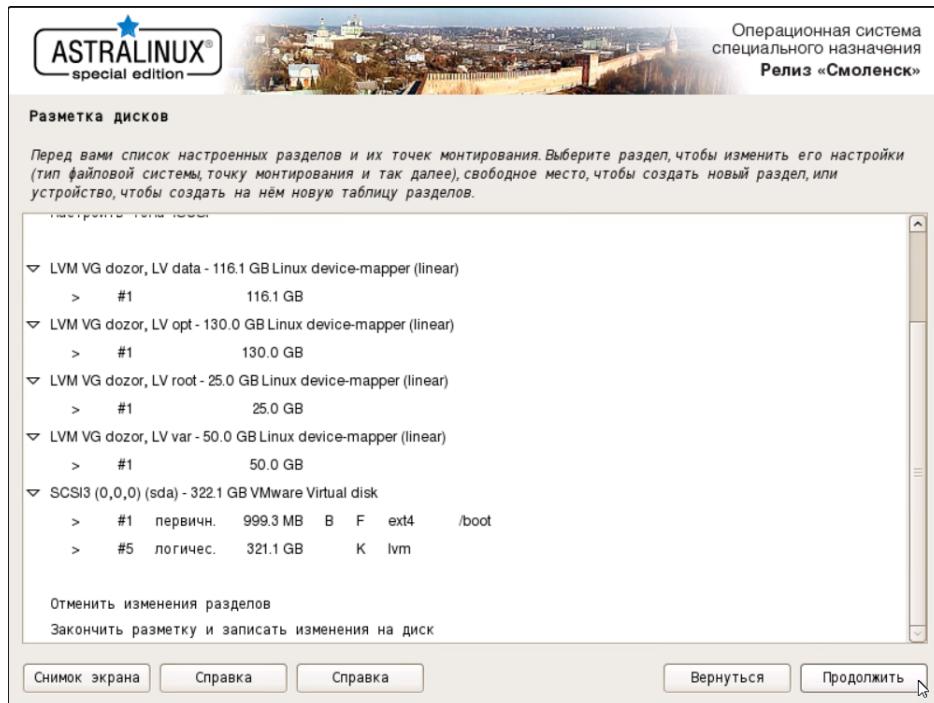


Рис. 4.25. Разметка дисков для slave-узла

32. Задайте точки монтирования и файловые системы для созданных томов. Например, для тома **root** выделите строку:

```
> #1 25.0 GB
```

Нажмите **Продолжить** (или выполните двойной щелчок на этой строке). В появившемся окне двойным щелчком мыши откройте параметры строки **Использовать как: не использовать**. В появившемся окне выберите строку **Журналируемая файловая система Ext4** и нажмите **Продолжить**. В окне настроек тома откройте параметры строки **Точка монтирования** и выберите точку монтирования **/ -- корневая файловая система**. В окне настроек тома выполните двойной щелчок по строке **Настройка раздела закончена**.

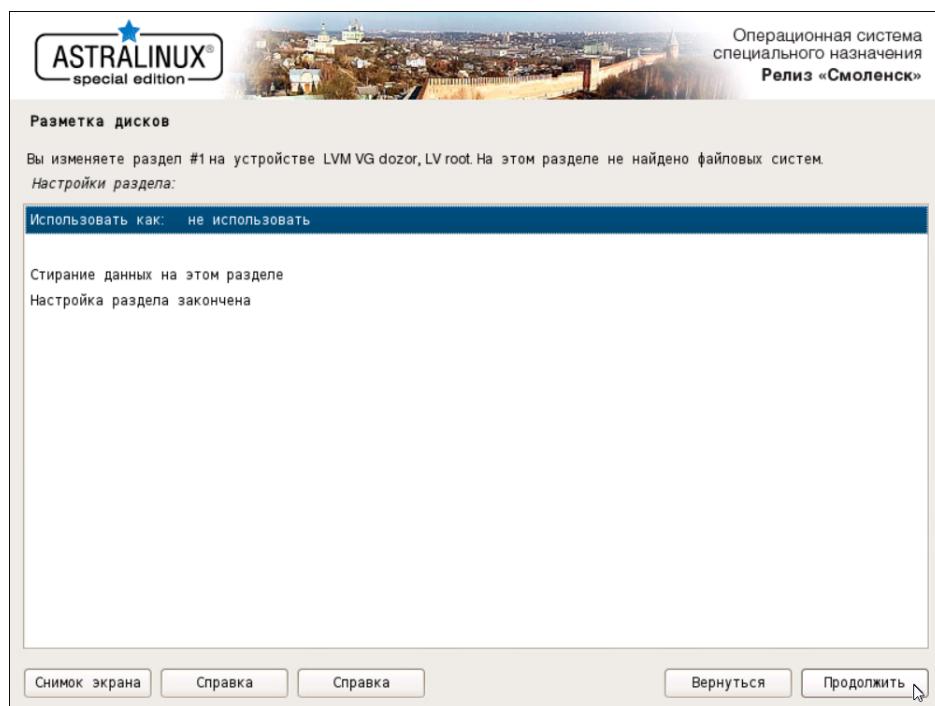


Рис. 4.26. Настройки тома root

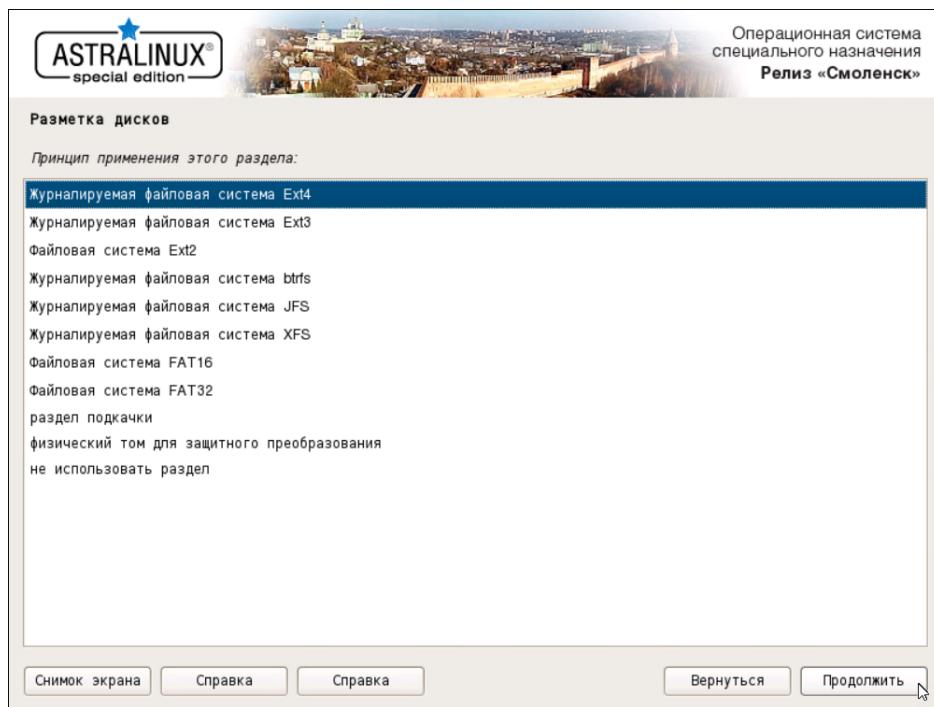


Рис. 4.27. Выбор файловой системы

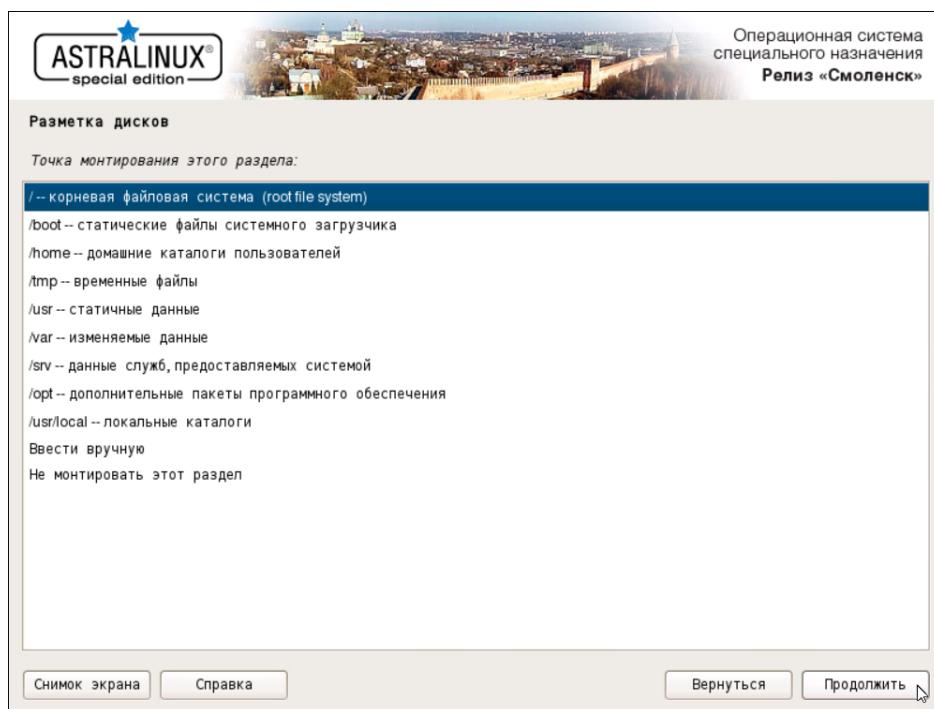


Рис. 4.28. Выбор точки монтирования

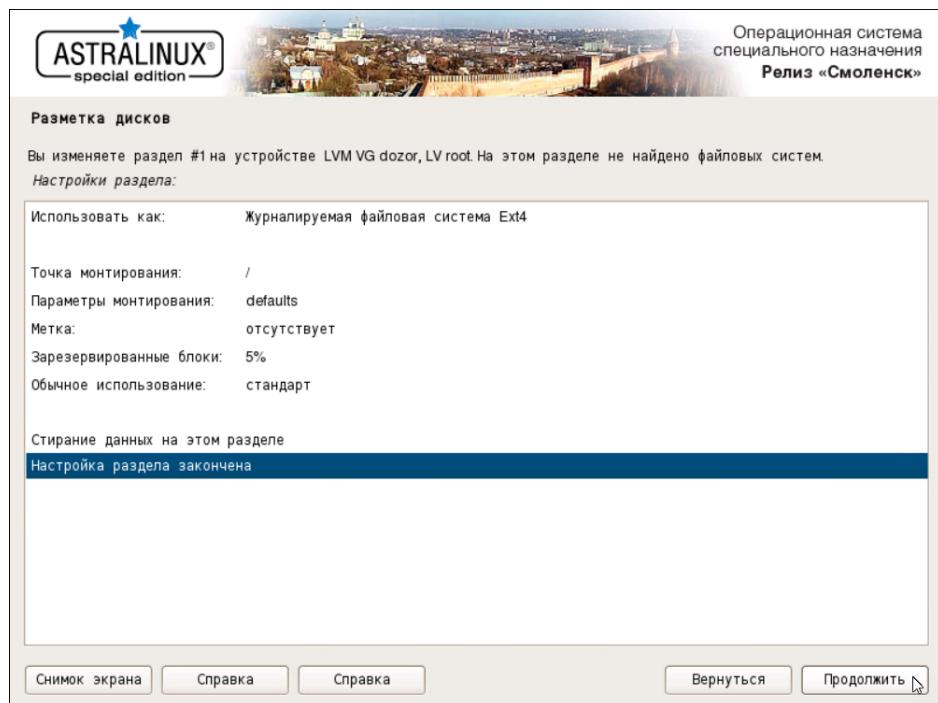


Рис. 4.29. Заполненные настройки тома root

33. Выполните действия предыдущего шага, задавая следующие точки монтирования и файловые системы:

- **var – /var, ext4**
- **data – /data, ext4 либо xfs** (см. примечание)
- **opt – /opt, ext4**

Примечание

Выберите значение ext4 или xfs в зависимости от задач.

При выборе точек монтирования для тома **data** следует выбирать пункт **Ввести вручную**.

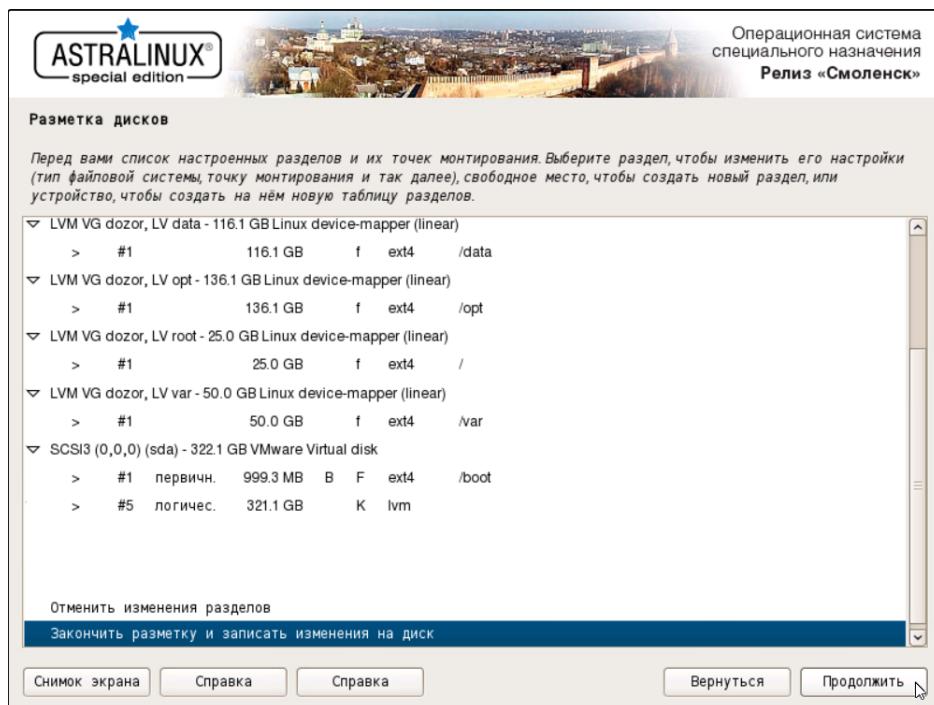


Рис. 4.30. Заполненные настройки томов для master-узла



Рис. 4.31. Заполненные настройки томов для slave-узла

34. Выберите строку **Закончить разметку и записать изменения на диск** и нажмите **Продолжить**.
35. В появившемся окне будет отображено предупреждение об отсутствии разделов для пространства подкачки. Следует выбрать **Нет** и нажать **Продолжить**.

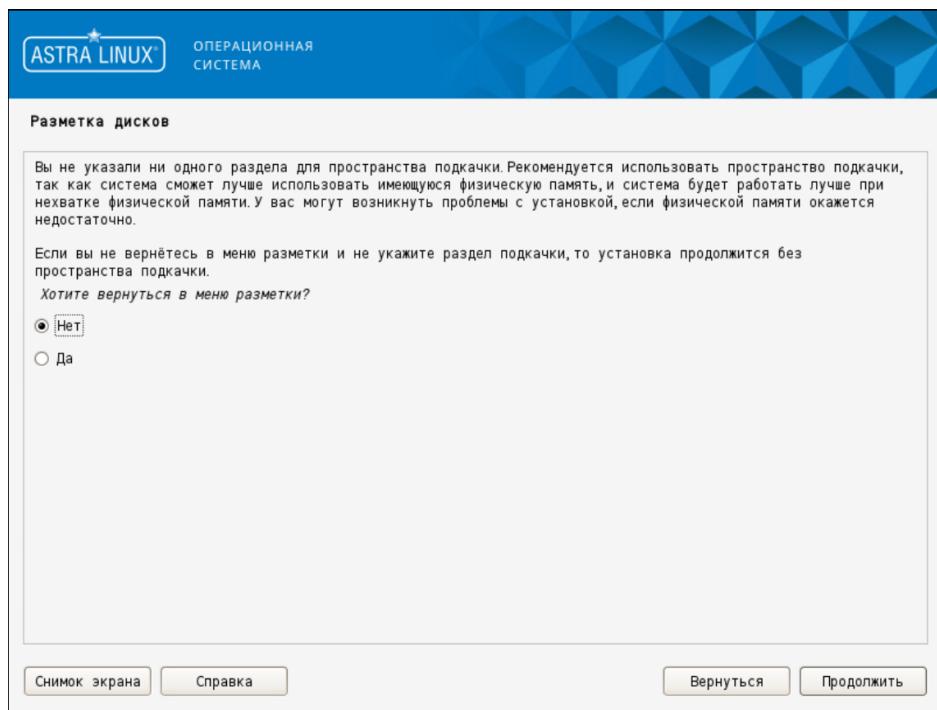


Рис. 4.32. Предупреждение об отсутствии разделов для пространства подкачки

36. В появившемся окне будет отображена информация о разметке дисков. Убедитесь, что эта информация верна, выберите **Да** и нажмите **Продолжить**.

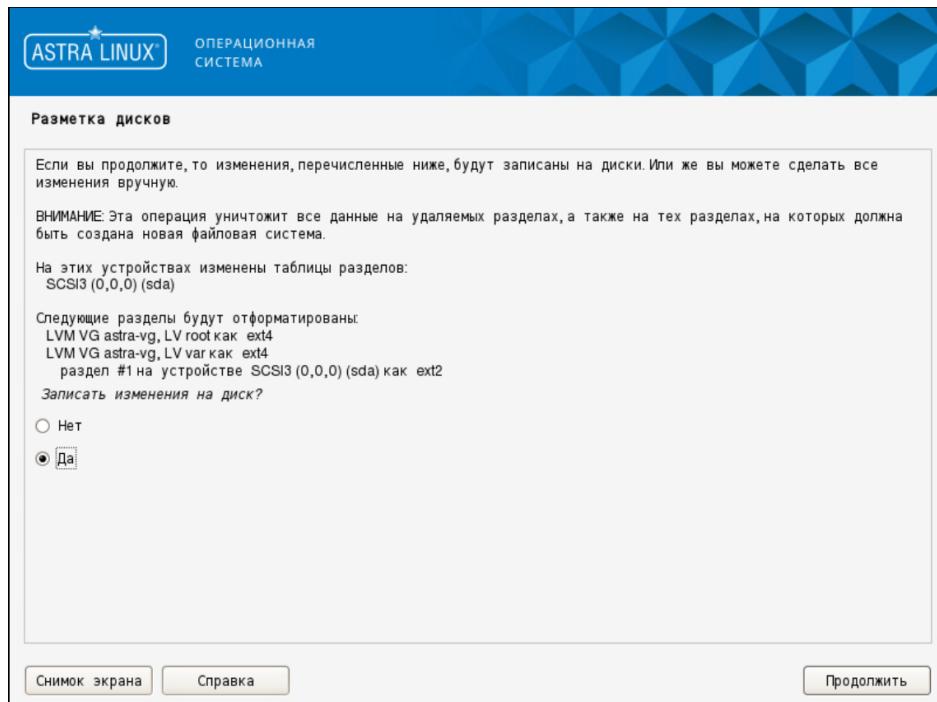


Рис. 4.33. Информация о разметке дисков

37. Дождитесь установки базовой системы. В появившемся окне выберите ядро **linux-5.10-generic**.

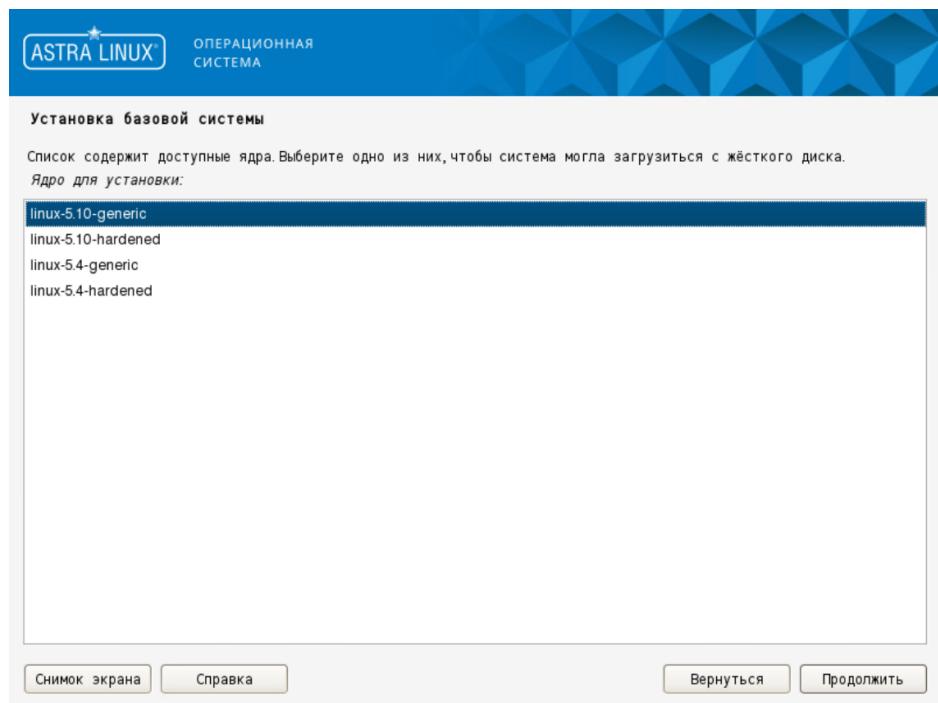


Рис. 4.34. Выбор ядра

Примечание

Версия ядра может меняться в зависимости от установленной версии ОС Astra Linux.

38. После окончания установки в появившемся окне **Выбор программного обеспечения** выберите варианты **Консольные утилиты** и **Средства удаленного доступа SSH**. Нажмите **Продолжить**.

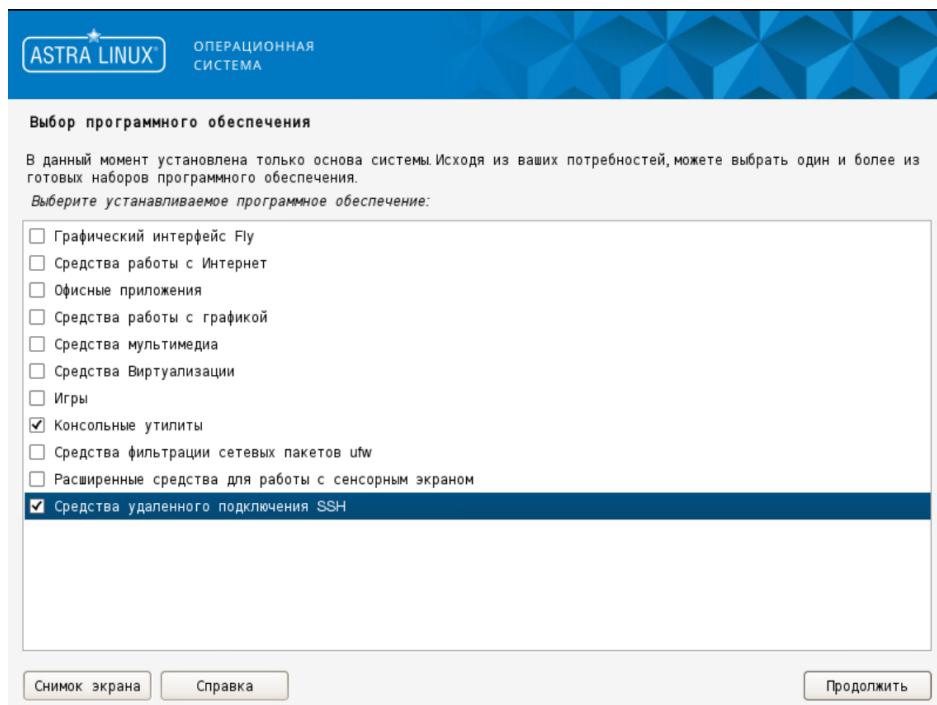


Рис. 4.35. Выбор программного обеспечения

39. В появившемся окне **Дополнительные настройки ОС** выберите **Максимальный уровень защищенности "Смоленск"**, если позволяет лицензия. Нажмите **Продолжить**.

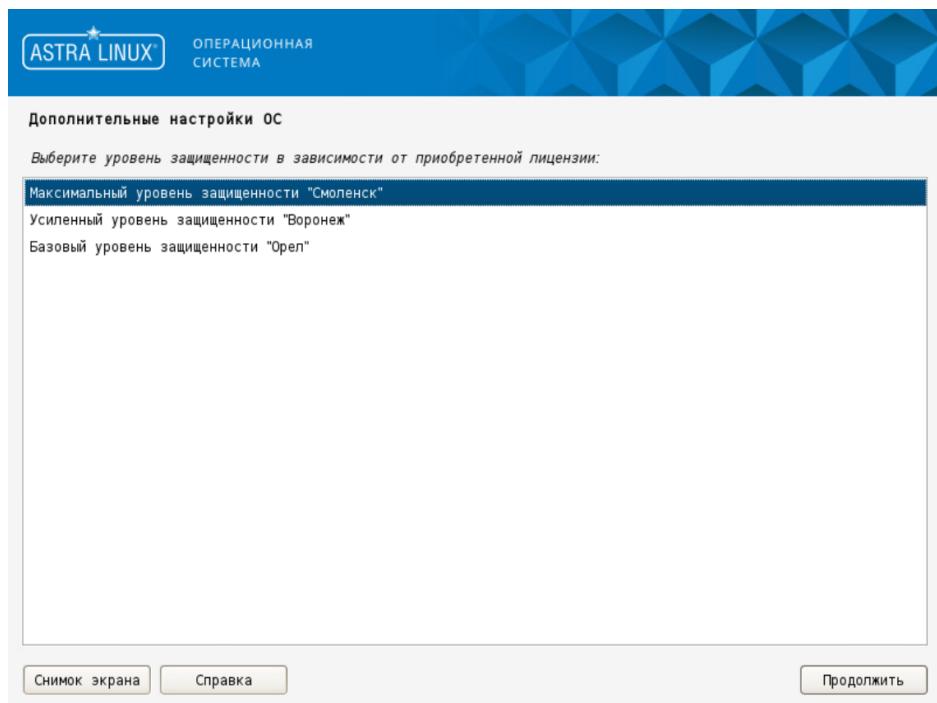


Рис. 4.36. Выбор уровня защищенности

40. В следующем окне снимите все флагки и нажмите **Продолжить**.

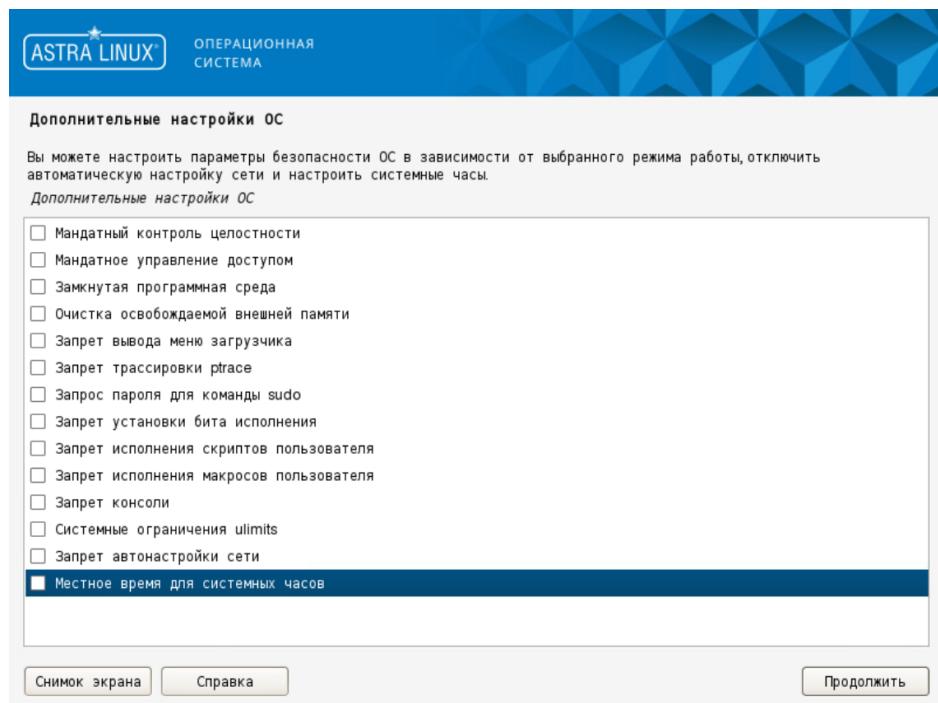


Рис. 4.37. Дополнительные настройки ОС

41. В появившемся окне **Установка системного загрузчика GRUB на жесткий диск** нажмите **Продолжить**.
42. В появившемся окне задайте пароль для системного загрузчика GRUB. Нажмите **Продолжить**, повторите ввод пароля и нажмите **Продолжить**.
43. После запроса системы отключите установочный носитель и нажмите **Продолжить**.
44. Перезагрузите систему и войдите под учетной записью администратора..
45. Запустите SSH-сервер, выполнив команды:

```
~$ sudo systemctl start ssh
```

```
~$ sudo systemctl enable ssh
```

Примечание

Здесь и далее команды CLI следует выполнять от имени суперпользователя, используя команду:

sudo

46. Узнайте имя сетевого интерфейса, выполнив команду:

```
~$ ip a
```

Вывод команды будет содержать пронумерованный список имен сетевых интерфейсов (включая локальную петлю под номером 1).

47. Откройте для редактирования файл **/etc/network/interfaces.d/eth0** (где **eth0** – имя сетевого интерфейса, полученного на предыдущем шаге) и внесите необходимые изменения в соответствии с существующей в компании сетевой архитектурой:

```
auto eth0
iface eth0 inet static
address <IP>/<mask>
gateway <IP>
```

Если файл **/etc/network/interfaces.d/eth0** пуст, выполните следующие действия:

- Откройте для редактирования файл **/etc/network/interfaces** и задайте конфигурацию сети. Пример для автоматического конфигурирования с использованием DHCP:

```
auto eth0
allow-hotplug eth0
iface eth0 inet dhcp
```

Пример для ручного конфигурирования:

```
auto eth0
iface eth0 inet static
address <IP>
netmask <mask>
gateway <gateway>
dns-nameservers <dns>
```

где:

- **<IP>** – статический IP-адрес сервера.
 - **<mask>** – маска сети.
 - **<gateway>** – адрес сетевого шлюза.
 - **<dns-nameservers>** – IP-адрес сервера DNS. Можно указать несколько адресов, перечисляя их через пробел.
- Выполните действия шага [a](#) для всех остальных сетевых интерфейсов.

48. Перезапустите сетевую службу, выполнив команду:

```
~$ sudo systemctl restart networking
```

49. Выполните команды:

```
~$ sudo systemctl disable ufw
```

```
~$ sudo init 6
```

Примечание

*Если политикой безопасности организации разрешено использование учетной записи суперпользователя **root**, выполните действия:*

a. Авторизуйтесь под учетной записью **root**, выполнив команду:

```
~$ sudo su -
```

b. Задайте пароль этой учетной записи, выполнив команду:

```
~$ passwd
```

c. Разрешите авторизацию и вход под этой учетной записью, выполнив команду:

```
~$ echo "PermitRootLogin yes" >> /etc/ssh/sshd_config
```

d. Перезапустите сервис **ssh**, выполнив команду:

```
~$ systemctl restart ssh
```

50. Если используется точка монтирования для раздела **/tmp**, убедитесь, что он находится на master-узле и примонтирован без использования параметра **noexec**. Для этого в CLI выполните команду:

```
# mount | grep /tmp | grep noexec
```

Вывод команды должен быть пустым. В противном случае следует поменять параметр монтирования для раздела **/tmp** и перемонтировать его. Для этого:

- a. Откройте для редактирования файл **/etc/fstab** и найдите в нем строку, относящуюся к разделу **/tmp**.
- b. Заменить параметр **noexec** на **exec**.
- c. Сохраните и закройте файл.
- d. Перемонтируйте раздел, выполнив команду:

```
# mount -o remount,exec /tmp
```

Примечание

Для увеличения производительности прокси-сервера на высоконагруженных системах в CLI в файле **etc/sysctl.conf** укажите значения параметров:

```
net.ipv4.tcp_max_syn_backlog = 40000
```

```
net.core.somaxconn = 40000
```

```
net.core.wmem_default = 8388608
```

```
net.core.rmem_default = 8388608
```

```
net.ipv4.tcp_sack = 1
```

```
net.ipv4.tcp_window_scaling = 1
```

```
net.ipv4.tcp_tw_reuse = 1
```

```
net.ipv4.tcp_moderate_rcvbuf = 1
net.core.rmem_max = 134217728
net.core.wmem_max = 134217728
net.ipv4.tcp_mem = 134217728 134217728 134217728
net.ipv4.tcp_rmem = 4096 277750 134217728
net.ipv4.tcp_wmem = 4096 277750 134217728
net.core.netdev_max_backlog = 300000
```

4.2. Подготовка к установке Solar webProxy

Приведенные в этом разделе процедуры предварительной настройки должны быть выполнены на всех серверах Solar webProxy.

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

4.2.1. Настройка DNS

Внимание!

Необходимо настроить FQDN на master-узле до установки Solar webProxy.

На вышестоящем прокси-сервере работа с FQDN серверов выполняется только с использованием DNS, без поддержки локального файла **/etc/hosts** или аналога.

Настройка DNS выполняется в файле **/etc/resolv.conf**. Информация из файла считывается только при запуске сервиса **wizor**, поэтому после внесения любых изменений в файле требуется перезапуск сервиса **wizor**.

Проверьте содержимое следующих файлов настройки DNS на всех узлах Solar webProxy:

- **/etc/hosts**

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

```
10.199.21.148 proxymaster.company.local proxymaster
10.199.21.149 filter1.company.local filter1
10.199.21.147 filter2.company.local filter2
```

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

Внимание!

Строки, содержащие информацию об узлах кластера, должны совпадать на всех узлах кластера (можно заполнить файл **hosts** на одном узле и затем скопировать его на все остальные).

При указании доменного имени узла нельзя использовать символ подчеркивания.

Ресурсные записи указанных DNS-серверов должны совпадать.

4.2.2. Настройка синхронизации времени

Синхронизация времени внутри кластера Solar webProxy 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 на всех узлах Solar webProxy выполните следующие действия:

1. Найдите нужную времененную зону, выполнив следующую команду:

```
# timedatectl list-timezones
```

Для удобства поиска можно воспользоваться сортировкой, например:

```
# timedatectl list-timezones | grep Europe
```

2. Установите нужную времененную зону, выполнив команду следующего вида:

```
# timedatectl set-timezone <timezone>
```

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

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

```
# timedatectl
```

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

```
# sudo apt-get install ntp
```

5. Откройте для редактирования файл **/etc/ntp.conf** и добавьте 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 счет 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. Запустите службу NTP и добавьте ее в автозагрузку, выполнив команды:

```
# systemctl start ntp
```

```
# systemctl enable ntp
```

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

```
# ntpq -p
```

4.2.3. Проверка и настройка БД Clickhouse (инструкции **sse4_2**)

Solar webProxy использует БД Clickhouse. Для корректного функционирования этой БД необходимо, чтобы процессор поддерживал набор инструкций **sse4_2**. Проверить наличие этой поддержки можно с помощью команды:

```
# grep sse4_2 /proc/cpuinfo
```

Вывод команды не должен быть пустым.

4.3. Установка Solar webProxy

Примечание

Для отключения отправки пакетов ICMP redirect (ICMP type 5) на узле:

1. В CLI в файле **etc/sysctl.conf** добавьте параметры:

```
net.ipv4.conf.all.accept_redirects = 0
```

```
net.ipv4.conf.all.send_redirects = 0
```

```
net.ipv4.conf.default.accept_redirects = 0
```

```
net.ipv4.conf.default.send_redirects = 0
```

2. Перезагрузите устройство.

Для установки Solar webProxy для ОС Astra Linux версии 1.7.6 на master-узле в CLI выполните команды:

```
# chmod +x /var/tmp/solar-wp-4.3.1-366.astra17-1.7.6-signed.run
```

```
# /var/tmp/solar-wp-4.3.1-366.astra17-1.7.6-signed.run --install
```

где **/var/tmp/solar-wp-4.3.1-366.astra17-1.7.6-signed.run** – путь к инсталлятору.

Для установки Solar webProxy для ОС Astra Linux версии 1.7.7 на master-узле в CLI выполните команды:

```
# chmod +x /var/tmp/solar-wp-4.3.1-366.astra17-1.7.7-signed.run
```

```
# /var/tmp/solar-wp-4.3.1-366.astra17-1.7.7-signed.run --install
```

где `/var/tmp/solar-wp-4.3.1-366.astra17-1.7.7-signed.run` – путь к инсталлятору.

Примечание

При необходимости после установки на master-узле повторите выполнение команд на каждом slave-узле кластера.

4.3.1. Отключение службы управления межсетевым экранированием

Для корректной работы Solar webProxy необходимо отключить системную службу управления межсетевым экраном ufw. Для этого в CLI выполните команды:

Чтобы после установки появился доступ в веб-интерфейс, отключите службы управления межсетевым экранированием, выполнив команды:

```
# systemctl stop ufw
```

```
# systemctl disable ufw
```

4.4. Обновление Solar webProxy

Для обновления Solar webProxy для ОС Astra Linux версии 1.7.6:

1. На master-узле в CLI выполните команды:

```
# /opt/dozor/bin/shell
```

```
# dsctl down
```

```
# chmod +x /var/tmp/solar-wp-4.3.1-366.astra17-1.7.6-signed.run
```

```
# /var/tmp/solar-wp-4.3.1-366.astra17-1.7.6-signed.run --install
```

где `/var/tmp/solar-wp-4.3.1-366.astra17-1.7.6-signed.run` – путь к инсталлятору.

2. Выполните команду:

```
# /opt/dozor/bin/shell
```

3. Запустите master-узел, выполнив команду:

```
# dsctl boot
```

4. Выполните перезагрузку monitor-server с помощью команды:

```
# dsctl restart monitor-server
```

5. В любом слое раздела **Политика** нажмите **Применить политику** или в CLI выполните команду:

```
# policy-tool apply
```

6. После обновления master-узла выполните обновление всех slave-узлов кластера. Для этого повторите выполнение шагов 1-6 на каждом slave-узле.
7. Для полного перезапуска сервисов и корректного применения конфигурации перезагрузите все узлы командой:

```
# reboot
```

Для обновления Solar webProxy для ОС Astra Linux версии 1.7.7:

1. На master-узле в CLI выполните команды:

```
# /opt/dozor/bin/shell
```

```
# dsctl down
```

```
# chmod +x /var/tmp/solar-wp-4.3.1-366.astra17-1.7.7-signed.run
```

```
# /var/tmp/solar-wp-4.3.1-366.astra17-1.7.7-signed.run --install
```

где `/var/tmp/solar-wp-4.3.1-366.astra17-1.7.7-signed.run` – путь к инсталлятору.

2. Обновите ОС Astra Linux Special Edition до версии 1.7.7 «Смоленск» с помощью команд:

```
# apt install astra-update -y;astra-update -A -r -T
```

```
# systemctl disable ufw
```

```
# reboot
```

3. Выполните команду:

```
# /opt/dozor/bin/shell
```

4. Запустите master-узел, выполнив команду:

```
# dsctl boot
```

5. Выполните перезагрузку monitor-server с помощью команды:

```
# dsctl restart monitor-server
```

6. В любом слое раздела **Политика** нажмите **Применить политику** или в CLI выполните команду:

```
# policy-tool apply
```

7. После обновления master-узла выполните обновление всех slave-узлов кластера. Для этого повторите выполнение шагов 1-6 на каждом slave-узле.

8. Для полного перезапуска сервисов и корректного применения конфигурации перезагрузите все узлы командой:

```
# reboot
```

4.5. Удаление Solar webProxy

Для удаления Solar webProxy:

1. Остановите процессы Solar webProxy, выполнив команду:

```
# /opt/dozor/bin/dsctl down
```

2. Удалите Solar webProxy, выполнив команду:

```
# apt remove `apt list --installed | grep -o '^[^"]*solar[^/]*'
```

3. Удалите каталоги установки Solar webProxy, выполнив команды:

```
# rm -rf /opt/dozor
```

4. Удалите каталог размещения репозитория Solar webProxy с данными, выполнив команду:

```
# rm -rf /data
```

5. Если не предполагается использовать в дальнейшем пользователя **dozor**, удалите:

- пользователя **dozor** из системы, выполнив команду:

```
# userdel dozor
```

- из файла **/etc/sudoers** запись:

```
dozor ALL=(ALL) NOPASSWD: ALL
```

6. Удалите почтовый ящик пользователя **dozor**, выполнив команду:

```
# rm /var/mail/dozor
```

7. При необходимости удалите из **/etc/krb5.conf** и **/etc/krb5.conf.save** записи вида:

```
default = FILE:/opt/dozor/var/log/krb5libs.log
kdc = FILE:/opt/dozor/var/log/krb5kdc.log
admin_server = FILE:/opt/dozor/var/log/kadmind.log
```

Примечание

После удаления Solar webProxy настройте и включите системную службу управления межсетевым экраном *ufw*.

5. Первоначальная настройка Solar webProxy

5.1. Настройка кластера

После установки пакетов Solar webProxy на все узлы кластера:

1. Примечание

Данный пункт не нужно выполнять, если система устанавливалась автоматически с помощью ISO-образа.

Выберите среди узлов кластера сервер, который планируется использовать как master-узел, подключитесь к нему по SSH и назначьте ему управляющую роль, выполнив следующие команды:

```
# /opt/dozor/bin/shell
```

```
# set-role master main
```

2. Запустите сервис, выполнив команду:

```
# dsctl boot
```

3. Зарегистрируйте slave-узлы в кластере, выполнив на всех slave-узлах следующие команды:

```
# /opt/dozor/bin/shell
```

```
# reg-slave <master-host> [name]
```

```
# dsctl boot
```

где **<master-host>** – FQDN master-узла (например, **proxymaster.company.local**), а **[name]** – имя регистрируемого узла, которое будет отображаться в GUI Solar webProxy.

4. Подключитесь к сервису ssh. Для этого:

a. На slave-узле сгенерируйте ключи под учетной записью **dozor** с помощью команды:

```
$ ssh-keygen -t rsa
```

b. В качестве директории, где будут храниться сгенерированные ключи, укажите папку **/opt/dozor/.ssh/**.

c. Скопируйте открытый ключ **id-rsa.pub** на main-узел в директорию **/opt/dozor/.ssh/** с помощью команды:

```
$ scp /opt/dozor/.ssh/id_rsa.pub dozor@<master-host>:/opt/dozor/.ssh/
```

d. Подключитесь на main-узел под учетной записью **dozor**, выполнив команду:

```
$ su - dozor
```

e. Создайте в папке **.ssh** файл **authorized_keys**, выполнив команды:

```
$ cd /opt/dozor/.ssh
```

```
$ touch authorized_keys
```

- f. Скопируйте содержимое файла **id-rsa.pub** в файл **authorized_keys**, выполнив команды:

```
$ cat id_rsa.pub > authorized_keys
```

- g. Проверьте настройки ssh в файле **/etc/ssh/sshd_config** с помощью команды:

```
$ nano /etc/ssh/sshd_config
```

В файле должны присутствовать строки:

```
AuthorizedKeysFile /opt/dozor/.ssh/authorized_keys
PubkeyAuthentication yes
```

- h. Перезапустите сервис ssh, выполнив команду:

```
~$ systemctl restart sshd
```

- i. Проверьте соединение со slave-узла под пользователем **dozor**, выполнив команду:

```
$ ssh dozor@<master-host>
```

5. На master-узле обновите мониторинг, выполнив команду:

```
# /opt/dozor/bin/dsctl restart monitor-server
```

5.2. Первый вход в систему и загрузка лицензии

После настройки кластера смените пароль по умолчанию для доступа к GUI:

1. Откройте браузер и перейдите по адресу <https://<master-host>:8443> либо <https://<master-ip>:8443>, где:
 - <master-host> – полное доменное имя master-узла. Например, **proxymaster.company.local**;
 - <master-ip> – IP-адрес master-узла. Например, 10.199.21.148.
2. В открывшемся окне авторизации введите имя пользователя и пароль по умолчанию: **admin/admin**. После этого система потребует изменить пароль.
3. Следует установить новый пароль требуемого уровня надежности (см. раздел [3.2.6](#)) и авторизоваться с новым паролем.

После первоначальной смены пароля в верхней части экрана появится уведомление об отсутствии лицензии.

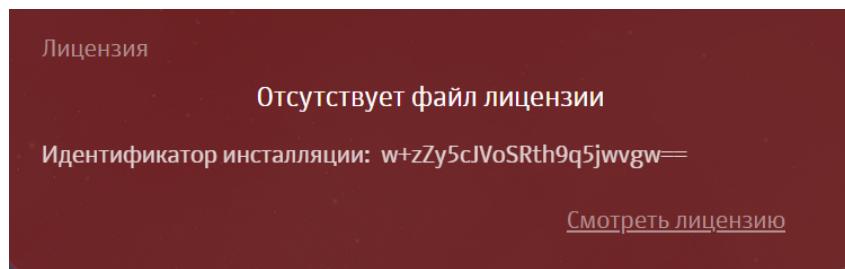


Рис. 5.1. Уведомление об отсутствии лицензии

Для загрузки лицензии:

1. В меню пользователя нажмите кнопку **Лицензия** и в окне **Лицензия** нажмите **Загрузить лицензию**.
2. В открывшемся окне укажите путь к файлу с лицензией, после чего нажмите кнопку **Открыть (Open)** и дождитесь загрузки лицензии. Она автоматически сохранится в файле с именем **license.xml**.

Примечание

Лицензия выдается на мажорную версию Solar webProxy. То есть лицензия на Solar webProxy версии 4 действует на все версии от 4.0 и далее.

Для просмотра сведений о лицензии Solar webProxy выберите пункт меню пользователя **Лицензия**.

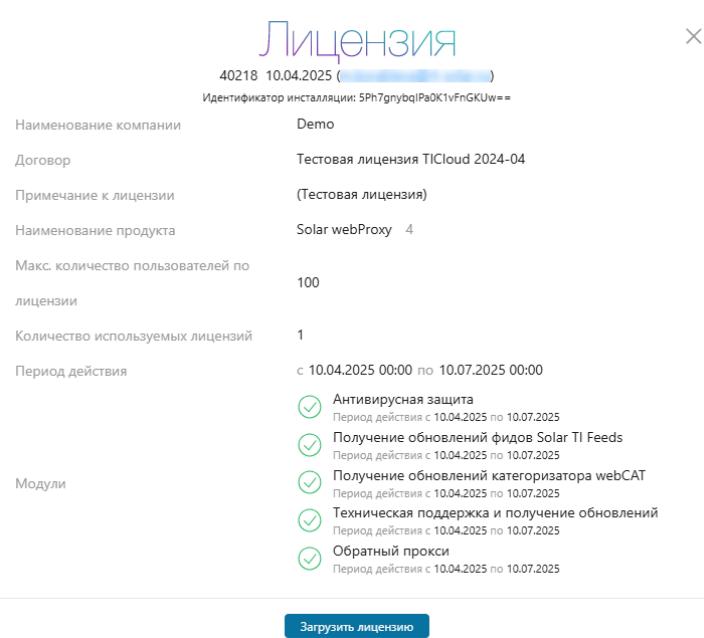


Рис. 5.2. Окно с информацией о лицензии

В Solar webProxy входят модули:

Табл. 5.1. Модули Solar webProxy в составе стандартной поставки

Название	Описание
Core	<p>Модуль реализует следующие функциональные возможности:</p> <ul style="list-style-type: none">● разграничение прав доступа к веб-ресурсам с использованием следующих механизмов аутентификации (в том числе SSO):<ul style="list-style-type: none">○ Basic,○ NTLM,○ Kerberos,○ по IP-адресам.● применение политик безопасности по следующим параметрам:<ul style="list-style-type: none">○ членство в группе,○ URL- или IP-адрес ресурса,○ ключевые слова,○ расписание,○ порты,○ протоколы (HTTP, HTTPS, FTP over HTTP и SOCKS5),○ тип передаваемого файла,○ категории веб-сайтов.● блокирование доступа, разрешение доступа как явное, так и с запросом подтверждения работника;● блокирование рекламных баннеров при помощи базы adBlock;● проверка на наличие вирусов в передаваемых файлах (при интеграции со сторонним антивирусом);● архивирование данных о передаваемой информации по результатам анализа;● категоризация веб-ресурсов встроенными механизмами (webCAT) и при интеграции с системами Symantec Blue Coat и SkyDNS;● ограничение доступа к веб-сайтам по базе данных категорий ресурсов (например, возможность ограничить доступ только к социальным сетям);● использование вышестоящего Solar webProxy, а также получения запроса по ICAP от другого Solar webProxy;● журналирование и составление журналов во всех стандартных форматах: Apache, Squid или Squid-detailed;

Название	Описание
	<ul style="list-style-type: none"> формирование статистических отчетов по критериям: адрес сайта, время доставки информации, объем доставляемой информации и т.д.
Antivirus	Модуль антивирусной защиты выполняет защиту устройств компьютерных сетей от внешних вирусных угроз

Табл. 5.2. Дополнительные модули Solar webProxy

Название	Описание
Обратный прокси	Подсистема обратного прокси выполняет ретрансляцию запросов, поступающих из внешней сети, на веб-сервер во внутренней сети, с возможностью их фильтрации
Агент	Модуль перенаправляет весь трафик рабочих станций на Solar webProxy, в том числе приложений. Поддерживает ОС Windows
Получение обновлений категоризатора webCAT	Модуль включает в себя автоматическое обновление баз категоризации webCAT. Поставляется только совместно с модулем Получение обновлений фидов Solar TI Feeds
Получение обновлений фидов Solar TI Feeds	Модуль включает в себя расширение источников фидов и их обновление. Поставляется только совместно с модулем Получение обновлений категоризатора webCAT
Централизованное управление	Единый интерфейс управления master-узлами Solar webProxy (модули Core). Является отдельной независимой инсталляцией
Контроль приложений	Модуль позволяет контролировать трафик приложений. Поставляется совместно с модулем Core

Примечание

Актуальные позиции прайса и соответствующие им модули можно получить в отделе продаж или на сайте rt-solar.ru.

Слева от названия модуля отображается его статус:

-  – модуль подключен;
-  – срок действия лицензии на модуль менее 30 дней, необходимо продлить лицензию;
-  – срок действия лицензии на модуль истек;
-  – при вычислении статуса произошла ошибка.

Постоянная лицензия Solar webProxy всегда жестко привязана к конкретной аппаратной платформе (виртуальной или физической) master-узла кластера Solar webProxy.

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 webProxy и передается инженерами внедрения в вендорскую службу поддержки, которая на его основе выпускает активированную лицензию для постоянного использования.

Примечание

Идентификатор инсталляции не зависит от характеристик оперативной памяти и жестких дисков. Их замена не приводит к прекращению действия лицензии.

Однако изменение хотя бы одной из характеристик master-узла, от которых зависит идентификатор инсталляции, приводит к недействительности выпущенной лицензии и неработоспособности Solar webProxy.

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.

5.3. Подключение к модулю MultiProxy

Для подключения Solar webProxy к модулю **MultiProxy** (подробнее см. *Руководство по работе с модулем MultiProxy*) выполните команду:

```
# /opt/dozor/bin/reg-control -h <multiproxy-host>
```

где **<multiproxy-host>** – FQDN узла с ролью **Централизованное управление** (например, `multiproximaster.company.local`).

Примечание

*По умолчанию внешний порт **MultiProxy** – 33088. Если порт был изменен, для подключения к модулю выполните команду:*

```
# /opt/dozor# reg-control -h <multiproxy-host> -p 33089
```

*где **33089** – внешний порт модуля **MultiProxy**.*

Чтобы отключить Solar webProxy от Централизованного управления выполните команду:

```
# /opt/dozor/bin/unreg-control -h <multiproxy-host>
```

где **<multiproxy-host>** – FQDN узла с ролью **Централизованное управление** (например, `multiproximaster.company.local`).

Примечание

Для корректного обновления модуля **MultiProxy** после обновления Solar webProxy на версию 4.3 в GUI необходимо внести любые изменения в разделе **Политика** и нажать кнопку **Применить политику**.

Если после обновления Solar webProxy на версию 4.3 в модуле **MultiProxy** отображается некорректная версия узла, удалите его – он будет добавлен в раздел **Инфраструктура > Нераспределенные узлы**, и оттуда перенесите его в нужную категорию раздела **Инфраструктура > Распределенные узлы**.

5.4. Управление настройками системы

Управлять конфигурацией и настройками системы в интерфейсе можно в следующих разделах системы:

- **Досье и Политика** на вкладке **Настройки**. Это значительно упрощает настройку системы и позволяет быстро вносить изменения в конфигурацию, не покидая раздела;
- **Система > Настройки**.

Для доступа к более широкому перечню настроек перейдите в раздел **Система > Настройки > Основные настройки > Досье** (см. [Рис.5.3](#)).

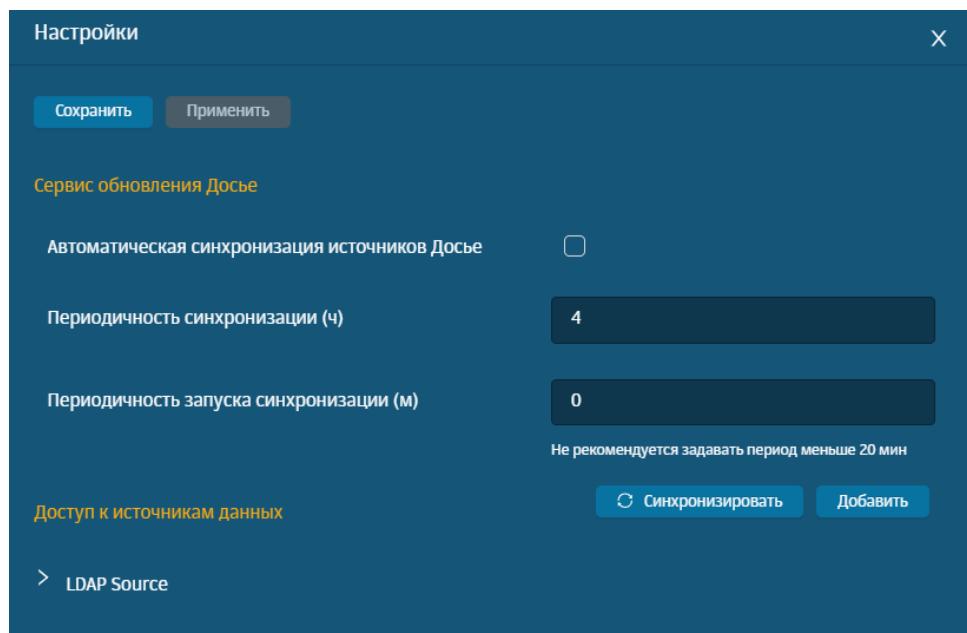


Рис. 5.3. Вкладка «Настройки» раздела «Досье»

Вкладка **Настройки** раздела **Политика** содержит те же параметры, что и раздел **Система > Настройки > Основные настройки > Работа системы** (см. [Рис.5.4](#)).

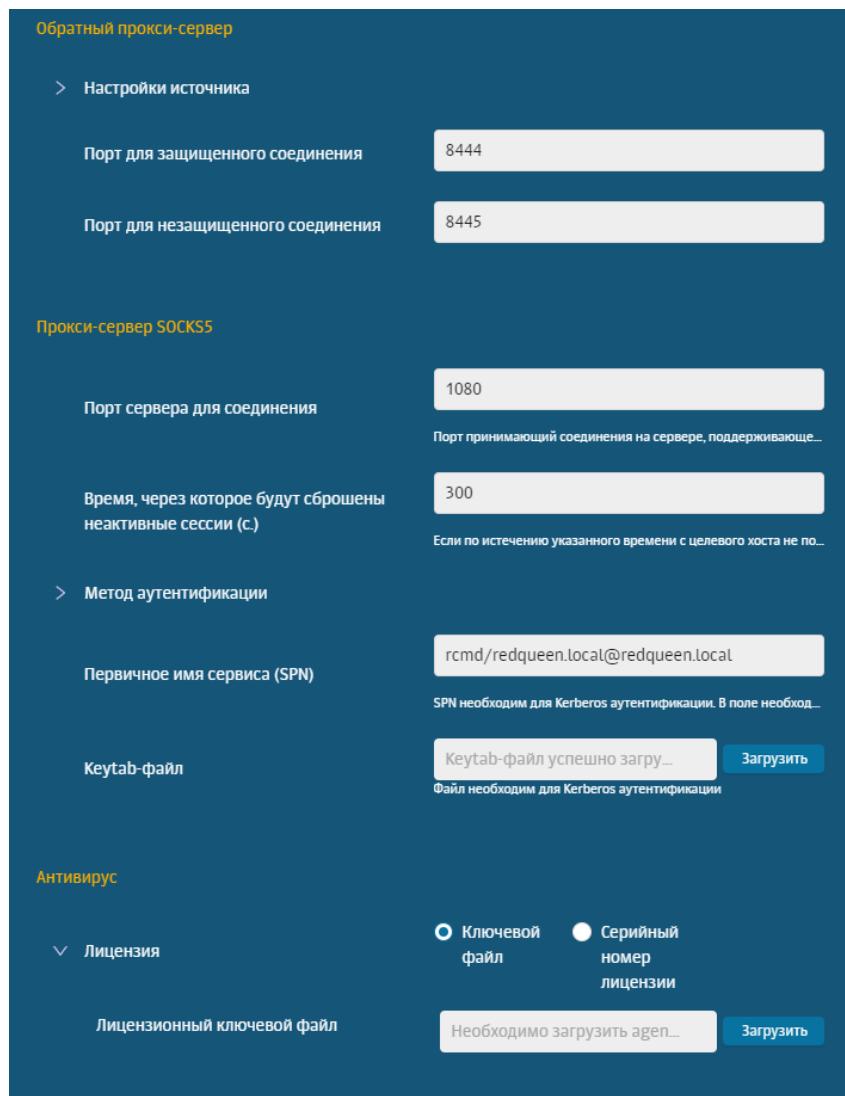


Рис. 5.4. Вкладка «Настройки» раздела «Политика»

В разделе **Система** на вкладке **Настройки** все параметры настройки сгруппированы по их назначению:

- для основных настроек системы – вкладка **Основные настройки** (см. [Рис.5.5](#));
- для использования расширенного набора настроек – вкладка **Расширенные настройки** (см. [Рис.5.6](#)).

Табл. 5.3. Группы основных настроек

Группа	Назначение
Аутентификация	Настройки аутентификации из внешних источников для фильтрации и веб-сервера: Kerberos, NTLM, LDAP и RADIUS аутентификация
Досье	Настройки взаимодействия с внешними системами, например, Active Directory. Содержит настройки обновления Досье и доступа к источникам данных для импорта данных пользователей из Active Directory
Журналирование	Настройка журналирования сервисов системы
Мониторинг	Определение перечня проверок и уведомлений от системы мониторинга
Производительность	Настройки производительности системы и потребления ресурсов

Группа	Назначение
Работа системы	Общая настройка работы системы: параметры фильтрации и анализа трафика системы, доступ администратора и лицензия антивируса

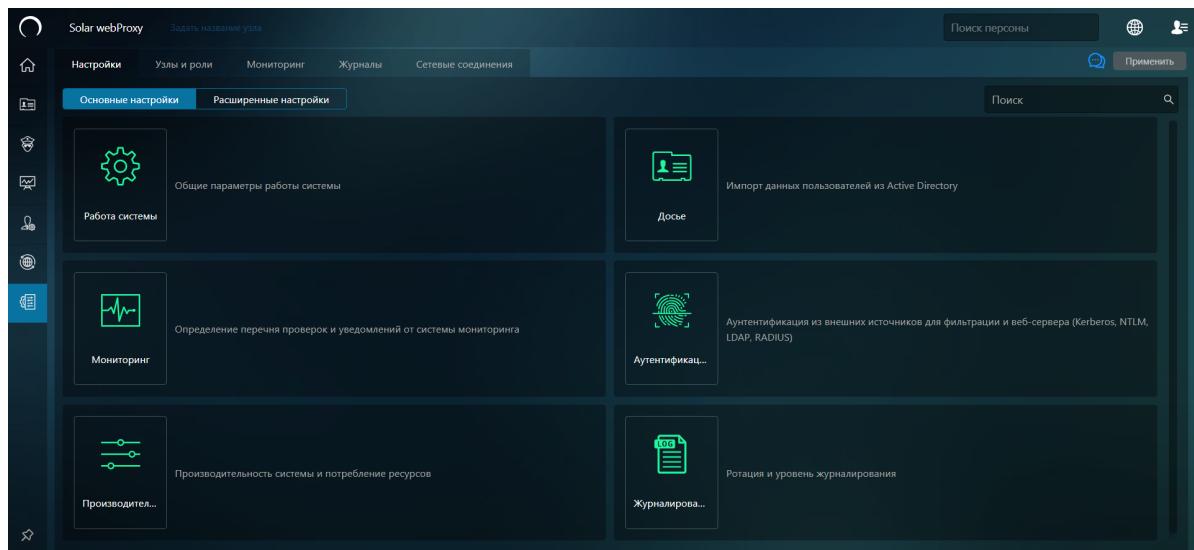


Рис. 5.5. Раздел «Система > Основные настройки»

Для корректной работы системы в большинстве случаев **достаточно задать основные настройки** (по умолчанию в Solar webProxy для всех параметров системы установлены рекомендуемые разработчиками значения).

Для более *детальной настройки системы* предусмотрены расширенные наборы параметров, сгруппированные по функциональным блокам системы. Следует учесть, что в основных и расширенных настройках параметры сгруппированы в разделы в зависимости от их назначения. Каждый раздел содержит секции, представляющие собой отдельные конфигурационные файлы.

Кроме того, из раздела с основными настройками можно быстро перейти по ссылке к расширенному списку параметров настройки.

Для более оперативной работы с конфигурацией предусмотрен поиск по названиям конфигурационных файлов, именам параметров и их значениям. Чтобы воспользоваться поиском, введите название искомого элемента или его часть в поле **Поиск**, расположенному в правой верхней части экрана (Рис.5.7). Чтобы перейти в раздел с искомым элементом, нажмите его имя (выделено синим).

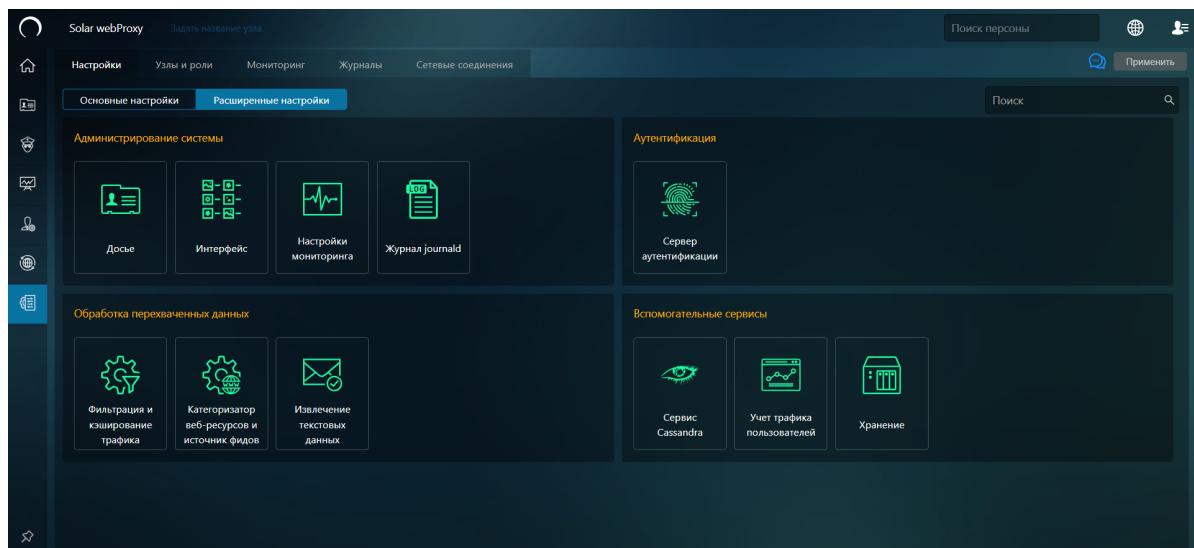


Рис. 5.6. Раздел «Система > Расширенные настройки»

Результаты поиска "host" в наборах настроек и отдельных параметрах			
название	идентификатор или файл	значение	перейти к настройкам ↑
Адрес сервера	host	ldap.example.ru	Общая конфигурация → Сервер аутентификации → Аутентификация / auth.scm
Адрес прокси-сервера	proxy-host	10.199.11.38	Общая конфигурация → Фильтрация и кэширование трафика → Обработка перехваченных данных / cache.json
Сетевой адрес сервиса ...	cassandra-host	\${node-ip}	Общая конфигурация → Фильтрация и кэширование трафика → Обработка перехваченных данных / config.json
Email получателя данн...	smtp-archiver-to	admin@localhost	Общая конфигурация → Фильтрация и кэширование трафика → Обработка перехваченных данных / config.json
Считать local host довер...	trust-local-host	true	Общая конфигурация → Фильтрация и кэширование трафика → Обработка перехваченных данных / config.json

Рис. 5.7. Поиск по конфигурации

После внесения изменений в значения параметров конфигурации сохраните их или отмените с помощью соответствующих кнопок:

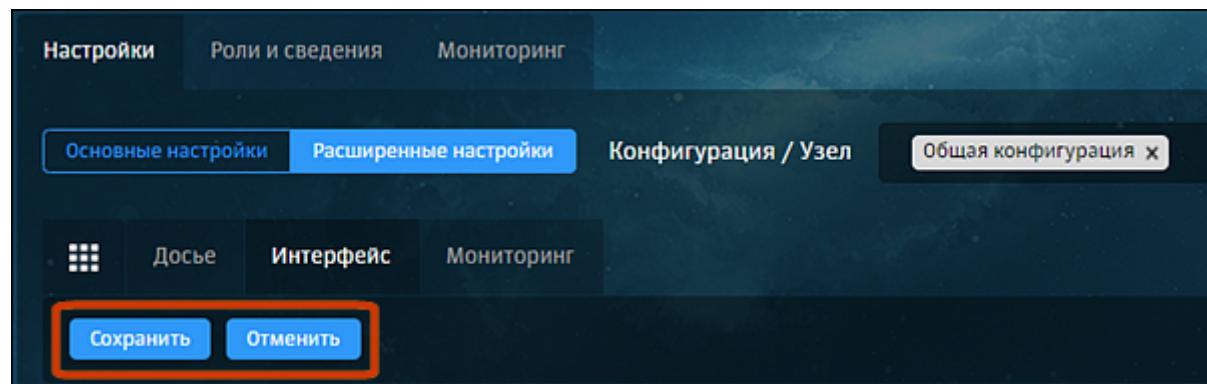


Рис. 5.8. Кнопки «Сохранить» и «Отменить»

Для применения настроек конфигурации нажмите кнопку **Применить**. Рядом с этой кнопкой расположена информационная иконка, при наведении курсора на которую появляются сведения о времени предыдущего применения настроек:

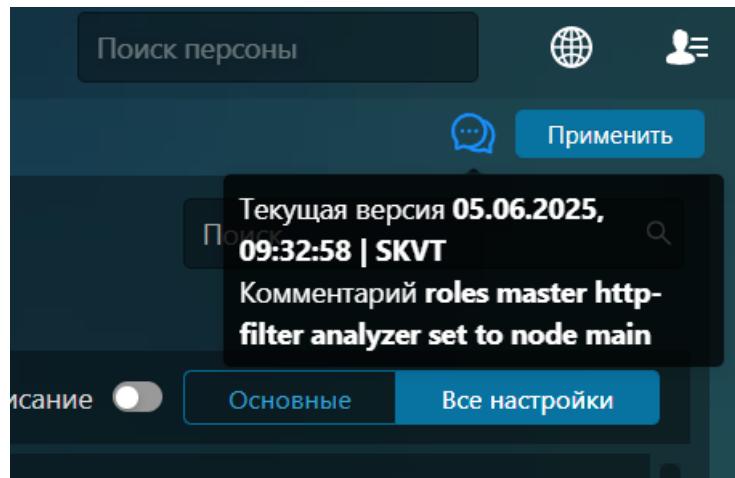


Рис. 5.9. Кнопка «Применить»

Для описания того или иного параметра можно отобразить подсказки к параметрам настройки конфигурации. Для отображения описания конкретного параметра наведите курсор мыши на его название.

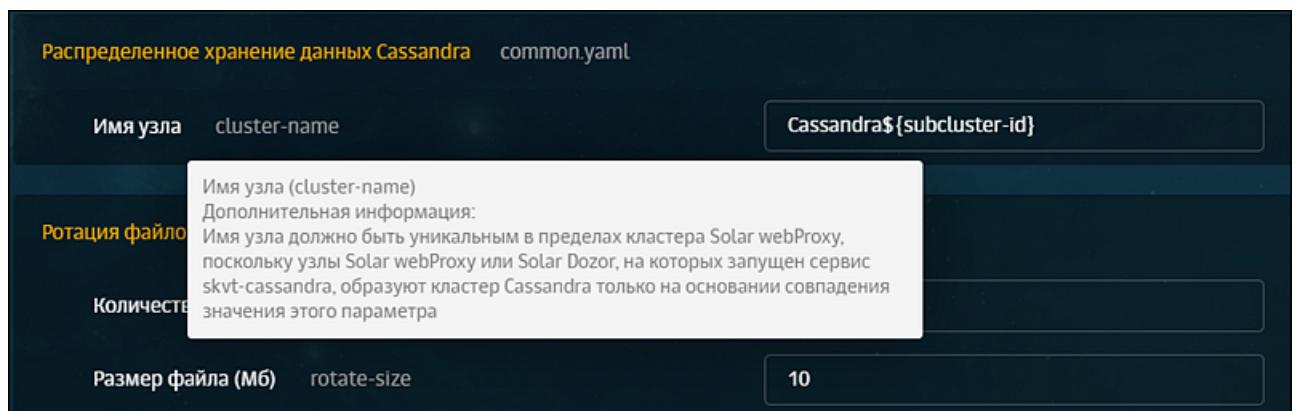


Рис. 5.10. Подсказка с описанием параметра

Для отображения всех подсказок включите **Показывать описание** в верхней части раздела.

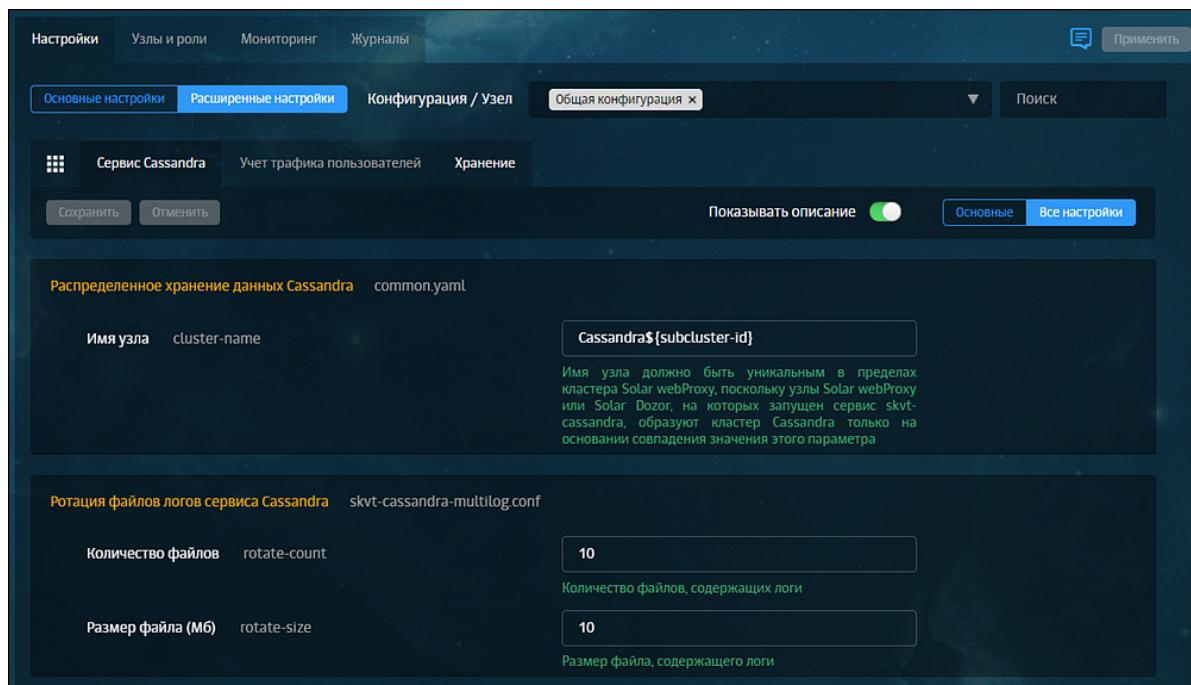


Рис. 5.11. Отображение подсказок

Чтобы задать индивидуальные параметры конфигурации для какого-либо узла, выберите этот узел в списке **Конфигурация/Узел** (Рис.5.12).

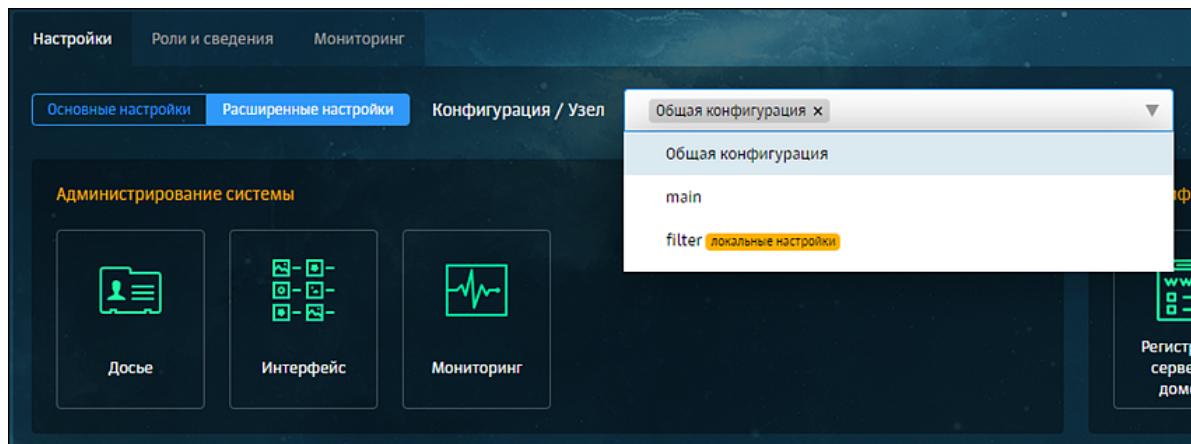


Рис. 5.12. Выбор узла

Если какой-либо узел имеет индивидуальные настройки (хотя бы один параметр), в списке **Конфигурация/Узел** рядом с названием этого узла будет расположена метка **локальные настройки**. Такая же метка будет расположена в записи об узле на вкладке **Узлы и роли**, а также на иконках тех разделов настроек, которые имеют индивидуальные настройки, при выборе этого узла в списке **Конфигурация/Узел**.

Примечание

*Информация о состоянии системы на вкладке **Узлы и роли** автоматически обновляется каждый раз при открытии вкладки.*

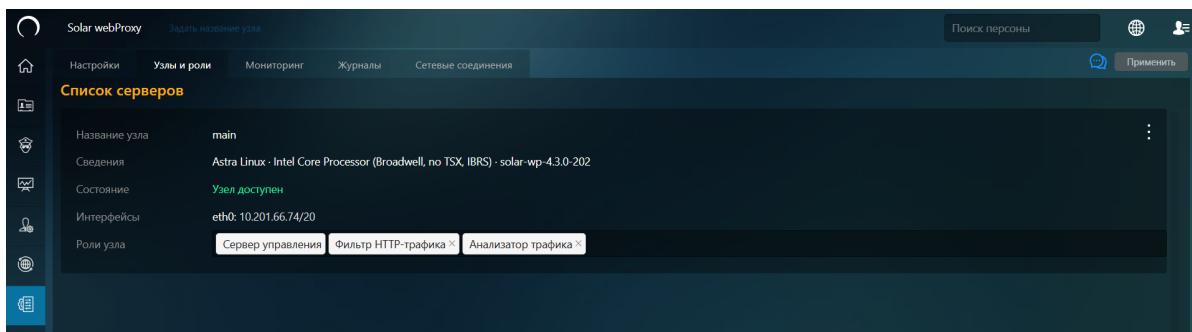


Рис. 5.13. Индикаторы индивидуальных настроек в списке узлов

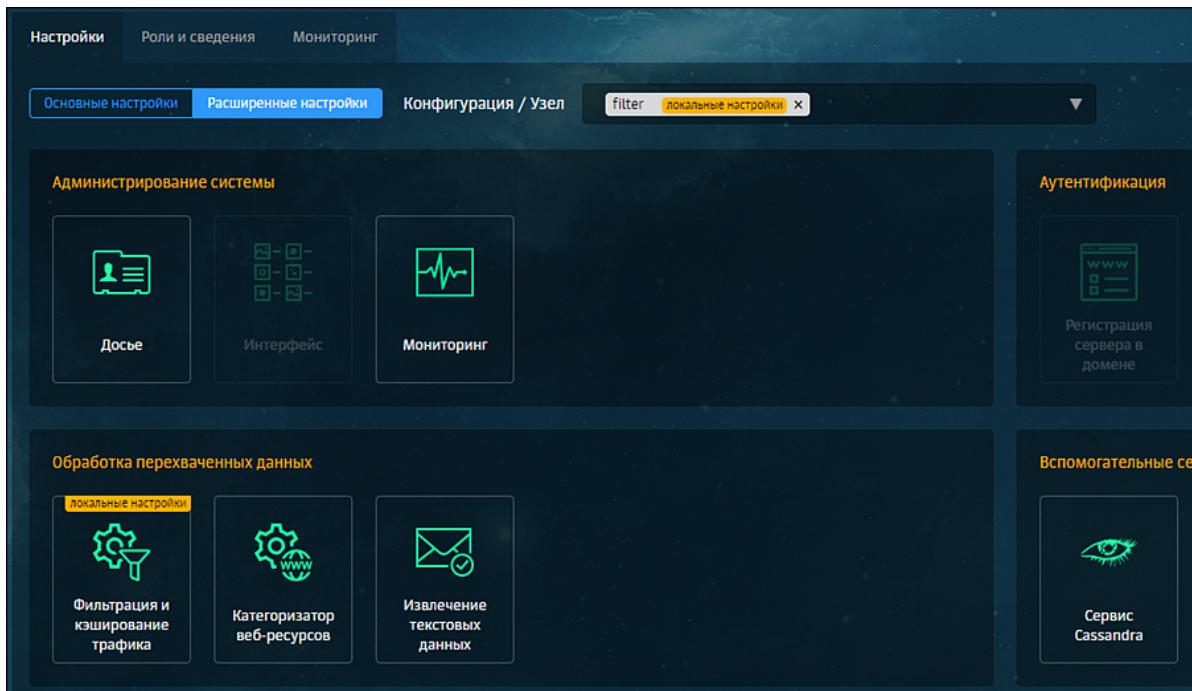


Рис. 5.14. Индикаторы индивидуальных настроек для выбранного узла

Чтобы индивидуальные (локальные) настройки конфигурации узла вступили в силу, включите **Использовать локальные настройки** справа от названия секции параметров (Рис.5.15). Каждая секция имеет свою опцию.

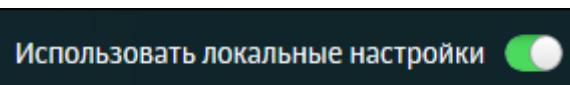


Рис. 5.15. Использовать локальные настройки

5.5. Назначение ролей

5.5.1. Назначение ролей

После загрузки лицензии и входа в систему можно назначать роли узлам с помощью GUI.

Для назначения ролей узлам используйте вкладку **Система > Узлы и роли**, содержащую информацию о состоянии и ролях всех узлов кластера Solar webProxy.

Для назначения роли узлу в разделе **Система > Узлы и роли** в секции с нужным узлом нажмите поле **Роли узла** и выберите в раскрывающемся списке одну или несколько ролей для него, а затем нажмите любую область за пределами списка. Назначенные узлу роли выделены в списке фоном голубого цвета.

Чтобы снять с узла роль, нажмите:

- значок с названием этой роли;
- выбранную роль в списке.

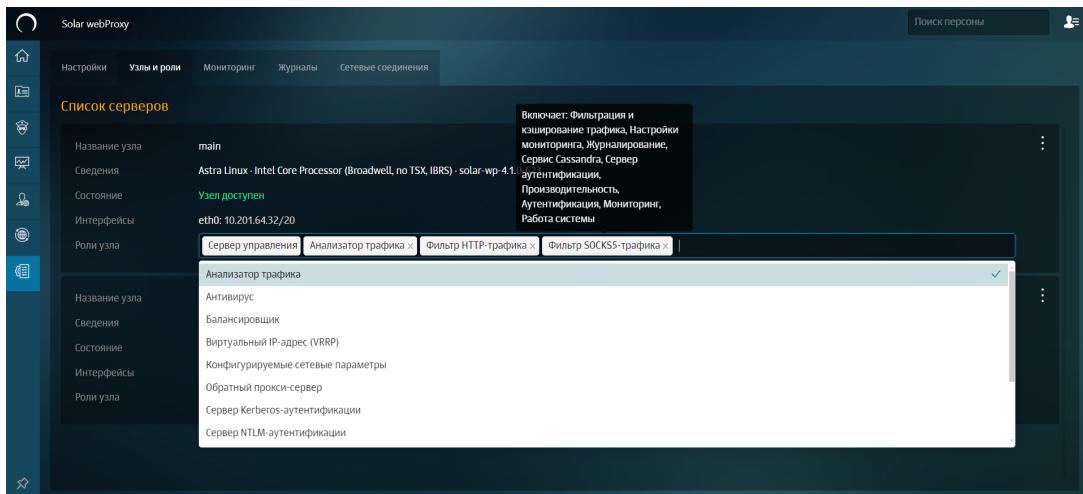


Рис. 5.16. Назначение и снятие ролей узла

После установки ролей для всех узлов нажмите **Сохранить** и **Применить**.

Примечание

Если лицензия не действует на какой-либо модуль, роль будет недоступна и информация об этом отобразится в списке ролей и в подсказке при наведении курсора мыши на роль, которую следует назначать для работы модуля. Если лицензия на модуль закончилась, роль для работы этого модуля останется назначеннной узлу, но сам модуль работать не будет.

Описание всех ролей, которые можно назначить узлу, приведено далее. Для каждой роли указан состав сервисов, обеспечивающих ее функционирование.

Табл. 5.4. Перечень ролей

Название роли в GUI	Название роли в CLI	Описание	Сервисы
Анализатор трафика	analyzer	Категоризация веб-ресурсов.	url-checker-next, smapikaserver
Антивирус	antivirus	Прием запросов на поиск вирусов по протоколу ICAP. При истечении лицензии на антивирус, модуль остановит свою работу.	antivirus
Балансировщик	balancer	Распределение трафика по серверам фильтрации Solar webProxy. Роль использует сервис балансировщика HAProxy.	haproxy

Название роли в GUI	Название роли в CLI	Описание	Сервисы
Виртуальный IP-адрес (VRRP)	vip	Объединение нескольких узлов под виртуальным IP-адресом.	keepalived
Конфигурируемые сетевые параметры	network-config	Централизованное управление статическими маршрутами и просмотр таблицы маршрутизации узлов, на которые установлена роль.	network-config-agent
Обратный прокси-сервер	reverse-proxy	Фильтрация и кэширование трафика в обратном режиме работы системы.	skvt-wizor, log-streamer, skvt-cassandra
Сервер интеграции	api-gateway	Работа с API Solar webProxy.	wp-api-service
Примечание			
<i>Роль доступна только для master-узла.</i>			
Сервер Kerberos-аутентификации	kerberos	Kerberos-аутентификация.	skvt-kerberos-server
Сервер NTLM-аутентификации	ntlm	Регистрация сервера в домене, NTLM-аутентификация.	skvt-winbind, skvt-ntlm-server
Сервис пересылки широковещательных igmp пакетов	igmproxy	Пересылка IGMP-пакетов из одной сети в другую через прокси-сервер.	igmproxy
Сервис репликации Досье на подчиненных узлах	abook-slave	<p>Дублирование части данных Досье. Роль предназначена для повышения отказоустойчивости в ситуациях, когда связь с master-узлом (и хранящимся на нем Досье) временно отсутствует.</p> <p>Синхронизация Досье с внешним источником возможна только на сервере управления (master). На abook-slave загружается копия Досье с master-узла и внесенные на нем изменения. Если на внешнем источнике есть изменения, используйте master-узел для синхронизации и передачи на сервис abook-slave.</p>	abook-daemon
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 веб-сервер для доступа к GUI, настраивается конфигурация, а также генерируется политика фильтрации, распространяемая на все остальные узлы кластера.	skvt-trafdaemon, database, monitor-server, monitor-https, abook-daemon, license-server, skvt-auth-server, skvt-cassandra, clickhouse
Фильтр инспекции пакетов	packet-inspection	<p>Фильтрация прикладных протоколов L7 (RDP, FTP, SSH и Telnet) и приложений.</p> <p>Примечание</p> <p>Роль можно установить только для узлов с ролями Фильтр HTTP-трафика или Фильтр SOCKS-трафика.</p>	ndpid.service, ndpisrvd.service

Название роли в GUI	Название роли в CLI	Описание	Сервисы
Фильтр HTTP-трафика	http-filter	Фильтрация и кэширование трафика.	skvt-wizor, skvt-auth-server, skvt-cassandra, skvt-cache, log-streamer
Фильтр SOCKS5-трафика	socks-proxy	Фильтрация и кэширование трафика по протоколу SOCKS5.	skvt-wizor, skvt-auth-server, skvt-cassandra, skvt-cache, log-streamer

5.5.2. Рекомендации по назначению ролей

В кластере Solar webProxy рекомендуется распределять роли по узлам следующим образом:

- Slave-узлу (узлам) назначить роль **Фильтр HTTP-трафика** (для применения политики фильтрации трафика), роли **Сервер NTLM-аутентификации** или **Сервер Kerberos-аутентификации** (в зависимости от используемого типа аутентификации пользователей, см. раздел [5.9.4](#)) и роль **Анализатор трафика** (если политика фильтрации трафика предусматривает возможность блокировки соединения в зависимости от типа содержимого и категорий).
- При наличии достаточного количества оперативной памяти slave-узлам с ролью **Фильтр HTTP-трафика** следует также назначить роль **Сервис репликации Досье на подчиненных узлах**. Чтобы оценить требуемый объем памяти, на master-узле выполните следующую команду:

```
curl -k -H "Content-type: application/json" --key /opt/dozor/etc/ssl/bus.key --cert /opt/dozor/etc/ssl/bus.pem --data-binary '{}' https://<hostname>:2269/persons/info?groups=true&addresses=true&department=true&ctl=true | wc -c
```

Имя узла (hostname) в команде следует заменить.

Полученное значение умножите на 10 – получится требуемое значение объема памяти в байтах. Переведите его в мегабайты и запишите в качестве значения параметра конфигурации **Макс. объем используемой ОЗУ (Мб)** в разделе **Система > Основные настройки > Производительность > Сервис репликации Досье на подчиненных узлах**. Если полученное значение оказалось меньше значения параметра по умолчанию, то уменьшать значения параметра не нужно.

5.6. Статическая маршрутизация

Для управления статическими маршрутами в разделе **Система > Узлы и роли** на управляемом узле кластера контентной фильтрации добавьте роль **Конфигурируемые сетевые параметры**.

Настройка параметров работы службы роли **Конфигурируемые сетевые параметры** выполняется в разделе **Система > Расширенные настройки > Управление сетевыми параметрами**.

В секции **Агент контроля сетевых параметров > Компоненты ядра сервиса** представлены параметры:

- VTYSH провайдер (vtysh-provider)** – сервис, который реализует провайдер для взаимодействия с FRRouting через vtysh. В этом разделе настраиваются параметры

таймаута для выполнения команд конфигурирования сетевых параметров в части статических маршрутов. Если за установленный в конфигурации таймаут выполнение команд управления параметрами маршрутизации не завершилось успешно, попытка выполнения команды повторяется до ее успешного применения. Единицы измерения – минуты.

- **Менеджер конфигурации (configuration-manager)** – сервис, который реализует периодический запуск (с заданным в настройках сервиса интервалом) задачи для контроля сетевой конфигурации. В рамках этой задачи должен выполняться контроль для всех компонентов конфигурации (на данный момент контроль только для компонента конфигурации **routing**).

В данной секции можно задать параметры:

- **Начальная задержка после запуска сервиса** – определяет величину задержки на инициализацию необходимых служб для применения конфигурации;
- **Интервал между проверками конфигурации** – определяет интервал времени, через который системой будет выполнена проверка соответствия текущей установленной конфигурации и, при необходимости, ее обновление.
- **Менеджер проверки состояния (state-checker)** – сервис, который отвечает за периодическую проверку состояния сетевой конфигурации. Сервис содержит сценарий, который на входе имеет периодическую (с заданным в настройках интервалом) инициацию проверок для всех компонентов конфигурации (на данный момент проверка только для компонента конфигурации **routing**).

В данной секции можно задать параметры:

- **Интервал между проверками состояния > Длительность** – определяет частоту выполнения проверок конфигурации;
- **Интервал между HEARTBEAT статусами > Длительность** – определяет частоту отправки состояния агентом подсистемы управления сетевыми параметрами на управляющий сервер.

В секции **Агент контроля сетевых параметров > HTTP-интерфейс (http)** можно задать настройки HTTP-сервера, обеспечивающего взаимодействие компонентов подсистемы управления сетевой конфигурацией:

- **HTTP-сервер > Порт** – не занятый другими службами TCP порт, на котором будет работать сервис;
- **Обработка SSE запросов > Размер буфера сообщений** – количество сообщений, которое может храниться сервером в очереди до их обработки.

Чтобы настроить маршруты, откройте раздел **Сеть** и выберите нужную вкладку:

- **Маршруты в присоединенные сети** – маршруты в сети, к которым у управляемого узла есть подключенные сетевые интерфейсы.

На данной вкладке маршруты доступны только для просмотра. Данные представлены по следующим полям:

- **Название маршрута**,

-
- **Статус,**
 - **Адрес назначения,**
 - **Интерфейс,**
 - **Шлюз,**
 - **Кем и когда изменено,**
 - **Административная дистанция.**

Для удобства маршруты можно отфильтровать по статусам, узлам или найти нужный маршрут с помощью поиска.

Чтобы отредактировать название маршрута, нажмите .

- **Маршруты по умолчанию** – маршруты, по которым будут отправлены пакеты, адрес назначения которых не совпадает ни с одним адресом назначения в таблице маршрутизации.

Чтобы создать маршрут:

1. В левом верхнем углу нажмите кнопку **Создать маршрут**.
2. Заполните поля:
 - **Название,**
 - **Адрес,**
 - **Шлюз,**
 - **Узел** (управляемый узел, на котором необходимо создать маршрут),
 - **Административная дистанция** (приоритет).
3. Последовательно нажмите кнопки **Сохранить** и **Применить изменения**.

Данные представлены по следующим полям:

- **Название маршрута,**
 - **Статус,**
 - **Адрес назначения,**
 - **Шлюз,**
 - **Кем и когда изменено,**
 - **Административная дистанция.**
- **Статические маршруты** – все остальные созданные маршруты.

Чтобы создать маршрут:

-
1. В левом верхнем углу нажмите кнопку **Создать маршрут**.
 2. Заполните поля:
 - **Тип** (узел или подсеть),
 - **Название**,
 - **Адрес**,
 - **Шлюз**,
 - **Узел** (управляемый узел, на котором необходимо создать маршрут),
 - **Административная дистанция** (приоритет).
 3. Последовательно нажмите кнопки **Сохранить** и **Применить изменения**.

Для удобства маршруты можно фильтровать по статусам, узлам или найти нужный маршрут с помощью поиска.

Примечание

Изменения настроек статической маршрутизации после их применения вступают в силу в течение двух минут.

5.7. Настройка ротации журналов доступа

Для настройки ротации журналов доступа на узле main в файле `/var/spool/cron/crontabs/dozor` внесите в расписание планировщика **cron** следующую запись:

```
0 0 1 * * /opt/dozor/clickhouse/bin/cleanup-db.sh -d <days>
```

где **<days>** – значение времени в днях. Данные журналов доступа старше этого значения будут удаляться. В данном примере вызов скрипта **cleanup-db.sh** будет происходить первого числа каждого месяца.

5.8. Настройка синхронизации Досье

5.8.1. Синхронизация с внешним источником

Модуль **Досье** а также ряд иных функциональных областей может взаимодействовать с внешними источниками данных для синхронизации и получения данных из них.

Синхронизация с Active Directory может происходить по протоколам LDAP (см. раздел [5.8.2](#)) и LDAPS (см. раздел [5.8.3](#)).

Синхронизировать Досье с внешним источником можно в нескольких разделах системы:

- для детальной настройки – раздел **Досье** основных настроек конфигурации;
- для более быстрого доступа – раздел **Досье > Настройки**. Набор параметров настройки аналогичен перечню в разделе **Досье** основных настроек конфигурации.

5.8.2. Синхронизация с внешним источником по протоколу LDAP

Чтобы настроить синхронизацию данных Досье с внешним источником, используя основные настройки конфигурации:

1. В CLI укажите в файлах:

- **/etc/hosts** – запись с адресом и именем контроллера домена Microsoft AD, с которым выполняется синхронизация по протоколу LDAP/LDAPS, вида:

```
10.199.21.100 proxymaster.company.local proxymaster
```

- **/etc/resolv.conf** – запись с адресами сервера домена DNS, с которым выполняется синхронизация, вида:

```
nameserver <namesrvIP>
```

где **<namesrvIP>** – IP-адрес контроллера домена. Если таких адресов несколько, добавьте несколько таких строк, в порядке уменьшения надежности контроллеров домена. В каждой строке может быть только один IP-адрес.

2. В разделе **Досье > Настройки > Доступ к источникам данных** для параметров источников данных **AD example** и **File example** установлены значения по умолчанию. Вы можете:

- Добавить новый источник данных без значений по умолчанию (кнопка **Добавить**). При необходимости может использоваться для расширенной настройки.
- Скопировать выбранный источник данных со всеми значениями. Для этого справа от названия источника данных нажмите .

Примечание

Для параметра источников данных **File example** используйте файл формата **.csv** с записями вида:

- Пример с описанием групп:

```
1  id;pid;group
2  1;;just_group_name
```

- Пример с персонами внутри групп:

```
1  id;group_id;fullname;title;submit_to;birth_day;email;telephone_number;ip;hired;privileges;image;image_preview;sid;hostname;skype;login
2  140;1;the first tester;;;;;;S-1-5-21-793904598-208165932-2932072800-1123;pc-name;kalinkin_55;ea.ershov
```

3. Установите переключатель **Параметры доступа к источнику данных** в положение **ldap**.

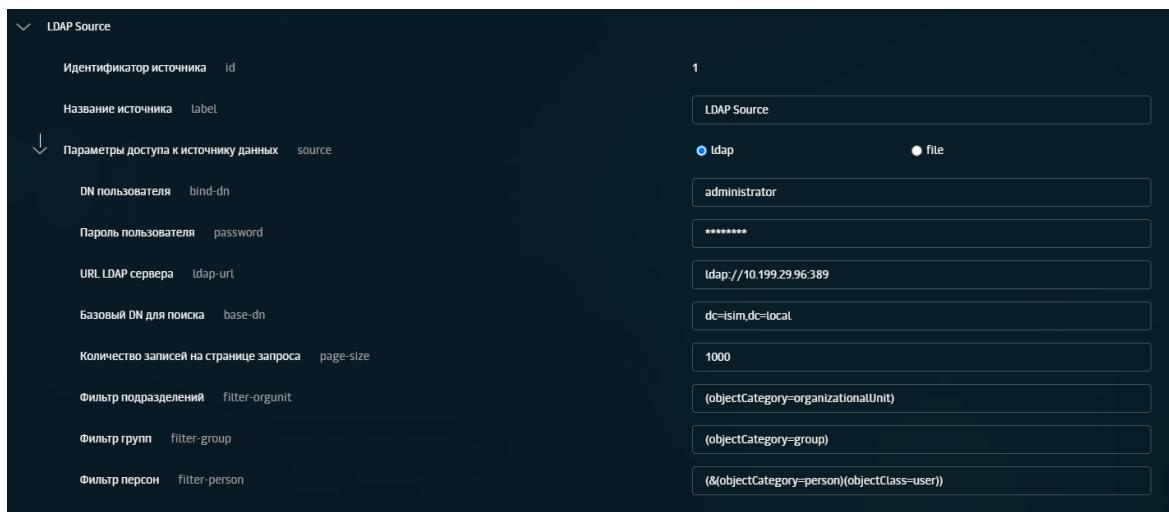


Рис. 5.17. Настройка синхронизации Досье

4. Задайте значения следующих параметров:

- **Название источника** – укажите произвольное название источника данных AD. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.
- **DN пользователя** – имя учетной записи с правами чтения каталога AD. Имя указывается вместе с доменом (например, `admin@organization.local`).
- **Пароль пользователя** – пароль учетной записи, указанной в предыдущем параметре.
- **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например, `ldap://ldap.organization.local:389`).
- **Базовый DN для поиска** – база поиска. Укажите значение в соответствии со структурой каталогов AD организации.

5. При необходимости раскройте группы параметров **Соответствия атрибутов персон**, **Соответствия атрибутов групп** и добавьте и/или исправьте соответствия между атрибутами AD и атрибутами Досье.

Примечание

Для Kerberos-аутентификации предусмотрен параметр `upn`. Для его настройки в поле **Атрибут персоны адресной книги** выберите **User principal name** и задайте значение LDAP-атрибута `userPrincipalName`.

Для NTLM-аутентификации предусмотрен параметр `windows-login`. Для его настройки в поле **Атрибут персоны адресной книги** выберите **Windows login** и задайте значение LDAP-атрибута `msDS-PrincipalName`.

Допускается использование параметров `upn` и `windows-login` для одного домена одновременно.

Если для пользователя в карточке предусмотрено оба атрибута, для его аутентификации будет использоваться параметр **Windows-login**. Если у персоны отсутствует **UPN** и/или **Windows-login**, аутентификация будет выполняться по логину.

*Kerberos-аутентификация работает как по параметру **upn**, так и по **windows-login**. Для NTLM-аутентификации же предусмотрен только параметр **windows-login**.*

6. Нажмите **Проверить** для проверки подключения к источнику данных. В случае неуспеха убедитесь в корректности заданных параметров.
7. Нажмите **Сохранить** и **Применить**.
8. Нажмите кнопку **Синхронизировать**. По окончании отобразится уведомление об удачной синхронизации.

Примечание

Синхронизация возможна только при выполнении следующих условий:

- *Хотя бы один источник данных включен (установлен флагок **Синхронизация включена**).*
 - *Настройки всех источников данных успешно применены.*
 - *В данный момент не выполняется другая синхронизация.*
-

9. Вернитесь в GUI и проверьте наличие оргструктур в разделе **Досье > Организационная структура**.
10. При изменении настроек в процессе эксплуатации (настроенной ранее синхронизации) необходимо произвести сброс текущей базы Досье с помощью команд:

```
# /opt/dozor/bin/dsctl stop abook-daemon
# /opt/dozor/abook-daemon/bin/abook-reset -hard
# /opt/dozor/bin/dsctl start abook-daemon
```

По окончании задайте интервал синхронизации:

1. Откройте секцию **Сервис обновления Досье > Работа в главном режиме**.
2. Установите флагок **Автоматическая синхронизация с источниками**.
3. Задайте значение параметра **Периодичность синхронизации**.

Примечание

Не рекомендуется устанавливать значение периодичности синхронизации меньше 20 минут, т.к. при объемном LDAP-каталоге и большом количестве пользователей для успешного завершения обновления данного времени может быть недостаточно.

При значении 0 часов 0 минут синхронизация работать не будет.

4. Нажмите Сохранить и Применить.

Для настройки синхронизации данных Досье с внешним источником в разделе **Досье** нажмите кнопку **Настройки** и выполните процедуру, описанную выше.

5.8.3. Синхронизация с внешним источником по протоколу LDAPS

5.8.3.1. Общий порядок настройки синхронизации

Трафик, передаваемый по протоколу LDAP, не является защищенным. Чтобы синхронизация данных была конфиденциальной и безопасной, используйте протокол LDAPS, который является защищенной версией LDAP, и в котором используется дефолтный порт 636 вместо 389, как у LDAP.

LDAPS представляет собой технологию «LDAP через SSL», которая позволяет шифровать процесс синхронизации данных и аутентификации.

Для настройки синхронизации по протоколу LDAPS:

1. Выпустите и импортируйте сертификат в центре сертификации домена (CA) – см. раздел [5.8.3.2](#);
2. Импортируйте сертификат центра сертификации домена (CA) в Solar webProxy – см. раздел [5.8.3.3](#);
3. В разделе **Досье > Настройки > Доступ к источникам данных** выполните процедуру, описанную в разделе [5.8.2](#), предварительно заменив порт назначения на 636 (вместо 389).

Примечание

Убедитесь, что адрес сервера в параметре **URL LDAP сервера** начинается с **ldaps://**.

После настроек проверьте связи с источником синхронизации. Для этого нажмите кнопку **Синхронизовать** на вкладке **Настройки** раздела **Досье** или в разделе **Система > Досье** основных настроек.

Примечание

Если не работает сразу, в CLI выполните рестарт сервисов **monitor-ng** и **abook-daemon** с помощью команд:

```
# dsctl restart monitor-ng  
# dsctl restart abook-daemon
```

5.8.3.2. Управление сертификатом

Установка допустимого сертификата на контроллере домена позволяет службе LDAP прослушивать и автоматически принимать подключения SSL как для LDAP, так и для глобального трафика каталогов.

Для генерации сертификата:

1. На сервере с ролью **Certification Authority** (CA) запустите консоль **Certification Authority Management Console**, перейдите в раздел с шаблонами сертификатов **Certificate Templates** и в контекстном меню выберите **Manage**.

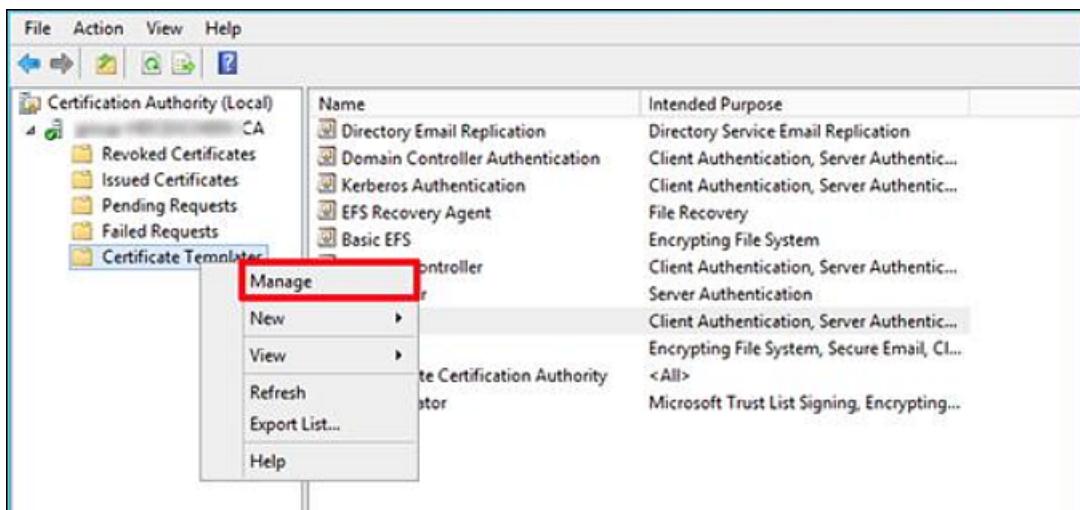


Рис. 5.18. Управление шаблонами сертификатов

2. Создайте копию шаблона **Kerberos Authentication certificate**, выбрав в контекстном меню команду **Duplicate Template**.

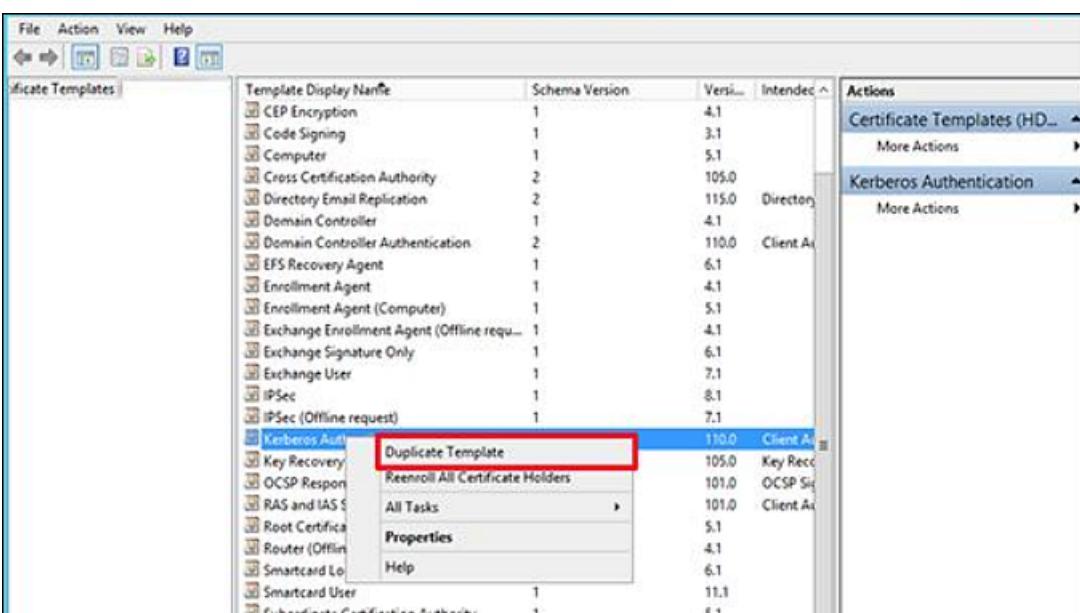


Рис. 5.19. Создание копии шаблона сертификата

3. В окне **Properties of New Template** на вкладке **General** переименуйте шаблон сертификата в **LDAPoverSSL**, указав период его действия, и опубликуйте его в AD (**Publish certificate in Active Directory**).

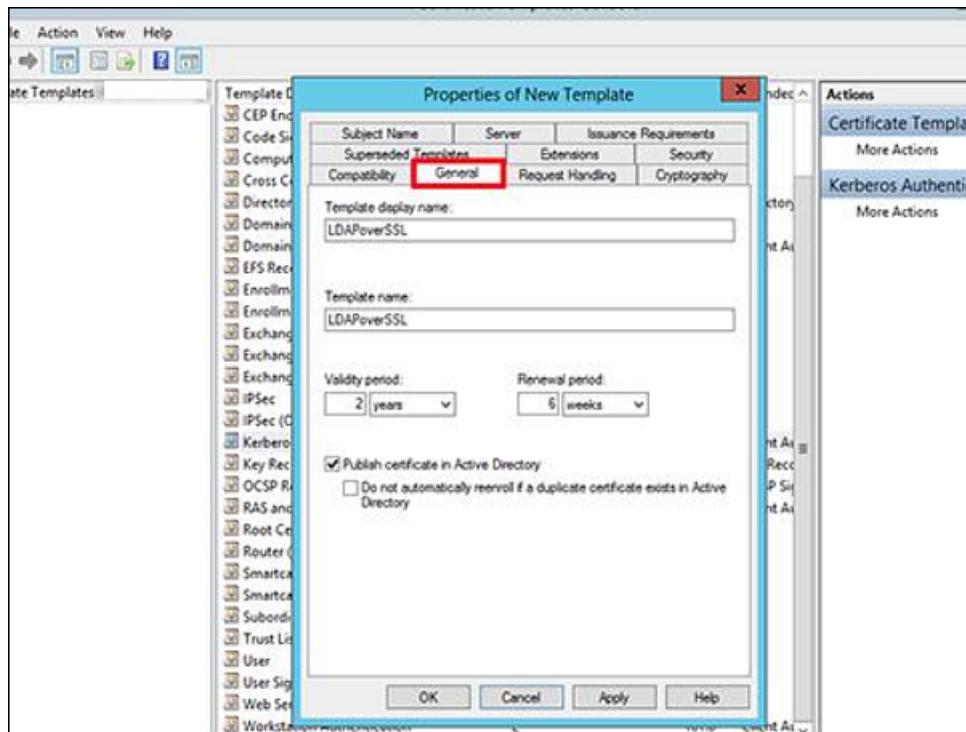


Рис. 5.20. Переименование и публикация шаблона сертификата

4. На вкладке **Request Handling** установите флажок **Allow private key to be exported** и сохраните шаблон.

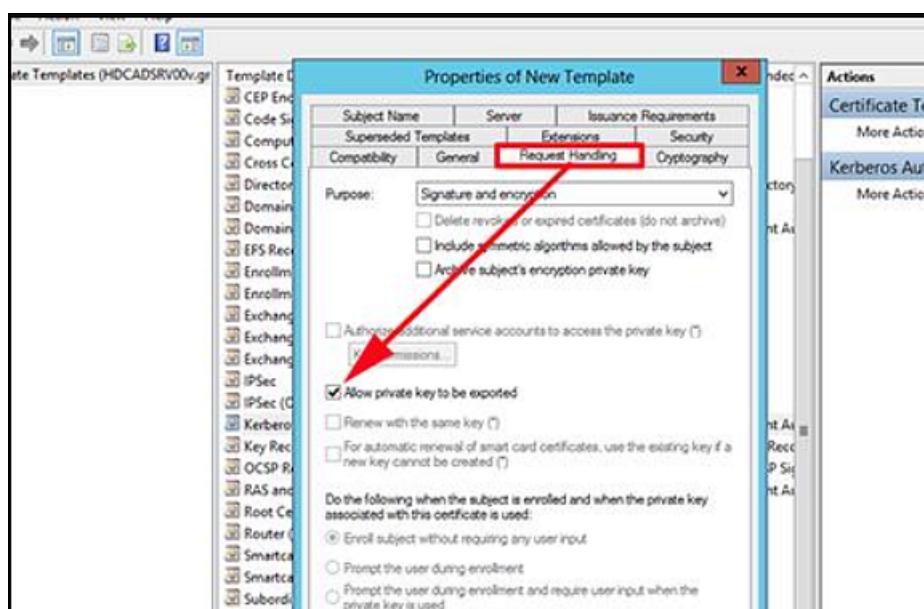


Рис. 5.21. Сохранение шаблона сертификата

5. Опубликуйте новый тип сертификата на базе созданного шаблона:

- В контекстном меню раздела **Certificate Templates** выберите команду **New > Certificate Template to issue**.

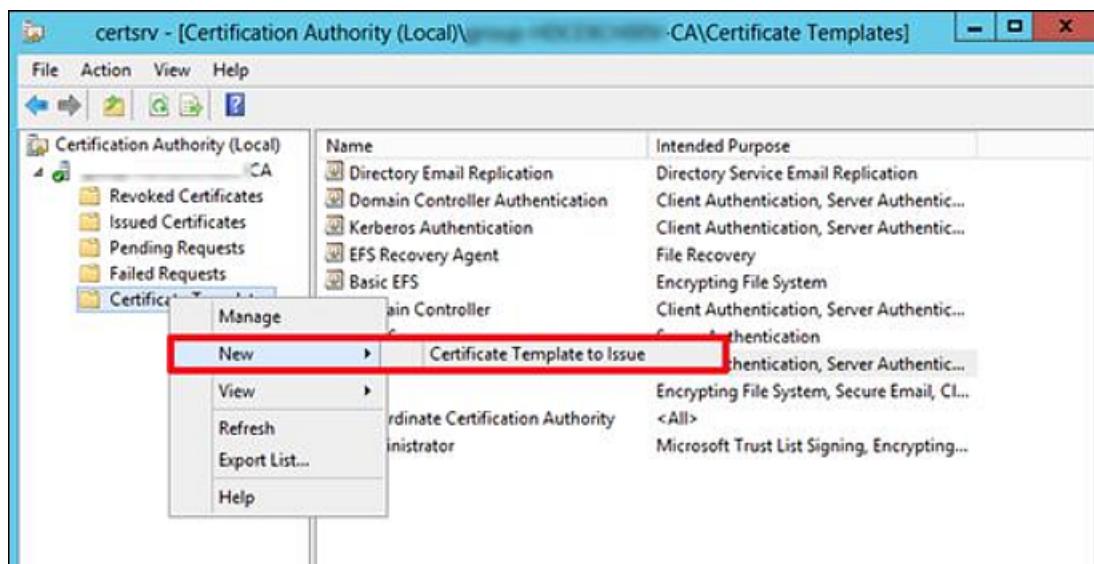


Рис. 5.22. Выбор сертификата для генерации

- В списке доступных шаблонов выберите **LDAPoverSSL** и нажмите **OK**.

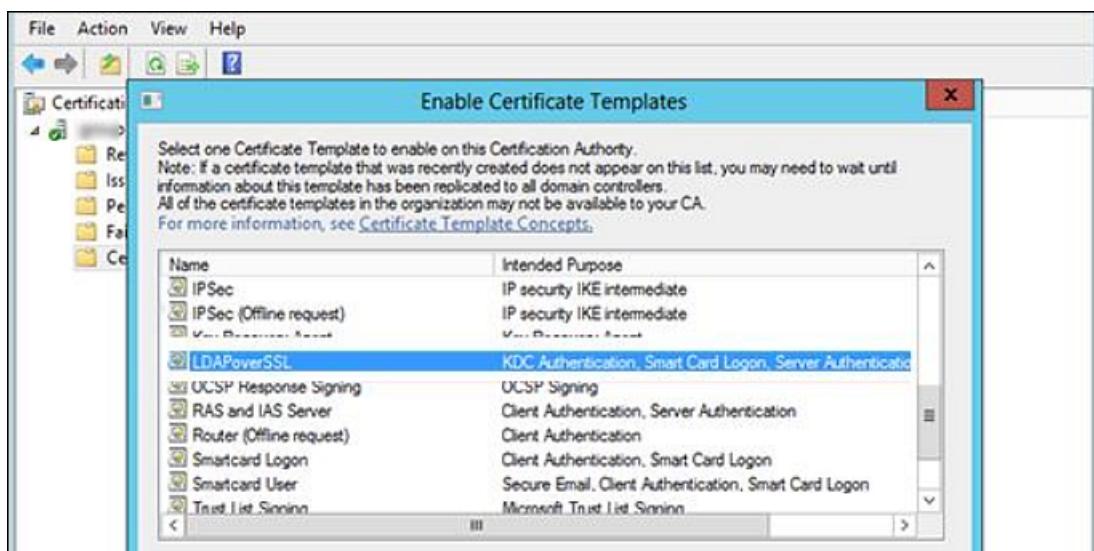


Рис. 5.23. Выбор типа сертификата LDAPoverSSL

6. На контроллере домена, для которого планируется задействовать LDAPS, откройте оснастку управления сертификатами и в хранилище сертификатов **Personal** запросите новый сертификат. Для этого в контекстном меню выберите команду **All Tasks > Request New Certificate**.

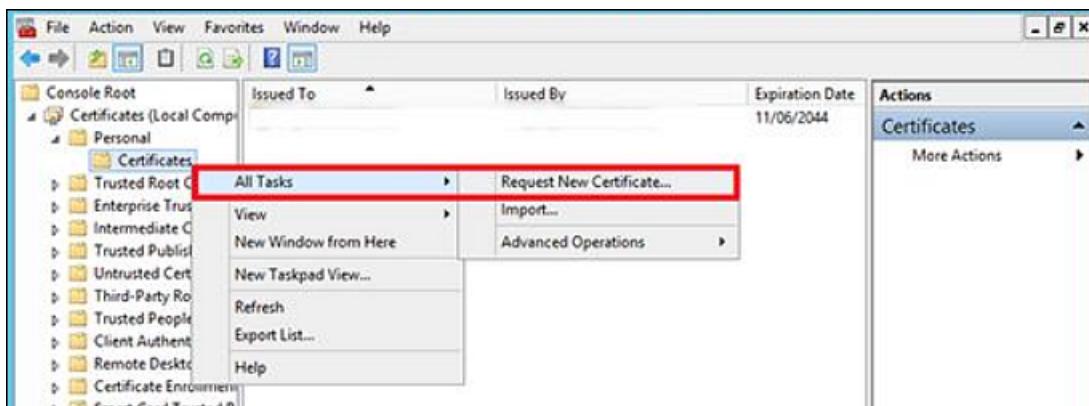


Рис. 5.24. Запрос нового сертификата

7. В списке доступных сертификатов выберите сертификат **LDAPoverSSL** и нажмите **Enroll**. Сертификат будет выпущен.

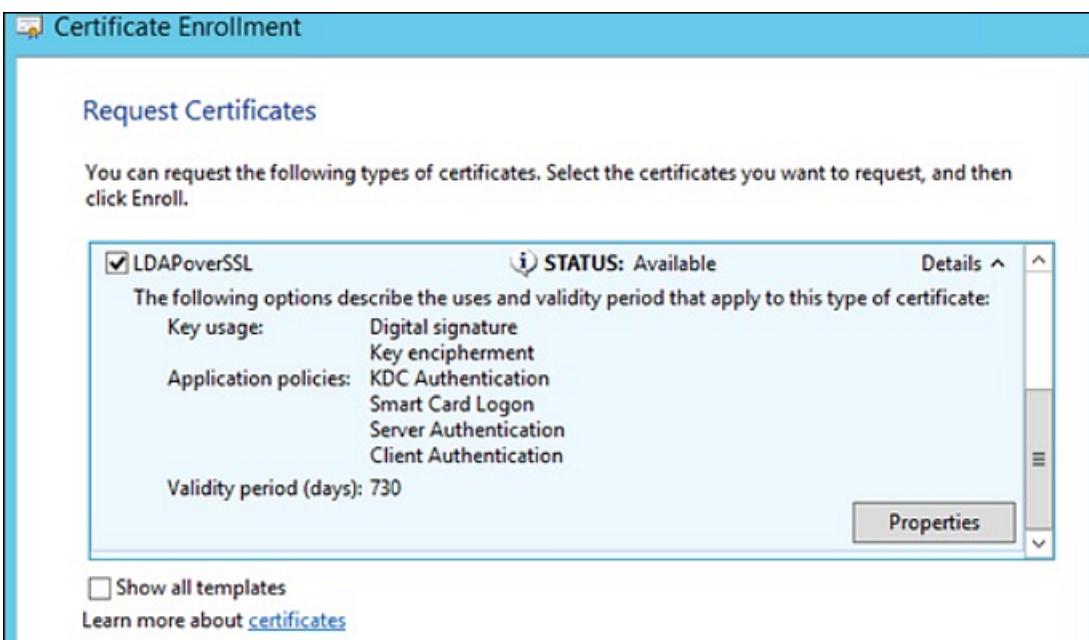


Рис. 5.25. Выпуск сертификата

8. В CLI выполните экспорт корневого сертификата удостоверяющего центра в файл, выполнив на сервере с ролью **Certification Authority** команду:
`certutil -ca.cert ca_name.cer`
. Файл сертификата сохранится в профиле текущего пользователя в файле формата **CER**. Например, *ca_name.cer*.
9. Добавьте экспортированный сертификат в контейнере сертификатов **Trusted Root Certification Authorities** хранилища сертификатов на клиенте и контроллере домена, выполнив в CLI команду:
`certmgr.exe -add C:\ca_name.cer -s -r localMachine ROOT`
. Полностью перезагрузите DC.

5.8.3.3. Добавление сертификата в центре сертификации домена (СА) в хранилище сертификатов Solar webProxy

Добавление сертификата в центре сертификации домена (СА) позволит открывать защищенные соединения с другими устройствами, имеющими сертификат, выпущенный этим же центром сертификации.

Для импорта сертификата УЦ в хранилище сертификатов Solar webProxy:

1. Скопируйте полученный сертификат на все узлы кластера. Перейдите в каталог с сертификатом и с помощью CLI сконвертируйте его в формат PEM, выполнив команду:

```
openssl x509 -inform der -in cert.cer -out cert.pem
```

2. Для импорта сертификата в хранилище выполните команду:

```
keytool -import -v -trustcacerts -alias <cert_alias> -file /var/tmp/cert.pem -keystore /opt/dozor/etc/ldap.jks -deststoretype JKS
```

где **<cert_alias>** – название сертификата в хранилище.

Примечание

После выполнения команды может быть запрошен пароль от ключевого хранилища. Если он не был задан ранее, придумайте новый.

Если в пароле используются специальные символы bash (например, \$), команда будет выдавать ошибку. Чтобы исправить ошибку, указывайте пароль в формате 'password'.

3. Проверьте, что у пользователя **dozor** есть разрешение на просмотр /opt/dozor/etc/ldap.jks.

5.8.4. Синхронизация с FreeIPA

Для настройки синхронизации данных Досье с существующей структурой каталогов 389 Directory Server Example:

1. В GUI перейдите в раздел **Система > Расширенные настройки > Досье > Доступ к источникам данных > 389 Directory Server Example** и задайте значения следующих параметров:

- **Идентификатор источника** – уникальный идентификатор источника данных.
- **Название источника** – укажите произвольное название источника данных FreeIPA. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.

Чтобы синхронизировать данные, установите флажок **Синхронизация включена**.

2. В блоке **Параметры доступа к источнику данных** задайте значения следующих параметров:

- При выборе **ldap**:

-
- **DN пользователя** – идентификатор пользователя для подключения к LDAP.
 - **Пароль пользователя** – пароль учетной записи, указанной в предыдущем параметре.
 - **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например, `ldap://ldap.organization.local:389`).
 - **Базовый DN для поиска** – база поиска. Укажите значение в соответствии со структурой каталогов FreeIPA.
 - **Количество записей на странице запроса** – значение параметра может быть от 0 до 65535. По умолчанию – 1000.
 - **Фильтр подразделений** – строковое представление фильтра, применяемого при поиске подразделений.
 - **Фильтр групп** – строковое представление фильтра, применяемого при поиске групп персон.
 - **Фильтр персон** – строковое представление фильтра, применяемого при поиске персон.
 - **Уникальный идентификатор персоны** – `nsUniqueId`.
 - **Порядковый номер обновления данных** – `entryusn`.
 - **Корневая запись в локальном сервере каталогов** – `netscapemdsuffix`.
 - **Порядковый номер последнего обновления данных** – `lastusn`.
- При выборе **file**:
 - **Каталог с данными ОШС**,
 - **Файл со списком групп**,
 - **Файл со списком сотрудников**.
3. При необходимости раскройте группы параметров **Соответствия атрибутов персон**, **Соответствия атрибутов групп** и добавьте и/или исправьте соответствия между атрибутами FreeIPA и атрибутами Досье.
 4. Нажмите **Проверить** для проверки подключения к источнику данных. В случае неуспеха убедитесь в корректности заданных параметров.
 5. Нажмите **Сохранить** и **Применить**.
 6. Нажмите кнопку **Синхронизировать**. По окончании отобразится уведомление об удачной синхронизации.

Примечание

Синхронизация возможна только при выполнении следующих условий:

-
- Хотя бы один источник данных включен (установлен флагок **Синхронизация включена**).
 - Настройки всех источников данных успешно применены.
 - В данный момент не выполняется другая синхронизация.
-

7. Вернитесь в GUI и проверьте наличие оргструктур в разделе **Досье > Организационная структура**.

5.8.5. Синхронизация с ALD Pro

Для настройки синхронизации данных Досье с ALD Pro:

1. В GUI перейдите в раздел **Система > Расширенные настройки > Досье > Доступ к источникам данных > ALD Pro** и задайте значения следующих параметров:
 - **Идентификатор источника** – уникальный идентификатор источника данных.
 - **Название источника** – укажите произвольное название источника данных ALD Pro. Рекомендуется выбрать название, отражающее реалии сетевой инфраструктуры организации.

Чтобы синхронизировать данные, установите флагок **Синхронизация включена**.

2. В блоке **Параметры доступа к источнику данных** задайте значения следующих параметров:
 - При выборе **ldap**:
 - **DN пользователя** – идентификатор пользователя для подключения к LDAP.
 - **Пароль пользователя** – пароль учетной записи, указанной в предыдущем параметре.
 - **URL LDAP сервера** – адрес LDAP-сервера организации с указанием протокола и порта (например, **ldap://ldap.organization.local:389**).
 - **Базовый DN для поиска** – база поиска. Укажите значение в соответствии с ALD Pro.
 - **Количество записей на странице запроса** – значение параметра может быть от 0 до 65535. По умолчанию – 1000.
 - **Фильтр подразделений** – строковое представление фильтра, применяемого при поиске подразделений.
 - **Фильтр групп** – строковое представление фильтра, применяемого при поиске групп персон.
 - **Фильтр персон** – строковое представление фильтра, применяемого при поиске персон.
 - **Уникальный идентификатор персоны** – **nsUniqueId**.

-
- Порядковый номер обновления данных – `entryusn`.
 - Корневая запись в локальном сервере каталогов – `netscapemdsuffix`.
 - Порядковый номер последнего обновления данных – `lastusn`.
- При выборе `file`:
 - Каталог с данными ОШС,
 - Файл со списком групп,
 - Файл со списком сотрудников.
3. При необходимости раскройте группы параметров **Соответствия атрибутов персон**, **Соответствия атрибутов групп** и добавьте и/или исправьте соответствия между атрибутами ALD Pro и атрибутами Досье.
 4. Нажмите **Проверить** для проверки подключения к источнику данных. В случае неуспеха убедитесь в корректности заданных параметров.
 5. Нажмите **Сохранить** и **Применить**.
 6. Нажмите кнопку **Синхронизировать**. По окончании отобразится уведомление об удачной синхронизации.
- Примечание**
- Синхронизация возможна только при выполнении следующих условий:*
- *Хотя бы один источник данных включен (установлен флагок **Синхронизация включена**).*
 - *Настройки всех источников данных успешно применены.*
 - *В данный момент не выполняется другая синхронизация.*
7. Вернитесь в GUI и проверьте наличие оргструктуры в разделе **Досье > Организационная структура**.

5.8.6. Синхронизация со сторонним Досье

Досье Solar webProxy может работать в подчиненном режиме, то есть использовать Досье другого кластера Solar webProxy или Solar Dozor. Для этого сторонний кластер должен иметь собственное хранилище Досье. В этом режиме локальный кластер Solar webProxy подключается к Досье стороннего кластера и загружает в оперативную память локальную копию Досье. Все изменения, вносимые в Досье со стороны любого из кластеров, становятся доступными со стороны другого кластера. В подчиненном режиме нельзя подключиться к Досье кластера, также использующего подчиненный режим.

Для настройки синхронизации данных Досье Solar webProxy с Досье Solar Dozor или Solar webProxy:

1. На master-узле в CLI выполните 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 удаленном master-узле.

2. В GUI в секции **Сервис обновления Досье** раздела **Досье** расширенных настроек конфигурации задать значения следующих параметров:

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

3. Нажмите **Сохранить, Применить**.

4. Перезапустите сервис **abook-daemon** на локальном и удаленном master-узлах.

5. В CLI выполните следующие команды:

```
# /opt/dozor/bin/shell
```

```
# dsctl restart clickhouse
```

Примечание

При переходе из подчиненного режима в главный значения параметров настройки главного режима остаются неизменными, т.е. дефолтными.

В Досье Solar webProxy есть особенности работы с вложенными группы безопасности Active Directory. Политика работает только для группы тех пользователей, которые были добавлены в Active Directory напрямую. Для группы, в которой есть вложенные группы пользователей, политика работать не будет.

5.9. Настройка аутентификации

5.9.1. Общие сведения

Механизм аутентификации Solar webProxy поддерживает следующие виды источников учетных записей:

- локальный список IP-адресов и диапазонов;
- локальный список учетных записей;
- LDAP;
- LDAPS;
- RADIUS;

-
- IMAP;
 - POP3.

При создании схемы аутентификации необходимо учитывать следующие особенности:

- Проверка по IP-адресам имеет наивысший приоритет.
- При доменной аутентификации используется только один источник в связи с уникальностью настроек **samba**, **krb5**, **winbind**.
- В тех схемах, где это нужно, следует снять флажок **abort-by-error** (Прерывать процесс аутентификации при возникновении ошибок) в разделе **Аутентификация > Источники Basic аутентификации** основных настроек. Параметр **abort-by-error** регулирует возможность прерывания процесса аутентификации при возникновении ошибок. Параметр предназначен для настройки разного поведения сервера аутентификации в случае возникновения ошибок с конкретным источником аутентификации. Например, если источник недоступен из-за сетевых проблем:
 - если флажок **abort-by-error** снят — поиск пользователей в БД данного источника не будет выполняться, и сервер аутентификации продолжит поиск подходящего пользователя в БД других заданных источников;
 - если флажок **abort-by-error** установлен — при появлении ошибок в процессе взаимодействия с данным источником сервер аутентификации будет выдавать ошибку, и дальнейший поиск выполняться не будет.

В Solar webProxy используются следующие методы аутентификации:

- по IP-адресам (раздел [5.9.2](#));
- Negotiate (раздел [5.9.3](#));
- NTLM (раздел [5.9.4](#));
- NTLM+Negotiate (примечание в разделе [5.9.3](#));
- Radius (раздел [5.9.6.5](#));
- прозрачная (раздел [5.9.5](#));
- basic (раздел [5.9.6](#)).

Режимы, в которых используются эти методы аутентификации перечислены далее в Таблице.

Табл. 5.5. Режимы аутентификации

Название	Описание
Permissive	Разрешительный режим. Аутентификация не разрешается только если запись пользователя заблокирована. Используется IP-аутентификация.
Prohibitory	Запретительный режим. Аутентификация разрешается только если запись пользователя существует и не заблокирована. Используется IP-аутентификация.
Basic	HTTP-аутентификация методом basic
NTLM	Доменная аутентификация методом NTLM

Название	Описание
Negotiate	Доменная аутентификация методом Negotiate. По выбору клиента выполняется методом Kerberos или NTLM.
NTLM+Negotiate	Доменная аутентификация методом Negotiate либо NTLM. Метод выбирается клиентом. Этот режим используется, если заранее неизвестно, поддерживает ли клиент метод Negotiate.
Radius	Basic-аутентификация для удаленного доступа к пользовательским сервисам, виртуальным частным сетям (VPN), точкам беспроводного доступа (Wi-Fi) и т.д.

5.9.2. Настройка аутентификации по IP-адресам

Аутентификация по IP-адресам может работать в одном из двух режимов:

- **Разрешительный** – доступ разрешен с любых IP-адресов без исключений.
- **Запретительный** – доступ разрешен только в соответствии с настроенным слоем политики **Правила аутентификации**. Подробная информация о настройке этого слоя приведена в документе *Руководство администратора безопасности*.

Режим аутентификации можно настроить:

- в разделе **Работа системы** основных настроек;
- на вкладке **Настройки** в разделе **Политика**.

Для настройки режима аутентификации:

1. В разделе **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения следующих параметров:
 - **Режим аутентификации – Proxy-Auth;**
 - **Метод аутентификации:**
 - **Permissive** – для разрешительного режима;
 - **Prohibitory** – для запретительного режима.
2. Нажмите **Сохранить и Применить**.

Для настройки режима аутентификации из раздела **Политика** нажмите кнопку **Настройки** в левом верхнем углу раздела и выполните действия, описанные выше.

5.9.3. Настройка аутентификации Negotiate

Для настройки аутентификации Negotiate:

1. Назначьте одному из узлов Solar webProxy роль **Сервер Kerberos-аутентификации**. Это будет сервер аутентификации Solar webProxy.
2. В разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения следующих параметров:
 - **Режим аутентификации – Proxy-Auth;**

-
- **Метод аутентификации – Negotiate.**
3. Создайте и зарегистрируйте ключ:
- **Создание ключа на контроллере домена MS AD:**
- В CLI на контроллере домена выполните команду:
- ```
ktpass.exe -out C:\krb5.keytab -princ HTTP/auth-skvt.solar.local@WINDOWS.DOMAIN -mapuser skvt2 -pass password -crypto All -ptype KRB5_NT_PRINCIPAL
```
- Примечание**
- Значения для замены:
- **auth-skvt.solar.local** – FQDN сервера аутентификации Solar webProxy;
  - **WINDOWS.DOMAIN** – имя домена;
  - **skvt2** – сервисный пользователь Windows AD, с помощью которого происходит выпуск билетов аутентификации;
  - **password** – пароль пользователя.
- 
- В результате выполнения этой команды будет создан ключ аутентификации. Ключ будет находиться в месте, указанном после ключа **-out**, в данном примере – **C:\krb5.keytab**.
- **Создание ключа на контроллере домена FreeIPA/ALD Pro:**
- a. Получите тикет с правами администратора на любом из клиентов FreeIPA домена (можно на контроллере) с помощью команды:
- ```
# kinit admin
```
- b. Создайте общую запись узла, например, **proxy.tsolar.ipa** с помощью команды:
- ```
ipa host-add <proxy.tsolar.ipa> --force
```
- где **<proxy.tsolar.ipa>** – FQDN сервера аутентификации Solar webProxy
- c. Создайте сервис SPN HTTP для узла с помощью команды:
- ```
# ipa service-add HTTP/<proxy.tsolar.ipa> --force
```
- d. Выгрузите ключ keytab для созданного ранее SPN с помощью команды:
- ```
ipa-getkeytab -p HTTP/<proxy.tsolar.ipa> -k ~/proxy.keytab
```
- e. Добавьте запись в DNS:
- ```
# ipa dnsrecord-add tsolar.ald. <proxy.tsolar.ipa>. --a-ip-address=<10.201.65.173>
```
- где **<10.201.65.173>** – IP-адрес Solar webProxy

-
- f. Перейдите к настройке, описанной в разделе [5.9.3.2](#).
4. В GUI Solar webProxy в разделе **Аутентификация > Keytab-файл**:
- установите переключатель **Режим использования keytab-файла** в положение **Загрузить из файла**;
 - нажмите **Загрузить**, выберите в открывшемся окне файл и нажмите **Открыть**;
 - нажмите **Сохранить и Применить**.

Примечание

В Solar webProxy есть возможность аутентификации с нескольких доменов. Для этого:

- 1. На каждом домене выполните шаги из [3](#).*
- 2. Поместите полученные файлы в любой каталог Solar webProxy с помощью SCP (Secure Copy Command).*
- 3. Выполните следующие команды:*

ktutil

```
read_kt <имя_первого_ключа.keytab>
read_kt <имя_второго_ключа.keytab>
write_kt krb5.keytab
quit
```

- 4. Просмотреть содержимое итогового файла можно с помощью команды:*

klist -k krb5.keytab

*Полученный файл **krb5.keytab** загружается на прокси-сервер (подробнее см. пункт [4](#)).*

При создании обоих файлов рекомендуется использовать разные пароли для учетных записей, ассоциированных с Solar webProxy.

Если серверов фильтрации несколько, ключ генерируется на общее доменное имя для всех этих серверов. Например, для двух серверов фильтрации с сетевыми именами **filter1.org.local** и **filter2.org.local** и IP-адресами 10.10.10.1 и 10.10.10.2 соответственно, выберите для них общее имя, например **proxy.org.local**. Ключ должен быть сгенерирован для имени **proxy.org.local**, и на каждом сервере фильтрации в конце файла **/etc/hosts** добавлена запись вида:

```
10.10.10.1 proxy.org.local
```

```
10.10.10.2 proxy.org.local
```

На каждом сервере фильтрации должна быть только одна из этих записей, соответствующая его IP-адресу.

Внимание!

При добавлении записей в конец файла **/etc/hosts** не заменяйте и не удаляйте текущие.

Для проверки корректности настроек Negotiate-аутентификации, выполните следующие настройки:

1. В настройках сервера Kerberos-аутентификации:

- Укажите имя домена.
- В качестве адреса KDC-сервера и адреса административного сервера укажите IP-адрес контроллера домена.

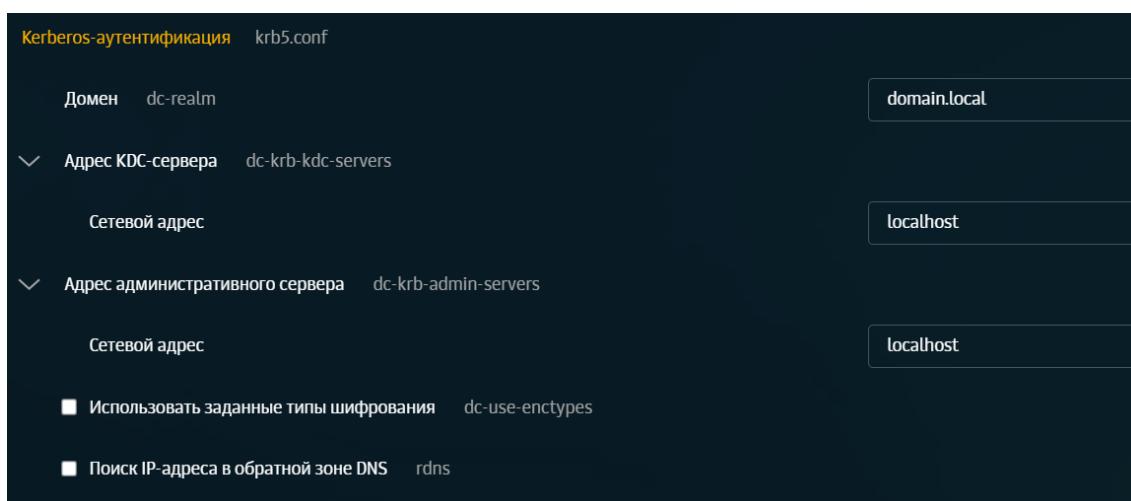


Рис. 5.26. Kerberos-аутентификация

2. Сохраните настройки.

3. В CLI выполните команду:

```
# kinit -V -k -p HTTP/<Общий FQDN webProxy>
```

Отсутствие сообщений об ошибке свидетельствует об успешной настройке аутентификации.

Примечание

Для настройки аутентификации NTLM+Negotiate выполните инструкции из разделов [5.9.4](#) и [5.9.3](#), учитывая, что параметр **Метод аутентификации** должен иметь значение **NTLM+Negotiate**.

5.9.3.1. Настройка Kerberos-аутентификации в многодоменной среде Microsoft AD

Отличие настройки Kerberos-аутентификации в многодоменной среде Microsoft AD от настройки для одного домена состоит в том, что при выпуске keytab-файлов с каждого домена необходимо объединить их в один файл.

Примечание

Названия Solar webProxy на каждом домене могут быть как одинаковые, так и разные. Главное, чтобы клиенты доменов обладали своими уникальными именами.

При создании сервисных пользователей каждого домена у них должны быть разные пароли или должны быть отключены алгоритмы DES-CBC-CRC|DES-CBC-MD5|RC4-HMAC-NT. То есть, при выпуске keytab-файлов необходимо указывать алгоритмы AES.

Перед настройкой Kerberos-аутентификации в многодоменной среде Microsoft AD необходимо выпустить keytab-файл.

Примечание

Перед настройкой задайте уникальный FQDN сервера аутентификации Solar webProxy. При изменении FQDN требуется повторный выпуск keytab-файла.

Чтобы выпустить keytab-файл:

1. От имени администратора откройте консоль Windows PowerShell.
2. Выполните команду:

```
ktpass.exe -princ HTTP/webproxy.domain.local@DOMAIN.LOCAL -mapuser  
wproxy@DOMAIN.LOCAL -pass password -crypto All -ptype KRB5_NT_PRINCIPAL  
-out C:\krb5.keytab
```

Примечание

Значения для замены:

- **webproxy.domain.local** – FQDN сервера аутентификации Solar webProxy;
- **DOMAIN.LOCAL** – имя домена;
- **password** – пароль пользователя.

В результате выполнения этой команды будет создан ключ аутентификации. Ключ будет находиться в месте, указанном после **-out**, в данном примере – **C:\krb5.keytab**.

3. Выпустите keytab-файлы для других доменов.

Чтобы объединить keytab-файлы с каждого домена в один файл:

1. Поместите полученные keytab-файлы в любой каталог Solar webProxy с помощью утилиты SCP (Secure Copy Command). В итоге получатся два файла с названиями, например, **ad1.keytab** и **ad2.keytab**.

2. Выполните следующие команды:

ktutil

read_kt <имя_первого_ключа.keytab>

read_kt <имя_второго_ключа.keytab>

write_kt krb5.keytab

quit

В результате в каталоге появится новый файл, содержащий записи SPN всех доменов.

3. Просмотреть содержимое итогового файла можно с помощью команды:

klist -e -k /etc/krb5.keytab

4. Полученный файл **krb5.keytab** скопируйте на свой ПК по SCP и загрузите его через GUI Solar webProxy.

Для проверки корректности настроек Kerberos-аутентификации в многодоменной среде Microsoft AD убедитесь, что содержимое файла **/etc/krb5.conf** выглядит следующим образом:

```
[logging]
default = FILE:/opt/dozor/var/log/krb5libs.log
kdc = FILE:/opt/dozor/var/log/krb5kdc.log
admin_server = FILE:/opt/dozor/var/log/kadmind.log

[libdefaults]
default_realm = DOMAIN1.LOCAL
dns_lookup_realm = true
dns_lookup_kdc = true
forwardable = false
proxiable = false
rdns = false

[realms]
DOMAIN1.LOCAL = {
kdc = 1.1.1.1
kpassword_server = 1.1.1.1
admin_server = 1.1.1.1
}
DOMAIN2.LOCAL = {
kdc = 2.2.2.2
kpassword_server = 2.2.2.2
admin_server = 2.2.2.2
}

[domain_realm]
.domain1.local = DOMAIN1.LOCAL
```

```
domain1.local = DOMAIN1.LOCAL
.domain2.local = DOMAIN2.LOCAL
domain2.local = DOMAIN2.LOCAL

[appdefaults]
pam = {
debug = false
ticket_lifetime = 36000
renew_lifetime = 360000
forwardable = true
krb4_convert = false
}
```

где **domain1.local** и **domain2.local** – имена доменов, а **1.1.1.1** и **2.2.2.2** – адреса Центра распределения ключей KDC.

5.9.3.2. Настройка Kerberos-аутентификации в доменной среде FreeIPA/ALD Pro

Чтобы настроить Kerberos-аутентификацию в доменной среде FreeIPA:

1. Получите строку base64 из файла **proxy.keytab** (подробнее см. [3](#)) с помощью команды:

```
# cat ~/proxy.keytab | base64
```

2. Выполните команды:

```
# FILTER_KEYTAB_B64='<BQIAAAfU1V...>'
```

где **<BQIAAAfU1V...>** – значение, полученное на предыдущем шаге.

```
# /opt/dozor/bin/config values set -p /skvt-kerberos-server/krb5-keytab-params/krb5-keytab/some/keytab-base64-string -v """$FILTER_KEYTAB_B64"""
```

5.9.4. Настройка NTLM-аутентификации

Для настройки NTLM-аутентификации:

1. Назначьте одному из узлов Solar webProxy роль **Сервер NTLM-аутентификации**. Это будет сервер аутентификации Solar webProxy.
2. В разделе основных настроек **Аутентификация > Подключение к Контроллеру домена (DC) для NTLM-аутентификации** укажите имя домена AD в поле **Домен**.

Также на усмотрение системного администратора можно указать:

- **Уровень отладки** – параметр уровня журналирования. По умолчанию режим отладки выключен (значение 0).
- **DOS-кодировка** – кодировка Solar webProxy для работы с DC. Эта опция указывает, какую кодировку использовать. По умолчанию CP866.
- **NETBIOS-имя для сервера Solar webProxy** – NetBIOS имя узла, по которому доступен Solar webProxy.

Примечание

По умолчанию значение `${node-hostname}`. Для корректного добавления сервера в домен замените значение `${node-hostname}` на имя узла.

- **Тип Контроллера домена (DC)** – тип безопасности доменного режима `{domain|ads}`. По умолчанию тип `ads`. В любом из этих режимов Solar webProxy работает как участник домена AD. Эти режимы не приводят к работе Solar webProxy в качестве доменного контроллера AD. Тип `ads` обеспечивает поддержку аутентификации Kerberos, а `domain` – нет. Для работы с типом `ads` потребуется настроить `krb5.conf`. При типе `domain` Solar webProxy передает имя пользователя и пароль для аутентификации первичному или резервному контроллеру домена.
 - **Сетевой адрес Контроллера домена (DC)** – имя узла или IP-адрес контроллера домена. По умолчанию – `*` (null).
 - **Использовать домен по умолчанию** – при установке флагка сервис `winbind` будет использовать указанный домен как домен по умолчанию. По умолчанию флагок не установлен.
 - **Период кэширования информации о пользователях (с)** – время кэширования (в секундах) информации о пользователях и группах сервисом `winbind`. По истечении этого периода запрос к DC повторится. Значение по умолчанию 300 (с).
 - **Аутентификация по данным из кэша** – параметр определяет, можно ли подключаться с модулем `param_winbind`, используя Cached Credentials. Если флагок установлен, сервис `winbind` сохранит в Solar webProxy пользовательские Credentials от успешных логинов в локальном кеше в зашифрованном виде.
 - **Макс. количество клиентов к Контроллеру домена (DC)** – максимальное количество одновременных запросов к АД. Значение по умолчанию 500.
 - **Использовать доверенные домены** – используется с параметром `dc-type` со значением `domain` или `ads`. Если флагок не установлен, попытки соединиться с ресурсом из другого домена или другой рабочей группы (кроме той, в которой выполняется служба `smbd`) будут неудачны, даже если между доменом Solar webProxy и сторонним доменом установлены доверительные отношения. По умолчанию флагок установлен.
 - **Использовать NTLMv2** – параметр определяет, будет ли Solar webProxy использовать шифрование NTLMv2 при передаче пароля. Если флагок установлен, пароли будут отправляться только в зашифрованном NTLMv2 и LMv2 виде (более безопасные, чем ранние версии). По умолчанию флагок не установлен.
 - **Рабочая группа** – параметр указывает на принадлежность сервера Solar webProxy к рабочей группе. По умолчанию значение не задано.
3. На сервере аутентификации Solar webProxy откройте для редактирования файл `/etc/resolv.conf` и добавьте в него строки следующего вида:

```
nameserver <namesrvIP>
```

где **<namesrvIP>** – IP-адрес контроллера домена. Если таких адресов несколько, добавьте несколько таких строк, в порядке уменьшения надежности контроллеров домена. В каждой строке может быть только один IP-адрес.

4. Добавьте сервер аутентификации в домен, выполнив на нем с помощью CLI команду следующего вида:

```
# net ads join -U <admin_login>
```

где **<admin_login>** – имя учетной записи пользователя с правами администратора контроллера домена.

5. В GUI в разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения следующих параметров:

- **Режим аутентификации** – **Proxy-Auth**;
- **Метод аутентификации** – **NTLM**.

6. Нажмите **Сохранить** и **Применить**.

7. В CLI выполните команду:

```
# dsctl restart skvt-winbind
```

5.9.5. Настройка прозрачной аутентификации

Прозрачная аутентификация применяется, когда настройка браузеров рабочих станций пользователей невозможна, затруднена или неприемлема. При этом имеются следующие ограничения на архитектуру корпоративной сети:

- каждому IP-адресу должен соответствовать только один пользователь;
- между рабочими станциями пользователей и Solar webProxy не должно быть других прокси-серверов и оборудования, выполняющих трансляцию адресов;
- работа терминальных серверов не поддерживается.

Режим прозрачной аутентификации заменяет обычную на прокси-сервере (HTTP 407: Proxy Authorization Required). При обращении к Solar webProxy рабочей станции пользователя, IP-адреса которой нет в хранилище Solar webProxy, ее запрос перенаправляется на служебную страницу. На этой странице пользователю предлагается ввести учетные данные (HTTP 401: Unauthorized), и в случае успешной авторизации IP-адрес добавляется в хранилище, и продолжается обработка первоначального запроса. Запросы с рабочих станций, IP-адреса которых есть в хранилище, обрабатываются без перенаправлений.

В первую очередь настройте пакетные фильтры на всех узлах фильтрации:

1. Включите IP-forwarding. Для этого в файле **etc/sysctl.conf** раскомментируйте строку **net.ipv4.ip_forward = 1** и примените изменения командой **/sbin/sysctl -p**

Примечание

После включения *IP-forwarding* операционная система будет работать как маршрутизатор.

2. Отключите параметры настройки фильтра Linux-ядра. Для этого в файле **etc/sysctl.conf** раскомментируйте строку
net.ipv4.conf.<название интерфейса>.rp_filter=0
и примените изменения командой
/sbin/sysctl -p

Фильтрация ядром ОС отключается, когда пакет принят одним интерфейсом и должен быть передан на другой интерфейс. Если устройство стоит между несколькими сетями, команда выполняется для всех интерфейсов, между которыми выполняется передача трафика, либо используется параметр **all**, чтобы отключить фильтрацию сразу на всех интерфейсах.

3. Включите поддержку TPROXY в подсистеме маршрутизации, выполнив команды:

```
# ip -f inet rule add fwmark 1 lookup 100
```

(весь трафик, пришедший на интерфейсы, помечается маркером 1 и передается в таблицу маршрутизации 100)

```
# ip -f inet route add local default dev eth0 table 100
```

(в таблицу маршрутизации 100 добавляется маршрут по умолчанию)

4. Подготовьте Solar webProxy к перенаправлению запросов, выполнив команды:

```
# iptables -t mangle -N DIVERT
```

```
# iptables -t mangle -A DIVERT -j MARK --set-mark 1
```

```
# iptables -t mangle -A DIVERT -j ACCEPT
```

```
# iptables -t mangle -A PREROUTING -p tcp -m socket -j DIVERT
```

5. Настройте правила перенаправления запросов в Solar webProxy, выполнив команды:

```
# iptables -t mangle -A PREROUTING -p tcp --dport 443 -j TPROXY --tproxy-mark 0x1/0x1 --on-port 2444
```

```
# iptables -t mangle -A PREROUTING -p tcp --dport 80 -j TPROXY --tproxy-mark 0x1/0x1 --on-port 2270
```

Примечание

Контентная фильтрация Solar webProxy работает только для трафика на портах 80 и 443. Остальной трафик, приходящий на другие порты, будет обрабатываться в соответствии с правилами маршрутизации самой операционной системы. Если нет необходимости в тонкой настройке транзитного трафика, рекомендуется заблокировать весь транзитный трафик, кроме попадающего под контентную фильтрацию на портах 80 и 443. Сделать это можно любым удобным способом:

- в *GUI* в разделе **Политика > Межсетевой экран > Фильтр транзитного трафика**, создав правило блокировки.

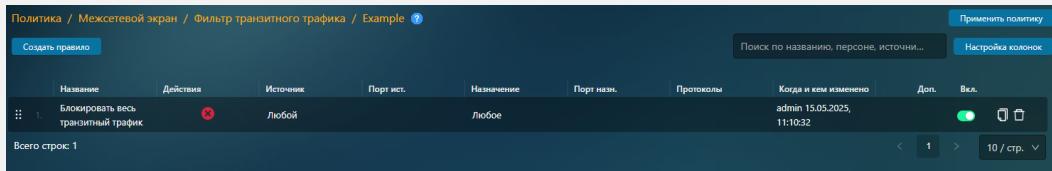


Рис. 5.27. Блокировка всего транзитного трафика

- в *CLI* с помощью команды:

```
# iptables -A FORWARD -j DROP
```

Примечание

При перезагрузке Solar webProxy настройки прозрачной аутентификации могут работать некорректно. Для успешного применения настроек после перезагрузки системы выполните повторно шаги 3-5.

Для включения режима прозрачной аутентификации в *GUI* Solar webProxy:

1. В разделе **Система > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей > Веб-сервер**, предоставляющий скачанные файлы расширенных настроек конфигурации в поле **Адрес веб-сервера** установите значение **\${node-hostname}** (по умолчанию установлено значение **mitm.it**).

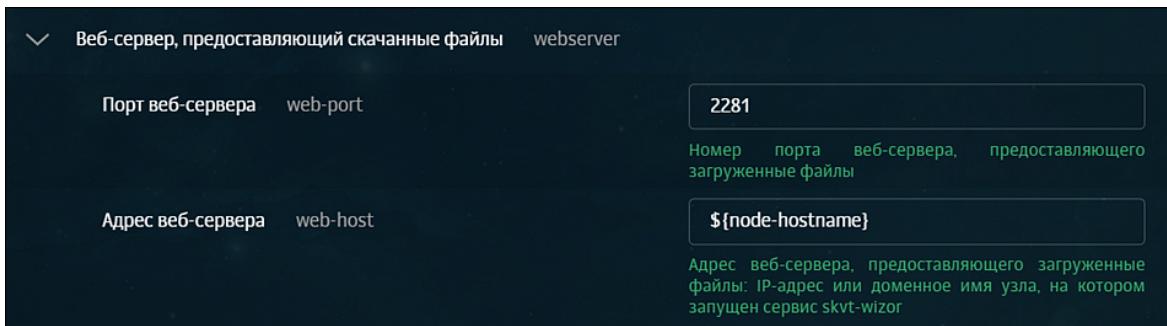


Рис. 5.28. Параметры настройки веб-сервера

2. В разделе **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации установите значение **Transparent** для параметра **Режим аутентификации**.
3. В разделе **Политика > Настройки > Параметры запуска фильтра** или **Система > Основные настройки > Работа системы > Параметры запуска фильтра** установите флажок **Запускать от имени пользователя root**.
4. Нажмите **Сохранить**, затем **Применить**.

-
5. Перезапустите сервис **skvt-wizor**. Для этого в CLI выполните команды:

```
# /opt/dozor/bin/shell
```

```
# dsctl restart skvt-wizor
```

6. Убедитесь, что skvt-wizor запущен от пользователя **root**. Для этого в CLI выполните команды:

```
# dsctl status
```

```
# /usr/lib/systemd/system/dozor_skvt-wizor.service:..... up (pid 3661) 63117 seconds
```

где **3661** — номер процесса skvt-wizor

```
# ps -ef --forest | grep 3661 -A 1
```

После успешного выполнения команды будет отображен вывод вида:

```
root@wp4:/opt/dozor# ps -ef --forest | grep 3661 -A 1
root 1458 31464 0 17:03 pts/0 00:00:00 | grep 3661 -A 1
root 30377 1121 0 17:02 ? 00:00:00 \_ sshd: root@notty
-
root 3661 1 0 14:56 ? 00:00:00 /bin/bash /opt/dozor/var/lib/service/skvt-wizor/run
root 3854 3661 1 14:56 ? 00:02:30 \_ /usr/lib/jvm/bellsoft-javat7-full-amd64//bin/java -Djdk.tls.server.enableSessionTicketExtension=false -add-opens=java.base/java.io=ALL-UNNAMED -add-opens=java.base/sun.nio.ch=ALL-UNNAMED -Dfile.encoding=UTF8 -Dsun.net.client.defaultConnectTimeout=30000 -server -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/tmp -XX:MaxJavaStackTraceDepth=100000 -XX:MaxDirectMemorySize=4096m -Xmx2048m -Xms256m -jar /opt/dozor/skvt/lib/nio_proxy.jar /data/repos/dozor/config-final.git/6b34cd8d-201d-48c8-a788-088d41241248/skvt-wizor/config.xml /opt/dozor/share/url-checker/categories.json
```

При выводе команды убедитесь, что дочерний процесс также запущен от пользователя **root**.

7. В CLI экспортируйте сертификат УЦ Solar webProxy, выполнив команду (в одну строку):

```
# keytool -exportcert -rfc -keystore /opt/dozor/skvt/var/lib/authority.jks -alias "web proxy" > proxy.crt
```

Во время выполнения команды будет запрошен пароль (по умолчанию – **secret**). Файл сертификата появится в текущем каталоге (по умолчанию – **/opt/dozor**).

8. Сконвертируйте экспортированный сертификат в формат PEM, выполнив команду:

```
# openssl x509 -in proxy.crt -outform PEM -out proxy.pem
```

9. Импортируйте полученный сертификат в списки доверенных сертификатов браузеров APM пользователей корпоративной сети. Подробно процесс импорта описан в разделах пользовательской поддержки на сайтах производителей соответствующих браузеров.

Примечание

Если серверов фильтрации несколько, экспортируйте сертификат на всех этих серверах. После экспорта выполните импорт всех полученных сертификатов на APM пользователей.

Также вы можете добавить время жизни сессии прозрачной аутентификации. Для этого перейдите в раздел **Система > Расширенные настройки > Фильтрация и кэширование трафика > Аутентификация и авторизация** и в полях **Тайм-аут неактивности прозрачной аутентификации** и **Жесткий тайм-аут прозрачной аутентификации** укажите необходимое время в секундах.

Примечание

При использовании *negotiate*-аутентификации совместно с прозрачным режимом необходимо на всех АРМ добавить FQDN узла Solar webProxy. Для этого:

1. Откройте **Свойства браузера > Безопасность**.
 2. Выберите **Местная интрасеть** и нажмите кнопку **Сайты**.
 3. В открывшемся окне нажмите кнопку **Дополнительно**.
 4. Добавьте записи **http://proxy.example.org** и **https://proxy.example.org**, где **proxy.example.org** – FQDN проксирующего узла.
-

5.9.6. Настройка basic-аутентификации

5.9.6.1. Типы хранилищ для basic-аутентификации

Для basic-аутентификации могут использоваться следующие типы хранилищ:

- локальный список (раздел [5.9.6.2](#));
- LDAP (раздел [5.9.6.3](#));
- LDAPS (раздел [5.9.6.4](#));
- RADIUS (раздел [5.9.6.5](#));
- Active Directory (раздел [5.9.6.6](#));
- IMAP (раздел [5.9.6.7](#));
- POP3 (раздел [5.9.6.8](#)).

5.9.6.2. Настройка параметров для basic-аутентификации по списку пользователей

Для настройки basic-аутентификации по списку пользователей в разделе **Политика > Объекты политики > Пользователи Basic и SOCKS5**:

1. В разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:
 - **Режим аутентификации – Proxy-Auth**;
 - **Метод аутентификации – Basic**.
2. Нажмите **Сохранить** и **Применить**.

5.9.6.3. Настройка параметров для basic-аутентификации с LDAP-сервером

Для настройки basic-аутентификации с источником аутентификации LDAP:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **Idap**.
2. Заполните появившиеся поля, описание которых приведено в документе *Руководство администратора безопасности*.
3. В разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:
 - **Режим аутентификации – Proxy-Auth;**
 - **Метод аутентификации – Basic.**
4. Нажмите **Сохранить** и **Применить**.

Примечание

Рекомендуется использовать в качестве LDAPs-сервера только Active Directory.

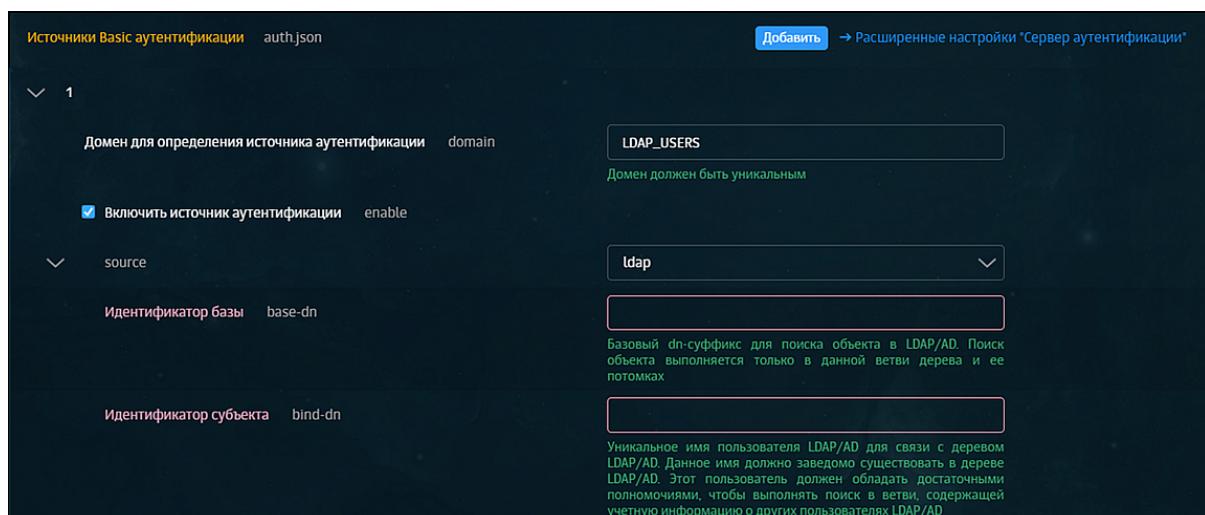


Рис. 5.29. Настройка basic- + LDAP-аутентификации

При выполнении аутентификации вы можете задать более одного домена. Для этого справа от названия секции **Источники Basic-аутентификации** нажмите **Добавить** — появится дополнительная секция для указания соответствующих параметров.

Для удаления добавленной секции используется кнопка  (корзина), расположенная в выбранном сегменте.

При указании нескольких равноправных серверов (в параметре **Адрес сервера**) для одного домена срабатывает механизм **failover**: сервер аутентификации делает запрос к первому из указанных серверов, при ошибке или таймауте новый запрос будет к следующему из списка серверу. При ошибке на последнем сервере из списка выбирается первый по счету. При превышении заданного времени выполнения запроса он прерывается, даже если еще не все серверы опрошены. Состояние между запросами запомина-

ется – при новом запросе сервер аутентификации сразу обращается к тому серверу, на котором был прерван предыдущий запрос.

Внимание!

Механизм failover поддерживается только для двух равноправных контроллеров домена.

5.9.6.4. Настройка параметров для basic-аутентификации с LDAPS-сервером

Для настройки basic-аутентификации с источником аутентификации LDAPS:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **Idaps**.
2. Заполните появившиеся поля, описание которых приведено в документе *Руководство администратора безопасности*.

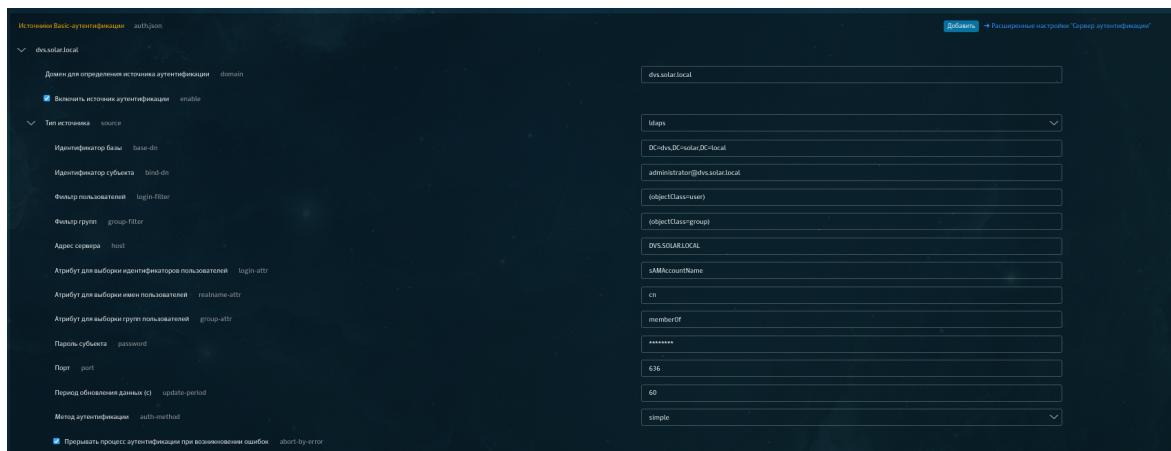


Рис. 5.30. Настройка basic- + LDAPS-аутентификации

3. В разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:
 - **Режим аутентификации – Proxy-Auth;**
 - **Метод аутентификации – Basic.**
4. Нажмите **Сохранить** и **Применить**.

Примечание

Рекомендуется использовать в качестве LDAPS-сервера только Active Directory.

При выполнении аутентификации вы можете задать более одного домена. Для этого нажмите **Добавить** справа от названия секции **Источники Basic-аутентификации**, в

результате чего появится дополнительная секция для указания соответствующих параметров.

Для удаления добавленной секции используется кнопка  (изображение корзины), расположенная в выбранном сегменте.

При указании нескольких равноправных серверов (в параметре **Адрес сервера**) для одного домена срабатывает механизм **failover**: сервер аутентификации делает запрос к первому из указанных серверов, а при ошибке или таймауте новый запрос происходит к следующему из списка серверу. В случае ошибки на последнем из списка сервере выбирается первый сервер. При превышении заданного времени выполнения запроса он прерывается, даже если еще не все серверы опрошены. Состояние между запросами запоминается – при новом запросе сервер аутентификации сразу обращается к тому серверу, на котором был прерван предыдущий запрос.

Внимание!

Механизм failover поддерживается только для двух равноправных контроллеров домена.

5.9.6.5. Настройка basic-аутентификации с RADIUS-сервером

RADIUS-аутентификация — метод basic-аутентификации для удаленного доступа к пользовательским сервисам, виртуальным частным сетям (VPN), точкам беспроводного доступа (Wi-Fi) и т.д.

RADIUS-протокол реализован в виде интерфейса между NAS, который выступает как RADIUS-клиент, и RADIUS-сервером — программным обеспечением, которое может быть установлено на сервере или специализированном устройстве. Таким образом, RADIUS-сервер не взаимодействует напрямую с устройством пользователя, а только через сетевой сервер доступа.

Для настройки RADIUS-аутентификации:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации:
 - Установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **radius**.
 - В списке отобразившихся параметров укажите IP-адрес RADIUS-сервера и пароль (см. [Рис.5.31](#)).

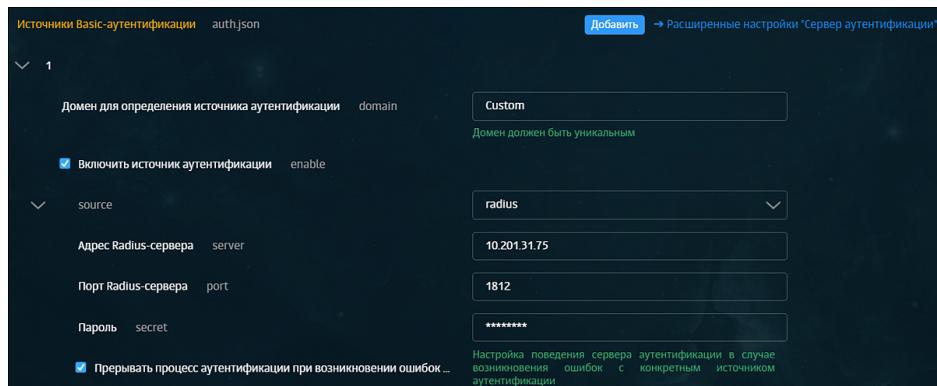


Рис. 5.31. Настройки basic-аутентификации с RADIUS-сервером

2. В разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:
 - **Режим аутентификации – Proxy-Auth;**
 - **Метод аутентификации – Basic.**

Примечание

Используйте параметр **Срок жизни автоматического связывания (мин)**, если необходимо установить время хранения аутентификационной сессии в кеше при автоматическом связывании персон в правилах словес **Политика > Правила доступа SOCKS5 > Доступ без аутентификации** и/или **Политика > Конtentная фильтрация > Правила аутентификации**. Значение параметра может быть от 1 до 43800, по умолчанию – 15 минут.

Параметр **Срок жизни автоматического связывания (мин)** распространяется только на пользователей, чья первоначальная аутентификация проходила с помощью домена (NTLM/Negotiate/Basic-аутентификации). Если пользователь отсутствует в разделе **Политика > Объекты политики > Пользователи Basic и SOCKS5** или он выключен, Solar webProxy аутентифицирует пользователя через AD, используя сервис *Auth Server* и логин.

3. Нажмите **Сохранить** и **Применить**.

5.9.6.6. Настройка basic-аутентификации со службой Active Directory

Для настройки basic-аутентификации со службой Active Directory:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **ad**.
2. Заполните появившиеся поля аналогично тому, как показано на [Рис.5.32](#):

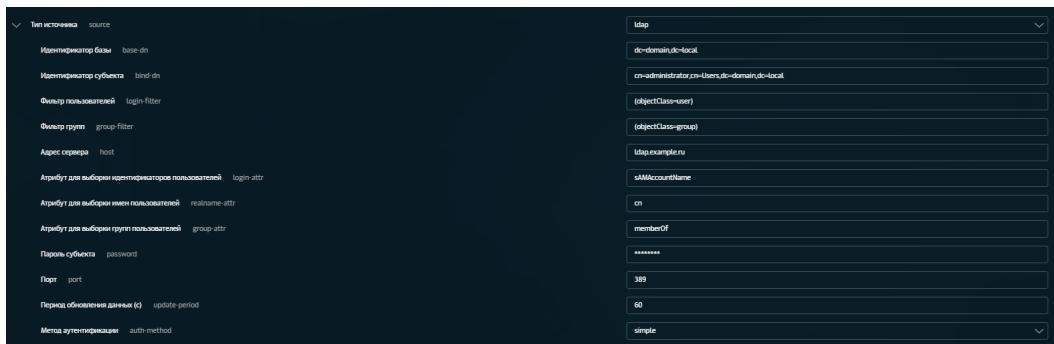


Рис. 5.32. Настройки сервера Active Directory

Примечание

В поле **Атрибут для выборки идентификаторов пользователей** можно также указать значение *userPrincipalName*. В этом случае при авторизации пользователь должен будет указать свой UPN вместо логина.

Не рекомендуется использовать *msDS-PrincipalName*, так как при аутентификации и авторизации пользователя обратная косая черта на конце логина будет рассматриваться системой как escape-последовательность.

3. В разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:
 - Режим аутентификации – **Proxy-Auth**;
 - Метод аутентификации – **Basic**.

Примечание

Используйте параметр **Срок жизни автоматического связывания (мин)**, если необходимо установить время хранения аутентификационной сессии в кеше при автоматическом связывании персон в правилах слоев **Политика > Правила доступа SOCKS5 > Доступ без аутентификации** и/или **Политика > Контентная фильтрация > Правила аутентификации**. Значение параметра может быть от 1 до 43800, по умолчанию – 15 минут.

Параметр **Срок жизни автоматического связывания (мин)** распространяется только на пользователей, чья первоначальная аутентификация проходила с помощью домена (NTLM/Negotiate/Basic-аутентификации). Если пользователь отсутствует в разделе **Политика > Объекты политики > Пользователи Basic и SOCKS5** или он выключен, Solar webProxy аутентифицирует пользователя через AD, используя сервис *Auth Server* и логин.

4. Нажмите **Сохранить** и **Применить**.

Вы можете задать более одного домена. Для этого нажмите **Добавить** справа от названия секции **Источники Basic-аутентификации**, в результате чего появится дополнительная секция для указания соответствующих параметров.

Для удаления добавленной секции используется кнопка  , расположенная в выбранном сегменте.

При указании нескольких равноправных серверов (в параметре **Адрес сервера**) для одного домена срабатывает механизм **failover**: сервер аутентификации делает запрос к первому из указанных серверов, а при ошибке или таймауте новый запрос происходит к следующему из списка серверу. В случае ошибки на последнем сервере, из списка выбирается первый сервер. При превышении заданного времени выполнения запроса он прерывается, даже если еще не все серверы опрошены. Состояние между запросами запоминается – при новом запросе сервер аутентификации сразу обращается к тому серверу, на котором был прерван предыдущий запрос.

Внимание!

Механизм failover поддерживается только для двух равноправных контроллеров домена.

5.9.6.7. Настройка basic-аутентификации с IMAP-сервером

Для настройки basic-аутентификации с источником аутентификации IMAP:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **imap**.

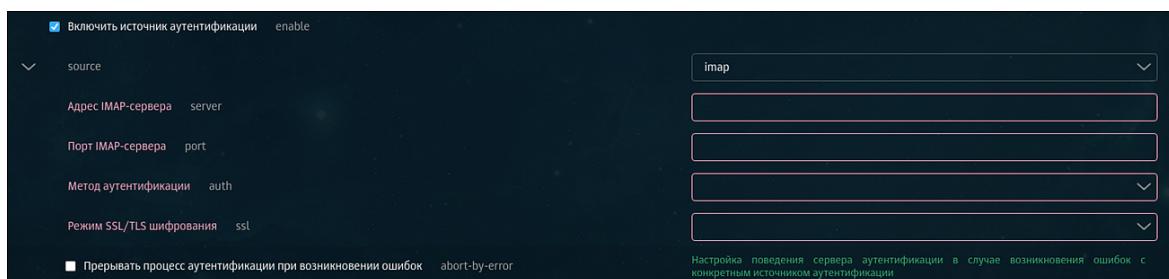


Рис. 5.33. Настройка аутентификации basic + IMAP

2. Задайте параметры:

- **Адрес IMAP-сервера** – IP-адрес IMAP-сервера;
- **Порт IMAP-сервера** – порт IMAP-сервера.

Выберите метод аутентификации и режим SSL/TLS-шифрования из предложенных вариантов.

3. В разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:

- **Режим аутентификации** – **Proxy-Auth**;
- **Метод аутентификации** – **Basic**.

Примечание

Используйте параметр **Срок жизни автоматического связывания (мин)**, если необходимо установить время хранения аутентификационной сессии в кеше при автоматическом связывании персон в правилах слоев **Политика > Правила доступа SOCKS5 > Доступ без аутентификации** и/или **Политика > Контентная фильтрация > Правила аутентификации**. Значение параметра может быть от 1 до 43800, по умолчанию – 15 минут.

Параметр **Срок жизни автоматического связывания (мин)** распространяется только на пользователей, чья первоначальная аутентификация проходила с помощью домена (NTLM/Negotiate/Basic-аутентификации). Если пользователь отсутствует в разделе **Политика > Объекты политики > Пользователи Basic и SOCKS5** или он выключен, Solar webProxy аутентифицирует пользователя через AD, используя сервис *Auth Server* и логин.

4. Нажмите Сохранить и Применить.

5.9.6.8. Настройка basic-аутентификации с POP3-сервером

Для настройки basic-аутентификации с источником аутентификации POP3:

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **pop3**.
2. Задайте параметры ([Рис.5.34](#)):
 - **Адрес POP3-сервера** – IP-адрес POP3-сервера;
 - **Порт POP3-сервера** – порт POP3-сервера.

Выберите режим SSL/TLS-шифрования из предложенных вариантов.

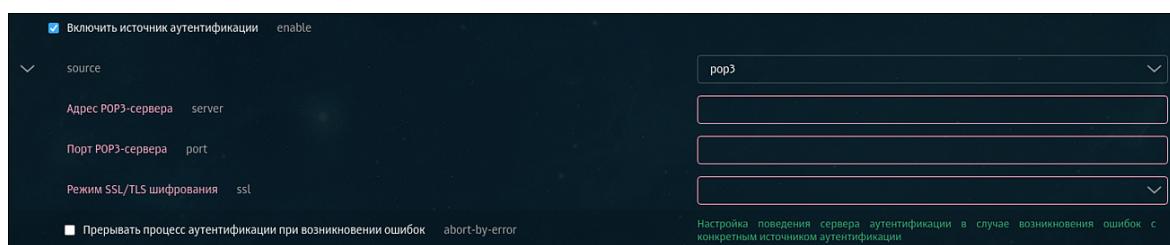


Рис. 5.34. Настройка аутентификации basic + POP3

3. В разделе **Политика > Настройки** или **Работа системы > Фильтрация и анализ трафика пользователей** основных настроек конфигурации задайте значения для параметров:
 - **Режим аутентификации** – **Proxy-Auth**;
 - **Метод аутентификации** – **Basic**.

Примечание

Используйте параметр **Срок жизни автоматического связывания (мин)**, если необходимо установить время хранения аутентификационной сессии в кеше при автоматическом связывании персон в правилах слоев **Политика > Правила доступа SOCKS5 > Доступ без аутентификации** и/или **Политика > Контентная фильтрация > Правила аутентификации**. Значение параметра может быть от 1 до 43800, по умолчанию – 15 минут.

Параметр **Срок жизни автоматического связывания (мин)** распространяется только на пользователей, чья первоначальная аутентификация проходила с помощью домена (NTLM/Negotiate/Basic-аутентификации). Если пользователь отсутствует в разделе **Политика > Объекты политики > Пользователи Basic и SOCKS5** или он выключен, Solar webProxy аутентифицирует пользователя через AD, используя сервис *Auth Server* и логин.

4. Нажмите **Сохранить** и **Применить**.

5.10. Настройка аутентификации SOCKS5

Примечание

Работа протокола SOCKS5 на вышестоящем прокси-сервере невозможна.

5.10.1. Настройка прокси-сервера SOCKS5 при Kerberos-аутентификации

Примечание

В данном разделе рассматривается примерный способ настройки прокси-сервера SOCKS5 при Kerberos-аутентификации.

Перед настройкой прокси-сервера SOCKS5 при Kerberos-аутентификации необходимо выпустить keytab-файл:

1. С помощью AD или консоли Windows PowerShell создайте нового пользователя для привязки SPN (Service Principal Name – уникальный идентификатор экземпляра сервиса) с помощью команды:

```
New-ADUser -Name "socks5-user" -GivenName "socks5-user" -SamAccountName "socks5-user" -UserPrincipalName "socks5-user@solar.local" -AccountPassword (ConvertTo-SecureString "password" -AsPlainText -force) -Enabled $true -PasswordNeverExpires $true -CannotChangePassword $true
```

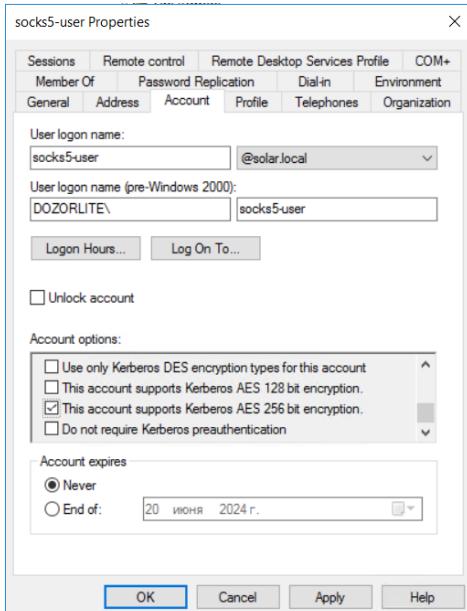
Примечание

Значения для замены:

- **socks5-user** – имя пользователя SOCKS5. Имя пользователя и путь к нему не должны содержать кириллические символы.

- **password** – пароль пользователя.

2. Перейдите в Active Directory Users and Computers и установите флажок **This account supports Kerberos AES 256 bit encryption**.



3. От имени администратора откройте консоль Windows PowerShell.

4. Выполните команду:

```
ktpass.exe -princ rcmd/webproxy.domain.local@DOMAIN.LOCAL -mapuser socks5-user -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -pass password -out C:\Users\Administrator\socks5-user.keytab -target 10.201.69.47
```

Примечание

Значения для замены:

- **webproxy.domain.local** – FQDN сервера аутентификации Solar webProxy;
- **DOMAIN.LOCAL** – имя домена;
- **password** – пароль пользователя;
- **10.201.69.47** – IP-адрес контроллера домена (KDC), с помощью которого был выпущен keytab-файл.

В результате выполнения этой команды будет создан ключ аутентификации. Ключ будет находиться в месте, указанном после **-out**, в данном примере – **C:\Users\Administrator\socks5-user.keytab**.

5. В разделе **Система > Узлы и роли** установите для узла роль **Сервер Kerberos-аутентификации**.

-
6. В разделе **Система > Расширенные настройки > Регистрация сервера в домене > Kerberos-аутентификация** в полях **Тип шифрования для KDC** и **Тип шифрования для клиентов** измените значение на **aes256-cts-hmac-sha1-96**.
 7. В разделе **Политика > Настройки > Прокси-сервер SOCKS5**:
 - В поле **Первичное имя сервиса (SPN)** укажите SPN вида rcmd/"DNS-имя службы в домене"@"UPN-суффикс". Например, rcmd/webproxy.domain.local@DOMAIN.LOCAL.
 - В поле **Keytab-файл** загрузите файл, полученный на шаге 4.
 - В поле **Порт сервера для соединения** укажите порт, принимающий соединения на сервере, который поддерживает протокол SOCKS5.
 - В поле **Время, через которое будут сброшены неактивные сессии (с.)** укажите значение в секундах, по истечению которого, если с целевого узла не получены данные, происходит обрыв соединения. Оптимальное время 300 секунд.

5.10.2. Настройка прокси-сервера SOCKS5 при доступе без аутентификации

Основная задача метода **Доступ без аутентификации** дать возможность пройти запросам пользователя при невозможности их аутентификации настроенным методом, т.к. некоторые приложения и пользователи могут не поддерживать Basic- и/или Kerberos-аутентификацию, настроенную в системе.

Чтобы включить возможность доступа без аутентификации по протоколу SOCKS5, в разделах **Политика > Настройки > Прокси-сервер SOCKS5 > Метод аутентификации** или **Система > Расширенные настройки > Фильтрация и кэширование трафика > Прокси-сервер SOCKS5 > Метод аутентификации** установите флажок **Доступ без аутентификации**.

5.10.3. Настройка прокси-сервера SOCKS5 при парольной аутентификации

Чтобы настроить прокси-сервер SOCKS5 при парольной аутентификации:

1. В разделах **Политика > Настройки > Прокси-сервер SOCKS5 > Метод аутентификации** или **Система > Расширенные настройки > Фильтрация и кэширование трафика > Прокси-сервер SOCKS5 > Метод аутентификации** установите флажок **Парольная аутентификация**.
2. Создайте пользователей в разделе **Политика > Объекты политики > Пользователи Basic и SOCKS5**.

Примечание

При добавлении пользователя убедитесь, что в поле **Тип аутентификации** включен переключатель **SOCKS5**.

Для прохождения парольной аутентификации пользователь SOCKS5 должен быть активным. Если он будет неактивен или отсутствовать, аутентификация будет выполняться через AD с помощью сервиса Auth Server с использованием логина.

5.11. Настройка вскрытия SSL-трафика

5.11.1. Настройка вскрытия SSL-трафика (MITM, RSA)

5.11.1.1. Настройка MITM с использованием УЦ организации

Если в организации имеется собственный УЦ, можно использовать его сертификат для вскрытия SSL-трафика. Допустимо использование сертификатов, сгенерированных алгоритмом строго выше SHA-1.

Для выпуска сертификата организации на каждом сервере Solar webProxy с ролью **Фильтр HTTP-трафика**:

1. В CLI перейдите во временный каталог (например, `/var/tmp/`), выполнив команду:

```
# cd /var/tmp
```

2. Создайте ключ RSA, выполнив команду:

```
# openssl genrsa -out wp.key -aes256 2048
```

Во время выполнения команды система потребует назначить пароль для ключа. Введите пароль и запомните его. После ввода подтвердите выбранный пароль.

3. Создайте в текущем каталоге файл с именем **openssl.cnf** и запишите в него данные:

```
[ req ]  
req_extensions = v3_req  
distinguished_name = req_distinguished_name  
prompt=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 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 сервера, на котором происходит настройка;
- **emailAddress_default** – контактный адрес электронной почты организации;
- **DNS.0** – значение, указанное в параметре **commonName_default**;
- **IP.0** – IP-адрес сервера, на котором происходит настройка.

4. Сгенерируйте запрос на подпись сертификата, выполнив команду:

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

В процессе выполнения команды система потребует ввести пароль, заданный на шаге 2.

5. На сервере организации, имеющем роль CA (Certification Authority), проверьте используемый алгоритм шифрования. Для этого откройте программу **Командная строка** от имени администратора и выполните в ней команду:

```
certutil -getreg ca\csp\CNGHashAlgorithm
```

Если значение параметра **REG_SZ** равно **SHA1**, выполните команды:

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
```

```
net stop CertSvc && net start CertSvc
```

Примечание

После изменения алгоритма все ранее выпущенные сертификаты нужно будет перевыпускать с помощью алгоритма SHA-256.

6. Снова выпишите корневой сертификат и перезапустите службу Certificate Services, выполнив команды:

```
certutil -renewCert ReuseKeys
```

net stop CertSvc && net start CertSvc

7. Зайдите на портал УЦ Windows.

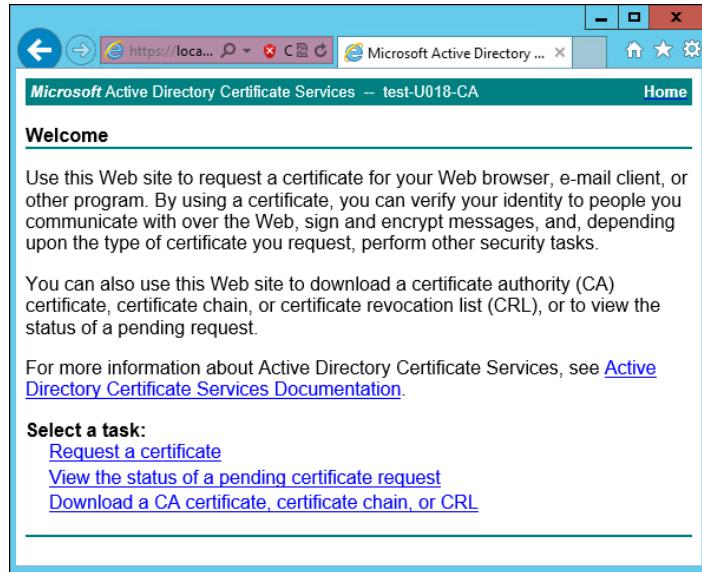


Рис. 5.35. Экран приветствия УЦ Windows

8. Нажмите **Request a certificate**.

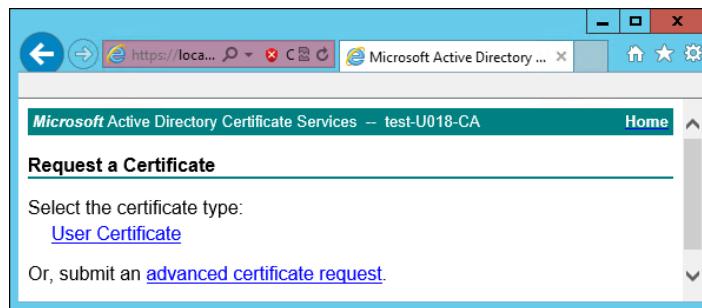


Рис. 5.36. Экран запроса сертификата

9. Нажмите **advanced certificate request**.

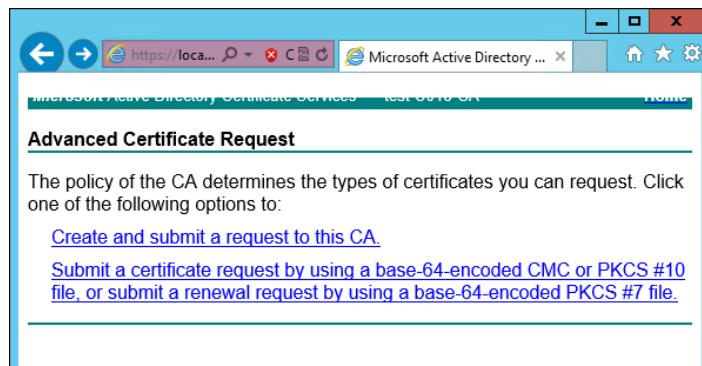


Рис. 5.37. Экран особого запроса сертификата

10. Нажмите **Submit a certificate request by using....**

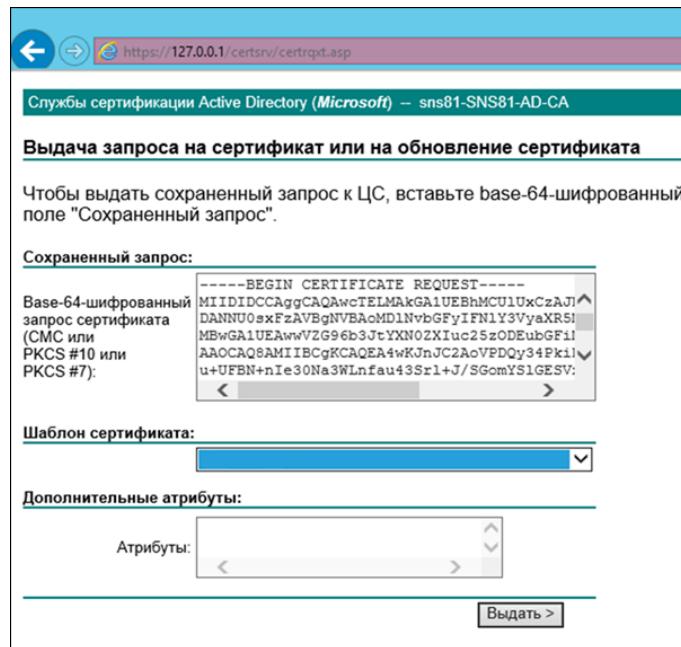


Рис. 5.38. Экран атрибутов сертификата

11. Выберите шаблон сертификата **Subordinate authority** (Подчинённый центр сертификации) и вставьте в поле **Base-64** содержимое файла, созданного на шаге 4. Нажмите **Выдать**.

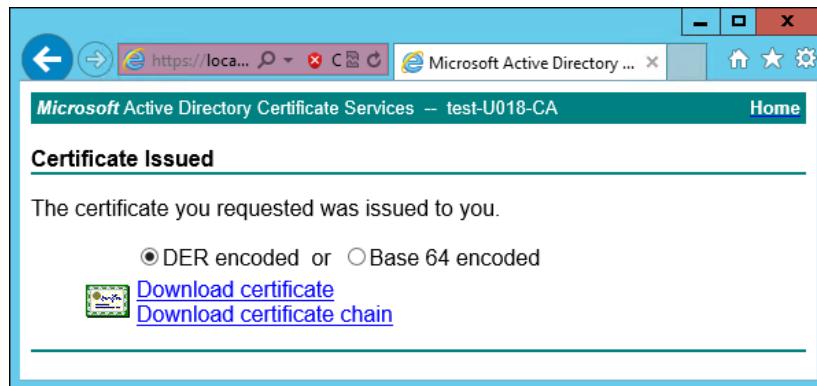


Рис. 5.39. Экран выдачи сертификата

12. Нажмите **Download certificate**. Сохраните файл сертификата с именем **wp.cer** во временный каталог, выбранный в шаге 1.

13. Перейдите на главную страницу портала УЦ и нажмите **Download a CA certificate, certificate chain or CRL**. Сохраните сертификат УЦ с именем **ca.cer** в тот же каталог.

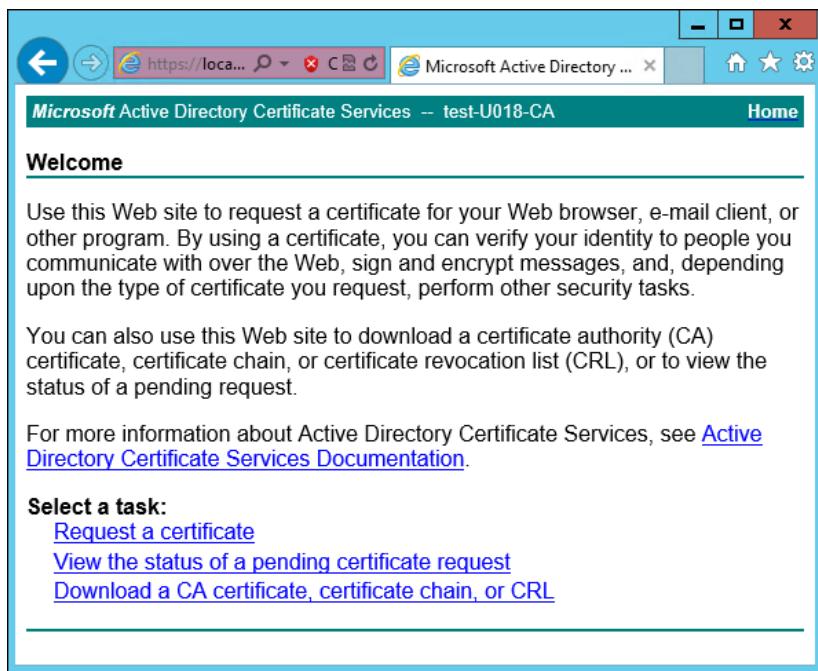


Рис. 5.40. Экран приветствия УЦ Windows

14. Вернитесь в CLI Solar webProxy, перейдите в выбранный временный каталог и сконвертируйте загруженные сертификаты в формат PEM, выполнив команды:

```
# openssl x509 -inform der -in wp.cer -out wp.pem
```

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

15. Объедините сертификаты и ключ в сертификат pkcs12, выполнив команду:

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

Во время выполнения команды система потребует ввести пароль.

16. Импортируйте Java-хранилище сертификатов, выполнив команду вида:

```
# keytool -importkeystore -deststorepass <password> -destkeypass <password> -destkeystore <wpN>.jks -srckeystore wp.p12 -srcstorepass <password> -deststoretype jks
```

где <password> – выбранный пароль, а <wpN> – имя сертификата для текущего сервера (например, wp1).

17. Скопируйте Java-хранилище в каталог Solar webProxy, выполнив команду вида:

```
# cp <wpN>.jks /opt/dozor/skvt/var/lib/
```

где <wpN> – значение, выбранное в предыдущем шаге.

18. Смените владельца хранилища, выполнив команду вида:

```
# chown dozor:dozor /opt/dozor/skvt/var/lib/<wpN>.jks
```

19. Проверьте, что сертификат находится в хранилище, выполнив команду вида:

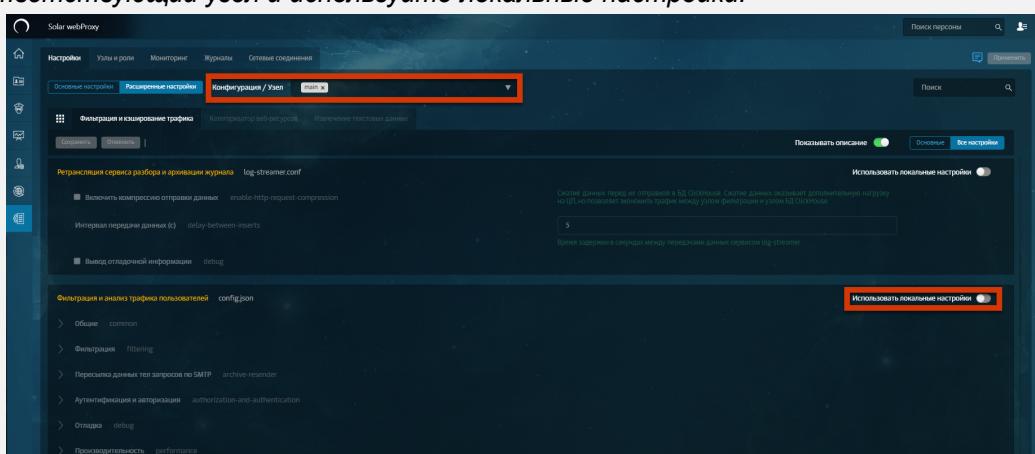
```
# keytool -list -keystore /opt/dozor/skvt/var/lib/<wpN>.jks
```

О наличии сертификата в хранилище будет свидетельствовать вывод следующего вида:

```
1, Jul 10, 2018, PrivateKeyEntry,  
Certificate fingerprint (SHA-256): B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
```

20. Примечание

Если для каждого фильтра необходимо выдать свой сертификат, перед выполнением данного шага в разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей** укажите в настройках соответствующий узел и используйте локальные настройки.



Далее выполните шаг инструкции для каждого фильтра.

В GUI в разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей** раскройте группу параметров **Сертификаты** и задайте значения параметров:

- Путь к хранилищу ключей – `/opt/dozor/skvt/var/lib/<wpN>.jks`
- Пароль к хранилищу ключей – пароль;
- Общее имя корневого сертификата (CA Common name) – 1.

21. Перезапустите сервис **skvt-wizor**, выполнив в CLI команды:

```
# /opt/dozor/bin/shell
```

```
# dsctl restart skvt-wizor
```

22. Импортируйте полученный сертификат в списки доверенных сертификатов браузеров APM пользователей корпоративной сети. Подробно процесс импорта описан в разделах пользовательской поддержки на сайтах производителей соответствующих браузеров.

Примечание

Если серверов фильтрации несколько, экспортируйте сертификат на всех этих серверах. После экспортации выполните импорт всех полученных сертификатов на АРМ пользователей.

5.11.1.2. Настройка хранилища сертификатов Windows для Mozilla Firefox

Браузер Mozilla Firefox по умолчанию использует собственное (не стандартное) хранилище сертификатов Windows. Процедура ручного добавления сертификатов Windows на АРМ пользователей, использующих этот браузер, как и процедура ручной настройки каждого браузера для использования стандартного хранилища, может быть весьма трудоемкой. Поэтому рекомендуется автоматически настроить браузеры пользователей с помощью js-скрипта, распространяемого механизмом Group Policy в домене. Для этого:

1. Создайте файл скрипта с именем **Enable sec-enterprise_roots.js** и добавьте в него строку:

```
pref ("security.enterprise_roots.enabled", true);
```

2. С помощью Group Policy распространите полученный скрипт по АРМ пользователей, использующих Mozilla Firefox. Путь, по которому должен быть размещен скрипт (в зависимости от разрядности ОС АРМ):

- C:\Program Files\Mozilla Firefox\defaults\pref
- C:\Program Files(x86)\Mozilla Firefox\defaults\pref

При запуске браузера его конфигурация будет обновлена. Проверить, что браузер настроен правильно, можно введя в адресной строке **about:config** и выполнив поиск по подстроке **roots**. Параметр **security.enterprise_roots.enabled** должен иметь значение **true**.

5.11.2. Настройка вскрытия SSL-трафика (MITM, ECDSA)

При установке Solar webProxy на новую систему будет создан JKS-контейнер, подписанный с помощью алгоритма ECDSA.

5.11.2.1. Получение сертификата

Для настройки вскрытия шифрованных соединений АРМ пользователей корпоративной сети с ресурсами сети Интернет:

1. Настройте прокси в браузере.
2. Перейдите по адресу: <http://mitm.it:2281/cert/manual>.
3. В зависимости от ОС выберите инструкцию и по ней выполните загрузку и установку сертификата.

5.11.2.2. Настройка MITM без УЦ организации

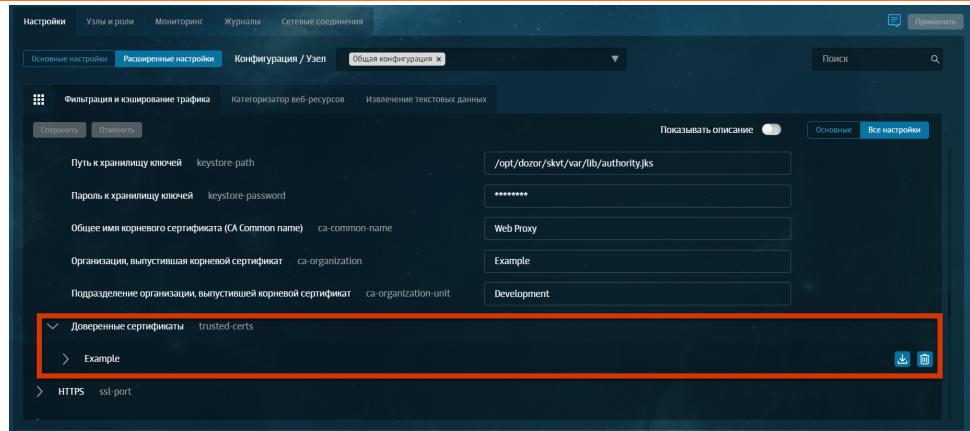
В Solar webProxy предусмотрена возможность установления доверительного отношения к загруженным сертификатам в формате PEM вручную через интерфейс. Для этого в

разделе **Система > Настройки > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей > Сертификаты > Доверенные сертификаты** нажмите кнопку **Добавить**. После добавления сертификат можно загрузить или удалить.

Примечание

Для наименования доверенного сертификата используйте только латинские буквы. С названием, написанным кириллицей, сертификат работать не будет.

Возможность скачать загруженный сертификат появляется после обновления страницы.



Для настройки вскрытия шифрованных соединений АРМ пользователей корпоративной сети с ресурсами сети Интернет через CLI:

1. Подключитесь к серверу фильтрации кластера Solar webProxy по протоколу SSH. Если в кластере несколько серверов фильтрации, выполните приведенные ниже шаги для каждого из них.
2. Экспортируйте сертификат УЦ Solar webProxy, выполнив команду (в одну строку):

```
# keytool -exportcert -rfc -keystore /opt/dozor/skvt/var/lib/authority.jks -alias "web proxy" > proxy.crt
```

Во время выполнения команды будет запрошен пароль (по умолчанию – **secret**). Файл сертификата появится в текущем каталоге (по умолчанию – **/opt/dozor**).

3. Импортируйте полученный сертификат в списки доверенных сертификатов браузеров АРМ пользователей корпоративной сети. Подробно процесс импорта описан в разделах пользовательской поддержки на сайтах производителей соответствующих браузеров.

Примечание

Если серверов фильтрации несколько, экспортируйте сертификат на всех этих серверах. После экспорта выполните импорт всех полученных сертификатов на АРМ пользователей.

5.11.2.3. Настройка MITM с использованием УЦ организации

Для настройки вскрытия SSL-трафика с использованием сертификата организации (алгоритм цифровой подписи ECDSA) на каждом сервере Solar webProxy с ролью **Фильтр HTTP-трафика**:

1. В CLI перейдите во временный каталог (например, **/var/tmp/**), выполнив команду:

```
# cd /var/tmp
```

2. Создайте ключ ECDSA, выполнив команду:

```
# openssl ecparam -name secp521r1 -genkey -noout -out wp.key
```

3. Создайте в текущем каталоге файл с именем **openssl.cnf** и запишите в него данные:

```
[ req ]  
req_extensions = v3_req  
distinguished_name = req_distinguished_name  
prompt=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 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 сервера, на котором происходит настройка;
 - **emailAddress_default** – контактный адрес электронной почты организации;
 - **DNS.0** – значение, указанное в параметре **commonName_default**;
 - **IP.0** – IP-адрес сервера, на котором происходит настройка.

4. Сгенерируйте запрос на подпись сертификата, выполнив команду:

```
# openssl req -new -sha256 -key wp.key -out wp.req -config openssl.cnf
```

5. На сервере организации, имеющем роль CA (Certification Authority), проверьте используемый алгоритм шифрования. Для этого откройте программу **Командная строка** от имени администратора и выполните в ней команду:

```
certutil -getreg ca\csp\CNGHashAlgorithm
```

Если значение параметра **REG_SZ** равно **SHA1**, выполните команды:

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
```

```
net stop CertSvc && net start CertSvc
```

6. Снова выпишите корневой сертификат и перезапустите службу Certificate Services, выполнив команды:

```
certutil -renewCert ReuseKeys
```

```
net stop CertSvc && net start CertSvc
```

7. Перейдите в настройки центра сертификации и добавьте шаблон **Подчиненный центр сертификации**.

8. Выпустите сертификат, выполнив следующую команду:

```
certreq -submit -attrib "CertificateTemplate: SubCA" c:\wp.req
```

В появившемся окне выберите центр сертификации и сохраните файл под именем **wp.cer**.

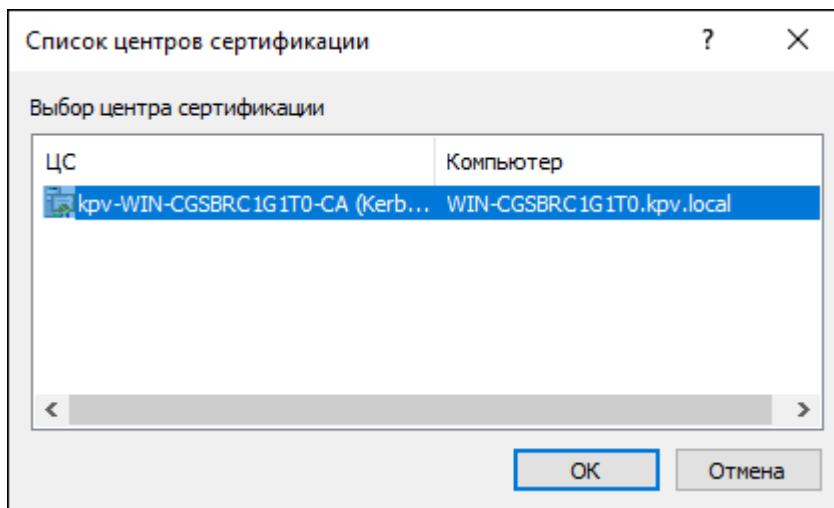


Рис. 5.41. Выбор центра сертификации

9. В CLI загрузите сертификат УЦ, выполнив команду:

```
certutil -ca.cert C:\ca.cer
```

10. Скопируйте файл **wp.cer** в каталог **/var/tmp** сервера Solar webProxy с ролью **Фильтр HTTP-трафика** и переименуйте его в **wp.pem**.

11. Сконвертируйте полученный сертификат УЦ в формат PEM, выполнив команду:

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

12. Объедините сертификаты и ключ в сертификат pkcs12, выполнив команду:

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

Во время выполнения команды система потребует ввести пароль.

13. Импортируйте Java-хранилище сертификатов, выполнив команду вида:

```
# keytool -importkeystore -deststorepass <password> -destkeypass <password> -destkeystore <wpN>.jks -srckeystore wp.p12 -srcstorepass <password>
```

где **<password>** – выбранный пароль, а **<wpN>** – имя сертификата для текущего сервера (например, **wp1**).

14. Скопируйте Java-хранилище в каталог Solar webProxy, выполнив команду вида:

```
# cp <wpN>.jks /opt/dozor/skvt/var/lib/
```

где **<wpN>** – значение, выбранное в предыдущем шаге.

15. Смените владельца хранилища, выполнив команду вида:

```
# chown dozor:dozor /opt/dozor/skvt/var/lib/<wpN>.jks
```

16. Проверьте, что сертификат находится в хранилище, выполнив команду вида:

```
# keytool -list -keystore /opt/dozor/skvt/var/lib/<wpN>.jks
```

О наличии сертификата в хранилище будет свидетельствовать вывод следующего вида:

```
1, Jul 10, 2018, PrivateKeyEntry,  
Certificate fingerprint (SHA-256): B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
```

17. В GUI в разделе **Система > Расширенные настройки > Фильтрация и анализ трафика пользователей** раздела **Фильтрация и кэширование трафика** раскройте группу параметров **Сертификаты**. Задайте значения параметров:

- Путь к хранилищу ключей – `/opt/dozor/skvt/var/lib/<wpN>.jks`;
- Пароль к хранилищу ключей – пароль;
- Организация, выпустившая корневой сертификат – название организации;
- Подразделение организации, выпустившей корневой сертификат – название подразделения.

18. Перезапустите сервис **skvt-wizor**, выполнив в CLI команды:

```
# /opt/dozor/bin/shell
```

```
# dsctl restart skvt-wizor
```

19. Импортируйте полученный сертификат в списки доверенных сертификатов браузеров APM пользователей корпоративной сети. Подробно процесс импорта описан в разделах пользовательской поддержки на сайтах производителей соответствующих браузеров.

Примечание

Если серверов фильтрации несколько, экспортируйте сертификат на всех этих серверах. После экспортта выполните импорт всех полученных сертификатов на APM пользователей.

5.11.2.4. Диагностика проблем с сертификатами

При возникновении ошибок во время вскрытия сертификата или цепочки сертификатов в Solar webProxy будет отображен список с загруженными сертификатами и отчет об успехе или ошибке их загрузки. Для удобства в цепочке под каждым сертификатом с проблемой отображается текстовое описание ошибки на английском и русском языках.

Error 502

Error message: PKIX path validation failed: java.security.cert.CertPathValidatorException: validity check failed

1.

Serial 99565320202650452861752791156765321481
Date from 09.04.2015
Date to 12.04.2015
Subject CN=*.badssl.com, OU=PositiveSSL Wildcard, OU=Domain Control Validated
Issuer CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
aia <http://crt.comodoca.com/COMODORSADomainValidationSecureServerCA.crt>
<http://ocsp.comodoca.com>

*Certificate is outdated or is not actual by date range
Сертификат на текущий момент не укладывается во временной диапазон актуальности*

2.

Serial 57397899143990363081023081275480378375
Date from 12.02.2014
Date to 11.02.2029
Subject CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Issuer CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
aia <http://crt.comodoca.com/COMODORSADAddTrustCA.crt>
<http://ocsp.comodoca.com>

*Certificate is outdated or is not actual by date range
Сертификат на текущий момент не укладывается во временной диапазон актуальности*

3.

Serial 52374340215108295845375962883522092578
Date from 30.05.2000
Date to 30.05.2020
Subject CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB
Issuer CN=AddTrust External CA Root, OU=AddTrust External TTP Network, O=AddTrust AB, C=SE
aia <http://ocsp.usertrust.com>

*Certificate is outdated or is not actual by date range
Сертификат на текущий момент не укладывается во временной диапазон актуальности*

Ошибка возникает, если:

- невозможно построить цепочку сертификатов;
- время действия сертификата истекло;
- имя владельца, прописанное в сертификате, не соответствует имени ресурса, предоставившего его.

В цепочке сертификатов для каждого сертификата отображаются поля:

- серийный номер,
- даты начала и окончания действия сертификата,
- имя владельца сертификата,
- имя издателя сертификата,
- адрес сервиса онлайн-получения статуса сертификата (по протоколу OCSP).

5.12. Настройка вскрытия шифрованного трафика

Для защиты локального трафика от прослушивания и MITM-атак при обращении к ресурсам сети Интернет по протоколу HTTP используется TLS-порт Solar webProxy – 2443.

Для АРМ, использующих TLS-порт, все передаваемые данные на участке клиент-прокси шифруются. При установлении TLS-соединения браузер АРМ проверяет сертификат Solar webProxy, и соединение устанавливается только при наличии доверенного серти-

фиката. Соединение на участке прокси-назначение происходит в обычном режиме, шифрование не выполняется.

Для работы TLS-порта требуется следующее:

1. Solar webProxy должен обладать сертификатом, подписанным доверенным УЦ. Работа с самоподписанными сертификатами не поддерживается. Можно использовать УЦ организации, в этом случае необходимо настроить Solar webProxy на использование настроенного системным администратором ключа и сертификата (см. раздел [5.11.1.1](#)). Системный администратор должен добавить УЦ, подписавший ключ Solar webProxy в список доверенных у пользователей АРМ.

Solar webProxy по умолчанию создает свой УЦ и сертификат. Сертификат и ключ УЦ Solar webProxy находятся в файле `/opt/dozor/skvt/var/lib/authority.jks`.

Сертификат можно экспортовать с помощью команды:

```
keytool --exportcert -rfc -keystore /opt/dozor/skvt/var/lib/authority.jks -alias "web proxy" > proxy.crt
```

Во время выполнения команды будет запрошен пароль (по умолчанию – `secret`). Файл сертификата появится в текущем каталоге (по умолчанию – `/opt/dozor`).

Полученный сертификат добавьте в список доверенных на АРМ, использующих TLS-порт (в случае выбора УЦ Solar webProxy).

2. В GUI Solar webProxy в разделе **Политика > Контентная фильтрация > Вскрытие HTTPS** создайте правило для вскрытия HTTPS-трафика. Нажмите **Сохранить** и **Применить политику**.

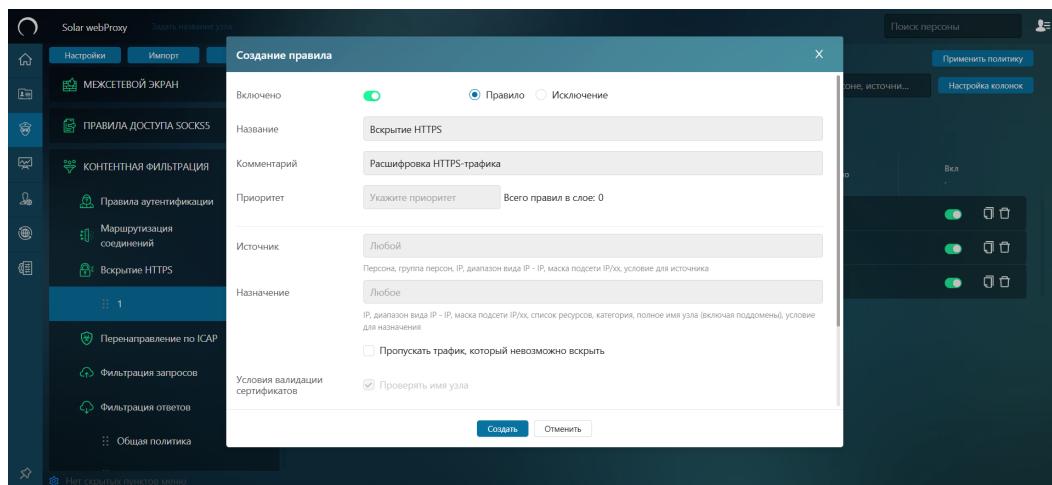


Рис. 5.42. Создание правила в слое политики «Вскрытие HTTPS»

Настройка прокси в браузере должна быть выполнена с помощью РАС-файла, поскольку через обычную конфигурацию такая настройка не поддерживается. В настройке прокси требуется использовать FQDN Solar webProxy. Задача создания РАС-файла ложится на системного администратора организации.

Работа TLS-порта поддерживается только для браузеров Mozilla Firefox и Google Chrome и для протокола HTTP.

Примечание

Во время вскрытия шифрованного трафика для десктопных приложений облачных хранилищ Яндекс Диск, OneDrive и Google Диск может быть запрещен доступ к интернету. Для решения этой проблемы необходимо предоставить приложениям доступ к сертификату Solar webProxy.

5.13. Контентное кэширование

Для кэширования данных, получаемых от внешних веб-серверов, служит сервис skvt-cache, который входит в роль **Фильтр HTTP-трафика**.

Примечание

На данный момент кэшируется только HTTP-трафик.

Сервис skvt-cache в Solar webProxy выполняет следующие функции:

- кэширование (временное локальное хранение) страниц сети Интернет, запрашиваемых по протоколу HTTP;
- выдача хранимых страниц из кэша по запросу пользователей рабочих станций;
- перенаправление запросов пользователей рабочих станций на ресурсы сети Интернет при отсутствии соответствующих страниц в кэше.

Solar webProxy кэширует:

- Сертификаты.

Примечание

Чтобы очистить кэш сертификатов, выполните команды:

```
# su dozor
# /opt/dozor/cassandra/bin/cqlsh -k wizor_ssl_cache --ssl `hostname -f
# truncate cn_keystore;
```

- Загрузку файлов без включенного антивируса.

Примечание

Если когда-то файл был загружен без включенного антивируса, он сохраняется в кэше и больше не проходит проверку антивирусом.

По умолчанию контентное кэширование выключено. Чтобы его включить:

1. В разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей > Вышестоящий прокси-сервер** выберите **Прокси-сервер**.
2. В поле **Адрес прокси-сервера** укажите значение **127.0.0.1**.
3. В поле **Порт прокси-сервера** укажите значение **2228**.
4. В разделе **Политика > Внешние подключения > Прокси-серверы** добавьте новый прокси-сервер (кнопка **Добавить прокси-сервер**) с параметрами:
 - **Имя сервера** – **HTTP-cache**;
 - **IP-адрес сервера** – **127.0.0.1**;
 - **Порт** – **2228**.

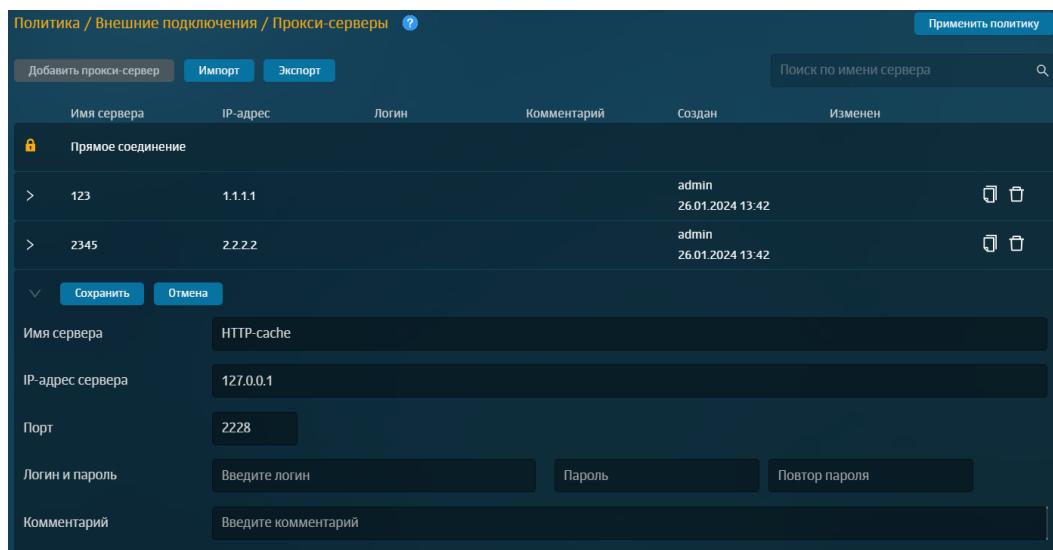


Рис. 5.43. Добавление прокси-сервера

5. В разделе **Политика > Контентная фильтрация > Маршрутизация соединений** создайте правило с действием **Отправить на прокси-сервер** и выберите **HTTP-cache**.

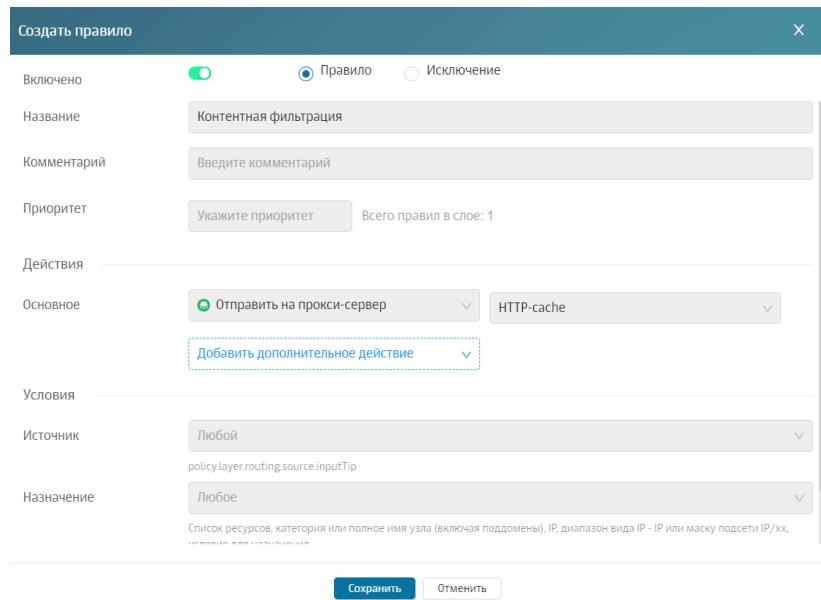


Рис. 5.44. Добавление правила контентной фильтрации в слое "Маршрутизация соединений"

Отключить контентное кэширование можно двумя способами:

- В разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей > Вышестоящий прокси-сервер** выберите **Не использовать прокси-сервер**.
- В CLI на slave-узлах выполните команды:

dsctl stop skvt-cache

dsctl disable skvt-cache

/opt/dozor/bin/check_skvt --no-shutdown

5.14. Настройка WCCP

Перед настройкой WCCP настройте прозрачный режим работы Solar webProxy (см. раздел [5.9.5](#)).

5.14.1. Настройка оборудования Cisco

Для настройки маршрутизатора Cisco:

1. Настройте сетевые интерфейсы маршрутизатора так, чтобы один интерфейс находился в локальной подсети организации, в которой размещен кластер Solar webProxy, а другой – в подсети провайдера сети Интернет.
2. Авторизуйтесь в CLI маршрутизатора и создайте обратную петлю, отвечающую за GRE-туннель, выполнив команды:

cisco> enable

```
cisco# configure terminal
```

```
cisco(config)# interface loopback 1
```

```
cisco(config)# ip address <loopback-IP> 255.255.255.255
```

где <loopback-IP> – IP-адрес обратной петли (выбирается сетевым администратором организации на его усмотрение).

3. Создайте список управления доступом со списком адресов WCCP-клиентов, выполнив команды:

```
cisco(config)# access-list 10 permit <WP-IP>
```

```
cisco(config)# ip wccp web-cache group-list 10
```

где <WP-IP> – IP-адрес узла фильтрации Solar webProxy.

4. Создайте список управления доступом с правилами маршрутизации трафика на Solar webProxy, выполнив команды:

```
cisco(config)# ip access-list extended WCCP_ACCESS
```

```
cisco(config-ext-nacl)# remark ACL for HTTP/HTTPS
```

```
cisco(config-ext-nacl)# remark WebProxy bypass WCCP
```

```
cisco(config-ext-nacl)# deny ip host <WP-IP> any
```

```
cisco(config-ext-nacl)# remark LAN clients proxy port 80/443
```

```
cisco(config-ext-nacl)# permit tcp <LAN-IP> <INV-LAN-MASK> any eq www 443
```

```
cisco(config-ext-nacl)# remark all others bypass WCCP
```

```
cisco(config-ext-nacl)# deny ip any any
```

где <WP-IP> – IP-адрес узла фильтрации Solar webProxy, <LAN-IP> – пространство IP-адресов локальной сети, в которой находятся АРМ сотрудников организации (например, **192.168.100.0**), <INV-LAN-MASK> – инверсная маска этой сети (в данном примере – **0.0.0.255**).

5. Установите правила перенаправления для WCCP, выполнив команды:

```
cisco(config)# ip wccp web-cache redirect-list WCCP_ACCESS
```

```
cisco(config)# ip wccp 70 redirect-list WCCP_ACCESS
```

6. Настройте перенаправление на внутреннем интерфейсе, выполнив команды:

```
cisco(config)# interface <ifname>
```

```
cisco(config-if)# ip wccp web-cache redirect in
```

```
cisco(config-if)# ip wccp 70 redirect in
```

где **<ifname>** – имя интерфейса маршрутизатора Cisco, находящегося в локальной сети.

7. Завершите конфигурирование маршрутизатора и сохраните конфигурацию, выполнив команды:

```
cisco(config)# end  
cisco# copy running-config startup-config
```

5.14.2. Настройка оборудования Solar webProxy

Для настройки Solar webProxy настройте GRE-туннель, выполнив в CLI команды:

```
iptunnel add wccp0 mode gre remote <CISCO-IP> local <WP-IP> dev eth0  
ip link set wccp0 up
```

где **<CISCO-IP>** – IP-адрес маршрутизатора Cisco, **<WP-IP>** – IP-адрес узла фильтрации Solar webProxy.

5.14.3. Проверка работоспособности WCCP

Для проверки работоспособности настроенной схемы авторизуйтесь в CLI маршрутизатора и выполните команду:

```
show ip wccp
```

На экране будет отображен вывод следующего вида:

```
Global WCCP information:  
Router information:  
  Router Identifier: 192.168.30.138  
  Protocol Version: 2.0  
  Service Identifier: web-cache  
    Number of Cache Engines: 1  
    Number of routers: 1  
    Total Packets Redirected: 0  
    Redirect access-list: WCCP_ACCESS  
    Total Packets Denied Redirect: 0  
    Total Packets Unassigned: 0  
    Group access-list: -none-  
    Total Messages Denied to Group: 0  
    Total Authentication failures: 0  
  Service Identifier: 70  
    Number of Cache Engines: 1  
    Number of routers: 1  
    Total Packets Redirected: 0  
    Redirect access-list: WCCP_ACCESS  
    Total Packets Denied Redirect: 0  
    Total Packets Unassigned: 0
```

Если схема настроена правильно, параметр **Number of Cache Engines** для обоих потоков WCCP будет отличен от нуля.

5.15. Настройка стороннего ICAP-прокси

В Solar webProxy предусмотрена возможность интеграции со сторонними прокси-серверами по протоколу ICAP.

Для настройки интеграции в настройках стороннего прокси-сервера в качестве ICAP-URL укажите значение вида `icap://<WP_IP>:2272/icaphandle`, где `<WP_IP>` – IP-адрес сервера фильтрации Solar webProxy.

Примечание

В предыдущих версиях Solar webProxy рекомендованное значение ICAP_URL было `icap://<WP_IP>:2272/KuroiNeko`. В данной версии оно также возможно.

Чтобы отключить интеграцию по протоколу ICAP:

1. Перейдите в раздел **Система > Расширенные настройки > Фильтрация и кэширование трафика**.
2. В блоке **Фильтрация и анализ трафика пользователей** откройте **ICAP > Интерфейс ICAP-сервера**.
3. В поле **IP-адрес** введите внешний IP.

Описание настроек политики фильтрации приведено в документе *Руководство администратора безопасности*, раздел *Управление политиками*.

5.16. Настройка баз категоризаторов

5.16.1. Используемые в системе категоризаторы

В Solar webProxy для фильтрации веб-трафика по умолчанию используются категоризатор **webCAT**, разработанный **Ростелеком-Солар**, и пользовательский категоризатор **customlist**. Администратор также может подключить и другие внешние категоризаторы в разделе расширенных настроек **Категоризатор веб-ресурсов и источник фидов**.

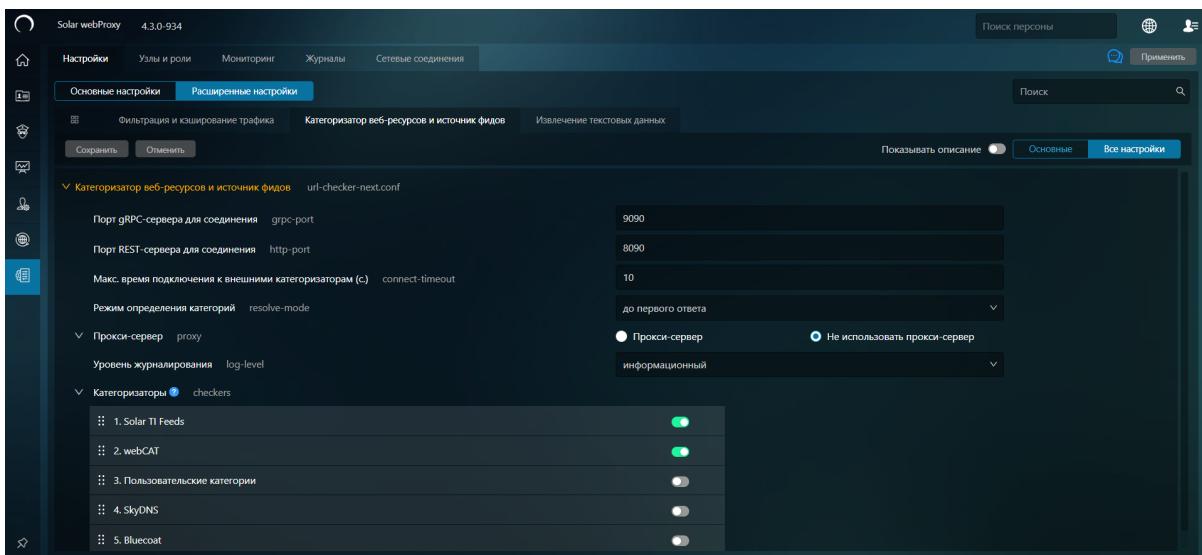


Рис. 5.45. Настройки категоризатора веб-ресурсов и источника фидов

В разделе **Система > Расширенные настройки > Категоризатор веб-ресурсов и источник фидов** можно указать значения параметров:

- **Порт gRPC-сервера для соединения** – значение параметра может быть от 1024 до 65535.
- **Порт REST-сервера для соединения** – значение параметра может быть от 1024 до 65535.
- **Макс. время подключения к внешними категоризаторам (с.)** – значение параметра может быть от 5 до 86400.
- **Режим определения категорий** – значение можно выбрать в раскрывающемся списке:
 - **До первого ответа** – категоризаторы опрашиваются в порядке выставленных приоритетов до первого срабатывания.
 - **Накопление ответов** – учитываются ответы от всех используемых баз категоризации.
- **Прокси-сервер** – выберите, использовать или нет вышестоящий прокси-сервер для сервиса категоризации. При использовании прокси-сервера можно задать значения:
 - **Адрес прокси-сервера**,
 - **Порт прокси-сервера**,
 - **Логин для Basic-аутентификации на прокси-сервере**,
 - **Пароль для Basic-аутентификации на прокси-сервере**.
- **Уровень журналирования** – выберите, начиная с какой критичности, будут показаны события в журнале событий: **отключено, критичный, ошибки, предупреждения, уведомления, информационный, отладочный**.

-
- **Категоризаторы** – включите/отключите необходимый категоризатор. Открыть настройки каждого категоризатора можно, нажав строку с ним.

Примечание

Опрос категоризаторов выполняется в порядке их приоритетов. Приоритет определяется расположением категоризаторов в списке. Чем меньше установленное значение – тем выше приоритет. Так, категоризатор со значением 1 будет опрошен раньше, чем категоризатор со значением 2. Чтобы изменить приоритет категоризатора, перетащите строку с ним с помощью значка .

Определение категории выполняется на основе URL веб-ресурса, к которому был выполнен запрос (раздел **Политика > База категоризации**).

Примечание

По умолчанию информация о ресурсах, у которых категорию нельзя определить, отправляется на внешний сервер для дальнейшего анализа с целью определения категории. Отправка информации о некатегоризованных ресурсах выполняется два раза в сутки в 01:00 и 13:00 (UTC +3). Чтобы отключить журналирование некатегоризованных ресурсов, перейдите в раздел **Система > Расширенные настройки > Интерфейс > Сервер веб-интерфейса** и снимите флажок **Включить отправку статистики по некатегоризованным ресурсам**.

В категоризаторе **webCAT** можно выполнять поиск ресурсов двумя способами:

- По полному URL ресурса. В данном случае ресурс будет найден строго по введенным данным. При несовпадении хотя бы одного символа ресурс не будет найден.
- По доменному имени. В данном случае поиск будет выполняться по совпадению доменного имени, и будут отображены все результаты с ним.

5.16.2. Настройка категоризатора **webCAT**

Для настройки категоризатора:

1. Проверьте наличие лицензии на этот модуль в окне с информацией о лицензии.
2. Назначьте узлу роль **Анализатор трафика** в разделе **Система > Узлы и роли**.
3. Нажмите кнопку **Применить**.

Примечание

Категоризатор **webCAT** входит в состав основных модулей **Solar webProxy**, однако автоматическое обновление его базы доступно только при наличии лицензии на модуль **Получение обновлений категоризатора webCAT**.

5.16.3. База Solar TI Feeds

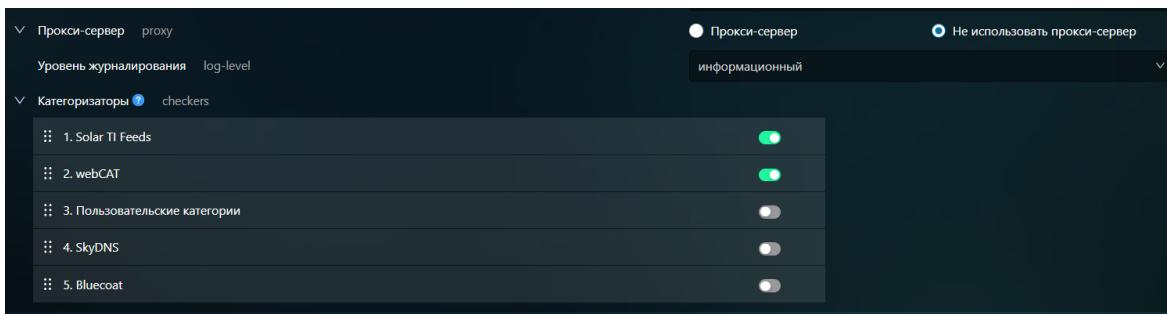
Примечание

База Solar TI Feeds не входит в состав основных модулей Solar webProxy. Для использования базы и ее автоматического обновления необходима лицензия на модуль **Получение обновлений фидов Solar TI Feeds**.

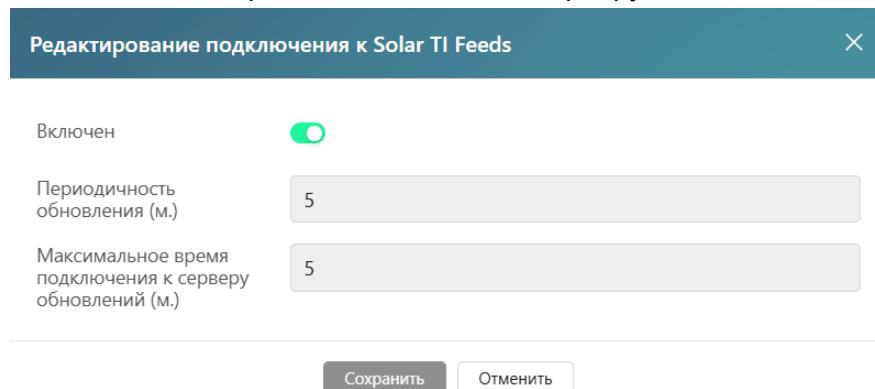
Solar TI Feeds — сервис поставки потоков данных (фидов) об актуальных угрозах для непрерывного усиления SOC, предотвращения атак и раннего реагирования. Их можно использовать для фильтрации и блокировки подозрительного трафика.

Для настройки базы Solar TI Feeds:

1. Убедитесь, что в разделе **Система > Расширенные настройки > Категоризатор веб-ресурсов и источник фидов > Категоризаторы** включен переключатель **Solar TI Feeds**.



2. Нажмите на строку **Solar TI Feeds** и в открывшемся окне укажите периодичность обновления и максимальное время подключения к серверу обновлений в минутах.



Примечание

Автоматическое обновление базы **Solar TI Feeds** доступно только при наличии лицензии на модуль **Получение обновлений категоризатора webCAT**.

3. Нажмите **Сохранить**.

5.16.4. База SkyDNS

SkyDNS – облачный сервис контент-фильтрации, в основе которого лежит технология доменных имен – протокол DNS (Domain Name System), который используется для сопоставления IP-адреса сайта и его доменного имени.

Возможны два варианта подключения к базе категоризации SkyDNS в интерактивном режиме через Categorization API:

- Использование API категоризации. Получение списка категорий осуществляется GET-запросом на URL одного из серверов авторизации с применением BASIC-авторизации. Для доступа могут использоваться адреса облачной инфраструктуры:
 - z.api.skydns.ru – для тестирования и анонимного доступа (количество запросов ограничено 10 запросами в минуту);
 - x.api.skydns.ru – для зарегистрированных пользователей (без ограничения числа запросов).

Примечание

Для запросов к x.api.skydns.ru необходимо использовать учетную запись, которая используется для Basic-аутентификации.

- Использование ежедневно обновляемой локальной базы данных в Docker контейнере (Y-API), которую предоставляет своим клиентам компания SkyDNS. Подробнее см. в разделе [5.16.4.1](#).

Ниже представлена схема подключения БД SkyDNS:

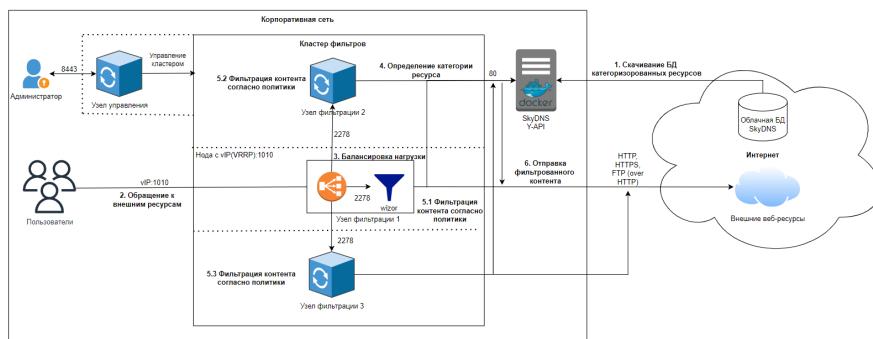


Рис. 5.46. Схема подключения БД SkyDNS

5.16.4.1. Установка контейнера Docker для доступа к локальной базе SkyDNS по Y-API

Примечание

Требуется установка контейнера Docker версии 20 и выше (работа на более ранних версиях не гарантирована).

Установка контейнера Docker должна быть на ОС Astra Linux Special Edition версии 1.7.5 и выше с уровнем защиты «Смоленск».

Архив с контейнером Docker можно запросить у представителей SkyDNS.

Чтобы установить контейнер Docker для доступа к базе SkyDNS по Y-API:

1. Отключите межсетевой экран с помощью команды:

```
# systemctl stop ufw && systemctl disable ufw
```

2. Скопируйте файлы контейнера на узел Docker любым способом.

3. Распакуйте файл с помощью команды:

```
# unzip skydns.zip
```

4. Установите дополнительные пакеты с помощью команды:

```
# sudo apt-get install -y curl bridge-utils
```

Примечание

Файл **y_api.tar.gz** будет разархивирован в папку **/root/SkyDNS/**.

5. Установите Docker с помощью команды:

```
# sudo apt install docker.io
```

6. Загрузите образ из архива с помощью команды:

```
# sudo docker load -i ./SkyDNS/y_api.tar.gz
```

7. Проверьте список контейнеров:

```
# docker container ls -a
```

8. Создайте отдельную подсеть Docker для данного контейнера:

```
# sudo docker network create --driver=bridge --subnet=193.33.33.0/24 y-api-net
```

9. Запустите контейнер в данной подсети:

```
# sudo docker run -it -d --net y-api-net --ip 193.33.33.33 -p 80:80/tcp -p 80:80/udp y-api:1
```

Примечание

После успешного выполнения команды запуска контейнера необходимо подождать неопределенное количество времени (зависит от скорости интернета).

Образ Docker не хранит в себе базы, он будет их скачивать через интернет каждый раз после запуска.

Сервис запускается на 80 порту, и он не запустится, пока не будут скачаны базы.

Порт, на котором запускается сервис, транслируется на узел Docker с помощью параметра **-p 80:80/tcp -p 80:80/udp**.

10. Выполните проверку работы SkyDNS:

```
# curl -v http://193.33.33.33/qwerty.com
```

Примечание

Если команда возвращает ошибку вида:

```
* Expire in 0 ms for 6 (transfer 0x14ff0f0)
*   Trying 193.33.33.33...
* TCP_NODELAY set
* Expire in 200 ms for 4 (transfer 0x14ff0f0)
* connect to 193.33.33.33 port 80 failed: В соединении отказано
* Failed to connect to 193.33.33.33 port 80: В соединении отказано
* Closing connection 0
curl: (7) Failed to connect to 193.33.33.33 port 80: В соединении отказано
```

Подождите окончания загрузки базы и выполните предыдущую команду несколько раз, пока вывод команды не станет вида:

```
* Expire in 0 ms for 6 (transfer 0x1e990f0)
*   Trying 193.33.33.33...
* TCP_NODELAY set
* Expire in 200 ms for 4 (transfer 0x1e990f0)
* Connected to 193.33.33.33 (193.33.33.33) port 80 (#0)
> GET /qwerty.com HTTP/1.1
> Host: 193.33.33.33
> User-Agent: curl/7.64.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Content-type: application/json
< Connection: keep-alive
* no chunk, no close, no size. Assume close to signal end
<
* Closing connection 0
{"category": [36, 49], "bad": false, "category_name": ["Образование и учебные учреждения", "Компьютеры и Интернет"]}
```

После получения ответа по категории сайта `qwerty.com` проверьте доступность контейнера из сети узла:

```
# curl http://10.201.69.124/qwerty.com
```

Ответ должен быть аналогичен предыдущему запросу с использованием IP-адреса контейнера SkyDNS (193.33.33.33).

11. Для упрощения дальнейшей настройки Solar Web Proxy добавьте в файл `/etc/hosts` узлов прокси сервера запись, указывающую на узел Docker:

```
# nano /etc/hosts
10.201.69.124 y.api.skydns.ru y
```

где 10.201.69.124 – адрес узла Docker с запущенным контейнером SkyDNS.

Примечание

Инкрементальное обновление локальной базы SkyDNS происходит каждые 2 часа.

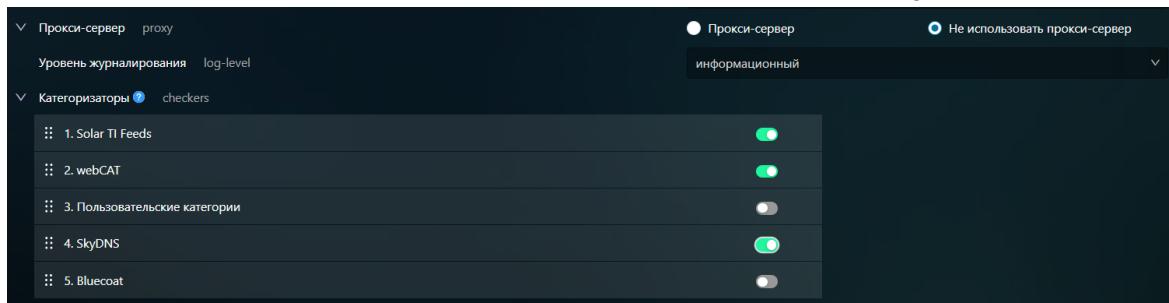
При повторном запуске контейнера база загружается заново.

Для работы Y-API требуется наличие открытого доступа в интернет (для обращения к сервисам авторизации, статистики, лицензирования, обновления). При отсутствии доступа к интернету работа сервиса прекратится частично или полностью.

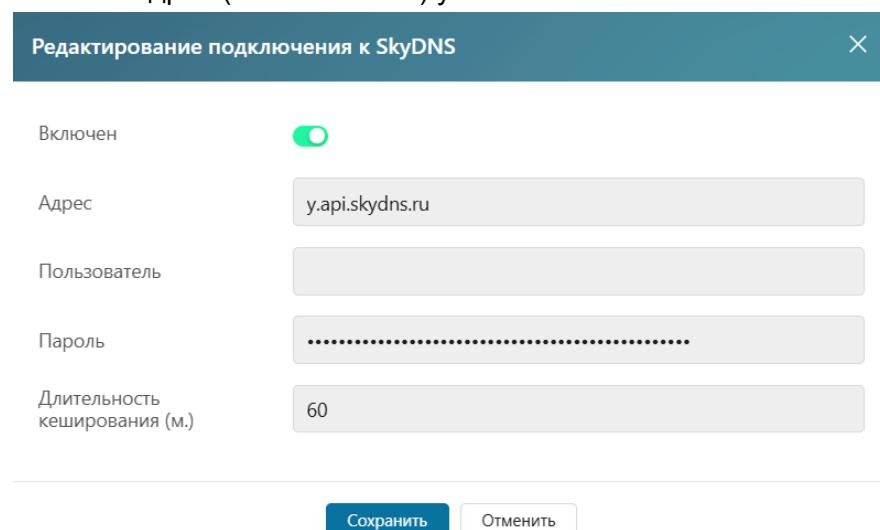
5.16.4.2. Проверка работы категоризатора

Для проверки работы категоризатора:

1. В разделе **Система > Расширенные настройки > Категоризатор веб-ресурсов и источник фидов > Категоризаторы** включите переключатель **SkyDNS**.



2. Нажмите на строку **SkyDNS** и в открывшемся окне в поле **Адрес** укажите полное доменное имя или IP-адрес (10.201.69.124) узла Docker.



Примечание

Заполнение полей **Пользователь** и **Пароль** не требуется.

3. Проверьте работу локальной БД SkyDNS в разделе **Политика > Управление категориями**, используя префиксы (`http://` или `https://`) с указанием полного доменного имени (FQDN) категоризируемого ресурса.

Далее при обработке правил/исключений во всех слоях разделов **Политика > Контентная фильтрация** и **Политика > Правила доступа SOCKS5** при наличии подкатегории/категории в атрибуте **Назначение** будет определяться категория ресурса согласно локальной базе SkyDNS.

Примечание

При использовании локальной базы SkyDNS нет возможности проверить категорию ресурса в GUI в разделе **Политика > Проверка по политике**, т.к. в GUI есть ограничение на использование префиксов.

5.16.5. База Blue Coat

Blue Coat – система категоризации веб-контента, используемая для фильтрации веб-трафика в корпоративных и образовательных сетях, а также провайдерами интернет-услуг.

Для настройки категоризатора Blue Coat:

1. В разделе **Система > Расширенные настройки > Категоризатор веб-ресурсов и источник фидов > Категоризаторы** включите переключатель **Bluecoat**.

2. Нажмите на строку **Bluecoat** и в открывшемся окне укажите адрес и порт.

Редактирование подключения к BlueCoat

X

Включен



Адрес

1.1.1.1

Порт

8080

Сохранить

Отменить

3. Нажмите **Сохранить**.

6. Антивирус

6.1. Настройка антивируса

Примечание

Для повышения производительности антивируса Dr.Web отключите его аудит.

```
# auditctl -A never,exit -S all -F exe=/opt/drweb.com/bin/drweb-se.real
```

Если система установлена с помощью ISO-образа, антивирус настроен по умолчанию. В других случаях необходима его настройка. Для этого:

1. В разделе **Система > Основные настройки > Работа системы > Антивирус** или **Политика > Настройки > Антивирус** выберите антивирус, который хотите использовать (**Антивирус Касперского** или **Антивирус Dr.Web**).
2. В поле **Лицензия** выберите **Ключевой файл** или **Серийный номер лицензии**:
 - **Ключевой файл** – введите содержимое лицензионного ключевого файла, полученного от вендора;
 - **Серийный номер лицензии** – введите серийный номер лицензии, полученный от вендора.
3. Укажите необходимые настройки антивируса.

При выборе антивируса Kaspersky можно задать параметры:

- **Количество процессов для сканирования** – значение от 1 до 256, по умолчанию – 4.
- **Количество потоков для сканирования** – значение от 1 до 256, по умолчанию – 8. Число потоков должно быть в два раза больше чем число процессов.
- **Длина очереди задач на сканирования** – значение от 128 до 16448, по умолчанию – 1024.
- **Таймаут для сканирования (с.)** – значение от 1 до 2147483647, по умолчанию – 30.
- **Размер диска для распаковки файлов (Кб)** – значение от 0 до 2147483647, по умолчанию – 10000000.

Примечание

Если значение этого параметра установлено 0, защита от ZIP-бомб отключена. Укажите максимальный объем дискового пространства (в килобайтах), который может быть выделен для распаковки архивов. Ограничение дискового пространства помогает защитить сервер от ZIP-бомб.

-
- **Режим сканирования** – раскрывающийся список с параметрами:
 - Сканирование сжатых исполняемых файлов;
 - Сканирование архивных файлов;
 - Сканирование файлов, содержащих БД электронной почты;
 - Уровень эвристического анализа – доступные значения: **Выключить**, **Поверхностный**, **Средний** и **Глубокий**;
 - Уведомить пользователя о макросах в Microsoft Office.
 - **Максимальная глубина сканирования архивов** – максимальная глубина вложенных архивов, которые необходимо распаковать во время сканирования. Значение от 0 до 2147483647, по умолчанию – 5.
 - **Частота обновлений в минутах** – значение от 0 до 44640, по умолчанию – 30. Если значение этого параметра является 0, то KAV SDK не выполняет автоматическое обновление.
 - **Ограничение на использование оперативной памяти (Мб)** – значение от 700 до 2147483647, по умолчанию – 700. Укажите максимальный объем оперативной памяти в Мб, который может быть выделен KAV SDK.

Примечание

Если сеть высоконагружена, при проверке большого количества соединений с антивирусом Kaspersky в журналах сервиса *wizor* может возникать ошибка вида:

AntiVirus service [ICAP:icap://localhost:1344/respmod] returned unexpected code: 503.

В этом случае рекомендуется выбрать оптимальное значение параметра **max-sessions-count**, который отвечает за максимальное число одновременных подключений к антивирусу Kaspersky. По умолчанию значение параметра 400. Значение необходимо увеличивать на 10%, пока ошибка не решится. Для этого в CLI выполните команду:

```
# set-config global /antivirus/antivirus.json/antivirus-config-params/kav/max-sessions-count <value>
```

где **<value>** – значение параметра (необходимо увеличивать на 10% при каждом новом выполнении команды, пока ошибка не решится).

При выборе антивируса Dr.Web можно задать параметры:

- **Интерфейс ICAP-сервера** – IP-адрес ICAP-сервера.
 - **Порт ICAP-сервера** – значение от 1 до 65535, по умолчанию – 1344.
 - **Уровень журналирования ICAP-сервера** – доступные значения: **DEBUG**, **INFO**, **NOTICE**, **WARNING** и **ERROR**.
4. Выберите, использовать или нет вышестоящий прокси-сервер для сервиса обновлений. При использовании прокси-сервера можно задать значения:

-
- Адрес прокси-сервера,
 - Порт прокси-сервера,
 - Логин для Basic-аутентификации на прокси-сервере,
 - Пароль для Basic-аутентификации на прокси-сервере.
5. Последовательно нажмите **Сохранить** и **Применить**.
 6. В разделе **Система > Узлы и роли** назначьте одному из узлов роль **Антивирус**.
 7. Сформируйте правило политики для перенаправления трафика на проверку антивирусом (см. далее).

Примечание

*Настройки по умолчанию позволяют проверять файлы с максимальным размером 1 Гб (для антивируса Kaspersky) и 4 Гб (для антивируса Dr.Web). Если необходима проверка файлов размером больше 4 Гб, воспользуйтесь антивирусом Kaspersky. Для этого в параметре **Ограничение на использование оперативной памяти (Мб)** укажите значение в два раза больше необходимого. Например, если необходима проверка файла размером 5 Гб, в параметре **Ограничение на использование оперативной памяти (Мб)** укажите значение 10 Гб.*

*Максимальный размер файла для проверки так же зависит от времени проверки. Если время проверки будет превышать таймаут (параметр **Таймаут для сканирования (с.)**), файл может быть пропущен или заблокирован (в зависимости от настроек). Поэтому при указании значение **Таймаут для сканирования (с.)** необходимо учитывать вес проверяемого файла.*

6.2. Формирование политики для работы антивируса

Для окончания настройки антивируса сформируйте политику ИБ. Для этого в разделе **Политика** в слое **Перенаправление по ICAP** создайте правило на обработку трафика антивирусом, как на рисунке далее. Примените политику.

Редактировать правило **icap resp** ×

Включено Правило Исключение

Название

Комментарий

Действие

Имя сервера

Шаблон блокировки

Уведомлять

Источник
Персона, Группа персон, IP-диапазон, IP диапазон вида IP - IP или маска подсети IP/xx

Назначение
Список ресурсов, категория, полное имя хоста (включая поддомены), IP или диапазон вида IP - IP

Расширенные настройки Показать

Рис. 6.1. Правило для перенаправления трафика антивирусу

7. Отказоустойчивость и балансировка трафика

7.1. Общие сведения

Кластер Solar webProxy 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 webProxy 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 обеспечения отказоустойчивости в Solar webProxy используется технология Virtual Router Redundancy Protocol (VRRP) или виртуальный IP-адрес (Virtual IP — VIP).

Использование VRRP позволяет объединить несколько маршрутизаторов в один виртуальный с общим IP-адресом. Другими словами, технология виртуального IP-адреса — это группа интерфейсов маршрутизаторов, которые находятся в одной сети и разделяют виртуальный идентификатор (Virtual Router Identifier — VRID) и один виртуальный IP-адрес.

7.2. Настройка балансировки подключений пользователей

Основным инструментом балансировки трафика в составе Solar webProxy является балансировщик HAProxy.

Схема подключения балансировщика приведена на [Рис.7.1](#).

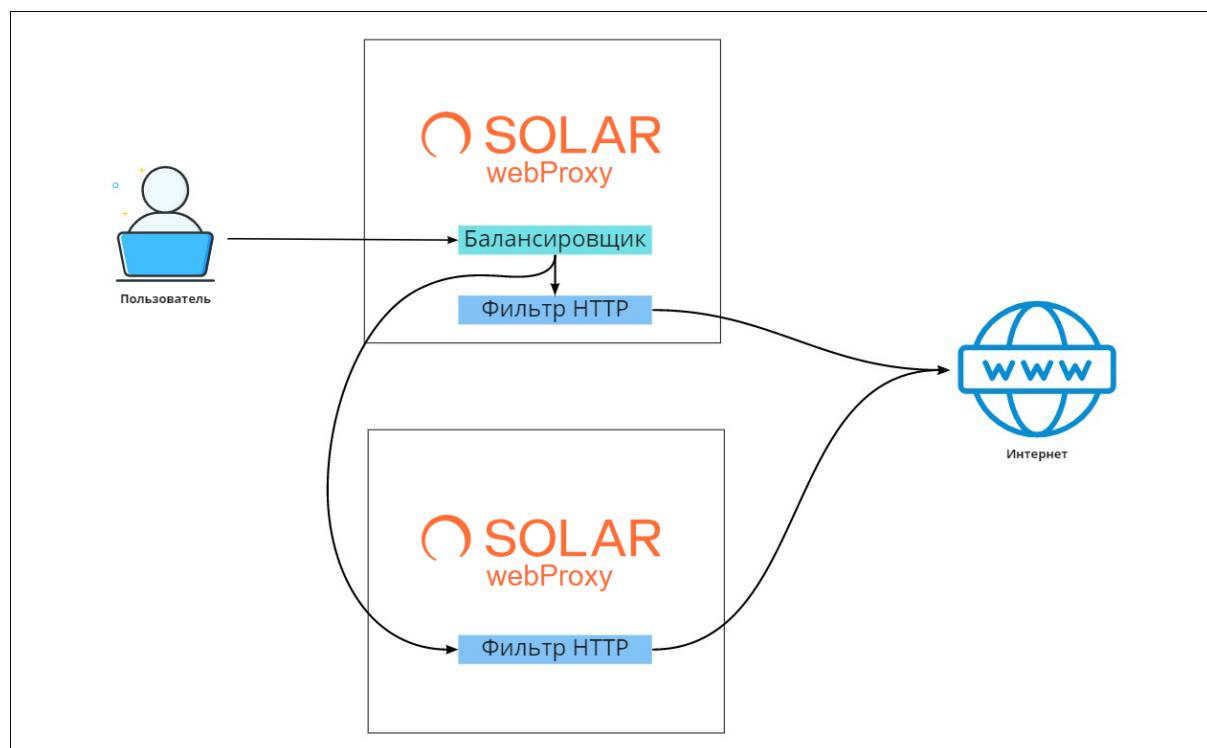


Рис. 7.1. Схема балансировки трафика Solar webProxy

Для настройки балансировщика HAProxy на узле:

1. В разделе **Система > Узлы и роли** назначьте одному из узлов роль **Балансировщик**.
2. В разделе **Отказоустойчивость > Сервис балансировки трафика > HTTP-FILTER** основных настроек конфигурации задайте параметры:
 - **Название конфигурации балансировки.**
 - **Порт для внешних соединений** – значение параметра может быть от 1 до 65535. Значение по умолчанию – 1010.
 - **Время ожидания запроса от клиента (с)** – значение параметра может быть от 0 до 2147483647. Значение по умолчанию – 10.
 - **Время ожидания ответа от сервера (с)** – значение параметра может быть от 0 до 2147483647. Значение по умолчанию – 10.
 - **Максимальное количество соединений** – значение параметра может быть от 0 до 2147483647. Значение по умолчанию – 1000.
 - **Метод балансировки** – доступны значения:
 - **roundrobin** — алгоритм кругового обслуживания. Передача запросов происходит по кругу: запросы по порядку передаются от одного узла к другому. После передачи запроса последнему узлу цикл начинается заново.
 - **leastconn** — алгоритм учитывает количество подключений, поддерживаемых узлами на текущий момент времени. Каждый следующий запрос передается серверу с наименьшим количеством активных подключений.

Примечание

Рекомендуется, если в сети находятся 4 и более узла с высокой сетевой нагрузкой.

- **source** — сервер, обрабатывающий запрос, выбирается из статической таблицы по IP-адресу отправителя.

Примечание

Рекомендуется для балансировки прикладного протокола FTP.

Рис. 7.2. Настройка балансировщика HAProxy

3. Нажмите **Сохранить** и **Применить**.

4. В настройках браузеров АРМ пользователей Solar webProxy в качестве прокси-сервера укажите адрес и порт балансировщика.

Для более гибкой настройки для параметра **Узлы для балансировки** выберите значение **Указать вручную**, напротив строки **Узлы** нажмите кнопку **Добавить** и укажите один или несколько резервных серверов (см. [Рис.7.3](#)). Запросы с АРМ пользователей будут перенаправлены на эти серверы при недоступности узлов фильтрации Solar webProxy.

Рис. 7.3. Гибкая настройка балансировки

Примечание

При использовании балансировки NTLM из-за специфики работы протокола необходимо выбирать в параметре **Тип балансировки** значение **tcp**.

С описанием параметров настройки можно ознакомиться по адресу: <http://cbonte.github.io/haproxy-dconv/2.5/configuration.html#5.2-weight>

Также можно настроить отправку информации о пользователе (включить отправку информации об источнике по Proxy-протоколу). Для этого в разделе **Отказоустойчивость** > **Сервис балансировки трафика** основных настроек конфигурации установите флагок **Добавлять информацию об источнике (proxy-protocol)** (см. рисунок выше).

7.3. Настройка балансировки антивируса

Чтобы поддерживать бесперебойную работу антивируса в многонодовой конфигурации в случае отключения одного из узлов, настройте балансировку трафика между ними.

Если кластер состоит из 2-3 узлов, каждому из которых назначены роли **Антивирус** и **Фильтр HTTP-трафика**, для балансировки трафика при использовании антивируса:

1. Назначьте каждому узлу роль **Балансировщик**.
2. В разделе **Политика > Внешние подключения > ICAP-серверы** создайте ICAP-сервер (см. [Рис.7.5](#)).
3. Сформируйте правило политики с этим ICAP-сервером (см. [6.2](#)).

Для настройки балансировки трафика антивируса в разделе **Политика**:

1. Проверьте, что каждому узлу кластера назначены роли **Антивирус**, **Фильтр HTTP-трафика** и **Балансировщик** (раздел **Система > Узлы и роли**).
2. Проверьте настройки антивируса, указанные в разделе **Система > Отказоустойчивость > Сервис балансировки трафика > Antivirus** (см. [Рис.7.4](#)).

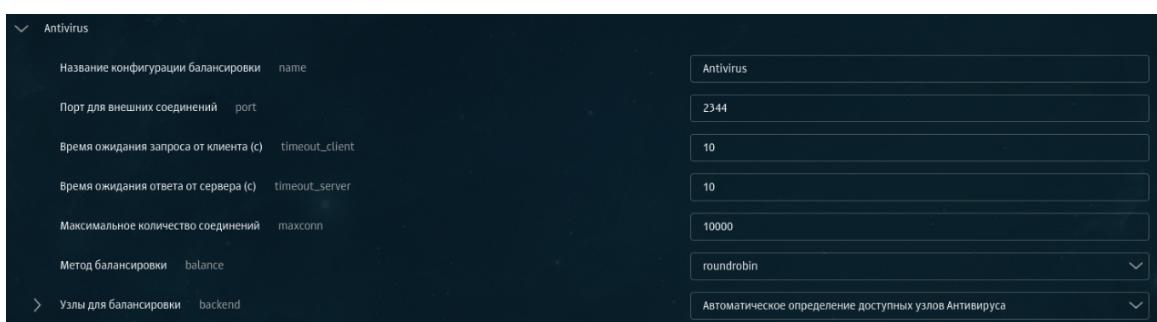


Рис. 7.4. Параметры настройки антивируса

3. В разделе **Политика > Внешние подключения** создайте новый ICAP-сервер, указав порт согласно настройкам конфигурации (см. [Рис.7.5](#)).

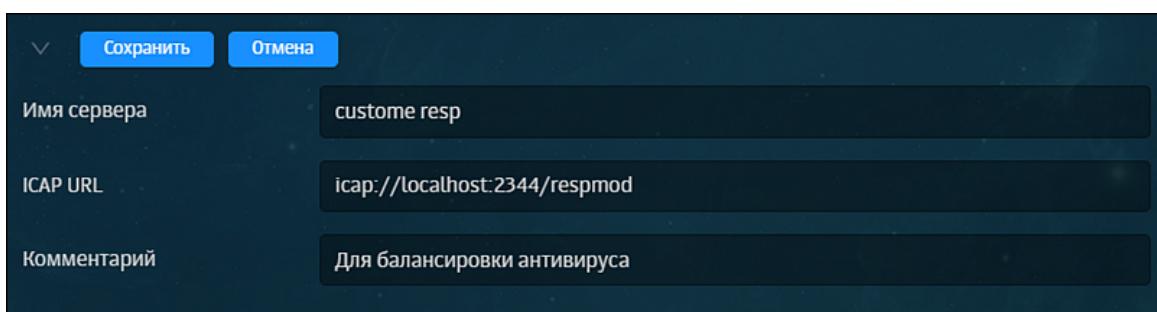


Рис. 7.5. Настройки ICAP-сервера для балансировки антивируса

4. Сформируйте правило политики с этим ICAP-сервером (см. документ *Руководство администратора безопасности*).

Примечание

Для корректной загрузки файлов при настроенных балансировщике и антивирусе рекомендуется увеличить значения в параметрах **Время ожидания запроса от клиента (с)** и **Время ожидания ответа от сервера (с)** до 300 секунд.

Проверка работоспособности антивируса описана в разделе [15](#).

7.4. Настройка балансировки соединений по протоколу SOCKS5

В Solar webProxy есть возможность балансировать трафик между фильтрующими узлами по протоколу SOCKS5.

Для этого:

1. В разделе **Система > Узлы и роли** назначьте узлам роль **Фильтр SOCKS5-трафика**.
2. В разделе **Отказоустойчивость > Сервис балансировки трафика > SOCKS5-FILTER** основных настроек конфигурации задайте параметры:
 - **Название конфигурации балансировки**.
 - **Порт для внешних соединений** – значение параметра может быть от 1 до 65535. Значение по умолчанию – 1082.
 - **Время ожидания запроса от клиента (с)** – значение параметра может быть от 0 до 2147483647. Значение по умолчанию – 10.
 - **Время ожидания ответа от сервера (с)** – значение параметра может быть от 0 до 2147483647. Значение по умолчанию – 10.
 - **Максимальное количество соединений** – значение параметра может быть от 0 до 2147483647. Значение по умолчанию – 10000.
 - **Метод балансировки** – доступны значения:
 - **roundrobin** — алгоритм кругового обслуживания. Передача запросов происходит по кругу: запросы по порядку передаются от одного узла к другому. После передачи запроса последнему узлу цикл начинается заново.
 - **leastconn** — алгоритм учитывает количество подключений, поддерживаемых узлами на текущий момент времени. Каждый следующий запрос передается серверу с наименьшим количеством активных подключений.

Примечание

Рекомендуется, если в сети находятся 4 и более узла с высокой сетевой нагрузкой.

- **source** — сервер, обрабатывающий запрос, выбирается из статической таблицы по IP-адресу отправителя.

Примечание

Рекомендуется для балансировки прикладного протокола *FTP*.

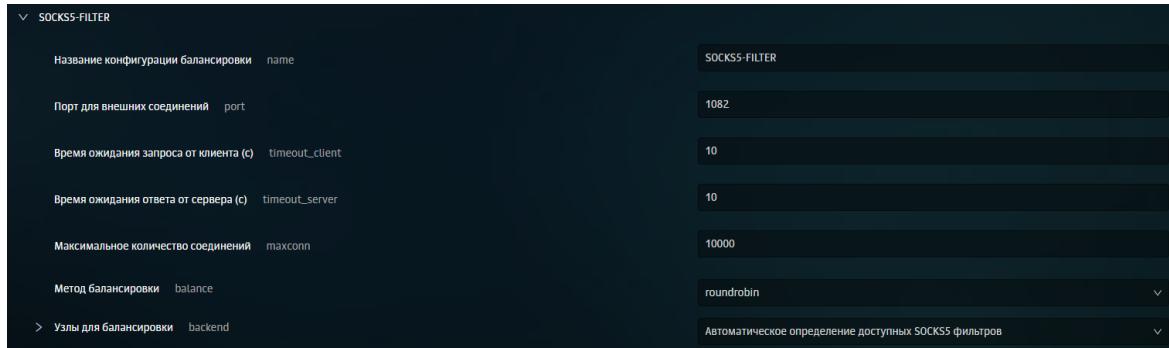


Рис. 7.6. Настройка балансировки трафика по протоколу **SOCKS5**

3. Нажмите **Сохранить** и **Применить**.

4. В настройках браузеров АРМ пользователей Solar webProxy в качестве прокси-сервера укажите адрес и порт балансировщика.

Для более гибкой настройки:

1. Для параметра **Узлы для балансировки** выберите значение **Указать вручную**.
2. Выберите тип балансировки **tcp**.
3. Напротив строки **Узлы** нажмите кнопку **Добавить**.
4. Укажите один или несколько резервных серверов.

Примечание

С описанием параметров настройки можно ознакомиться по адресу:
<http://cbonte.github.io/haproxy-dconv/2.5/configuration.html#5.2-weight>

Запросы с АРМ пользователей будут перенаправлены на эти серверы при недоступности узлов фильтрации Solar webProxy.

Также можно настроить отправку информации о пользователе (включить отправку информации об источнике по Proxy-протоколу). Для этого в разделе **Отказоустойчивость > Сервис балансировки трафика** основных настроек конфигурации установите флажок **Добавлять информацию об источнике (proxy-protocol)** (см. рисунок выше).

7.5. Настройка отказоустойчивости (VRRP)

Использование Сервиса виртуального IP-адреса обеспечивает отказоустойчивость предоставления сервиса пользователям путем переключения VIP с одного узла на другой.

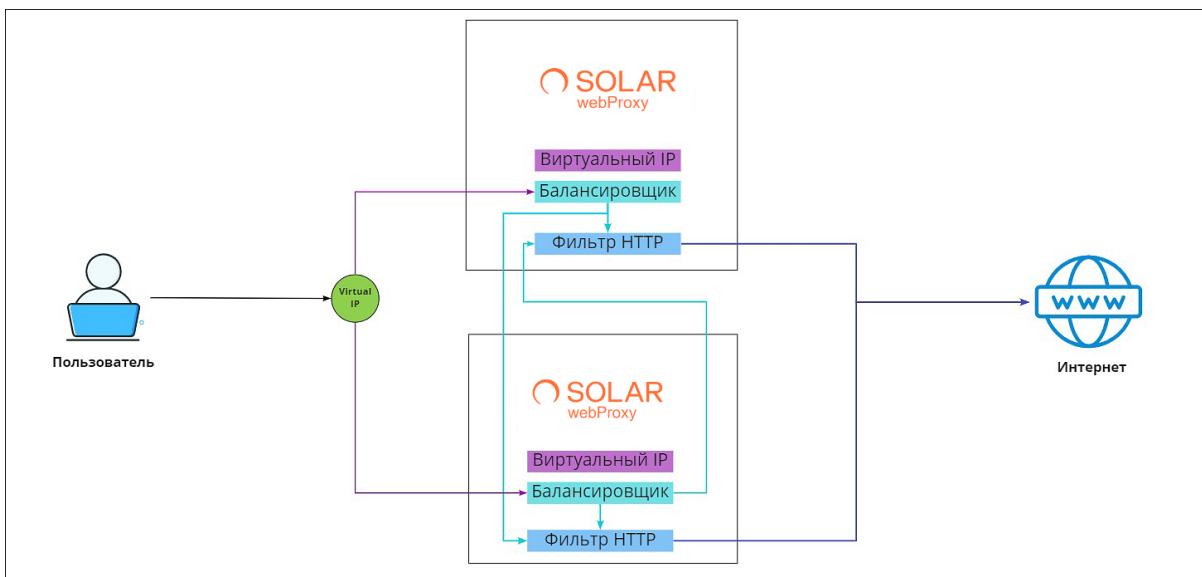


Рис. 7.7. Схема работы Solar webProxy при использовании VRRP

Для настройки отказоустойчивости системы (VRRP):

1. В разделе **Система > Узлы и роли** master-узлу назначьте роль **Виртуальный IP-адрес (VRRP)** и проверьте, что узлу назначена роль **Балансировщик**.
2. Настройте балансировщик трафика HAProxy (см. раздел [7.2](#)).
3. В разделе **Отказоустойчивость > Сервис виртуального ip (VRRP)** основных настроек конфигурации укажите сетевой интерфейс, на котором будет работать VRRP, и проверьте корректность указанных параметров настройки сервиса (см. [Рис.7.8](#)).

Примечание

Сетевой интерфейс или IP-адрес следует указывать в соответствии с инфраструктурой организации. Сетевой интерфейс можно просмотреть в разделе **Система > Узлы и роли**.

4. Нажмите **Сохранить** и **Применить**.

Примечание

Для корректного назначения виртуального IP-адреса на сетевой интерфейс в основных настройках конфигурации в разделе **Отказоустойчивость > Сервис виртуального ip (VRRP)** для параметра **Уникальный идентификатор VRRP экземпляра**, должен совпадать на **всех серверах** поменяйте значение на **уникальное в сети**.

Если в поле **Приоритет переключения** не менять значение по умолчанию, для всех узлов будет выбрано произвольное значение.

Сервис виртуального IP (VRRP) keepalive.json

Название группы VRRP	group	CL-1
Начальное состояние при запуске	state	BACKUP
Приоритет переключения	priority	100
<input checked="" type="checkbox"/> Не отслеживать восстановление приоритетного узла no-preempt		
Экземпляр VRRP instance		
VRRP-01		
Название экземпляра VRRP	name	VRRP-01
Интерфейс, на котором будет работать VRRP	interface	eth1
Уникальный идентификатор VRRP экземпляра	router_id	100
Виртуальный IP адрес	vip	172.20.20.1
<input type="checkbox"/> Отслеживать работу сервиса балансировки haproxy_detect		

Рис. 7.8. Настройка отказоустойчивости

Примечание

Для более подробной настройки перейдите в соответствующий раздел расширенных настроек, нажав ссылку в правом верхнем углу секции.

Для настройки VRRP на двух и более узлах используйте локальные настройки этих узлов. Сначала внесите изменения локальных настроек одного узла, дождитесь их применения, и только потом приступайте к изменению локальных настроек второго узла.

7.6. Отказоустойчивость сервиса балансировки

Для повышения уровня отказоустойчивости конфигурации с двумя или более узлами можно переносить виртуальный IP-адрес (VIP) с одного узла на другой, в случае недоступности сервиса балансировки HAProxy на одном из узлов.

Для этого в разделе **Отказоустойчивость > Сервис виртуального IP (VRRP)** основных настроек конфигурации установите флажок **Отслеживать работу сервиса балансировки (haproxy_detect)**.

Сервис виртуального IP (VRRP) keepalive.json

Название группы VRRP	group	CL-1
Начальное состояние при запуске	state	BACKUP
Приоритет переключения	priority	100
<input checked="" type="checkbox"/> Не отслеживать восстановление приоритетного узла no-preempt		
Экземпляр VRRP instance		
VRRP-01		
Название экземпляра VRRP	name	VRRP-01
Интерфейс, на котором будет работать VRRP	interface	eth1
Уникальный идентификатор VRRP экземпляра	router_id	100
Виртуальный IP адрес	vip	172.20.20.1
<input checked="" type="checkbox"/> Отслеживать работу сервиса балансировки haproxy_detect		

Рис. 7.9. Настройка отказоустойчивости

Если флагок установлен, сервис проверяет, назначена ли роль **Балансировщик** данному узлу (например, *slave*-узел). В случае отсутствия роли или отсутствия возможности запустить сервис, VIP «переходит» на другой узел (например, *master*-узел), которому назначена роль **Балансировщик**.

7.7. Настройка уведомлений от сервера мониторинга

Для удобства вы можете подключить получение уведомлений от сервера мониторинга по электронной почте.

Для этого в разделе **Система > Настройки мониторинга > Сервер мониторинга > Оповещения** расширенных настроек конфигурации установите флагок **Отправлять уведомления по электронной почте** и задайте значения параметров:

- **Адрес/порт SMTP-сервера > Сетевой адрес** – IP-адрес сервиса, который отвечает за отправку электронных писем.
- **Адрес/порт SMTP-сервера > Порт** – порт, по которому будет выполняться отправка электронных писем.
- **Отправитель** – адрес, с которого будут отправлены сообщения. Чтобы найти сообщения от сервера мониторинга, отсортируйте сообщения по этому адресу.
- **Адреса для отправки уведомлений о проблемах чрезвычайной критичности** – электронный адрес, на который будут поступать сообщения о проблемах чрезвычайной критичности.
- **Адреса для отправки уведомлений о проблемах высокой и средней критичности** – электронный адрес, на который будут поступать сообщения о проблемах высокой и средней критичности.
- **Адреса для отправки уведомлений о проблемах низкой критичности** – электронный адрес, на который будут поступать сообщения о проблемах низкой критичности.

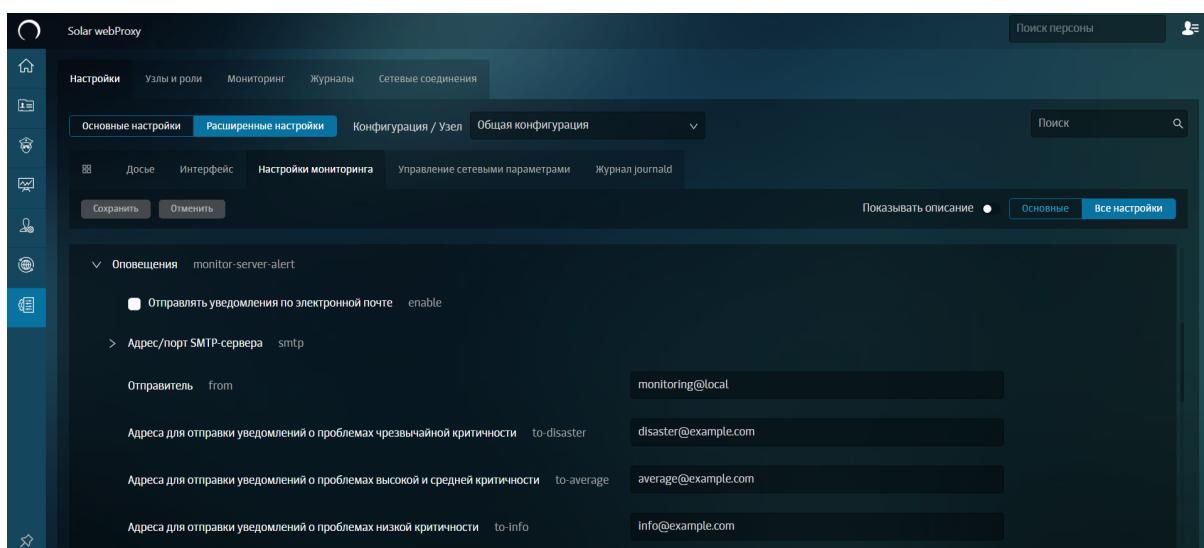


Рис. 7.10. Настройка отправки уведомлений от сервера мониторинга

8. Обратный прокси

8.1. Основные настройки

Solar webProxy обеспечивает контроль и управление трафиком пользователей не только в прямом, но и в обратном режиме (Reverse proxy).

Примечание

Режим обратного прокси поддерживает только HTTPS-соединения.

Работа в обратном режиме позволяет публиковать внутренние ресурсы организации на внешние источники. Например, с помощью обратного прокси организация может предоставить доступ к корпоративной почте своим сотрудникам, находящимся за пределами организации. При этом Solar webProxy проверяет и блокирует файлы с конфиденциальной информацией при их выгрузке. Можно опубликовать как один, так и несколько ресурсов. Количество ресурсов не ограничено.

Примечание

*Перед настройкой обратного прокси проверьте наличие лицензии на этот модуль. Если лицензия отсутствует, загрузите ее в окне с информацией о лицензии с помощью кнопки **Загрузить лицензию**.*

Для настройки Solar webProxy в обратном режиме:

1. В разделе **Система > Узлы и роли** назначьте выбранному узлу роль **Обратный прокси**.
2. В разделе **Работа системы > Обратный прокси-сервер (reverse-proxy.json)** основных настроек конфигурации в секции **Настройки источника** выберите доступность по внешнему протоколу безопасности:
 - **HTTP** – при доступе извне на опубликованный внешний адрес, перенаправляемый к внутреннему ресурсу, обращение будет только по незащищенному HTTP-протоколу с использованием порта для незащищенного соединения.
 - **HTTPS** – при доступе извне на опубликованный внешний адрес, перенаправляемый к внутреннему ресурсу, обращение будет только по защищенному HTTPS-протоколу с использованием порта для защищенного соединения.
 - **HTTP_AND_HTTPS** – при доступе извне на опубликованный внешний адрес, перенаправляемый к внутреннему ресурсу, допускается обращение как по протоколу HTTP, так и HTTPS.
3. Укажите параметры настройки в разделе **Работа системы > Обратный прокси-сервер (reverse-proxy.json)** основных настроек конфигурации в секции **Настройки источника > Внутренний адрес сервиса**:

- **Сетевой адрес (host)** – сетевой адрес внутреннего ресурса, к которому необходимо предоставить доступ. Необходимо указать IP-адрес или доменное имя внутреннего ресурса.
- **Порт (port)** – порт публикуемого ресурса. Значение по умолчанию: 443.
- **Сертификат (certificate)** – сертификат для работы обратного прокси.

Примечание

Можно использовать как собственный сертификат, так и сертификат, поставляемый с продуктом.

Также можно сгенерировать сертификат вручную и импортировать его с помощью кнопки **Загрузить** (см. [8.2](#)).

При использовании своего сертификата, подписанного центром сертификации (СА), необходимо добавить его в список доверенных корневых центров сертификации. Иначе, при переходе на ресурс, в браузере отобразится уведомление об ошибке сертификата.

- **Порт для защищенного соединения (reverse-proxy-port)** – порт обратного прокси при указании порта HTTPS в разделе **Обратный прокси-сервер > Настройки источника > Доступность по внешнему протоколу безопасности**. Значение по умолчанию: 8444.
- **Порт для незащищенного соединения (reverse-proxy-http-port)** – порт обратного прокси при указании порта HTTP в разделе **Обратный прокси-сервер > Настройки источника > Доступность по внешнему протоколу безопасности**. Значение по умолчанию: 8445.

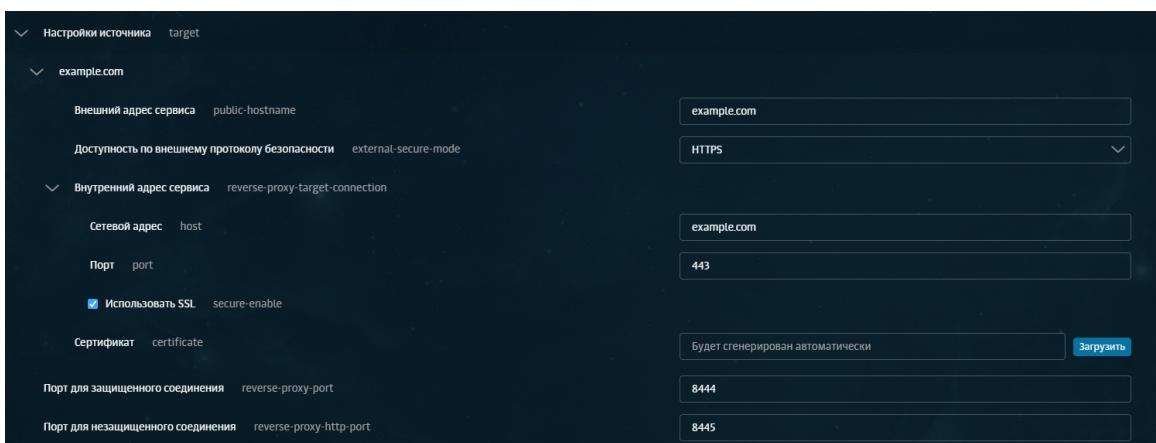


Рис. 8.1. Параметры настройки обратного прокси

4. Установите флагок **Использовать SSL**, чтобы обращение к внутреннему ресурсу было по защищенному соединению (протоколу HTTPS). При снятом флагке обращение к внутреннему ресурсу будет по незащищенному соединению (протоколу HTTP).

Примечание

При настройке доступа через обратный прокси по протоколу HTTPS для построения правильной цепочки необходимо добавить сертификат публикуемого ресурса в разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей > Доверенные сертификаты**.

5. Для сохранения и применения настроек последовательно нажмите кнопки **Сохранить** и **Применить**.
6. Настройте аутентификацию.

Примечание

Режим обратного прокси поддерживает только Basic и NTLM аутентификацию.

7. Для минимальной работы с консолью, если обратный прокси запускается на master-узле, установите флажок **Перенаправление с 443 порта на 8443 порт** в разделе **Система > Расширенные настройки > Интерфейс**.
8. В разделе **Политика** сформируйте политику контентной фильтрации.

Примечание

Политика фильтрации для прямого и обратного режима работы системы является общей. Однако в обратном режиме по умолчанию настроено вскрытие HTTPS-трафика.

*При формировании политики для обратного прокси в разделе **Система > Работа системы > Обратный прокси-сервер** основных настроек конфигурации в секции **Настройки источника** необходимо указывать внешний адрес сервиса (public-hostname).*

9. Для проверки работы обратного прокси с ролью обратного прокси в браузере перейдите на адрес публикуемого ресурса, например, на корпоративную почту **webmail.rt-solar.ru**.

Добавить новый публикуемый ресурс можно одним из способов:

- нажав кнопку **Добавить**;
- скопировав уже существующий ресурс и изменив параметры настройки.

Примечание

Обычно на одном IP-адресе размещается один ресурс. Но бывают ситуации, когда несколько ресурсов размещены на одном IP-адресе. Оба случая работоспособны.

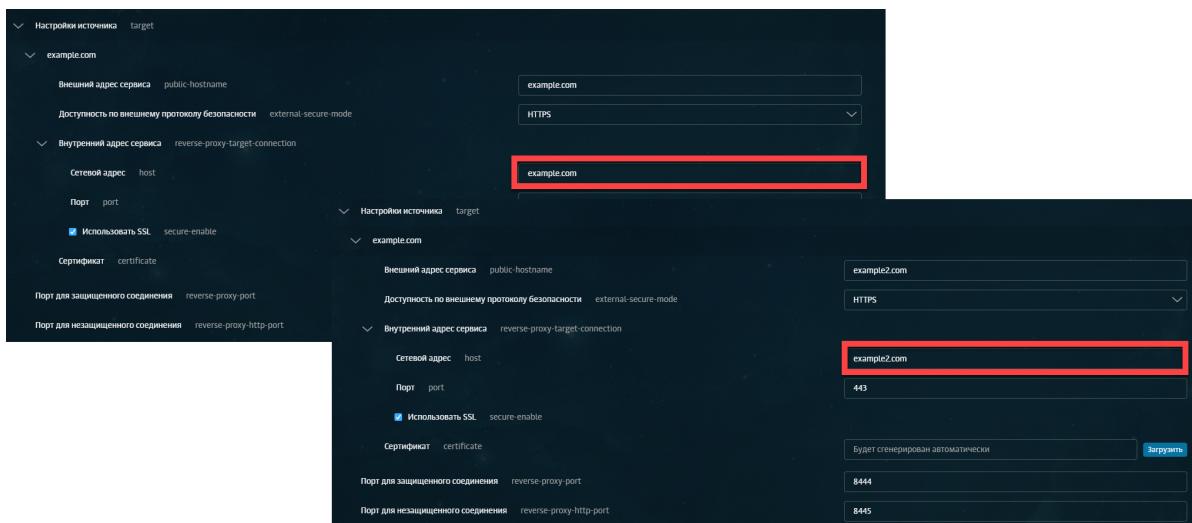


Рис. 8.2. Несколько публикуемых ресурсов

8.2. Создание сертификата для обратного прокси-сервера

Если в организации есть собственный Удостоверяющий центр, можно использовать его сертификат для обратного прокси.

Для выпуска сертификата с помощью УЦ Windows в CLI:

1. На АРМ с ОС Linux в CLI выполните следующие действия:

- Сгенерируйте ключ, используя одну из команд (в зависимости от выбранного алгоритма шифрования):

RSA:

```
# openssl genpkey -out wp.key -algorithm RSA -pkeyopt rsa_keygen_bits:2048
```

ECDSA:

```
# openssl genpkey -out wp.key -algorithm EC -pkeyopt ec_paramgen_curve:P-256
```

- Сформируйте файл конфигурации **wp.cnf** для создания запроса на подпись сертификата (CSR) и заполните его данными:

```
[req]
prompt = no
distinguished_name = dn
req_extensions = ext
input_password = PASSPHRASE
[dn]
CN = webmail.rt-solar.ru
emailAddress = webmaster@rt-solar.ru
O = Solar Security
L = Moskau
C = RU
[ext]
subjectAltName = DNS:webmail.rt-solar.ru
```

Выделенные значения параметров замените на актуальные значения в организации:

-
- **CN** – FQDN сервера, на котором происходит публикация;
 - **emailAddress** – контактный адрес электронной почты организации;
 - **O** – название организации;
 - **L** – название города, в котором расположена организация;
 - **C** – двухбуквенный код страны;
 - **subjectAltName** – FQDN публикуемого ресурса: DNS.
- Сгенерируйте CSR:

```
# openssl req -new -config wp.cnf -key wp.key -out wp.csr
```

2. На АРМ с ОС Windows выполните следующие действия:

- Скопируйте CSR во временный каталог на АРМ с Windows, например, в **c:\wp.csr**.
- Сгенерируйте сертификат из CSR:

```
# certreq -submit -attrib "CertificateTemplate: WebServer" c:\wp.csr
```

- Сохраните во временный каталог на АРМ пользователя сертификат с именем **wp.cer** и выберите в открывшемся окне **Получить PEM**.
- Выгрузите сертификат УЦ, подчиненного УЦ (при наличии):

```
# certutil -ca.cert c:\ca.cer
```

```
# certutil -subca.cer c:\subca.cer
```

3. На АРМ с ОС Linux в CLI выполните следующие действия:

- Сконвертируйте сертификат УЦ и подчиненного УЦ (при наличии) в формат PEM:

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

```
# openssl x509 -inform der -in subca.cer -out subca.pem
```

- Объедините ключ с сертификатом УЦ и подчиненного УЦ (при наличии):

```
# cat wp.key wp.pem ca.pem subca.pem > webmail.pem
```

4. В GUI Solar webProxy выполните следующие действия:

- a. В разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика** откройте секцию **Обратный прокси > Настройки источника**.
- b. В строке **Сертификат** нажмите кнопку **Загрузить файл**.
- c. В открывшемся окне проводника выберите файл с сертификатом (**webmail.pem**) и нажмите кнопку **Открыть**. Если сертификат успешно загружен, в поле **Сертификат** отобразится надпись **Загружен сертификат**.

-
- d. Сохраните и примените настройки конфигурации, последовательно нажав кнопки **Сохранить** и **Применить**.
 - 5. Для проверки работы обратного прокси с ролью обратного прокси в браузере перейдите на адрес публикуемого ресурса, например, на корпоративную почту **webmail.rt-solar.ru**.

8.2.1. Конвертация сертификатов в формат PEM

В Solar webProxy загрузить SSL-сертификат можно только в формате PEM. Если сертификат в другом формате (например, DER, P7B, PFX), его можно конвертировать в нужный формат.

8.2.1.1. Конвертация SSL-сертификатов с помощью OpenSSL

OpenSSL – надежный полнофункциональный инструмент для работы с протоколами Transport Layer Security (TLS) и Secure Sockets Layer (SSL). Конвертация с использованием библиотеки OpenSSL считается одним из самых безопасных способов: все данные будут сохранены непосредственно на устройстве, на котором будут выполняться операции по конвертированию.

Чтобы сконвертировать сертификат в формат PEM с помощью OpenSSL, на АРМ с ОС Linux в CLI выполните следующие команды:

- Для формата DER:

```
# openssl x509 -inform der -in site.der -out site.pem
```

- Для формата P7B:

```
# openssl pkcs7 -print_certs -in site.p7b -out site.pem
```

- Для формата PFX:

```
# openssl pkcs12 -in site.pfx -out site.pem -nodes
```

Примечание

Также вы можете использовать скрипт **openssl-toolkit**. Работа с этим скриптом является безопасным решением, т.к. сертификаты и их ключи используются исключительно на вашем сервере.

Сертификаты в формате PEM могут быть с расширениями .pem, .crt, .cer, .key. Чтобы сменить расширение, в CLI выполните следующие команды:

```
# openssl rsa -in server.key -text > private.pem
```

```
# openssl x509 -inform PEM -in server.crt > public.pem
```

```
# openssl x509 -in certificate.cer -outform PEM -out certificate.pem
```

8.3. Просмотр статистики по работе обратного прокси

Просмотреть информацию о работе Solar webProxy в обратном режиме можно в разделе **Рабочий стол** или в **Журнале запросов**. Для отображения информации о запросах в обратном режиме выберите режим **Обратный прокси** в **Журнале запросов**. Запросы помечены значком .



Рис. 8.3. Статистика по работе обратного прокси на Рабочем столе

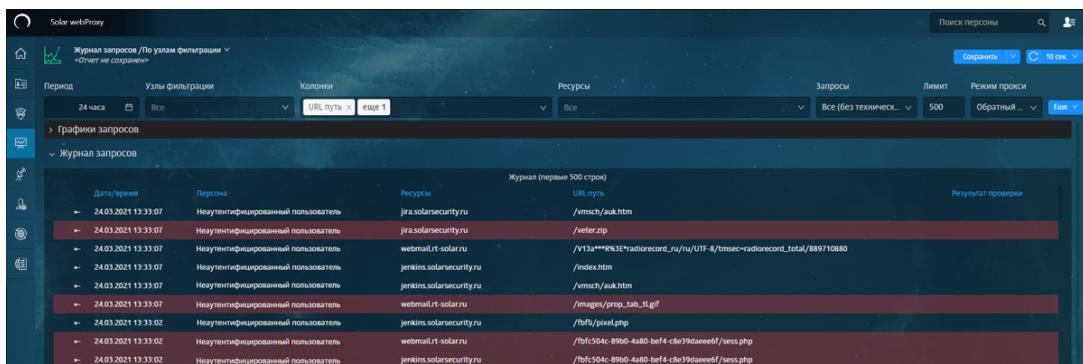


Рис. 8.4. Мониторинг работы обратного прокси в Журнале запросов

9. Дополнительные настройки Solar webProxy

9.1. Настройка сервиса skvt-wizor

Вы можете управлять параметрами запуска сервиса skvt-wizor в файле `/opt/dozor/service/skvt-wizor/run` с помощью команд:

- **# -XX:+HeapDumpOnOutOfMemoryError**
– создать файл формата HProof при нехватке оперативной памяти;
- **# -XX:HeapDumpPath=/var/tmp**
– указать путь для хранения файла формата HProof;
- **# -Xmx\${MAX_MEMORY}m**
– задать максимальный объем оперативной памяти, используемой skvt-wizor. Например, чтобы задать объем оперативной памяти в 60 Гб, используйте команду
-Xmx60g

Примечание

Если значение параметра **MAX_MEMORY** больше объема доступной оперативной памяти в ОС, сервис `skvt-wizor` не будет работать.

Выделяя больший объем оперативной памяти, используемой `skvt-wizor`, его может не хватить для других процессов ОС или программ.

9.2. Настройка журналирования сообщений сервисов `skvt-wizor` и `skvt-play-server`

При необходимости можно организовать запись сообщений сервисов `skvt-wizor` и `skvt-play-server` в файл `syslog-ng` и в отдельный файл.

9.2.1. Настройка журналирования сообщений сервиса `skvt-wizor` в файл `syslog-ng`

Для настройки журналирования сообщений сервиса `skvt-wizor` в файл `syslog-ng` выполните следующие действия:

1. В разделе **Система > Расширенные настройки > Фильтрация и кэширование трафика > Фильтрация и анализ трафика пользователей > Форматы записи в syslog** выберите формат записи в системный журнал сообщений (access-log, siem-log или ip-translation-log) (см. [Рис.9.1](#)).

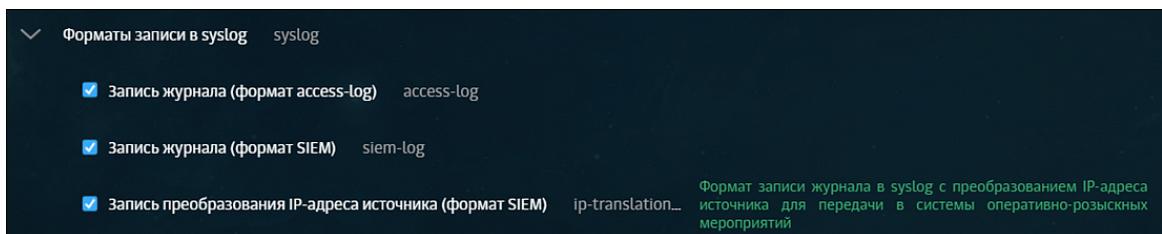


Рис. 9.1. Выбор формата записи журнала

Примечание

Для быстрого доступа к текущим настройкам журналов используйте меню **Система > Основные настройки > Журналирование**, секция **Фильтрация и анализ трафика пользователей**.

Далее приведено описание полей каждого формата записей в системный журнал.

Табл. 9.1. Описание полей сообщений в формате access-log

Поле сообщения	Описание
<date time>	Дата и время создания записи журнала syslog
<host>	Имя компьютера (источника)
java	Системная служба java
reqTime	Время начала запроса (float unix time)
filterTime	Общее время обработки запроса в миллисекундах
accountIP	IP-адрес источника (с учетом XFF)
filterStatus	Код состояния HTTP-узла фильтрации
responseSize	Размер тела ответа
method	HTTP-метод (GET, POST)
url	URL запроса
user	Имя авторизованного пользователя
user-agent	Информация о запросе
serverHost	IP-адрес ресурса назначения
mimeType	MIME-тип ответа (если он определен) – см. Приложение D.2

Пример записи из журнала запросов в **syslog-ng**:

```
Jan 23 17:06:22 avm118 java: 1327323982.533 13 10.31.6.126 TCP_MISS/200 2779 GET
http://lenta.ru/news/2012/01/23/shortsightedness/_Printed.htm DIRECT/81.19.85.116 text/html
Mozilla/5.0 (compatible; Yahoo! Slurp; http://help.yahoo.com/help/us/ysearch/slurp)
```

Примечание

Настроить журналирование сообщений в формате **SIEM** также можно, установив флагок **Запись журнала (формат SIEM)** в разделе **Политика > Настройки** или в разделе **Система > Основные настройки > Работа системы**.

Табл. 9.2. Описание полей сообщений в формате siem-log

Поле сообщения	Описание
<date time>	Дата и время создания записи журнала syslog
<host>	Имя компьютера (источника)
java	Системная служба java
acc-domain	Домен источника
acc-groups	Название групп источника из Досье
acc-ip	IP-адрес источника
acc-port	Порт источника
bytes-in	Объем скачанных (полученных) данных (Б)
bytes-out	Объем загруженных (отправленных) данных (Б)
flt-categories	Категории фильтрации политики
flt-codes	Код фильтрации политики (см. Приложение <i>Описание HTTP-кодов фильтрации</i>)
flt-policy	Название сработавшего слоя политики фильтрации
flt-rules	Названия правил политики, которые были применены при фильтрации
flt-status	Код состояния HTTP-узла фильтрации
flt-time	Общее время обработки запроса в миллисекундах
req-hostname	Сетевое имя ресурса назначения
req-method	HTTP-метод запроса
req-pathname	Путь запроса
req-protocol	Идентификатор протокола запроса
req-query	Параметры запроса
req-referer	Значение HTTP-заголовка Referer
req-time	Метка времени начала запроса от источника
req-user-agent	Информация о запросе
res-datatype	MIME-тип ответа (см. Приложение D.2)
res-ip	Числовое представление IP-адреса назначения
traf-mode	Режим направления трафика: прямой (forward)/обратный (reverse)
req-port	Порт ресурса назначения
flt-reason	Причина фильтрации
x-virus-id	Идентификатор вируса (значение в заголовках x-infection-found и x-virus-id, когда сервер ICAP (антивирус или песочница) возвращает ответ 403)

Пример записи из журнала запросов в **syslog-ng**:

```
Feb 2 16:49:55 wp java: [acc-domain:LDAP_USERS] [acc-groups:] [acc-ip:10.201.65.189]
[acc-name:idf] [acc-port:57348] [bytes-in:0] [bytes-out:0] [flt-categories:0] [flt-codes:11,0,0,2]
[flt-policy:Test_layer1] [flt-rules:https,Переход к слою Icap Response Icap Request,Переход к слою
Test_layer1,Test1] [flt-status:403] [flt-time:8] [req-hostname:gitlab.solar.local] [req-method:GET]
[req-pathname:/favicon.ico] [req-protocol:https] [req-query:]
[req-referer:https://gitlab.solar.local:8444/users/sign_in] [req-time:2023-02-02T13:49:55.666Z]
[req-user-agent: Mozilla/5.0 (compatible; Yahoo! Slurp;
http://help.yahoo.com/help/us/ysearch/slurp)][res-datatype:application/skvt-unchecked]
[res-ip:10.199.28.7] [traf-mode:reverse] [x-virus-id] [req-port:8444] [flt-reason:URL(gitlab.solar.local)]
```

Табл. 9.3. Описание полей сообщений в формате ip-translation-log

Поле сообщения	Описание
<date time>	Дата и время создания записи журнала syslog
<host>	Имя компьютера (источника)
java	Системная служба java
transport-protocol	Протокол передачи данных
acc-ip	IP-адрес источника
acc-port	Порт источника
req-proxy-ip	IP-адрес прокси-сервера
req-proxy-port	Порт прокси-сервера
flt-ip	IP-адрес узла фильтрации
flt-port	Порт узла фильтрации
res-ip	IP-адрес ресурса назначения
res-port	Порт ресурса назначения

Пример записи из журнала запросов в **syslog-ng**:

```
Jul 6 12:08:08 tyur java: [sys-time:2021-07-06T09:08:08.985Z] [transport-protocol:TCP]
[acc-ip:10.199.177.212] [acc-port:53337] [req-proxy-ip:10.201.29.113] [req-proxy-port:2270]
[flt-ip:10.201.29.113] [flt-port:33824] [res-ip:10.199.30.12] [res-port:443]
```

2. Последовательно нажмите **Сохранить** и **Применить**.

Журналы сообщений сервиса **skvt-wizor** будут находиться в файле **/var/log/messages**.

9.2.2. Настройка журналирования сообщений сервиса **skvt-play-server** в **syslog-ng**

Для настройки журналирования сообщений сервиса **skvt-play-server** в разделе **Система > Основные настройки > Журналирование > Сервер веб-интерфейса** установите флагок **Журналировать действия пользователей в messages**. Журналы действий пользователей будут находиться в файле **/var/log/messages**.

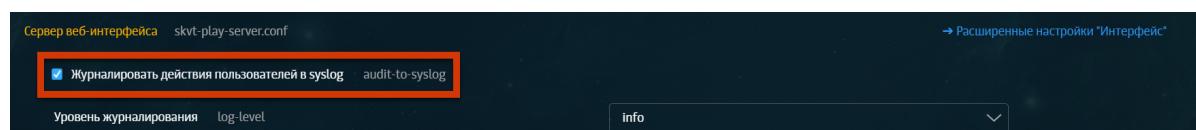


Рис. 9.2. Журналировать действия пользователей в messages

9.2.3. Настройка журналирования сообщений сервисов **skvt-wizor** и **skvt-play-server** в файл

Для настройки журналирования сообщений сервисов **skvt-wizor** и **skvt-play-server** через **syslog-ng** в отдельный файл:

1. Создайте файл **/var/log/skvt-log**, выполнив команду:

```
# touch /var/log/skvt-log
```

2. Для ограничения доступа к файлу **/var/log/skvt-log** выполните команду:

```
# chmod 600 /var/log/skvt-log
```

3. Создайте файл **touch etc/syslog-ng/conf.d/skvt.conf** с содержимым:

```
filter f_local0 {facility("local0");};  
destination d_skvt-log {  
    file("/var/log/skvt-log" group("root") owner("root") perm(0600));  
};  
log {  
    source(s_src); filter(f_local0); destination(d_skvt-log); flags(final);  
};
```

4. Перезапустите **syslog** командой:

```
# systemctl restart syslog-ng.service
```

9.2.4. Остановка записи данных syslog в файл messages

Сохранение журнальных записей в файл и остановка их передачи в файл **messages** определяется файлом **/etc/syslog-ng/syslog-ng.conf**.

Для прекращения передачи данных в файл **messages**:

1. Добавьте запись:

```
@define allow-config-dups 1  
filter f_local0 {facility("local0");}  
filter f_messages { level(info,notice,warning) and  
    not facility(auth,authpriv,cron,daemon,mail,news) and  
    not filter(f_local0); };  
filter f_syslog3 { not facility(auth, authpriv, mail) and  
    not filter(f_debug) and  
    not filter(f_local0); };  
  
destination d_skvt-log {  
    file("/var/log/skvt-log" group("root") owner("root") perm(0600));  
};  
log {  
    source(s_src); filter(f_local0); destination(d_skvt-log); flags(final);  
};
```

2. Перезапустите **syslog** командой:

```
# systemctl restart syslog-ng.service
```

9.3. Настройка принудительного использования HTTPS

Для настройки принудительного использования протокола HTTPS:

1. В разделе **Система > Основные настройки > Работа системы** установите флагок **Принудительное использование HTTPS**.
2. Последовательно нажмите кнопки **Сохранить** и **Применить**.

9.4. Настройка сервиса igmproxy

Управлять сервисом пересылки широковещательных IGMP-пакетов (igmproxy) можно с помощью файла `/opt/dozor/etc/igmproxy.conf`. Файл содержит информацию о:

- сетевых интерфейсах,
- статусе сетевых интерфейсов относительно приема multicast-трафика,
- направлении multicast-трафика (upstream, downstream),
- перечне сетей, от которых будет возможен прием multicast-трафика.

Пример содержания файла `/opt/dozor/etc/igmproxy.conf`:

```
root@wp:/opt/dozor# cat /opt/dozor/etc/igmproxy.conf
#####
#
# Example configuration file for the IgmpProxy
#
#
# The configuration file must define one upstream
# interface, and one or more downstream interfaces.
#
# If multicast traffic originates outside the
# upstream subnet, the "altnet" option can be
# used in order to define legal multicast sources.
# (See example...)
#
# The "quickeave" should be used to avoid saturation
# of the upstream link. The option should only
# be used if it's absolutely necessary to
# accurately imitate just one Client.
#
#####
##-----
## Enable Quickeave mode (Sends Leave instantly)
##-----
quickeave

##-----
## Configuration for eth0 (Upstream Interface)
##-----
phyint eth0 upstream ratelimit 0 threshold 1
    altnet 10.0.0.0/8
    altnet 192.168.0.0/24

##-----
## Configuration for eth1 (Downstream Interface)
##-----
phyint eth1 downstream ratelimit 0 threshold 1

##-----
## Configuration for eth2 (Disabled Interface)
##-----
phyint eth2 disabled
```

Параметры, которые можно настроить в файле:

- **quickleave** – разрешает быструю отписку от multicast-группы. При получении сообщения своего клиента (с downstream-интерфейса) об отписке от группы сервис igmproxy отправляет сообщение об отписке со своего upstream-интерфейса, и сам перестает получать поток этой группы. Параметр нужен, если за маршрутизатором один клиент, если клиентов больше, параметр использовать не следует, так как отписка от потока одного из клиентов прервёт поток ко всем клиентам. Опция размещается в файле конфигурации отдельной строкой.
- **phyint interface role [ratelimit limit] [threshold ttl] [altnet networkaddr ...]** – описание сетевого интерфейса (для каждого сетевого интерфейса в системе должно быть описание). Список интерфейсов можно получить с помощью команд **ifconfig** или **ip a l**.
- **interface** – название сетевого интерфейса, обязательный параметр.
- **role** – роль сетевого интерфейса, обязательный параметр. Может иметь одно из трех значений:
 - **upstream** – сетевой интерфейс, через который проходят multicast-потоки (как правило, интерфейс к провайдеру). Может быть только один в системе.
 - **downstream** – сетевой интерфейс, на который передается трафик multicast-потоков, к нему подключаются клиенты. Может быть несколько.
 - **disabled** – сетевой интерфейс, не участвующий в распространении multicast-потоков. Может быть несколько.
- **ratelimit** – определяет ограничение полосы для интерфейса. По умолчанию – не ограничено.
- **threshold** – определяет минимальное значение TTL, при котором пакеты пропускаются через прокси. По умолчанию – 1.
- **altnet** – определяет сети, к которым принадлежат источники пересылаемых потоков. Можно задать только для upstream-интерфейса.

10. Сопровождение Solar webProxy

10.1. Управление сервисами

Для управления сервисами используется утилита **dsctl**, формат команды запуска которой:

dsctl

(boot|down|start|stop|restart|reload|status|enable|disable|service-list) [services]

Services are:

- abook-daemon
- antivirus
- clickhouse
- database
- grafana
- haproxy
- igmpproxy
- keepalived
- license-server
- log-streamer
- monitor-agent
- monitor-ng
- monitor-server
- network-config-agent
- skvt-auth-server
- skvt-cache
- skvt-cassandra
- skvt-kerberos-server
- skvt-ntlm-server
- skvt-play-server
- skvt-trafdaemon
- skvt-winbind
- skvt-wizor
- smap-tikaserver
- url-checker-next

В качестве аргумента при запуске утилиты **dsctl** укажите одно из значений:

Табл. 10.1. Команды для утилиты **dsctl**

Роль	Описание
boot	Запуск системы управления сервисами
down	Остановка системы управления сервисами
start	Запуск сервиса
stop	Остановка сервиса
restart	Перезапуск сервиса, при выполнении команды сервис завершает работу и запускается заново, используя новую конфигурацию
reload	Повторное считывание настроек сервисом, при выполнении команды сервис перечитывает конфигурацию и продолжает работу с новой конфигурацией
enable	Подключение сервиса к системе управления сервисами

Роль	Описание
	<p>Примечание</p> <p><i>При выборе значения необходимо указывать сервисы.</i></p>
disable	<p>Отключение сервиса от системы управления сервисами</p> <p>Примечание</p> <p><i>При выборе значения необходимо указывать сервисы.</i></p>
service-list	Вывод списка сервисов, подключенных к системе управления сервисами
status	Вывод информации о статусах сервисов

Для вывода информации о статусе сервисов также используется скрипт **status**, который запускается командой:

status

Примечание

*Если не запущен ни один из сервисов, при запуске скрипта **status** выводится пустой список.*

Список сервисов приведен в разделе [2.2](#).

Примечание

При аварийном завершении работы какого-либо сервиса Solar webProxy автоматически будет предпринимать попытки перезапустить остановившийся сервис. Под аварийной причиной следует понимать остановку компонентов вследствие ошибок в ПО или наличия проблем с окружением.

10.2. Использование скриптов

10.2.1. Использование скриптов для получения информации о работе системы

Для сопровождения системы используются специальные скрипты и утилиты, расположенные в каталоге **/opt/dozor/bin**.

Перечень и назначение скриптов приведены в [Табл.10.2](#).

Табл. 10.2. Скрипты для сопровождения работы системы

Название	Описание
Основные	
accept-settings	Утилита для управления системными настройками Solar webProxy
config	Утилита для управления кластером

Название	Описание
dsctl	Утилита для управления сервисами
reg-slave	Утилита для регистрации узла в кластере
status	Скрипт для просмотра информации о статусе сервисов
user-tool	Утилита для управления учетными записями пользователей
Расширенные	
accept-policy	Утилита для управления политиками
bug-report	Утилита для формирования отчета об ошибках
cassandra-optimize	Скрипт для синхронизации данных между узлами кластера
check_skvt	Утилита для проверки целостности файлов Solar webProxy
get-config	Утилита для вывода конфигурации узла
get-role	Утилита для просмотра ролей, назначенных узлу
license-tool	Утилита для просмотра информации о лицензии
seelog	Скрипт для просмотра журнальных файлов Solar webProxy
set-config	Утилита для записи конфигурации узла
set-role	Утилита для назначения ролей узлу
unreg-slave	Утилита для отзыва регистрации узла в кластере

Внимание!

*Если не указано иного, данные скрипты и утилиты необходимо запускать из командной оболочки Solar webProxy, имея права суперпользователя **root**. Переход в командную оболочку выполняется с помощью команды:*

```
# /opt/dozor/bin/shell
```

10.2.2. Запуск скриптов из веб-интерфейса

Для минимизации обращений администратора системы в консоль используется механизм запуска скриптов для узлов кластера. Запустить выполнение скрипта можно в разделе **Система > Узлы и роли** при наличии прав на работу с разделом **Система**.

Скрипты необходимы, например, инженерам поддержки Solar webProxy для получения информации о работе системы в случае сбоев в ее работе. Одним из таких скриптов является **bug-report**, который собирает диагностические данные с узла об ошибках.

При нажатии на значок  в правом углу секции с узлом раскрывается список доступных для выполнения на этом узле скриптов. Для запуска скрипта нажмите на его название. В верхней части экрана отобразится уведомление об успешном запуске. По окончании отобразится уведомление с предложением скачать текстовый файл с собранными журнальными записями.

Примечание

Возможен запуск только одного скрипта на одном узле из-под одного пользователя. Если скрипт уже выполняется, его перезапуск невозможен.

На данный момент из интерфейса можно запустить следующие скрипты:

- **bug-report** – позволяет собирать и выводить информацию о системе, настройках и показателях ПО. Перечень видов информации, которую можно просмотреть с помощью утилиты **bug-report**, приведен в разделе [Приложение С. Отчет об ошибках: утилита bug-report](#).
- **check-system** – позволяет проверить целостность файлов Solar webProxy на текущий момент времени (в CLI скрипт называется **check_skvt**).

Скрипт **check-system** использует стандартный механизм проверки целостности установленных файлов относительно содержащихся в исходных RPM-пакетах. Кроме того, скрипт содержит механизм, позволяющий отслеживать состояние произвольных файлов или каталогов, а также обрабатывать исключения среди установленных файлов.

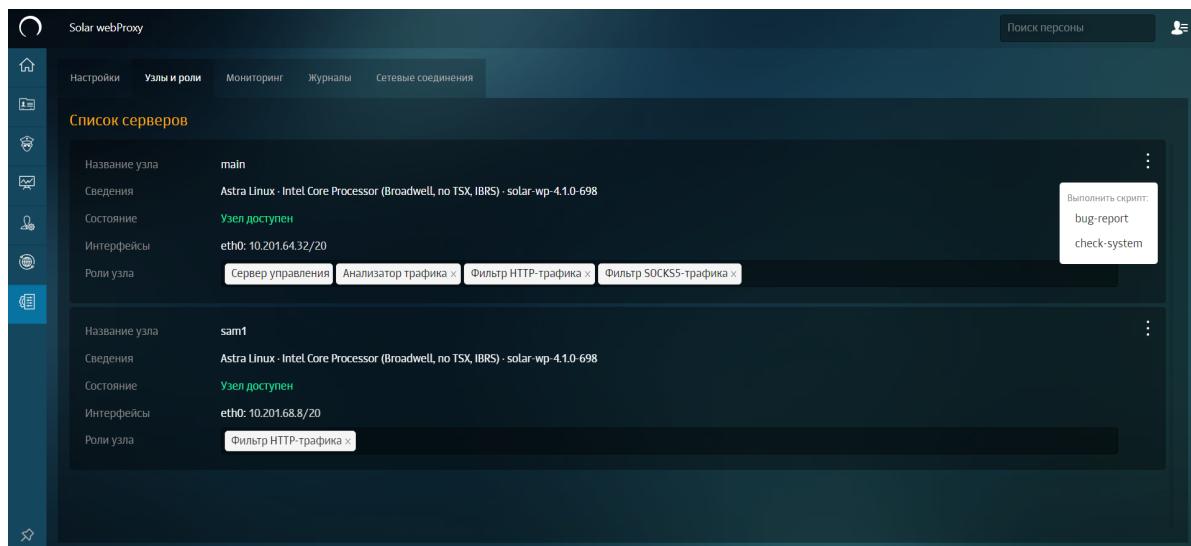


Рис. 10.1. Запуск скриптов из веб-интерфейса

10.2.3. Использование скрипта **user-tool**

Если пользователь забыл пароль, можно изменить его с помощью скрипта **user-tool**.

Этот скрипт также позволяет:

- заблокировать/разблокировать учетную запись пользователя;
- сменить вид авторизации пользователя. Необходимо для вывода пользователя из домена: изменения доменной авторизации на локальную.

Для запуска **user-tool** в CLI:

1. Выполните команду для запуска утилиты и вызова инструкции:
user-tool --help
2. В зависимости от поставленной цели выберите и выполните одну из перечисленных команд.

Инструкция по действиям **user-tool** имеет следующий вид:

```
user-tool 1.0
Usage: user-tool [change-password|block-user|unblock-user|set-user-local] [options]

--help
Command: change-password [options]
change user password
-l, --login <value> login of user
-p, --password <value> password of user
Command: block-user [options]
block user
-l, --login <value> login of user
Command: unblock-user [options]
unblock user
-l, --login <value> login of user
Command: set-user-local [options]
change user auth method to local
-l, --login <value> login of user
```

Пример команды для изменения пароля от учетной записи пользователя:

```
ds-mode@rick /opt/dozor # user-tool change-password -l admin -p etyutqweo1w3
```

Примечание

После изменения пароля в CLI войдите в GUI системы для повторной смены пароля, как при первом входе в систему, и авторизуйтесь.

После выполнения других действий в GUI по умолчанию произойдут изменения:

- *после активации/блокировки учетной записи пользователя в карточке пользователя переключатель изменит свое положение;*
- *после изменения вида авторизации пользователя в его карточке исчезнет флагок Пользователь домена.*

10.3. Резервное копирование Solar webProxy

10.3.1. Общие сведения

Резервное копирование в Solar webProxy применяется для решения задач:

- восстановление после сбоя;
- полное обновление операционной системы.

Процедура восстановления после сбоя зависит от характера сбоя, и в ряде случаев сводится к полному восстановлению ранее зарезервированных данных. Ниже описана процедура полного резервирования и восстановления данных. Эту процедуру, с небольшими изменениями, можно использовать для обновления операционных систем на серверах комплекса (в случае использования распределенной конфигурации).

10.3.2. Резервное копирование данных

10.3.2.1. Резервное копирование программного обеспечения

Создайте копию установочных RPM-пакетов и сохраните ее на надежном носителе данных. Это необходимо проделать один раз, сразу после установки или обновления, настройки и ввода комплекса в эксплуатацию.

10.3.2.2. Резервное копирование конфигурации системы

Резервное копирование конфигурации системы необходимо делать в случае внесения существенных изменений в конфигурацию комплекса, либо по расписанию.

Для резервного копирования конфигурации предназначены утилиты командной строки (скрипты) **export-config** и **import-config**, которые позволяют «одним движением» экспортировать и импортировать конфигурацию.

Примечание

Следует отметить, что утилиты работают только на master-узле и только от пользователя dozor или root.

Для экспортации всей конфигурации в файл на master-узле в CLI выполните команду **export-config <output-file.json>**.

Для импорта конфигурации из файла в CLI на master-узле:

1. Выполните команду **import-config <input-file.json>**.
2. Примените настройки с помощью команды **accept-settings**.

10.3.2.3. Резервное копирование политики

Для оптимизации резервного копирования политики фильтрации предназначены команды утилиты **policy-tool**, которые позволяют экспортировать и импортировать политику фильтрации. При этом файл с резервной копией политики имеет меньший объем на диске, чем дамп БД.

Примечание

При импорте и экспорте политик, в которых указаны конкретные узлы в поле Узлы фильтрации, передаются имена узлов, а не их идентификаторы. Поэтому убедитесь, что при копировании названия узлов и перечень ролей на них совпадают.

Для экспортации политики на master-узле в CLI выполните команды:

1. Зайдите в **shell: /opt/dozor/bin/shell**
2. Экспортируйте политику:
policy-tool export

или

policy-tool export -f /var/tmp/test_policy_export.json.

Для импорта политики:

1. На **master-узле** в CLI выполните команды:

/opt/dozor/bin/shell

policy-tool import -f policy_for_import_policytool.json

2. В GUI перейдите в раздел **Политика** и нажмите кнопку **Применить политику**.

Для сброса всех правил политики к дефолтным настройкам:

1. На **master-узле** в CLI выполните команды:

/opt/dozor/bin/shell

policy-tool reset

2. В GUI перейдите в раздел **Политика** и нажмите кнопку **Применить политику**.

Поскольку политика может довольно часто изменяться, то ее резервное копирование лучше делать по расписанию: раз в день и раз в неделю.

Перед копированием также необходимо временно отключить веб-интерфейс администратора.

10.3.3. Восстановление зарезервированных данных

При восстановлении зарезервированных данных необходимо учесть следующее:

- Если речь идет о **slave-узле**, следует восстановить его и ввести в кластер с помощью утилиты **reg-slave**.
- Если речь идет о **master-узле**, следует установить программное обеспечение заново и восстановить конфигурацию. Процедура восстановления программного обеспечения заключается в установке или переустановке набора RPM-пакетов.
- Процесс восстановления конфигурации происходит на каждом из узлов, где есть необходимость в этом. В случае обновления операционной системы необходимо восстановить все узлы.
- После установки новой операционной системы и установки набора пакетов **Solar webProxy** каждый узел будет работать в режиме **master-узла**.
- Процесс восстановления политики начинается с восстановления данных на **master-узле**.
- Восстановление политики на **slave-узлах** происходит после ее восстановления на **master-узле**.

10.3.4. Плановое резервное копирование

Плановое резервное копирование производится встроенными в Solar webProxy или внешними программными средствами, работающими на основе описанных выше процедур резервного копирования Solar webProxy.

10.4. Просмотр журнальных файлов Solar webProxy

Для просмотра журнальных файлов сервисов используется скрипт **seelog**. Для его запуска необходимо выполнить команду:

seelog <service-name>

где **<service-name>** – имя сервиса, журналный файл которого требуется просмотреть.

Скрипт позволяет просматривать журналные файлы в реальном времени. Файлы формируются с использованием значений, выводимых в стандартный поток вывода сообщений и в стандартный поток вывода ошибок. После выполнения команды запуска скрипта, например, для просмотра журнального файла сервиса **skvt-wizor**:

seelog skvt-wizor

На экран выводится информация вида:

```
2009-10-19 14:05:09.280829500 5268523 [Reactor-18] DEBUG nio_proxy - proc@15999328: writing
290 bytes
2009-10-19 14:05:09.280832500 5268524 [Reactor-18] DEBUG nio_proxy - proc@15999328: writing
done
2009-10-19 14:05:09.280835500 5268524 [Reactor-18] DEBUG nio_proxy - proc@15999328:
clientWriteDone, state=WRITE_GENERATED_PAGE readingPreview=false download=false
serverDone=true
2009-10-19 14:05:09.280851500 5268524 [Reactor-18] DEBUG nio_proxy - proc@15999328: Changing
state to NEW_REQUEST
2009-10-19 14:05:09.280855500 5268524 [Reactor-18] DEBUG nio_proxy - proc@15999328:
fireRequestFinished
2009-10-19 14:05:09.280885500 5268524 [Reactor-18] DEBUG nio_proxy - proc@15999328: Running
NEW_REQUEST filters; threaded=false
2009-10-19 14:05:09.280889500 5268524 [Reactor-18] DEBUG nio_proxy - proc@15999328: Running
FilterHelper:su.msk.jet.nioproxy.auth.AuthFilter@5db5ae
2009-10-19 14:05:09.280893500 5268524 [Reactor-18] DEBUG nio_proxy - proc@15999328: Running
FilterHelper:su.msk.jet.nioproxy.rule.engine.RuleEngineFilter@1efe475
2009-10-19 14:05:09.280926500 5268524 [Reactor-18] DEBUG nio_proxy - proc@15999328: Changing
state to READING_REQUEST_LINE
2009-10-19 14:05:09.280930500 5268524 [Reactor-18] DEBUG nio_proxy - proc@15999328: expectInput
```

В таблице ниже приведен перечень существующих уровней детализации информации в журнальных файлах.

Табл. 10.3. Уровни детализации информации журналных файлов

Уровень	Описание
DEBUG	Отладочная информация (для разработчиков)
INFO	Дополнительная информация, относящаяся к процедуре обработки данных
TRACE	Подробная отладочная информация (для разработчиков)
WARN	Уведомления о том, что некоторые компоненты не работают (без нарушения обработки данных)

Уровень	Описание
ERROR	Сообщения об ошибках, способных нарушить обработку данных
FATAL	Критическая ошибка

Уровень детализации информации в журнальных файлах можно указать в веб-интерфейсе:

- на вкладке **Система > Основные настройки > Журналирование**;
- на вкладке **Система > Расширенные настройки**.

Далее приведен перечень уровней детализации информации, которые можно задать.

Табл. 10.4. Уровни детализации информации

Роль	Описание
Уровень отладки (log-level)	Задает уровень журналирования для тех подсистем фильтра, для которых отсутствуют дополнительные настройки уровня журналирования.
Уровень отладки аутентификации (log-auth)	Задает уровень журналирования подсистемы аутентификации.
Уровень отладки политики (log-policy)	Задает уровень отладки выполнения политики. Сюда же входит работа с внешними сервисами, необходимыми для работы политики – url-checker-next, антивирус и др.
Уровень отладки сетевого ввода-вывода (log-network)	Задает уровень журналирования подсистемы проксирования HTTP-протокола, управления сокетами, работы мультиплексированного ввода-вывода.
Уровень отладки архивации данных (log-archive)	Задает уровень журналирования подсистемы архивации POST-запросов и их передачи в Solar Dozor.

Перечисленные параметры можно найти с помощью поиска по конфигурации. Все настройки журналирования имеют стандартные уровни (ERROR, WARN, INFO, DEBUG, TRACE) – за исключением **Уровень отладки архивации данных** и **Уровень отладки аутентификации** – отсутствует TRACE. Кроме того, для других сервисов в веб-интерфейсе задается уровень журналирования VERBOSE (подробная информация) и DEBUG (отладочная информация).

Примечание

Наиболее объемным является журналирование процессов сетевого ввода-вывода (log-network), поэтому уровни DEBUG и TRACE включать в штатном режиме функционирования Solar webProxy не рекомендуется.

В распределенном режиме просмотр журнальных файлов производится с помощью скрипта **seelog** для каждого узла по отдельности.

Действия администраторов по настройке политик фильтрации и конфигурации Solar webProxy, такие как создание, редактирование, удаление и просмотр правил/ресурсов/параметров, фиксируются в журнальном файле сервиса **skvt-play-server**. Пример записи из журнала:

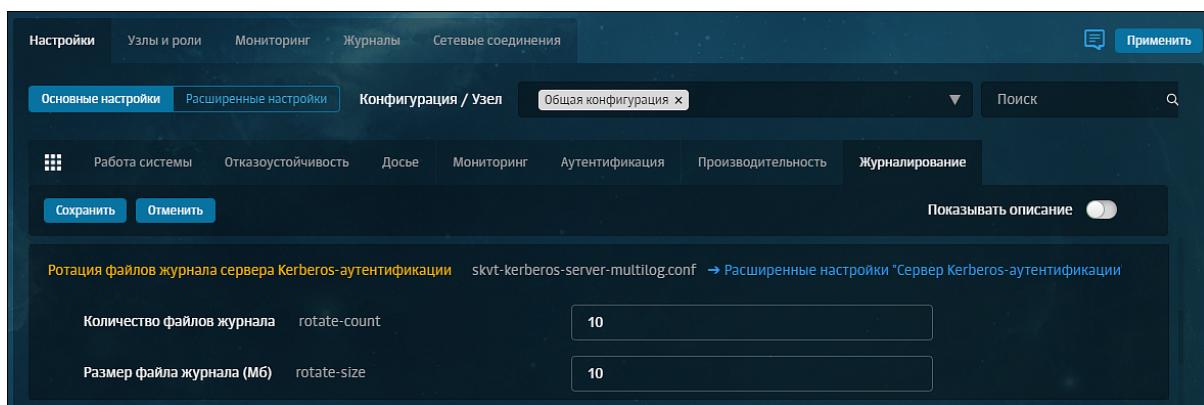
```
2018-04-13 14:29:40.379898500 INFO application - Read item of type 'ruleset' with name 'a'  
(41275174-c3e2-492a-ac1c-bbe29ac128b1) by user 'admin'  
2018-04-13 14:30:04.803325500 INFO application - Connected to Address book daemon realtime
```

```
stream
2018-04-13 14:30:09.092094500 INFO application - Update item of type 'ruleset' with name 'a'
(41275174-c3e2-492a-ac1c-bbe29ac128b1) by user 'admin':
Add rule Rule(4f7df7b2-77cc-4c52-b49f-a98db6d54487,Правило
1,true,List(And((MatchUser(Some(3d4ffa9a-de30-4ee6-a60b-bece8c1d5acf),"")),"")),
List(Notify(840fc4c3-3a7c-4441-b49f-df4c4a55be3a,4a17763c-59a4-4fd2-99f3-1992d331f87c,")),Some())
```

10.5. Настройки журналирования

Для настройки журнальных файлов через GUI:

1. В меню **Система > Основные настройки > Журналирование** для секции настроек ротации журналов конкретного сервиса установите необходимые значения.
2. Нажмите **Сохранить** и **Применить**.



Текущие настройки журналирования идентичны тем, которые используются в расширенных настройках системы. Для удобства использования раздела в каждом блоке настроек предусмотрен переход по ссылке к расширенным настройкам соответствующего сервиса.

10.6. Управление кластером

10.6.1. Регистрация узла в кластере

Для регистрации узлов в кластере используется утилита **reg-slave**, которая выполняет следующие функции:

- преобразует узел в подчиненный узел кластера вне зависимости от его предыдущего состояния (**master-узел**, **slave-узел**);
- обеспечивает применение конфигурации как на главном узле, так и на подчиненном. После запуска и успешного завершения утилиты **reg-slave** все остальные действия по управлению подчиненным узлом производятся централизованно через веб-интерфейс.

Чтобы зарегистрировать узел в кластере (добавить его в кластер):

1. С помощью протокола **ssh** зайдите на узел, который необходимо добавить в кластер.
2. Выполните команду:

```
# /opt/dozor/bin/shell
```

3. Выполните команду:

```
# reg-slave <master-host> [name]
```

где **<master-host>** – FQDN master-узла (например, **proxymaster.company.local**), а **<name>** – имя регистрируемого узла, которое будет отображаться в GUI Solar webProxy.

При регистрации узлов изменения в конфигурации кластера записываются в следующие файлы:

- **/data/repos/dozor/config-base.git/cluster.json** на главном узле (master-host);
- **/opt/dozor/config/control** на подчиненном узле (slave-host).

Если данный узел уже был зарегистрирован, то файл **/data/repos/dozor/config-base.git/cluster.json** обновляться не будет. Если имя узла изменилось, то оно будет обновлено, а идентификатор (**uuid**) узла останется прежним.

При запуске утилиты **reg-slave** при отсутствии ошибок файл **/opt/dozor/config/control**, находящийся на подчиненном узле, всегда обновляется. Таким образом, используемый главный узел, а следовательно, и параметры **config-repository** и **policy-repository** всегда актуальны.

Если идентификатор (**uuid**) данного узла совпадает с идентификатором (**uuid**) master-узла в кластере, то регистрируемому узлу будет автоматически сгенерирован новый идентификатор (**uuid**).

При запуске утилиты **reg-slave** без параметров, а также с ключами **-h**, **--help**, выводится справка:

```
# reg-slave
Usage: reg-slave master-host name roles...
```

Пример вывода команды **# reg-slave wp-filter-1.solar.local filter <полное доменное имя>**:

```
Checking ssh connection to master...
Connected successfully
Checking master...
Copying ssl certificates from master...
ca.crt          100% 1359  287.4KB/s 00:00
ca.key          100% 1704  331.5KB/s 00:00
bus.pem          100% 4170  939.3KB/s 00:00
Generating SSL certificates for slave...
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to '/tmp/tmp.w2q2RM8Qrk/client.key'
-----
Using configuration from /tmp/tmp.w2q2RM8Qrk/ca.config
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName      :PRINTABLE:'RU'
stateOrProvinceName :ASN.1 12:'Moscow'
localityName     :ASN.1 12:'Moscow'
```

```

organizationName    :ASN.1 12:'SolarSecurity'
organizationalUnitName:ASN.1 12:'OPR'
commonName         :ASN.1 12:'wp.solar.local'
Certificate is to be certified until Mar 11 11:57:23 2032 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
Initializing repositories...
Клонирование в «config-final.git»...
remote: Перечисление объектов: 4868, готово.
remote: Подсчет объектов: 100% (4868/4868), готово.
remote: Сжатие объектов: 100% (4548/4548), готово.
remote: Всего 4868 (изменения 2778), повторно использовано 0 (изменения 0)
Получение объектов: 100% (4868/4868), 540.32 KiB | 2.40 MiB/s, готово.
Определение изменений: 100% (2778/2778), готово.
Node hostname: wp.solar.local
Using existing node ID: 834a08c6-b2d4-4b1a-a0f2-5cb72e46d8d7
Updating control-file...
Registering node on master...
Updating existing node...
No changes to commit
Running accept-settings...
Уже обновлено.
Enabling services...
Service monitor-ng already enabled
Restarting services...
accept-setting completed successfully

```

10.6.2. Управление структурой кластера

Для управления структурой кластера предназначен скрипт **config cluster**. Формат команды для запуска скрипта:

\$ config cluster [общий ключ] <действие> [ключ действия]

где указаны следующие параметры:

- **[общий ключ]** – ключ, используемый при выполнении любого действия;
- **<действие>** – действие, которое требуется совершить;
- **[ключ действия]** – ключ, который используется для того или иного действия.

В таблице [Табл.10.5](#) перечислены общие ключи, используемые в скрипте **config cluster**:

Табл. 10.5. Перечень общих ключей

Ключ	Описание
-R <FILE>, --roles-dir <DIR>	Директория, содержащая файлы с описанием ролей узлов
-C <FILE>, --cluster-file <FILE>	Файл, содержащий описание кластера

Все действия по управлению структурой кластера приведены в таблице [Табл.10.6](#):

Табл. 10.6. Перечень действий

Действие	Описание
add-node	Добавление узла кластера. Работает с ключами: <ul style="list-style-type: none"> • -i <ID>, --id <ID> – идентификатор узла (UUID); • -n <NAME>, --name <NAME> – имя узла; • -h <HOSTNAME>, --hostname <HOSTNAME> – значение hostname узла; • -S <SUBCLUSTER>, --subcluster <SUBCLUSTER> – идентификатор или имя подкластера.
add-roles	Добавление ролей узла. Работает со следующими ключами: <ul style="list-style-type: none"> • -N <NODE>, --node <NODE> – идентификатор (UUID) или имя узла; • -r <ROLES>, --roles <ROLES> – список ролей через запятую.
add-subcluster	Добавление подкластера. Работает со следующими ключами: <ul style="list-style-type: none"> • -i <ID>, --id <ID> – идентификатор подкластера (UUID); • -n <NAME>, --name <NAME> – имя подкластера.
delete-node	Удаление узла кластера. Работает с ключами действия add-node .
delete-roles	Удаление ролей узла. Работает с ключами действия add-roles .
delete-subcluster	Удаление подкластера. Работает с ключами действия add-subcluster .
disable-services	Отключение сервисов. Работает с ключами действия add-roles .
enable-services	Включение сервисов. Работает со следующими ключами: <ul style="list-style-type: none"> • -N <NODE>, --node <NODE> – идентификатор (UUID) или имя узла; • -s <SERVICES>, --services <SERVICES> – список сервисов через запятую.
print	Вывод текущего состояния кластера. Работает с ключом: <ul style="list-style-type: none"> • -f <FORMAT>, --format <FORMAT> – вывести состояние кластера в формате <FORMAT>. Принимает значения text, json и edn. По умолчанию (без ключа) используется text.
set-roles	Установка ролей узла. Работает с ключами действия add-roles .
update-node	Модификация узла кластера. Работает с ключами действия add-node .
update-subcluster	Модификация подкластера. Работает с ключами действия add-subcluster .

Пример вывода команды **# config cluster print**:

Common nodes:

```
Node: main
ID: 0f676af8-e25d-481e-a193-2aaecb2a2eed
Hostname: t28132.solar.local
Roles: master
Services:
  skvt-trafdaemon
  database
  monitor-server
  abook-daemon
  skvt-cassandra
  clickhouse
```

```
skvt-play-server
grafana
monitor-ng
monitor-agent
Node: wp-filter-2.solar.local
ID: 1a84121c-c1fc-4aaf-8f3b-05f2be527bc1
Hostname: wp-filter-2.solar.local
Roles: http-filter, abook-slave, analyzer
Services:
skvt-wizor
skvt-auth-server
skvt-cassandra
skvt-cache
log-streamer
monitor-ng
monitor-agent
abook-daemon
url-checker-next
smap-tikaserver
Node: wp-filter-3.solar.local
ID: f068f01b-0fdd-4cd4-9efb-73d78b93edda
Hostname: wp-filter-3.solar.local
Roles: http-filter, abook-slave, analyzer
Services:
skvt-wizor
skvt-auth-server
skvt-cassandra
skvt-cache
log-streamer
monitor-ng
monitor-agent
abook-daemon
url-checker-next
smap-tikaserver
Subclusters:
```

В данном примере видно, что в кластер входит один master-узел **t28132.solar.local** и два slave-узла **wp-filter-2.solar.local** и **wp-filter-3.solar.local**.

10.6.3. Диагностика кластера Cassandra

Для диагностики кластера Cassandra служит утилита командной строки **nodetool**. Для ее запуска выполните команду:

```
# /opt/dozor/cassandra/bin/nodetool --ssl status
```

На экран будет выведена информация вида:

```
Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address      Load      Tokens  Owns      Host ID            Rack
DN 10.201.69.74 303.72 KB  256    48.1%  6018d262-7331-4c01-8c16-7cb42fed2ac8  rack1
UN 10.201.69.193 332.6 KB  256    51.9%  55175322-e8a1-4c82-8b9a-4ed89d10e01c  rack1
```

Первая буква первой записи в каждой строке означает статус узла:

-
- **D** – выключен или недоступен (down);
 - **U** – включен и доступен (up).

Вторая буква первой записи в каждой строке означает состояние узла:

- **N** – узел работает normally (normal);
- **L** – узел покидает кластер Cassandra (leaving);
- **J** – узел присоединяется к кластеру Cassandra (joining).

Вторая запись (**Address**) в каждой строке отображает IP-адрес узла.

Третья запись (**Load**) в каждой строке отображает объем данных, хранимых на узле.

Пятая запись (**Owns**) в каждой строке отображает долю от общего количества уникальных данных кластера, хранимую на узле.

Шестая запись (**Host ID**) в каждой строке отображает идентификатор узла кластера Cassandra.

10.6.4. Удаление узла из кластера Cassandra

В некоторых случаях возникает необходимость удаления одного или нескольких узлов из кластера Cassandra.

10.6.4.1. Проверка статуса узла

Узнать состояние удаляемого узла можно с помощью скрипта **nodetool**:

```
# /opt/dozor/cassandra/bin/nodetool --host --ssl <имя или адрес удаляемого узла>
status
```

Команда выполняется на любом узле, за исключением того, который следует удалить. Например:

```
ds-mode@bvm224 /data/spool # /opt/dozor/cassandra/bin/nodetool --host --ssl avm229 status
```

где **bvm224** — главный узел (master-host), **avm229** — удаляемый узел.

В результате будет отображена информация:

```
Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address      Load      Tokens  Owns      Host ID            Rack
DN 10.201.69.74 303.72 KB  256   48.1%  6018d262-7331-4c01-8c16-7cb42fed2ac8  rack1
UN 10.201.69.193 332.6 KB  256   51.9%  55175322-e8a1-4c82-8b9a-4ed89d10e01c  rack1
```

Если каждая строка начинается со значения **UN** (Up/Normal), все узлы функционируют normally. В этом случае чтобы удалить узел, воспользуйтесь инструкцией из раздела [**10.6.4.2.**](#)

Если удаляемый узел имеет состояние, отличное от **UN**:

-
- **DN, DL, DJ** или **DM** — узел выключен. Включите узел и дождитесь его загрузки, после чего повторите проверку состояния.
 - **UJ** — узел присоединяется к кластеру. Дождитесь завершения операции и выполните все шаги инструкции из раздела [10.6.4.2](#).
 - **UL** — узел покидает кластер Cassandra. Дождитесь завершения операции, после чего выполните все шаги инструкции из раздела [10.6.4.2](#), начиная с пункта 3.
 - **UM** — узел переносит свои данные на другой. Дождитесь завершения операции и выполните все шаги инструкции из раздела [10.6.4.2](#), начиная с пункта 3.

Если данные Cassandra утеряны или не удается привести узел в нормальное состояние, для удаления узла воспользуйтесь инструкцией из раздела [10.6.4.3](#).

10.6.4.2. Удаление узла в нормальном состоянии

Для удаления узла из кластера Cassandra:

1. Перенесите данные Cassandra на другой узел с помощью скрипта **nodetool**:

```
# /opt/dozor/cassandra/bin/nodetool --host --ssl <имя удаляемого узла>
decommission
```

2. На главном узле (master-host) уточните идентификатор (ID) удаляемого узла с помощью команд:

```
# /opt/dozor/bin/shell
```

```
# cat /data/repos/dozor/config-base.git/cluster.json
```

```
{
  "nodes": [ {
    "name": "main",
    "hostname": "master.solar.local",
    "id": "c34a294b-cc07-4088-8c52-c69fc181345c",
    "roles": [ "kerberos", "analyzer", "network-config", "master", "http-filter", "antivirus" ],
    "services": [ {
      "name": "database" ,
```

3. На главном узле (master-host) удалите требуемый узел с помощью команды:

```
# unreg-slave <идентификатор узла>
```

```
ds-mode@bvm224 /opt/dozor # unreg-slave c34a294b-cc07-4088-8c52-c69fc181345c
```

где **bvm224** — главный узел (master);

unreg-slave — удаляемый узел;

c34a294b-cc07-4088-8c52-c69fc181345c — идентификатор (ID) удаляемого узла.

4. Убедитесь, что в файле конфигурации отсутствует удаляемый узел с помощью команды:

```
# cat /data/repos/dozor/config-base.git/cluster.json
```

-
5. Удалите Solar webProxy с удаляемого узла. Для этого выполните все шаги инструкции из раздела [4.5](#).
 6. Перезапустите Cassandra на главном узле (master-host) командой (запуск из shell):

```
# dsctl restart skvt-cassandra
```

Для диагностики используйте скрипт **nodetool**, который запускается из командной оболочки Solar webProxy . Запускайте команду на каждом узле, ответы на всех должны быть одинаковыми:

```
ds-mode@avm239 /opt/dozor # /opt/dozor/cassandra/bin/nodetool --ssl bvm224 status
Note: Ownership information does not include topology; for complete information, specify a keyspace
Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address Load Owns Host ID Token Rack
UN 10.31.7.224 169.13 KB 45.6% ea06d8cb-5657-4b84-8545-2ce8b378e31c
-9089968438401001742 rack1
UN 10.31.6.239 120.11 KB 54.4% 9a6e5a5c-6988-4fbd-9cec-375f29cb698d
-9193948100233974008 rack1

ds-mode@bvm224 /opt/dozor # /opt/dozor/cassandra/bin/nodetool --ssl avm239 status
Note: Ownership information does not include topology; for complete information, specify a keyspace
Datacenter: datacenter1
=====
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
-- Address Load Owns Host ID Token Rack
UN 10.31.7.224 169.13 KB 45.6% ea06d8cb-5657-4b84-8545-2ce8b378e31c
-9089968438401001742 rack1
UN 10.31.6.239 120.11 KB 54.4% 9a6e5a5c-6988-4fbd-9cec-375f29cb698d
-9193948100233974008 rack1
```

10.6.4.3. Удаление узла в других случаях

Если данные Cassandra утеряны или не удается привести узел в нормальное состояние:

1. На главном узле (master-host) уточните идентификатор (ID) удаляемого узла с помощью команд:

```
# /opt/dozor/bin/shell
```

```
# cat /data/repos/dozor/config-base.git/cluster.json
```

```
{
  "nodes": [ {
    "name": "main",
    "hostname": "master.solar.local",
    "id": "c34a294b-cc07-4088-8c52-c69fc181345c",
    "roles": [ "kerberos", "analyzer", "network-config", "master", "http-filter", "antivirus" ],
    "services": [ {
      "name": "database" ,
```

2. На любом другом узле выполните команду:

```
ds-mode@bvm224 /opt/dozor # /opt/dozor/cassandra/bin/nodetool --ssl bvm224 removenode  
c34a294b-cc07-4088-8c52-c69fc181345c
```

где **bvm224** — имя этого узла, **c34a294b-cc07-4088-8c52-c69fc181345c** — идентификатор (ID) удаляемого узла.

3. На всех остальных узлах по очереди выполните команду:

```
# /opt/dozor/cassandra/bin/nodetool --ssl <hostname> repair
```

где **<hostname>** — имя узла, на котором выполняется команда.

4. Удалите Solar webProxy с удаляемого узла. Для этого выполните все шаги инструкции из раздела [4.5](#).
5. Перезапустите Cassandra на главном узле (master-host) командой (запуск из shell):

```
# dsctl restart skvt-cassandra
```

Для диагностики используйте скрипт **nodetool**, который запускается из командной оболочки Solar webProxy. Запускайте команду на каждом узле, ответы на всех должны быть одинаковыми:

```
ds-mode@avm239 /opt/dozor # /opt/dozor/cassandra/bin/nodetool --ssl bvm224 status  
Note: Ownership information does not include topology; for complete information, specify a keyspace  
Datacenter: datacenter1  
=====  
Status=Up/Down  
/| State=Normal/Leaving/Joining/Moving  
-- Address Load Owns Host ID Token Rack  
UN 10.31.7.224 169.13 KB 45.6% ea06d8cb-5657-4b84-8545-2ce8b378e31c  
-9089968438401001742 rack1  
UN 10.31.6.239 120.11 KB 54.4% 9a6e5a5c-6988-4fbd-9cec-375f29cb698d  
-9193948100233974008 rack1
```

```
ds-mode@bvm224 /opt/dozor # /opt/dozor/cassandra/bin/nodetool --ssl avm239 status  
Note: Ownership information does not include topology; for complete information, specify a keyspace  
Datacenter: datacenter1  
=====  
Status=Up/Down  
/| State=Normal/Leaving/Joining/Moving  
-- Address Load Owns Host ID Token Rack  
UN 10.31.7.224 169.13 KB 45.6% ea06d8cb-5657-4b84-8545-2ce8b378e31c  
-9089968438401001742 rack1  
UN 10.31.6.239 120.11 KB 54.4% 9a6e5a5c-6988-4fbd-9cec-375f29cb698d  
-9193948100233974008 rack1
```

10.7. Изменение доменного имени

При необходимости изменения hostname выполните следующие действия:

1. Выполните команду:

```
# hostnamectl set-hostname newhostname.domain.domain
```

где **newhostname.domain.domain** указано новое имя узла и домен.

2. Внесите изменения в файле:

```
# vi /etc/hosts
```

в файле измените имя для master-узла (например, с **wp.solar.local** на **newhostname.domain.domain**).

3. Проверьте новое имя:

```
# hostname -f
```

4. Измените имя в конфигурации:

- Необходимо узнать идентификатор инсталляции (ID узла):

```
# /opt/dozor/bin/shell
```

```
# get-role
```

В строке **node-id** появится идентификатор узла.

- После выполните команды:

```
# config cluster update-node -i <node-id> -h <hostname>
```

, где **node-id** – идентификатор узла, а **hostname** – новое имя узла.

```
# cd /data/repos/dozor/config-base.git
```

```
# git add cluster.json
```

```
# git commit -m 'change hostname'
```

```
# chown -R dozor:dozor /data/repos/dozor/config-base.git
```

5. Замените сертификат:

```
# /opt/dozor/bin/shell
```

```
# rm -rf /opt/dozor/etc/ssl/*
```

```
# cert /opt/dozor/etc/ssl/bus.key /opt/dozor/etc/ssl/bus.pem
```

Примечание

Если Solar webProxy установлен на нескольких узлах, после генерации на master-узле новых ключей необходимо заново выполнить регистрацию slave-узлов.

6. Перезагрузите ПК Solar webProxy:

```
# /opt/dozor/bin/shell
```

```
# dsctl down
```

```
# dsctl boot
```

accept-settings

11. Настройка авторизации в веб-интерфейсе с учетной записью в домене

Для настройки аутентификации с доменной учетной записью (речь идет о любом виде basic-аутентификации):

1. В разделе **Аутентификация > Источники Basic-аутентификации** основных настроек конфигурации установите флажок **Включить источник аутентификации** и для параметра **Тип источника** выберите значение **Idap**.
2. Заполните появившиеся поля аналогично тому, как показано на [Рис.11.1](#):

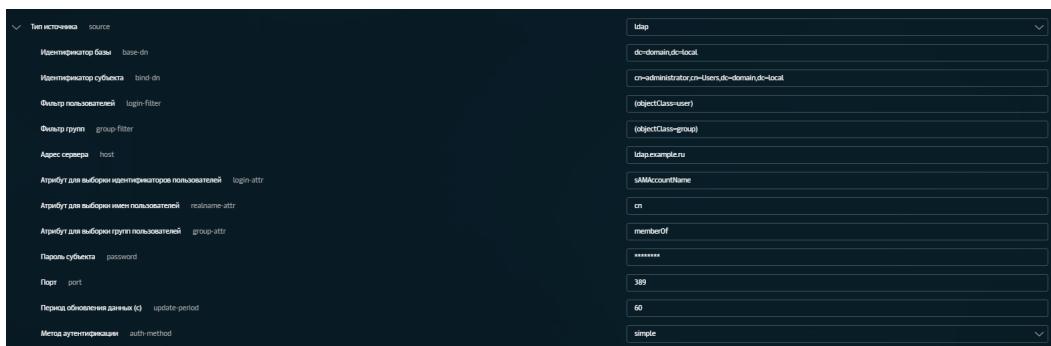


Рис. 11.1. Настройки сервера Active Directory

Параметр **Идентификатор субъекта** также можно задать в формате **administrator@ad.local**.

3. Создайте доменную учетную запись пользователя согласно инструкции раздела *Создание учётной записи пользователя* документа *Руководство администратора безопасности*. Имя создаваемой учетной записи должно совпадать с именем учетной записи в Active Directory.

Внимание!

Функция смены пароля для доменных учетных записей недоступна в веб-интерфейсе.

12. Выпуск сертификата организации для веб-интерфейса

Если в организации имеется собственный УЦ, можно использовать его сертификат для установления соединения с GUI Solar webProxy. Для выпуска сертификата организации на master-узле Solar webProxy:

1. В CLI перейдите во временный каталог (например, `/var/tmp/`), выполнив команду:

```
# cd /var/tmp
```

2. Создайте ключ ECDSA, выполнив команду:

```
# openssl genrsa -out wp.key -aes256 2048
```

Во время выполнения команды система потребует назначить пароль для ключа. Введите пароль и запомните его. После ввода подтвердите пароль.

3. Создайте в текущем каталоге файл с именем `openssl.cnf` и добавьте в него данные:

```
[ req ]  
req_extensions = v3_req  
distinguished_name = req_distinguished_name  
prompt=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 значения параметров замените на актуальные значения 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.

4. Сгенерируйте запрос на подпись сертификата, выполнив команду:

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

В процессе выполнения команды система потребует ввести пароль, заданный на шаге 2.

5. На сервере организации, имеющем роль CA (Certification Authority), проверьте используемый алгоритм шифрования. Для этого откройте программу **Командная строка** от имени администратора и выполните в ней следующую команду:

```
certutil -getreg ca \ csp \ CNGHashAlgorithm
```

Если значение параметра **REG_SZ** равно **SHA1**, выполните команды:

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
```

```
net stop CertSvc && net start CertSvc
```

6. Перевыпишите корневой сертификат и перезапустите службу Certificate Services, выполнив следующие команды:

```
certutil -renewCert ReuseKeys
```

```
net stop CertSvc && net start CertSvc
```

7. Зайдите на портал УЦ Windows.

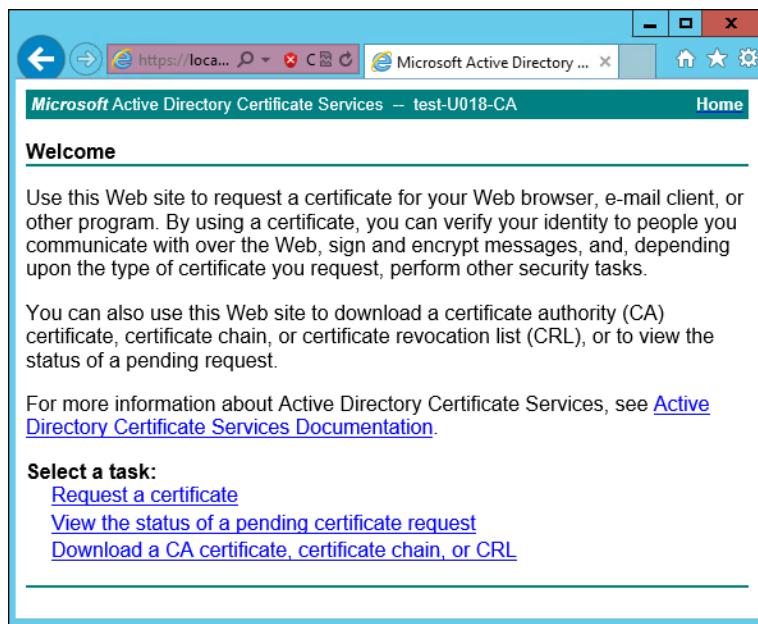


Рис. 12.1. Экран приветствия УЦ Windows

8. Нажмите **Request a certificate**.

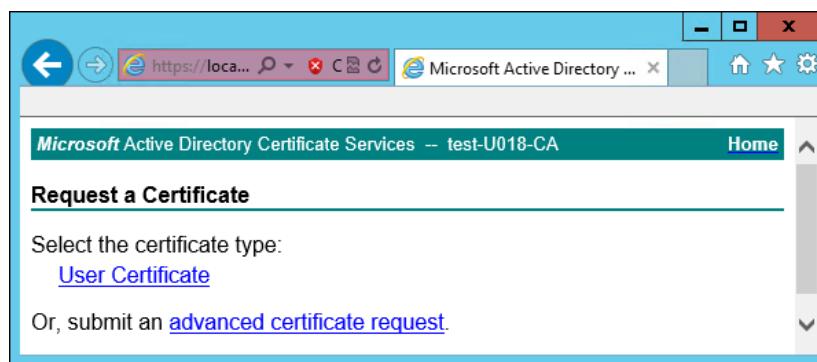


Рис. 12.2. Экран запроса сертификата

9. Нажмите **advanced certificate request**.

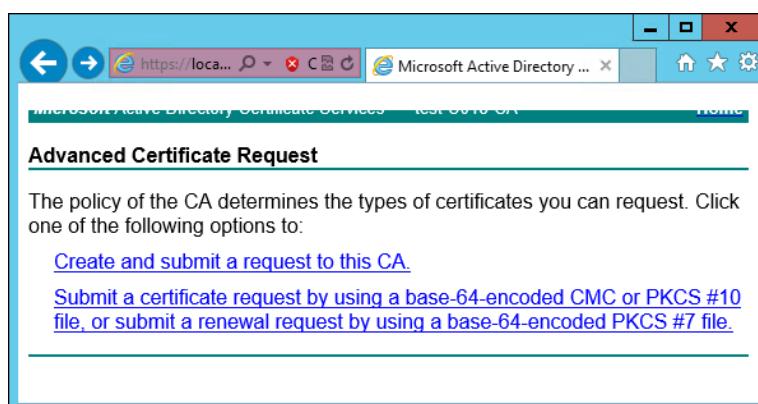


Рис. 12.3. Экран особого запроса сертификата

10. Нажмите **Submit a certificate request by using....**

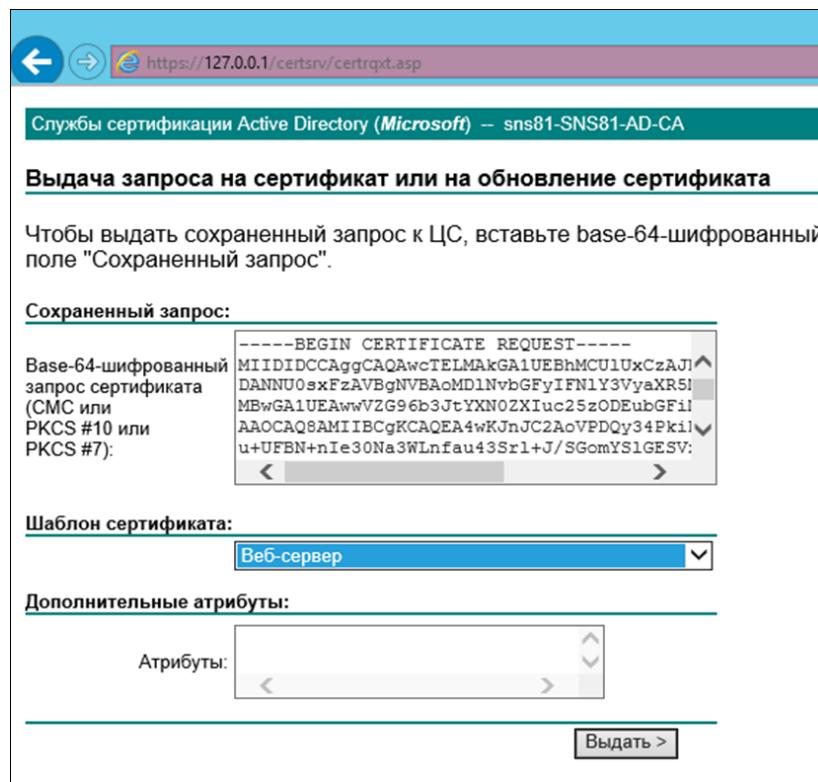


Рис. 12.4. Экран атрибутов сертификата

11. Выберите шаблон сертификата **Веб-сервер** и вставьте в поле **Base-64** содержимое файла, созданного на шаге 4. Нажмите **Выдать**.

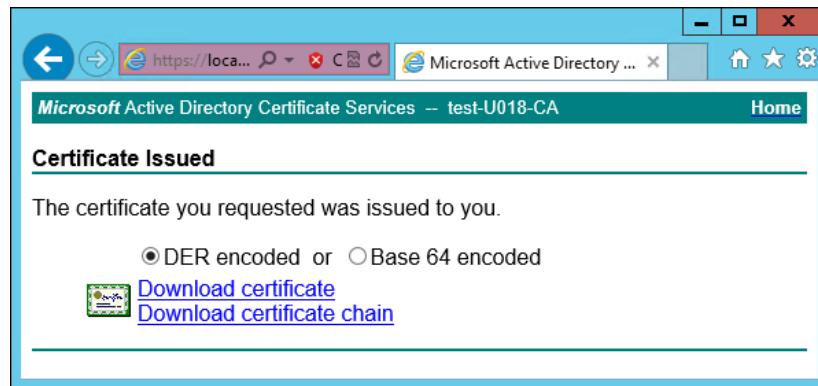


Рис. 12.5. Экран выдачи сертификата

12. Нажмите **Download certificate**. Сохраните файл сертификата с именем **wp.cer** во временный каталог, выбранный на шаге 1.

13. Перейдите на главную страницу портала УЦ и нажмите **Download a CA certificate, certificate chain or CRL**. Сохраните сертификат УЦ с именем **ca.cer** в тот же каталог.

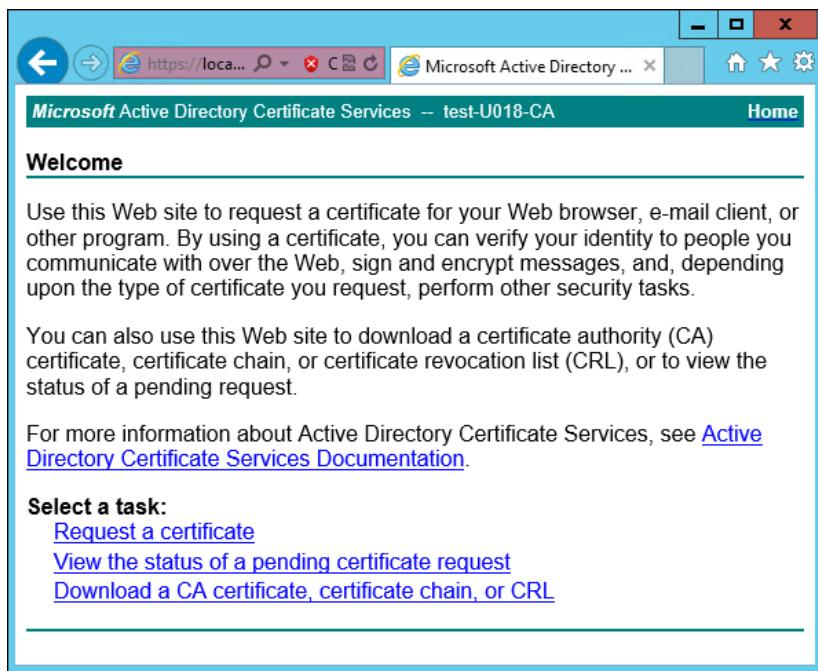


Рис. 12.6. Экран приветствия УЦ Windows

14. Вернитесь в CLI Solar webProxy, перейдите в выбранный временный каталог и сконвертируйте загруженные сертификаты в формат PEM, выполнив команды:

```
# openssl x509 -inform der -in wp.cer -out wp.pem
```

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

15. Объедините сертификаты и ключ в сертификат pkcs12, выполнив команду:

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

Во время выполнения команды система потребует ввести пароль.

16. Импортируйте Java-хранилище сертификатов, выполнив команду вида:

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

где <password> – выбранный пароль.

17. Скопируйте Java-хранилище в каталог Solar webProxy, выполнив команду:

```
# cp WEB.jks /opt/dozor/skvt/var/lib/
```

18. Смените владельца хранилища, выполнив команду вида:

```
# chown dozor:dozor /opt/dozor/skvt/var/lib/WEB.jks
```

19. Проверьте, что сертификат находится в хранилище, выполнив команду вида:

```
# keytool -list -keystore /opt/dozor/skvt/var/lib/WEB.jks
```

О наличии сертификата в хранилище будет свидетельствовать вывод:

```
1, Jul 10, 2018, PrivateKeyEntry,  
Certificate fingerprint (SHA-256): B2:03:57:46:8E:61:02:D0:0C:55:28:06:33:72:88:F1:AB:E0:4D:9C
```

20. В GUI в разделе **Система > Расширенные настройки > Интерфейс > Сервер веб-интерфейса** задайте значения параметров:

- Путь к хранилищу ключей –
`/opt/dozor/skvt/var/lib/WEB.jks`
;
- Пароль к хранилищу ключей – пароль.

21. Перезапустите сервис **skvt-play-server**, выполнив в CLI команды:

```
# /opt/dozor/bin/shell
```

```
# dsctl restart skvt-play-server
```

13. Настройка передачи информации в пользовательский сервер Zabbix

Примечание

В Solar webProxy нельзя изменять настройки внутреннего мониторинга, который используется с настроенными параметрами, собственными скриптами и т.д. Для работы с собственными параметрами мониторинга используйте дополнительный сервер Zabbix (пользовательский сервер мониторинга) с отправкой на него информации с Solar webProxy и созданием на нем необходимых схем мониторинга.

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

1. В разделе **Система > Расширенные настройки > Настройки мониторинга > Агенты мониторинга** задайте значения параметров:
 - **Порт** – 10050
 - **Пользовательский сервер мониторинга** – пользовательские серверы мониторинга, используемые для пассивных проверок (упрощенных запросов). В качестве значения можно задавать список IP-адресов или имен узлов через запятую, допускается использование маски CIDR в формате X.X.X.X/N. Пример значений: 127.0.0.1, 192.168.1.0/24, ::1, 2001:db8::/32, zabbix.domain.
 - **Тип проверки доступа в интернет** – тип авторизации для тестирования соединения с сетью Интернет. Принимает значения: **OFF** (выключено), **Simple** (для авторизации Basic или по IP), **NTLM** (для NTLM-авторизации) и **Negotiate** (для Kerberos-авторизации).
 - **Прокси-сервер для проверки доступа в интернет (как для пользователей)** – адрес и порт прокси-сервера, используемого для доступа к интернету. При использовании Kerberos-авторизации следует указывать только FQDN прокси-сервера (не localhost).
 - **Пользователь для проверки доступа в интернет** – учетная запись (УЗ) пользователя для тестирования соединения с интернетом. Раз в 40 секунд под этой УЗ будут выполняться попытки соединения с сайтами yandex.ru, mail.ru и google.ru. Указанные сайты должны быть доступны для этой УЗ.
 - **Реакция при срабатывании bypass сценария** – доступные значения: **Остановка сервисов** – подходит для исключения узла из балансировки (в том числе WCCP); **Перезапуск сервисов** – подходит для перезапуска фильтрующего ядра.

Для сбора дополнительной статистики по параметрам из каталога */etc/zabbix/zabbix_agentd.d/* установите флагок **Выход отладочной информации**.

2. Нажмите **Сохранить** и **Применить**.

Примечание

Для взаимодействия с агентом Zabbix использует протокол на основе JSON.

Zabbix воспринимает до 16 МБ данных, закодированных в Base64, в формате XML, но одиночное декодированное значение должно быть не больше 64 КБ, иначе значение будет обрезано до 64 КБ в процессе декодирования.

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

Примечание

За рекомендациями относительно настройки **Userparameter** обращайтесь к руководству по Zabbix.

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.

14. Мониторинг системы

Мониторинг системы доступен на вкладке **Мониторинг** раздела **Система**.

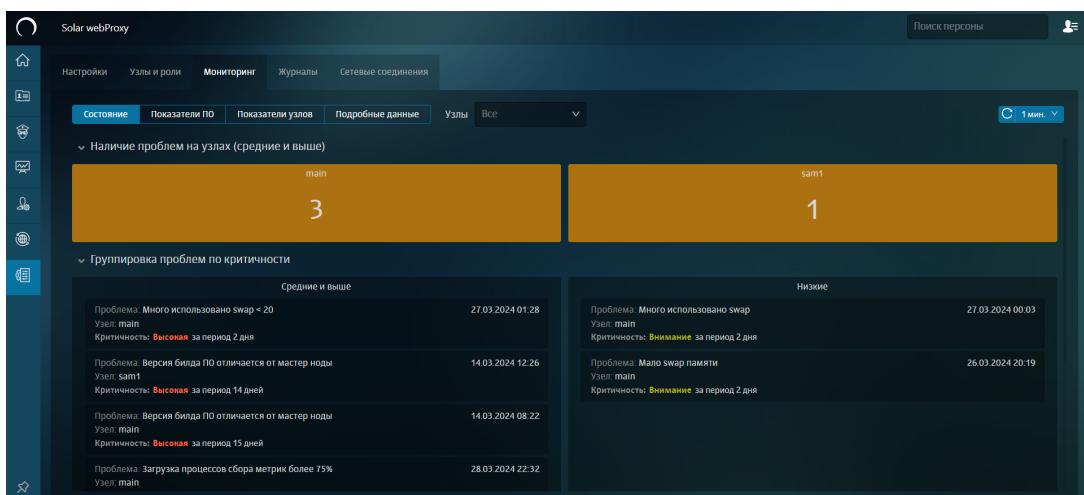
14.1. Состояние узлов кластера

На вкладке **Состояние** представлена информация о состоянии узлов кластера.

В верхней части расположен список узлов для отображения. По умолчанию отображаются все узлы. Для отображения определенного набора узлов откройте список узлов и выделите курсором все требуемые узлы. Сбросить группировку можно с помощью значка .

Состояние узла отображается как **OK**, если в настоящий момент на нем нет проблем с уровнем критичности **Средняя** или выше. Если на узле есть проблемы с уровнем критичности **Средняя** или выше, в соответствующем прямоугольном блоке отображается их количество.

В нижней части расположены списки проблем всех выбранных узлов: слева – с уровнем критичности **Средняя** и выше, справа – с уровнем критичности **Низкая**.



Средние и выше	Низкие
Проблема: Много использовано swap < 20 Узел: main Критичность: Высокая за период 2 дня	Проблема: Много использовано swap Узел: main Критичность: Внимание за период 2 дня
Проблема: Версия бинда ПО отличается от мастер ноды Узел: sam1 Критичность: Высокая за период 14 дней	Проблема: Мало swap памяти Узел: main Критичность: Внимание за период 2 дня
Проблема: Версия бинда ПО отличается от мастер ноды Узел: main Критичность: Высокая за период 15 дней	
Проблема: Загрузка процессов сбора метрик более 75% Узел: main	

Рис. 14.1. Вкладка «Состояние»

14.2. Мониторинг показателей Solar webProxy

На вкладке **Показатели ПО** представлена информация о работе Solar webProxy на узлах кластера.

В верхней части расположен список узлов для отображения и инструмент для выбора временного отрезка, за который необходимо получить данные.

Ниже расположены блоки с названиями узлов. Принцип их отображения такой же, как и на вкладке **Состояние**.

В нижней части расположены графики:

- **Наличие проблем на узлах (средние и выше);**
- **Количество уникальных персон на узлах фильтрации (в минутах);**

-
- Время загрузки сайтов напрямую (без прокси);
 - Время загрузки сайтов через узлы фильтрации;

Примечание

Из-за отключенной проверки доступа в интернет для агентов мониторинга на графике **Время загрузки сайтов через узлы фильтрации** может не быть данных. Чтобы данные отображались, в разделе **Система > Основные настройки > Мониторинг > Агенты мониторинга** для параметра **Тип проверки доступа в интернет** установите значение, отличное от **OFF** (например, **Simple**).

-
- Коды загрузки сайтов;
 - База статистики.

На каждом графике можно выбрать определенный интервал для отображения на всю длину шкалы. Для этого поместите курсор в один из концов требуемого интервала и с зажатой левой кнопкой мыши переместите курсор к другому концу интервала, а затем отпустите кнопку мыши.

14.3. Мониторинг показателей аппаратного обеспечения

На вкладке **Показатели узлов** представлена информация о состоянии аппаратного обеспечения узлов кластера.

В верхней части расположен список узлов для отображения и инструмент для выбора временного отрезка, за который необходимо получить данные.

Ниже расположены блоки с названиями узлов (см. далее). Принцип их отображения такой же, как и на вкладке **Состояние**.

Табл. 14.1. Блоки данных вкладки "Показатели узлов"

Блок	Описание
Время работы	Время непрерывной работы узла, прошедшее с момента последней перезагрузки (включения)
Средняя загрузка (load average)	Значение Load average за последнюю минуту в выводе команды top на узле
Количество ядер ЦПУ	Количество ядер процессора на узле
Доступно памяти	Объем свободной оперативной памяти на узле

Ниже расположена группа графиков для каждого выбранного узла, отображающих следующие данные (см. далее).

Табл. 14.2. Группа графиков выбранного узла

График	Описание
ЦПУ	История загрузки процессора
Память	История потребления оперативной памяти
Свободное место для разделов	Свободное пространство на жестком диске в процентах

График	Описание
Свободные индексные дескрипторы для разделов	Количество свободных индексных дескрипторов для разделов на файловой системе в процентах
Свободное место для разделов	Свободное пространство на жестком диске в абсолютном исчислении
Активное время дисков	Процент, отражающий время, которое жесткий диск занят чтением/записью
Количество операций чтения/записи на дисках в секунду	Количество операций ввода-вывода в секунду, выполняемых системой хранения данных
Время ожидания чтения/записи дисков	Время, затрачиваемое на операции ожидания чтения и записи дисков в миллисекундах
Объем чтения/записи на дисках в секунду	Объем жесткого диска, занимаемый операциями чтения/записи
Сетевой трафик	История скорости передачи данных через сетевые интерфейсы узла

14.4. Подробные данные

В разделе **Система > Мониторинг > Подробные данные** системный администратор может построить отчеты по необходимым статистическим показателям, выбрав определенный набор узлов и период времени.

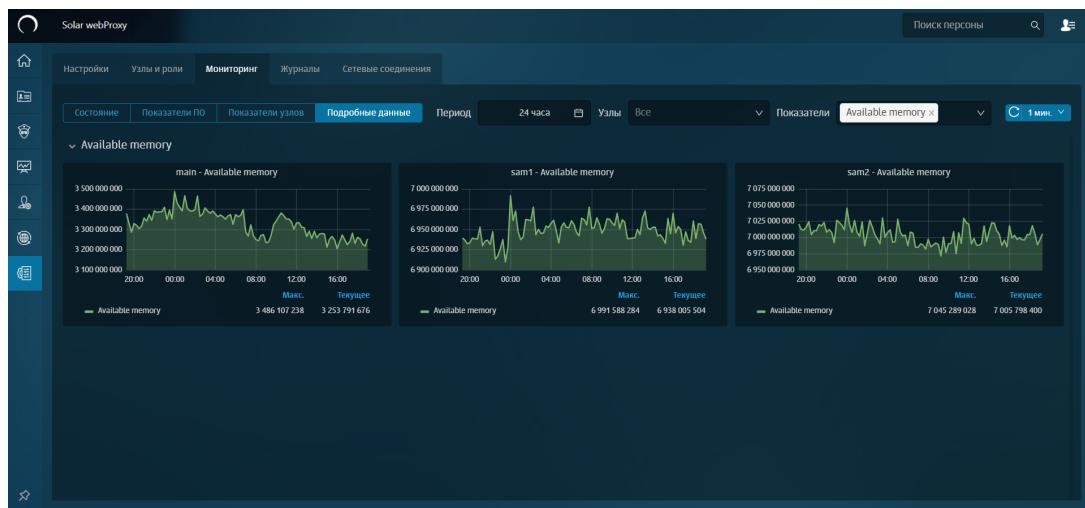


Рис. 14.2. Вкладка «Подробные данные»

Для построения отчетов по конкретным показателям в выпадающем списке выделите курсором необходимые показатели.

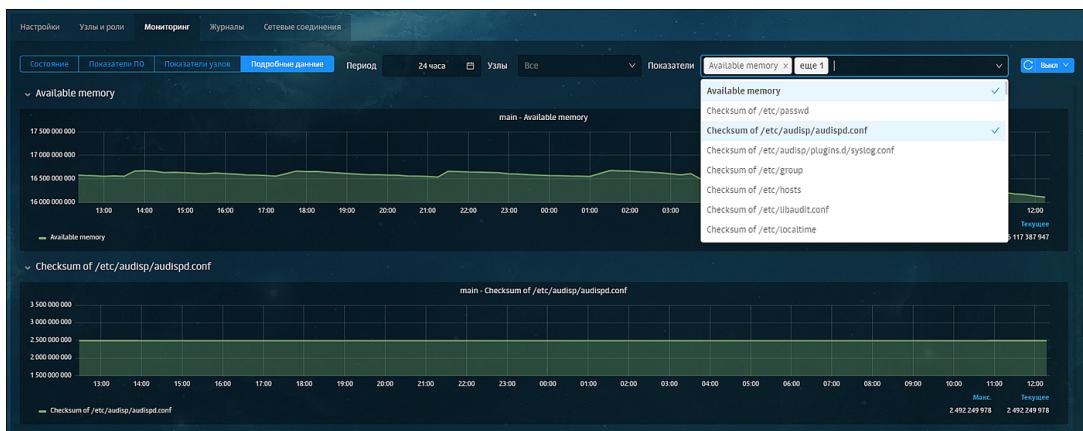


Рис. 14.3. Выбор показателей для построения отчетов

14.5. Журналы событий: просмотр записей журнальных файлов в интерфейсе

Журналы событий содержат информацию о действиях пользователей и работе системы, которая представлена в интерфейсе в форме записей журнальных файлов на вкладке **Журналы** раздела **Система**.

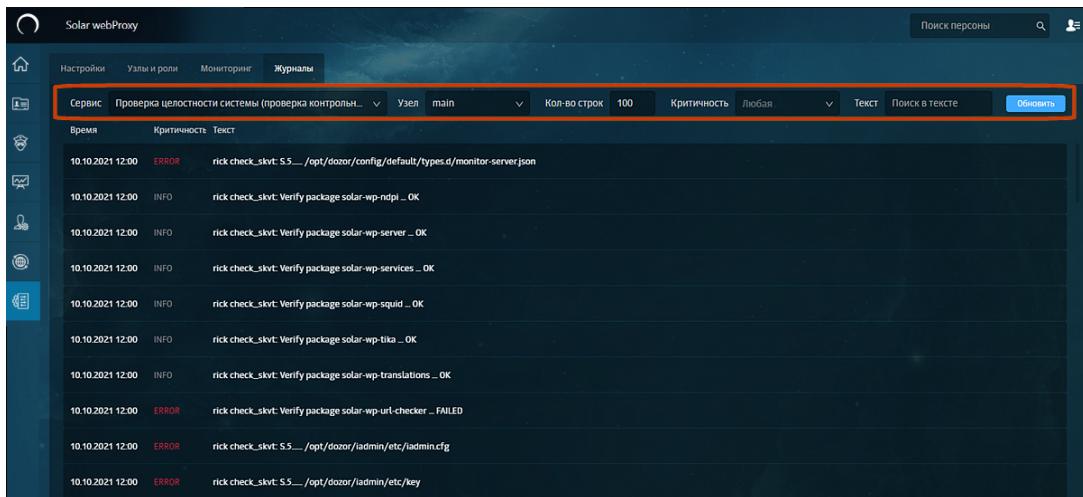


Рис. 14.4. Журнал событий

На вкладке **Журналы** можно просмотреть информацию по следующим сервисам и категориям информации о работе системы:

- **Сервер аутентификации:** параметры аутентификации и ошибки генерации ключа для аутентификации;
- **Веб-сервер:** активность администратора и внесенные в политику изменения (перечень журналируемых действий описан в приложении *Аудит действий пользователей Solar webProxy*);
- **HTTP и SOCKS5-фильтр:** состояние фильтрации трафика и возникшие ошибки взаимодействия;
- **Системные сообщения:** события, произошедшие в системе с момента ее запуска;

- **Проверка целостности системы:** контрольные суммы файлов (установочных пакетов) и ошибки при их подсчете;
- **Безопасность операционной системы:** события, произошедшие в операционной системе;
- **Межсетевое экранирование:** срабатывание правил политики.

Отобразить информацию по конкретной категории можно, выбрав соответствующий фильтр из списка в поле **Сервис**.

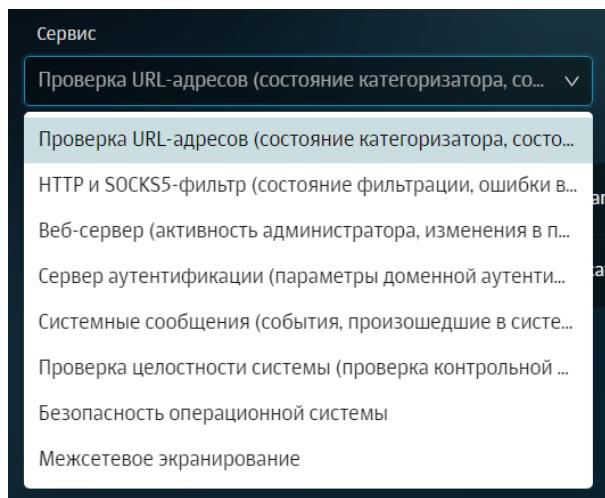


Рис. 14.5. Фильтры журнала событий

Для настройки более детального отображения сведений воспользуйтесь другими фильтрами в верхней части раздела, с помощью которых можно выбрать:

- узел, для которого будут отображаться журнальные записи;
- число выводимых записей журнальных файлов;
- критичность отображаемого события:
 - **Info** – информационная запись;
 - **Warning** – предупреждение, выводится в том случае, если обнаружено некое несоответствие ожидаемому поведению;
 - **Error** – запись об ошибке, позволяющей продолжить нормальное функционирование подсистемы;
 - **Debug** – отладочная информация.

Вы можете отсортировать информацию по дате и времени обновления от ранней до поздней и наоборот. Для этого воспользуйтесь фильтром **Время**. По умолчанию события, произошедшие раньше, отображаются наверху.

Также вы можете воспользоваться поиском по тексту, указав искомое слово в поле **Текст**.

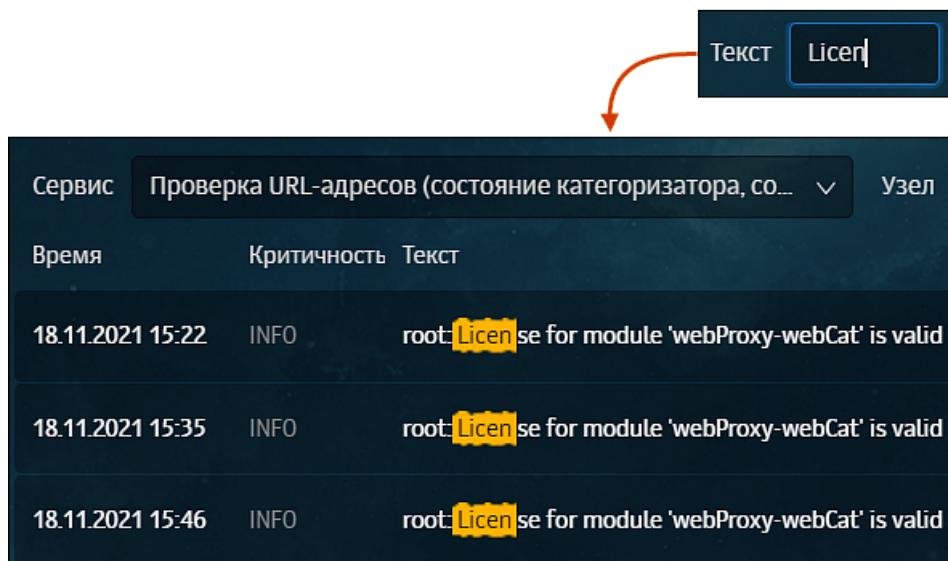


Рис. 14.6. Поиск по тексту в журнале событий

Для сервиса **Веб-сервер** с помощью фильтра **Категория** можно выбрать список выводимых данных:

- **Любой** – все события веб-сервера;
- **User actions** – все события, связанные с действиями пользователей (изменение лицензии, ролей, атрибутов в Досье и применение правил/исключений из раздела **Политика**).

Для работы с журналами событий реализована правовая модель доступа, которая основана на разграничении данных по категориям журналов событий:

- **системные** (сведения о работе сервиса управления, кэш-сервиса, сервиса фильтрации трафика, сервиса проверки URL по категориям и системного файла «messages»);
- **фильтрации** (сведения о срабатывании правил политики: слои **Фильтр транзитного трафика**, **Фильтр входящего трафика**, **Фильтр исходящего трафика** и **Трансляция адресов**);
- **безопасности** (сведения о работе сервиса управления, кэш-сервиса, сервисов NTLM- и Kerberos-аутентификации, сервиса аутентификации).

Пользователь может просмотреть записи только тех категорий журналов, права на которые ему выданы. Все доступные для просмотра журналы отображаются в списке фильтров поля **Сервис**.

Подробную информацию приведена в документе *Руководство администратора безопасности*.

14.6. Просмотр сетевых соединений

Таблица сетевых соединений содержит сведения о состоянии фактических сетевых соединений и слушаемых на выбранном узле портах. А также, для отображения статистических данных по сетевым интерфейсам и протоколам (например, TCP, UDP и т. д.).

Просмотреть сведения о соединениях можно в разделе **Система > Сетевые соединения** ([Рис.14.7](#)).

ID	Состояние	Протокол	Источник	Порт источника	Назначение	Порт назначения
469385536	ESTABLISHED	tcp	127.0.0.1	60016	127.0.0.1	5434
469385216	ESTABLISHED	tcp	192.168.205.200	62373	185.5.137.235	443
3659259072	ESTABLISHED	tcp	10.201.29.13	39721	10.201.28.205	7001
3258876864	ESTABLISHED	tcp	10.201.28.205	42050	10.201.28.205	2269
2168695936	ESTABLISHED	tcp	127.0.0.1	36476	127.0.0.1	5434
1992349952	ESTABLISHED	tcp	127.0.0.1	36526	127.0.0.1	5434
3809586304	ESTABLISHED	tcp	127.0.0.1	37012	127.0.0.1	5434
1338615680	ESTABLISHED	tcp	127.0.0.1	43624	127.0.0.1	5434
53102464	ESTABLISHED	tcp	127.0.0.1	32952	127.0.0.1	5434
2855237248	ESTABLISHED	tcp	127.0.0.1	36439	127.0.0.1	5434
443160512	ESTABLISHED	tcp	10.199.164.5	49161	10.201.28.205	8443

Рис. 14.7. Таблица сетевых соединений

Для управления отображаемой информацией используйте фильтры, расположенные над таблицей ([Рис.14.8](#)).

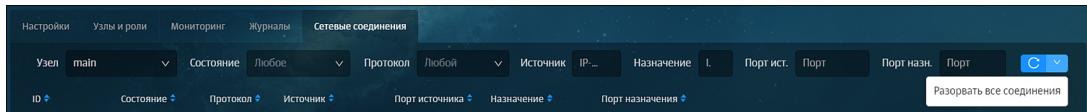


Рис. 14.8. Фильтры таблицы сетевых соединений

С помощью фильтров можно найти следующие виды информации о соединении:

- узел, на котором установлено соединение;
- состояние соединения: установлено, ожидает, закрыто или нет информации;
- протокол;
- источник и/или назначение;
- используемые порты для передачи трафика.

Для сброса соединений нажмите кнопку **Разорвать все соединения** в правом верхнем углу ([Рис.14.8](#)).

Содержимое таблицы можно отсортировать по выбранному столбцу, нажав на его название или счетчик рядом с его названием.

15. Проверка работоспособности настроенного Solar webProxy

Для успешной работы настроенного Solar webProxy выполните проверки, перечисленные в [Табл. 15.1](#).

Табл. 15.1. Проверки работоспособности системы

№	Проверка	Действия
1.	Состояние узлов и назначение ролей	В разделе Система > Узлы и роли проверьте наличие условий: <ul style="list-style-type: none">отображаются все узлы кластера;состояние каждого узла: Узел доступен.
2.	Наличие уведомлений и работа мониторинга	В разделе Система > Мониторинг проверьте наличие условий: <ul style="list-style-type: none">на виджетах не отображаются ошибки;на странице отсутствуют надписи: Нет данных.
3.	Интеграция Досье с внешними источниками	В разделе Досье > Персоны проверьте наличие условий: <ul style="list-style-type: none">список персон организации актуален;отсутствуют ошибки связи с источником.
4.	Работа категоризатора	В разделе Политика > База категоризации проверьте отображение результатов проверки ресурсов на корректность: <ul style="list-style-type: none">название категоризатора;категория ресурса.
5.	Вскрытие HTTPS	<ol style="list-style-type: none">В разделе Политика > Вскрытие HTTPS создайте правило на вскрытие.Проверьте соблюдение условий:<ul style="list-style-type: none">При посещении ресурса через прокси-сервер сертификат на пользовательском АРМ должен совпадать с сертификатом, указанным в конфигурации системы.В Журнале запросов раздела Статистика должен быть виден мониторинг URL ресурсов (параметр URL путь). <p>Следует учесть, что внешнее ПО, например DLP-система Solar Dozor, может использовать свой самоподписанный сертификат.</p>
6.	Работа антивируса	<ol style="list-style-type: none">В разделе Политика > Перенаправление по ICAP проверьте или сформируйте правило для перенаправления трафика в антивирус (см. раздел 6.2).Проверьте работу вскрытия HTTPS-трафика (см. выше).Перейдите с клиента через прокси-сервер (порт 2270) по адресу https://www.eicar.org/download-anti-malware-testfile/ и скачайте тестовый вирус eicar:<ul style="list-style-type: none">если в браузере отображается страница блокировки, антивирус успешно работает;если тестовый вирус загружается на компьютер, проверьте мониторинг URL ресурсов (параметр URL путь) в Журнале запросов.

16. Аварийные ситуации

16.1. БД Clickhouse

БД Clickhouse в некоторых ситуациях может занимать всю предоставленную оперативную память и приостанавливать свою работу в ожидании освобождения дополнительного объема памяти. Это связано с внутренними значениями лимита на использование памяти по умолчанию, которые могут превосходить объем доступной памяти на конкретном узле Solar webProxy. Примеры штатной и аварийной работы БД Clickhouse приведены ниже.

```
ds-mode@w4-test /opt/dozor # seelog clickhouse
2023-02-27 10:45:14.769649 [ 3355 ] {b0650665-6ca3-4eb0-bcbb-7b52c1f72162} <Information> execute
Query: Read 65 rows, 7.23 KiB in 0.001158538 sec., 56105 rows/sec., 6.10 MiB/sec.
2023-02-27 10:45:15.827912500 2023.02.27 10:45:15.827820 [ 3355 ] {36aeb9f8-c3a8-4958-ba60-67456a01a32f} <Information> execute
Query: Read 57 rows, 6.44 KiB in 0.001096656 sec., 51976 rows/sec., 5.73 MiB/sec.
2023-02-27 10:45:16.873188500 2023.02.27 10:45:16.873119 [ 3355 ] {f04a232f-cfb0-4704-b099-88a9e67fbeb7} <Information> execute
Query: Read 57 rows, 6.44 KiB in 0.001236975 sec., 46080 rows/sec., 5.08 MiB/sec.
2023-02-27 10:45:56.601389500 2023.02.27 10:45:56.601304 [ 3355 ] {7a1cfea9-968b-4e48-9f4f-d8c40bb8270b} <Information> execute
Query: Read 57 rows, 6.44 KiB in 0.001245457 sec., 45765 rows/sec., 5.05 MiB/sec.
2023-02-27 10:46:14.861591500 2023.02.27 10:46:14.861431 [ 3355 ] {41494cb0-f48c-4947-b865-478872b19963} <Information> execute
Query: Read 65 rows, 7.23 KiB in 0.001474526 sec., 44081 rows/sec., 4.79 MiB/sec.
2023-02-27 10:46:15.872268500 2023.02.27 10:46:15.871850 [ 3355 ] {c6f17a1e-324b-4f62-a267-1115f3cb7d3b} <Information> execute
Query: Read 57 rows, 6.44 KiB in 0.002029974 sec., 28079 rows/sec., 3.10 MiB/sec.
2023-02-27 10:46:16.887381500 2023.02.27 10:46:16.887305 [ 3355 ] {1e0e18ca-da02-4770-9b32-3ec458c143a9} <Information> execute
Query: Read 57 rows, 6.44 KiB in 0.00119806 sec., 47576 rows/sec., 5.25 MiB/sec.
2023-02-27 10:46:25.868645500 2023.02.27 10:46:25.868543 [ 3355 ] {8627a841-6da4-4f80-9eal-eacd326e631e} <Information> execute
Query: Read 375 rows, 16.39 KiB in 0.005815619 sec., 64481 rows/sec., 2.75 MiB/sec.
2023-02-27 10:46:26.952854500 2023.02.27 10:46:26.952754 [ 3355 ] {78c0aa82-733c-4691-96c5-a70883bb11d5} <Information> execute
Query: Read 375 rows, 19.41 KiB in 0.007591372 sec., 49398 rows/sec., 2.50 MiB/sec.
2023-02-27 10:46:56.660621500 2023.02.27 10:46:56.660512 [ 3355 ] {492d1b9-5189-49b0-87f0-a26b529cd4b5} <Information> execute
Query: Read 57 rows, 6.44 KiB in 0.001329225 sec., 42882 rows/sec., 4.73 MiB/sec.
```

Рис. 16.1. Штатная работа БД Clickhouse

```
2023-02-28 11:50:54.970153500 (version 21.4.3.21 (official build))
2023-02-28 11:50:58.415907500 2023.02.28 11:50:58.410280 [ 12288 ] {f4464421-8c9f-45a3-ae01-1a03b04da64b} <Error> executeQuery
: Code: 241, e.displayText() = DB::Exception: Memory limit (for query) exceeded: would use 8.18 MiB (attempt to allocate chunk
of 4366336 bytes), maximum: 4.03 MiB: (While reading the value of key req.pathname) (version 21.4.3.21 (official build)) (from
m 10.201.31.202:54818) (in query: INSERT INTO events FORMAT JSONEachRow ), Stack trace (when copying this message, always incl
ude the lines below):
2023-02-28 11:50:58.415940500
2023-02-28 11:50:58.415940500 0. DB::Exception::Exception(std::_1::basic_string<char, std::_1::char_traits<char>, std::_1::
allocator<char> > const&, int, bool) @ 0x88b64ca in /usr/bin/clickhouse
2023-02-28 11:50:58.415941500 1. DB::Exception::Exception<char const*, char const*, std::_1::basic_string<char, std::_1::cha
r_traits<char>, std::_1::allocator<char> >, long&, std::_1::basic_string<char, std::_1::char_traits<char>, std::_1::allocat
or<char> > >(int, std::_1::basic_string<char, std::_1::char_traits<char>, std::_1::allocator<char> > const&, char const&
, char const&, std::_1::basic_string<char, std::_1::char_traits<char>, std::_1::allocator<char> >&, long&, std::_1::bas
ic_string<char, std::_1::char_traits<char>, std::_1::allocator<char> >&) @ 0x88cae9 in /usr/bin/clickhouse
2023-02-28 11:50:58.415951500 2. MemoryTracker::alloc(long) @ 0x88ca86d in /usr/bin/clickhouse
2023-02-28 11:50:58.415951500 3. MemoryTracker::alloc(long) @ 0x88ca5d4 in /usr/bin/clickhouse
2023-02-28 11:50:58.415951500 4. Allocator<false, false>::realloc(void*, unsigned long, unsigned long, unsigned long) @ 0x8902
b26 in /usr/bin/clickhouse
2023-02-28 11:50:58.415951500 5. void DB::PODArray<char8_t, 4096ul, Allocator<false, false>, 15ul, 16ul>::insertPrepare<char
, char const>(char*, char const*) @ 0x89131fb in /usr/bin/clickhouse
2023-02-28 11:50:58.415954500 6. void DB::readJSONStringInto<DB::PODArray<char8_t, 4096ul, Allocator<false, false>, 15ul, 16ul
>, void>(DB::PODArray<char8_t, 4096ul, Allocator<false, false>, 15ul, 16ul>, DB::ReadBuffer&) @ 0x8907baf in /usr/bin/clickho
use
2023-02-28 11:50:58.415955500 7. DB::SerializationString::deserializeTextJSON(DB::IColumn&, DB::ReadBuffer&, DB::FormatSetting
s const&) const @ 0x107beb in /usr/bin/clickhouse
2023-02-28 11:50:58.415958500 8. DB::JSONEachRowRowInputFormat::readField(unsigned long, std::_1::vector<COW<DB::IColumn>::mu
table_ptr<DB::IColumn>, std::_1::allocator<COW<DB::IColumn>::mutable_ptr<DB::IColumn> >&) @ 0x1015a056 in /usr/bin/clickhou
se
2023-02-28 11:50:58.415962500 9. DB::JSONEachRowRowInputFormat::readJSONObject(std::_1::vector<COW<DB::IColumn>::mutable_ptr<
```

Рис. 16.2. Работа БД Clickhouse с ошибками, указывающими на превышение лимита памяти

Для решения этой проблемы:

1. Откройте конфигурационный файл `/data/repos/dozor/config-final.git/{node-id}/clickhouse/clickhouse.conf` для редактирования.
2. Отредактируйте значение параметра `max_memory_usage`, задав для него значение лимита памяти в байтах.
3. В том же разделе создайте параметры `max_memory_usage_for_user` и `max_memory_usage_for_all_queries` и задайте для них то же значение.
4. Сохраните и закройте файл.

5. Перезапустите процесс **clickhouse**, выполнив команды:

```
# /opt/dozor/bin/shell  
# dsctl restart clickhouse
```

17. Получение технической поддержки

Для получения консультации по техническим вопросам можно обратиться по адресу support@rt-solar.ru.

С условиями поддержки можно ознакомиться на сайте компании [«Ростелеком-Солар»](#) (по адресу: <http://solar-rt.ru/support>). При оформлении запроса укажите номер контракта на техническую поддержку, опишите проблему, укажите свое полное имя, адрес электронной почты и номер телефона.

Приложение А. Коды фильтрации политики

В данном приложении приведено описание возможных кодов фильтрации политики и их значений, которые можно увидеть в записях журнала **syslog**. Например, **FilterCodes=[11, 0, 0, 31]**.

Табл. А.1. HTTP-коды фильтрации

Код фильтрации	Значение	Описание действий
0	CONTINUE	Ничего не делать и продолжить обработку политикой дальше
1	ALLOW	Разрешить запрос/ответ
2	DENY	Заблокировать запрос/ответ и отобразить страницу с шаблоном блокировки
3	NOTIFY	Уведомить системного администратора
4	ARCHIVE	Архивировать журнальные файлы в сервис Clickhouse
5	CONFIRM	Запросить подтверждение
6	DETECT_DATATYPE	Определить MIME-тип данных (см. D.2)
8	MODIFY_HEADERS	Добавить, удалить и/или изменить значение заголовка
9	NOLOG	Не журналировать события в Clickhouse и siemlog
10	REDIRECT	Перенаправить на указанный в правиле URL
11	MITM	Вскрыть трафик
12	CHECK_CERTIFICATE	Проверить сертификат
30	BAD_NETWORK	Запрещенная сеть
31	NOT_AUTHORIZED	Не аутентифицировать пользователя
34	PROXY	Выбор направления трафика через вышестоящий прокси-сервер либо напрямую
35	BIND	Подставить исходящий IP-адрес
36	DSCP_SETUP	Установить DSCP-метку
37	WS_BLOCKING_NOTIFICATION	Модификация HTML-документа в виде добавления системы уведомления пользователя о блокировке протоколов WS и WSS
38	MESSAGE	Принудительный вывод страницы с сообщением об ошибке

Приложение В. Матрица МЭ Solar webProxy

Матрица сетевого доступа нужна для настройки сетевого оборудования и доступа к/из сети предприятия на месте установки Solar webProxy. В ней отражены рекомендуемые настройки МЭ Solar webProxy и корпоративной сети.

Табл. В.1. Перечень сетей

Сеть	Описание
Cluster int network	Внутренние подсети/диапазон адресов/VLAN для взаимодействия узлов кластера
Cluster ext network	Внешние подсети/диапазон адресов/VLAN для доступа к сети Интернет
Trusted networks	Защищаемые внутренние сети
Admin hosts/net	Диапазон адресов/подсеть АРМ администраторов
DCs	Подсеть/диапазон адресов/перечень узлов DC
DNS servers	Подсеть/диапазон адресов/перечень DNS-серверов (может включать внешние DNS-сервера)
DMZ	Сегмент зоны DMZ с публикуемыми веб-серверами
SIEM	Системы SIEM для сбора и обработки журналов в целях ИБ
Mail servers	Почтовый сервер организации
NTP servers	Серверы времени внутри периметра сети или внешние серверы
Internet	Сеть Интернет
webCAT server	Сервер обновления баз категоризатора wp-update.rt-solar.ru
Antivirus update server	Серверы обновления баз антивируса update.geo.drweb.com

Табл. В.2. Общая матрица доступов для explicit-прокси

Источник	Назначение	Протокол и порт назначения	Состояние соединения	Комментарий
Cluster int network	Cluster int network	ICMP, IGMP (опционально), TCP/All, UDP/All	New, Established, Related	Полный взаимный доступ между узлами кластера Solar webProxy для обеспечения их связности и взаимодействия
Cluster int network	Cluster int network	VRRP multicast, TCP/22, TCP/2269, TCP/2225, TCP/2226, TCP/2230, TCP/2278, TCP/5555, TCP/7000, TCP/8123, TCP/5434, TCP/2344, TCP/1010, TCP/3004, TCP/10051	New, Established, Related	При ограниченном доступе между узлами кластера должны быть открыты следующие порты
Trusted networks	Cluster int network/vIP	ICMP, IGMP, TCP/80, TCP/443	New, Established, Related	Доступ для АРМ и устройств пользователей (первичные соединения, TCP/2281 при необходимости локальной установки сертификатов пользователями)
Cluster int network/vIP	DCs	TCP/389, TCP/689, TCP/3268	New, Established, Related	Доступ к контроллерам домена для синхронизации Досье
Cluster int/ext network/vIP	DNS	UDP/53, TCP/53	New, Established, Related	Доступ к внутренним DNS-серверам

Источник	Назначение	Протокол и порт назначения	Состояние соединения	Комментарий
Cluster int network/vIP	SIEM	TCP/514 (опционально), UDP/514	New, Established, Related	Выгрузка журналов в SIEM
Cluster int network/vIP	Mail Server	TCP/25	New, Established, Related	Соединение с почтовым сервером для отправки отчетов и данных о категориях ресурсов
Cluster int network/vIP	Средства DLP, антивирус, пе-сочница	TCP/1344	New, Established, Related	Соединения со вспомогательными средствами по ICAP
Средства DLP, Антивирус, Пе-сочница	Cluster int network/vIP	TCP/2272	Established, Related	Трафик по ранее установленным соединениям
Cluster int/ext network/vIP	NTP servers	UDP/123	New, Established, Related	Доступ к данным о времени по NTP
Cluster ext network/vIP	Internet	TCP/80, TCP/443, TCP/21	New, Established, Related	Доступ прокси-сервера к внешним ресурсам (вторичные соединения)
Admin hosts/net	Cluster int network/vIP	ICMP, IGMP, TCP/22, TCP/8443, TCP/443, TCP/80	New, Established, Related	Доступ к интерфейсу управления и службам для администрирования/доступа в Интернет
Cluster ext network/vIP	webCAT server	TCP/443	New, Established, Related	Подключение для обновления БД категоризатора
Cluster ext network/vIP	Antivirus update server	TCP/80, TCP/443	New, Established, Related	Подключение для обновления БД антивируса
Дополнительные доступы для узлов с ролью Реверс-прокси				
Internet	Cluster ext network/vIP	Публикуемые TCP-порты для HTTP/HTTPS (в соответствии с конфигурацией реверс-прокси)	New, Established, Related	Доступ к опубликованным портам на внешнем интерфейсе реверс-прокси раздельно для протоколов HTTP и HTTPS
Cluster int network/vIP	DMZ	TCP-порты веб-сервисов на узлах в DMZ (в соответствии с конфигурацией реверс-прокси)	New, Established, Related	Вторичные соединения с веб-серверами внутри защищаемого периметра сети
DMZ	Cluster int network/vIP	TCP-порты веб-сервисов на узлах в DMZ (в соответствии с конфигурацией реверс-прокси)	Established, Related	Ответный трафик для клиентов, подключенных за пределами периметра сети к реверс-прокси
Cluster ext network/vIP	webCAT server	TCP/443	New, Established, Related	Подключение для обновления БД категоризатора
Cluster ext network/vIP	Antivirus update server	TCP/80, TCP/443	New, Established, Related	Подключение для обновления БД антивируса
Дополнительные доступы для узлов в режиме прозрачного прокси				
Cluster int network	Cluster int network	ICMP, IGMP (опционально), TCP/All, UDP/All	New, Established, Related	Полный взаимный доступ между узлами кластера Solar webProxy для обеспечения их связности и взаимодействия
Cluster int network	Cluster int network	VRRP multicast, TCP/22, TCP/2269,	New, Established, Related	При ограниченном доступе между узлами кластера

Источник	Назначение	Протокол и порт назначения	Состояние соединения	Комментарий
		TCP/2225, TCP/2226, TCP/2230, TCP/2278, TCP/5555, TCP/7000, TCP/, 8123, TCP/5434, TCP/2344, TCP/1010, TCP/3004, TCP/10051		должны быть открыты следующие порты
Trusted networks	Cluster int network/vIP	ICMP, IGMP, TCP/80, TCP/443	New, Established, Related	Доступ для АРМ и устройств пользователей (первичные соединения)
Cluster int network/vIP	DCs	TCP/389, TCP/689, TCP/3268	New, Established, Related	Доступ к контроллерам домена для синхронизации. Досье
Cluster int/ext network/vIP	DNS	UDP/53, TCP/53	New, Established, Related	Доступ к внутренним DNS-серверам
Cluster int network/vIP	SIEM	TCP/514 (опционально), UDP/514	New, Established, Related	Выгрузка журналов в SIEM
Cluster int network/vIP	Mail Server	TCP/25	New, Established, Related	Соединение с почтовым сервером для отправки отчетов и данных о категориях ресурсов
Cluster int network/vIP	Средства DLP, Антивирус, Печаточница	TCP/1344	New, Established, Related	Соединения со вспомогательными средствами по ICAP
Средства DLP, Антивирус, Печаточница	Cluster int network/vIP	TCP/2272	Established, Related	Интеграция по ICAP с Solar webProxy
Cluster int/ext network/vIP	NTP servers	UDP/123	New, Established, Related	Доступ к данным о времени по NTP
Cluster ext network/vIP	Internet	TCP/80, TCP/443, TCP/21	New, Established, Related	Доступ прокси-сервера к внешним ресурсам (вторичные соединения)
Admin hosts/net	Cluster int network/vIP	ICMP, IGMP, TCP/22, TCP/8443, TCP/443, TCP/80	New, Established, Related	Доступ к интерфейсу управления и службам для администрирования/доступа в Интернет
Cluster ext network/vIP	webCAT server	TCP/443	New, Established, Related	Подключение для обновления БД категоризатора
Cluster ext network/vIP	Antivirus update server	TCP/80, TCP/443	New, Established, Related	Подключение для обновления БД антивируса
Cluster int network/NTLM	NTLM server	TCP/2225, TCP/88, TCP/445, TCP/135, TCP/389	New, Established, Related	Доступ к доменной аутентификации
Cluster int network/Kerberos	Kerberos server	TCP/2226	New, Established, Related	Проверка подлинности пользователя

Приложение С. Отчет об ошибках: утилита bug-report

Для формирования отчета об ошибках используется утилита **bug-report**.

В отчете отображается следующая информация:

- информация о лицензии;
- системные журнальные файлы и журнальные файлы Solar webProxy;
- запущенные процессы и установленные сетевые соединения;
- информация об аппаратном обеспечении и используемых ресурсах;
- информация о запущенных процессах;
- основные конфигурационные файлы Solar webProxy;
- файлы **crontab** суперпользователя root, пользователя skvt и общие;
- информация о наличии и состоянии пакетного фильтра;
- информация о системном окружении;
- данные последних 100 пользователей, которые входили в систему.

С содержанием отчета можно ознакомиться далее в [Табл.С.1](#).

Табл. С.1. Информация отчета об ошибках: bug-report

Тип информации	Примеры вывода данных
Информация о лицензии	license-info license.xml
Системные журнальные файлы и журнальные файлы Solar webProxy	tail -n1000 /var/log/maillog tail -n1000 /var/log/messages dmesg dmesg.err
Запущенные процессы и установленные сетевые соединения	ps -fax netstat -nap netstat -nlp
Информация об аппаратном обеспечении и используемых ресурсах	iostat -N 5 vmstat -s 5 top -b -n20 -d03 free -m cat /proc/meminfo cat /etc/hosts uname -a df -h cat /etc/hostname installed-packages cat /etc/resolv.conf fdisk -l ifconfig

Тип информации	Примеры вывода данных
	lsof mount route -n
Информация об установленной ОС	/etc/os-release
Основные конфигурационные файлы Solar webProxy	/opt/dozor/config /data/repos/dozor/policy-base.git /data/repos/dozor/policy-final.git /data/repos/dozor/config-base.git /data/repos/dozor/config-final.git
Файлы crontab суперпользователя root , пользователя skvt и общие	cat /var/spool/cron cat /etc/crontab
Информация о наличии и состоянии пакетного фильтра – файлы	iptables -L -v -n iptables -L -v -n -t nat
Информация об окружении	Содержимое файла env
Данные последних 100 пользователей, которые входили в систему. Ниже приведен пример таких данных	last Пример ответа команды будет вида: root pts/0 pc-ifadeev6.lpr. Thu Feb 10 17:45 - 15:34 (21:48) reboot system boot 2.6.18-238.el5 Thu Feb 10 17:45 (15+20:20) reboot system boot 2.6.18-238.el5 Thu Feb 3 17:12 (00:14) root tty1 Thu Feb 3 16:53 - 16:54 (00:00) reboot system boot 2.6.18-238.el5 Thu Feb 3 16:38 (00:19) reboot system boot 2.6.18-238.el5 Thu Feb 3 16:36 (00:00)

Приложение D. Справочник MIME-типов

D.1. Краткое описание стандарта MIME

Для передачи данных по сети Интернет был принят стандарт MIME (Multipurpose Internet Mail Extension – многоцелевое расширение интернет-почты). Этот стандарт определяет способы передачи и кодирования данных.

Типичное применение стандарта MIME – пересылка графических изображений, аудио- и видеофайлов, документов MS Word и MS Excel, программ, а также текстовых файлов. Другими словами, MIME-типы были введены чтобы обеспечить присоединение к сообщениям электронной почты файлов различных типов. Задание типа файла позволяет почтовой программе определить, какое ПО должно использоваться для просмотра вложенного файла. Позже MIME-типы стали использоваться не только почтовыми службами, но и другими программами для унификации действий по обработке файлов. Например, по MIME-типу принятого файла веб-браузер определяет, что с ним требуется делать: если это HTML-документ, то он отображается как веб-страница, а если это файл формата MPEG, то он исполняется подключаемым модулем обозревателя, предназначенным для показа видеофильмов.

Для определения MIME-типов файлов применяется популярная модульная JAVA-система TIKA, которая используется как в составе отдельного микросервиса Solar webProxy, так и в составе проксирующего узла. В основе алгоритма определения MIME-типов лежит сигнатурный анализ файлов по его первым байтам (magic bytes) и/или глубокая аналитика исследуемого файла с разбором на составные части и с глубоким исследованием (например, сложные файлы, такие как ZIP-папки и файлы форматов xlsx, docx, pptx и т.д.).

Примечание

При загрузке файлов на облачные хранилища могут наблюдаться некоторые ограничения. Если передаваемый файл превышает объем 4096 Кб, он будет передан по частям. 2/3 MIME-типов от всего поддерживаемого количества достаточно для определения первой части файла самим Solar webProxy, но для оставшейся 1/3 части MIME-типов для определения требуется целый файл. В связи с архитектурными ограничениями постепенно собирать файл не получится, так как каждая часть передается как совершенно отдельный запрос, и Solar webProxy не может корректно определить связь между частями файла. Поэтому при передаче файлов размером больше 4096 Кб могут наблюдаться отклонения в определении типа файла, что приводит к некорректной сработке правил и исключений контентной фильтрации. Файлы меньше 4096 Кб передаются единым файлом, и проблемы, описанные ранее, не наблюдаются.

Система TIKA может преобразовывать в чистый текст следующие форматы:

- *application/vnd* (например, *.openxmlformats-officedocument.**),
- *application/vnd\l.sun\l.xml* (*.writer.**, например, *application/vnd.sun.xml.writer.template* (шаблон документа StarOffice)),
- *application/msword.** (например, *application/msword.6* (документ MS Word)),
- *application/msexcel.**,
- *application/x-pivottables* (сводная таблица),

- *application/vnd (.ms-powerpoint", например, application/vnd.ms-powerpoint (презентация MS PowerPoint)),*
- *application/pdf" (документ PDF),*
- *application/x-tika-ooxml (документ MS Word),*
- *application/rtf" (документ в формате RTF),*
- *application/x-tika-msoffice" (документ MS Word).*

Согласно стандарту MIME, в передаваемых данных должен указываться специальный заголовок, определяющий тип передаваемой информации. Этот заголовок характеризуется парой тип/подтип. Поле подтип уточняет используемый тип.

В настоящее время стандартом MIME определяется 8 основных типов содержимого:

Табл. D.1. Типы содержимого

Уровень	Описание
text	Используется для передачи текстовой информации в разных кодировках, а также форматированного текста
multipart	Используется для объединения нескольких различных взаимонезависимых типов, таких как текст, изображение, аудио и видео
application	Используется для передачи приложений или бинарных данных
model	Используется для передачи многомерных структур, состоящих из объектов. Такими многомерными структурами могут быть, например, трехмерные модели
message	Используется для передачи вложенного почтового сообщения, состоящего из вложенных сообщений. Рекурсия в данном случае не ограничивается, и составные части также могут состоять из вложенных сообщений
image	Используется для передачи изображений
audio	Используется для передачи звуковых файлов
video	Используется для передачи видеинформации

В отличие от типов, подтипы не имеют жесткой спецификации в стандарте, и при создании нового формата данных могут быть добавлены соответствующие новые подтипы. Подтипы могут образовывать деревья вида **тип/корень.подтип**. MIME определяет три стандартных корня:

- личные подтипы (personal tree), начинающиеся с `prs`;
- корпоративные подтипы (vendor tree), начинающиеся с `vnd`;
- подтипы индексации (index tree), начинающиеся с `index`.

Для локального и корпоративного использования допускаются незарегистрированные MIME-типы. При этом имя подтипа должно начинаться с `x`- . Например, скрипты Microsoft Internet Explorer 5.x имеют тип `text/x-scriptlet`.

С большинством MIME-типов связаны соответствующие форматы файлов. Например, тип `text/css` задает стили (файлы формата `*.css`), тип `text/html` – html-данные (файлы формата `*.htm, *.html`), тип `text/xml` – xml-данные (файлы формата `*.xml`) и т.д. Однако

необходимо учитывать, что данные разных типов не обязательно должны быть в отдельных файлах, то есть в одном файле могут быть разнотипные данные. Например, HTML-документы позволяют использовать как внешние файлы с определением стилей, так и внедрять данные этого типа непосредственно на страницу.

D.2. Описание MIME-типов

При формировании политики безопасности в системах класса Solar Dozor используются MIME-типы, представленные в таблицах ниже. Каждой таблице соответствует определенный тип файлов, который можно выбрать при создании правила или исключения.

Табл. D.2. MIME-типы, относящиеся к типу файлов «Служебные файлы»

ID	MIME-тип	Описание	Расширения
95	ФАЙЛЫ ПРИЛОЖЕНИЙ		
101	application/x-1c-metadata	Файл метаданных 1С	CF, CFU
102	application/x-freelance-presentation	Файл Lotus Freelance Presentation	PLZ
96	application/vnd.ms-works	Файл MS Works	WCM, WDB, WKS, WPS
98	application/x-installshield	Файл InstallShield	WIS
100	application/x-repligo.vpf	Файл данных RepliGo для конвертации файлов для мобильных устройств	RGO
97	application/x-notes-id	ID-файл Lotus Notes	ID
99	application/x-bittorrent	Файл BitTorrent	TORRENT
44	ОБРАЗЫ НАКОПИТЕЛЕЙ ДАННЫХ И ДАМПЫ ПАМЯТИ		
56	application/x-iso9660	ISO-образ диска	ISO
55	application/x-coredump	Дамп памяти	DMP, ELF
54	application/x-binary-image	Образ флоппи-диска (3.5" дискеты)	IMG, ISO, FLP
269	application/x-apple-diskimage.zlib-compressed	Образ файлов приложения Apple	DMG
	application/x-binary-image		
	application/x-binary-image		
93	ИСПОЛНЯЕМЫЕ ФАЙЛЫ И ДИНАМИЧЕСКИЕ БИБЛИОТЕКИ		
57	application/palmos	Приложение Palm OS	PRC, PDB
58	application/vnd.ms-installer	Пакет инсталляции (обновления) приложений MS Windows	MSI, MST, MSM, WIM
60	application/x-executable-binary	Приложение MS Windows	EXE
59	application/x-g3	Программа процессора G3	
61	application/x-scr.samsung.c100	Программа-скринсейвер для телефонов Samsung	SCS
62	application/macos.x	Приложение MacOS X	APP
255	application/java-vm	Байт-код приложения, предназначенный для выполнения на VM Java (JVM)	CLASS
4	АРХИВЫ И СЖАТЫЕ ФАЙЛЫ		
67	application/x-compressed-simple	Архив SCZ	SCZ
71	application/x-compressed-alz	Архив ALZip	ALZ, EGG
	text/x-egg		

ID	MIME-тип	Описание	Расширения
73	application/x-compressed-bza	Архив BZA	BZA
64	application/x-compressed-lha	Архив LHA	LHA
79	application/x-sfx-7z	Самораспаковывающийся архив типа 7Z для MS Windows	SFX, EXE
69	application/x-sfx-zip	Самораспаковывающийся архив типа Zip для MS Windows	SFX, EXE
76	application/x-compressed-yz	Архив YZ1	YZ1
21	application/x-composite-rar-jpeg	Архив RAR	RAR
	application/x-composite-rar-msword		
	application/x-composite-rar-pdf		
	application/x-compressed-rar		
	application/x-rar-compressed		
53	application/x-compressed-zip	Архив ZIP	ZIP
	application/zip		
65	application/x-compressed-pae	Зашифрованный архив PowerArchiver	PAE, PAE2
82	application/x-svr4-package	Установочный пакет в формате PKG для Mac OS X	PKG
72	application/x-debian-package	Пакет Debian	DEB
70	application/x-compressed-gzip	Архив GZIP	GZ, RAR, TGZ
	application/gzip		
5	application/x-zip-bomb	Архив типа zip-бомба	ZIP
68	application/x-compressed-arj	Архив ARJ	ARJ
78	application/x-compressed-xz	Архив LZMA	XZ
66	application/x-rpm	Установочный пакет в формате RPM (Red Hat Package Manager)	RPM
25	application/x-iscab	Архив CAB	CAB
	application/x-mscab		
	application/vnd.ms-cab-compressed		
75	application/x-compressed-bzip2	Архив BZIP2	BZ2, TBZ
	application/x-bzip2		
83	application/x-compressed-ace	Архив WinAce	ACE
80	application/x-compressed-sit	Архив Stuffit	SIT
22	application/x-compressed-7zip	Архив 7-Zip	7Z
74	application/x-cpio	Архив POSIX CPIO	CPIO
48	application/x-tar	Архив Tar	TAR
77	application/x-compressed-bh	Архив BlackHole	BH
81	application/x-sfx-rar	Самораспаковывающийся архив типа RAR для MS Windows	SFX, EXE
272	application/x-apple-app-archive.x-gtar-compressed	Архивы приложений для macOS	APP.TAR, APP.TAR.BZ2
	application/x-apple-app-archive.x-gtar-bzip2-compressed		
	application/x-apple-app-archive		

ID	MIME-тип	Описание	Расширения
276	application/vnd.android.package-archive	Пакет ОС Android	APK
42	СИСТЕМНЫЕ ФАЙЛЫ		
90	application/x-empty	Пустой файл или файл, превышающий допустимый размер	
92	application/x-folder.info	Описание каталога MacOS X	DS_STORE
84	image/vnd.microsoft.icon	Пиктограмма в формате ICO	
	image/x-icon		
86	application/x-mschm	Файл контекстной справки MS Windows	CHM
	application/vnd.ms-htmlhelp		
91	image/x-animated-cursor	Анимированный курсор Windows	ANI
87	application/x-thumbs	Кэш эскизов предварительного просмотра (Windows Thumbnail Cache)	DB
85	application/x-not-regular-file	Директория, очередь или другой нерегулярный файл в UNIX-системах	SOCK
88	application/x-ms-shortcut	Ярлык MS Windows	LNK
89	application/x-mshelp	Файл справки MS Windows	HLP
103	ЖУРНАЛ СОБЫТИЙ		
107	application/bug-report	Диагностический отчет Solar Dozor	
104	application/log-data	Файл журнала	LOG
108	application/gzipped-bug-report	Сжатый диагностический отчет Solar Dozor	GZIP, GZ
93	ИСПОЛНЯЕМЫЕ ФАЙЛЫ И ДИНАМИЧЕСКИЕ БИБЛИОТЕКИ		
94	application/java-archive	Java-архив	JAR

Табл. D.3. MIME-типы, относящиеся к типу файлов «Информационные технологии»

ID	MIME-тип	Описание	Расширения
105	БЕЗОПАСНОСТЬ		
106	application/x-hp-arcserve:arb	Пакет HP ArcSight	ARB
126	СКРИПТЫ		
43	text/javascript	Файл скрипта на языке JavaScript	JS
	application/javascript		
	application/json		
	application/x-javascript		
128	application/x-executable-script	Скрипты BASH и SHELL	SH, CSH
270	text/x-component	HTML-компонент (behavior)	HTC
127	application/x-windows-batch	Пакетный файл для выполнения команд в Windows Command Prompt	BAT
120	ВЕБ-СТРАНИЦЫ		
121	text/html	Веб-страница	HTML, ACGI, HTM, HTMLS, HTX, SHTML, STM

ID	MIME-тип	Описание	Расширения
123	text/css	Каскадная таблица стилей	CSS
122	application/x-mht	Архив веб-страницы, сохраненной в Internet Explorer	MHT, MHTML
175	text/x-php	PHP-скрипты	PHP
124	ИСХОДНЫЕ КОДЫ		
125	application/x-msvba	Код программы на языке BASIC	BAS
271	text/x-java-source	Файлы исходного кода на языке Java	JAVA
23	БАЗЫ ДАННЫХ (БД)		
113	application/x-sql-light.journal	Журнал транзакции СУБД SQLite	DB-JOURNAL
112	application/vnd.oasis.opendocument.base	БД OpenDocument	ODB
24	application/x-dbf	Файл БД dBASE	DBF
114	application/x-paradox-idx	Индексный файл типа IDX для СУБД Paradox и других программ	IDX
3	application/access-2007 application/msaccess	БД MS Access	ACCDB, MDB
37	text/x-oracle-trace-dump	Файл трассировки СУБД Oracle	TRC
110	application/x-sql-light.database	Файл БД SQLite	SQLITE, SQLITE3, DB3
111	application/x-paradox-db	Файл БД СУБД Paradox	DB, DBC, DBF, DBX
38	text/x-pgsql-db-dump	Дамп БД PostgreSQL	DUMP
12	ЗАШИФРОВАННЫЕ ДАННЫЕ		
118	application/pgp-signature	Сигнатуры PGP	ASC, SIG, PGP
116	application/agent.enc	Зашифрованные данные в формате ENC	ENC
117	application/pgp-encrypted	Зашифрованные данные в формате PGP	PGP, GPG
119	application/pgp-keys	Ключи PGP	PGP
115	application/mac-binhex40	Зашифрованные данные в формате BinHex 4.0	HQX

Табл. D.4. MIME-типы, относящиеся к типу файлов «Графика»

ID	MIME-тип	Описание	Расширения
160	ПЕЧАТЬ		
161	application/pjl	Файл HP Printer Job Language	PGL
30	ИЗОБРАЖЕНИЯ		
34	image/x-bitmap	Растровое изображение в формате BMP	BMP
	image/x-bitmap-corrupt		
	image/x-msw3bmp		
130	application/x-adobe-illustrator	Векторное изображение в формате Adobe Illustrator	AI
	application/pdf		

ID	MIME-тип	Описание	Расширения
137	drawing/cmx	Векторное изображение с метаданными Corel	CMX
144	application/x-msimage-obj	Векторное изображение (метафайл графики Windows)	WMF, WMZ, EMF
	image/msemf		
	image/mswmf		
	image/x-emf		
132	image/x-wpg	Векторное изображение в формате WordPerfect	WPG
45	image/tiff	Растровое изображение в формате TIFF без сжатия	TIFF, TIF
146	application/photoshop	Растровое изображение в формате Adobe Photoshop и PhotoDeluxe	PSD, PDD
	image/x-adobephotoshop		
143	image/xcf	Растровое изображение в формате GIMP	XCF
136	drawing/corel-symbol.library	Внешняя библиотека символов Corel Graphics Suite	CSL
131	image/x-coreldraw	Векторное изображение в формате CorelDRAW	CDR, CDT
145	image/pcx	Растровое изображение в формате PCX	PCX
141	image/targa	Растровое изображение в формате Targa Graphic	TGA, VDA, ICB
140	drawing/corel-rave	Проект Corel R.A.V.E	CLK
31	image/gif	Растровое изображение в формате GIF	GIF
138	image/psp	Растровое изображение в формате Paint Shop Pro	P S P , PSPIMAGE
135	image/fig	Векторное изображение в формате Xfig	FIG
142	image/jpeg2000	Растровое изображение в формате JPEG 2000	JP2, J2K
	image/x-j2k		
134	image/x-cgm	Векторное изображение в формате CGM	CGM
133	image/x-portable-bitmap	Растровое изображение в формате Portable Pixmap	PPM, PBM, PGM
	image/x-portable-graymap		
	image/x-portable-pixmap		
32	image/jpeg	Растровое изображение в формате JPEG	JPEG, JPG, JPE, JFIF, JIF, JFI, JFIF-TBNL
147	application/x-msphotoedit	Растровое изображение в формате MS Photo Editor	WDP
33	image/png	Растровое изображение в формате PNG без сжатия	PNG, X-PNG, 9.PNG, PNS, APNG
139	image/x-corelphotopaint	Растровое изображение в формате Corel Photo-Paint	CPT
253	image/svg+xml	Масштабируемая векторная графика	SVG

ID	MIME-тип	Описание	Расширения
264	application/x-iges	Векторное изображение САПР	IGS
273	image/heic	Растровое изображение в формате HEIC	HEIC
7	ШРИФТЫ		
149	application/ms-embedded-font-source	Встроенный шрифт MS Office	
150	application/x-font-type1	Шрифт Type	PFA, PFB, PFM, AFM
148	application/x-font-ttf application/x-screenfont.data	Шрифт в формате TTF (TrueType)	TTF, TTC
254	font/woff	Шрифт в формате WOFF	WOFF, WOFF2
	font/woff2		
	application/font-woff		
268	font/opentype	Шрифты OpenType	OTF
151	ВЕРСТКА И ПУБЛИКАЦИИ		
153	application/x-macromedia-freehand-doc	Документ Adobe FreeHand	FH, FHC, FH4, FH5, FH7
157	application/postscript	Описание страниц на языке Adobe PostScript	PS, EPS
158	application/x-pagemaker	Документ разметки страницы в формате Adobe PageMaker	PM4, PM5, PM7
156	image/dcxd	Изображение в формате FAXserve	DCX
154	application/x-mspublisher	Документ MS Publisher	PUB
159	application/quarkxpress-mime	Файл QuarkXPress	QXD, QXT, QWD, QWT, QXL, QXB
152	application/x-pfr-fax	Факсимильное сообщение Пенсионного фонда РФ	
155	application/x-dvi	Документ DVI системы TeX	DVI

Табл. D.5. MIME-типы, относящиеся к типу файлов «Документы»

ID	MIME-тип	Описание	Расширения
14	ПРЕЗЕНТАЦИИ		
19	application/vnd.oasis.opendocument.presentation	П р е з е н т а ц и я OpenDocument	ODP
162	application/vnd.openxmlformats-officedocument.presentationml.presentation-write-protected	Презентация OpenOffice, недоступная для редактирования	PPTX
15	application/mspowerpoint-2007	Презентация MS PowerPoint	PPT, PPTX, PPS, PPSX, POT, POTX, PPA
	application/vnd.ms-powerpoint		
	application/vnd.openxmlformats-officedocument.presentationml.slideshow		
	application/vnd.openxmlformats-officedocument.presentationml.template		
	application/vnd.openxmlformats-officedocument.presentationml.presentation		

ID	MIME-тип	Описание	Расширения
164	application/vnd.openxmlformats-officedocument.presentationml.presentation	Презентация OpenOffice	PPTX, THMX
163	application/vnd.stardivision.impress	Презентация StarOffice	SDP, SXI
	application/vnd.sun.xml.impress		
17	ДАННЫЕ ДОКУМЕНТОВ		
171	application/vnd.oasis.opendocument.image	Изображение OpenDocument	ODI
176	application/vnd.sun.xml.impress.template	Шаблон презентации StarOffice	STI
182	application/vnd.ms-officetheme-write-protected	Тема MS Office, недоступная для редактирования	THMX
174	application/x-msclipart	Упакованная галерея изображений в формате MS Clip Gallery	CIL
172	application/vnd.oasis.opendocument.chart	Диаграмма OpenDocument	ODC
165	application/x-msdraw	Файл MS Draw	
177	application/x-msole-broken	Поврежденная библиотека OLE-объектов для MS Office	OLB
183	application/vnd.stardivision.draw	Графика StarOffice	SDA
	application/vnd.sun.xml.draw		
178	application/vnd.sun.xml.draw.template	Шаблон графики StarOffice	STD
181	application/vnd.stardivision.math	Формула StarOffice	SMF, SXM
	application/vnd.sun.xml.math		
16	application/vnd.oasis.opendocument.formula	Формула OpenDocument	ODF
180	application/x-msole.data	Библиотека OLE-объектов для MS Office	OLB
18	application/vnd.oasis.opendocument.graphics	Графика OpenDocument	ODG
169	application/msole-word.picture	Графический OLE-объект в MS Word	
184	application/vnd.sun.xml.calc.template	Шаблон таблицы StarOffice	STC
166	application/x-msequation	Файл MS Equation	
179	application/vnd.sun.xml.writer.template	Шаблон документа StarOffice	STW
185	application/ms-graph.x-ms-excel	Диаграмма MS Graph	
168	application/x-vnd.oasis.opendocument.formula-template	Шаблон для создания формул в формате OTF	OTF
173	application/x-msole-encrypted	Зашифрованная библиотека OLE-объектов для MS Office	OLB
170	application/vnd.ms-officetheme	Тема MS Office	THMX
26	application/x-ole-storage	OLE хранилище	DAT, WID
167	application/x-msole-unknown	Неизвестная библиотека OLE-объектов для MS Office	OLB
175	application/msole-excel.picture	Графический OLE-объект в MS Excel	
53	application/zip	Расширения для программ OpenOffice и StarOffice	OXT

ID	MIME-тип	Описание	Расширения
265	application/vnd.openofficeorg.extension	Расширение OpenOffice	
277	application/vnd.google-earth.kmz	Упакованные изображения в формате Keyhole Markup Language	KMZ
198	ТЕКСТОВЫЕ ФАЙЛЫ		
36	text/x-fouled-text	Файл, в котором встречаются нетекстовые символы	TXT
199	text/plain	Текстовый файл	TXT
9	ТЕКСТОВЫЕ ДОКУМЕНТЫ		
191	application/x-rocketbook	Электронная книга в формате Rocket eBook	RB
187	image/x-djvu	Электронная книга или пакет изображений DjVu	DJV, DJVU
189	application/x-wordperfect-text	Текстовый документ в формате Corel WordPerfect	WPD
196	application/ms-office.x-vba-project application/vnd.ms-excel.addin.macroenabled.12 application/vnd.ms-excel.template.macroenabled.12 application/vnd.ms-powerpoint.presentation.macroenabled.12 application/vnd.ms-powerpoint.slideshow.macroenabled.12 application/vnd.ms-powerpoint.template.macroenabled.12	Файл MS Office с поддержкой макросов (VBA)	DOCX, DOTM, XLAM, XLSM, XLTM, POTM, PPSM, PPTM
190	application/vnd.openxmlformats-officedocument.wordprocessingml.document-write-protected	Документ MS Word, недоступный для редактирования	DOC, DOCX, DOT, DOTX, DOCM
188	application/vnd.oasis.opendocument application/vnd.oasis.opendocument.text application/vnd.oasis.opendocument.text-template	Документ OpenDocument	ODT, ODT
194	application/pdf-with-forms	Документ PDF с формой	PDF
186	text/ms-word-xml	Документ MS Word в формате XML	XML
195	application/vnd.stardivision.writer application/vnd.stardivision.writer-global application/vnd.sun.xml.writer application/vnd.sun.xml.writer.global	Документ StarOffice	SDW, SGL, SXW, SXG
52	application/pdf	Документ PDF	PDF
192	application/x-palm	Электронная книга в формате Palm Doc или БД Palm OS	PRC, PDB
10	application/msword application/msword.6 application/msword-2007 application/vnd.ms-word2006ml application/vnd.openxmlformats-officedocument.wordprocessingml.document application/vnd.openxmlformats-officedocument.wordprocessingml.template application/vnd.ms-word.document.macroenabled.12	Документ MS Word	DOC, DOCX, DOT, DOTX, DOCM

ID	MIME-тип	Описание	Расширения
	application/vnd.ms-word.template.macroenabled.12		
	application/vnd.ms-wordml		
	application/x-tika-msoffice		
	application/x-tika-ooxml		
197	application/rtf	Документ в формате RTF	RTF, DOC
2	ТАБЛИЦЫ		
20	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	Таблица OpenOffice	XLSX, XLTX
	application/vnd.openxmlformats-officedocument.spreadsheetml.template		
202	application/vnd.ms-excel.sheet.binary.macroEnabled.12	Двоичная книга MS Excel	XLSB
8	application/msexcel	Книга MS Excel	XLS, XLM, XLA, XLC, XLT, XLW, XLSX
	application/msexcel-2007		
	application/msexcel-before-97		
	application/msexcel-old		
	application/vnd.ms-excel		
201	application/vnd.stardivision.calc	Таблица StarOffice	SDC, SXC
	application/vnd.sun.xml.calc		
46	application/x-pivottables	Сводная таблица	XLS
204	application/x-123	Таблица Lotus 1-2-3	WK1, WKS
200	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet-write-protected	Таблица OpenOffice, недоступный для редактирования	XLSX
203	application/vnd.oasis.opendocument.spreadsheet	Таблица OpenDocument	ODS
274	application/vnd.apple.numbers	Таблица Numbers	NUMBERS

Табл. D.6. MIME-типы, относящиеся к типу файлов «Мультимедиа»

ID	MIME-тип	Описание	Расширения
49	АНИМАЦИЯ		
206	application/x-shockwave-flash	Анимация в формате Adobe Flash	SWF, SWFL
205	video/x-flc	Анимационные видеофайлы формата FLIC	FLC, FLI
	video/x-fli		
256	application/vnd.unity	Анимационные файлы для запуска игр в Unity Web Player	UNITYWEB
40	ВИДЕО		
209	video/x-shockwave-flash	Видео в формате Adobe Flash	FLV
	video/x-flv		
41	application/x-unknown-mv2	Видео в формате MPEG, MPEG-4, MPEG-TS	MPEG, MPG, MPE, M1V, M2V, MP2, MP3, MP4, MPA, MPV2, TS, TSV, TSA, MV2
	video/mpeg		
	video/mp4		
51	video/x-msvideo	Видео в формате AVI	AVI

ID	MIME-тип	Описание	Расширения
207	video/asf	Мультимедийные файлы формата ASF	ASF, ASX, ASR
	video/x-ms-asf		
208	video/quicktime	Видео в формате Apple QuickTime	QT, MOV, MOOV
210	video/vnd.rn-realmedia	Видео в формате RealMedia	RM
28	АУДИО		
222	audio/x-mod	Звуковой модуль в формате MOD, PSM, XM, XMZ, 669	
228	audio/x-ape	Звукозапись в формате APE, APL	
	audio/x-monkeys	Звукозапись в формате Monkeys Audio со сжатием без потери качества	
	audio/x-monkeys-audio		
50	audio/x-wav	Звукозапись в формате WAV без сжатия	WAV, WAVE
227	audio/midi	Файл в формате MIDI	MID, MIDI, KAR, RMI
229	audio/basic	Звукозапись, используемая в OC Unix, Mac OS, Akai MPC, Amiga и пр.	AU, SND
220	audio/voxware	Звукозапись в формате VoxWare Dialogic для хранения человеческой речи	VOX
224	audio/ac3	Звукозапись в формате AC-3 (Dolby Digital)	AC3
219	audio/vnd.rn-realmedia	Звукозапись в формате RealMedia	RM
214	audio/x-nice-aud	Звукозапись компьютерных игр в формате NICE Media Player	AUD
215	audio/aiff	Звукозапись в формате AIF, AIFF, AIFC	
221	audio/amr	Звукозапись в формате AMR со сжатием	AMR
223	audio/x-voc	Звукозапись в формате Creative Labs	VOC
218	audio/x-s3m	Звуковой модуль в формате ScreamTracker 3.0 и выше	S3M
226	audio/x-oggmedia	Звукозапись в формате Ogg Vorbis	OGA, OGG
225	audio/x-flac	Звукозапись в формате FLAC со сжатием без потери качества	FLAC
213	audio/x-pat	Звуковой модуль в формате Gravis UltraSound GF1	PAT
217	audio/x-creative-sf-bank	Звуковой модуль в формате SoundFont 2	SF2
216	audio/x-twinvq	Звукозапись в формате TwinVQ	VQF
29	audio/mpeg	Звукозапись в форматах MPEG, MPEG-2, MPEG-4	MP2, MP2A, M2A, MPA, MPG, MPEGA, M4A, MPGA,
	audio/mpeg2		
	audio/mp4		

ID	MIME-тип	Описание	Расширения
			MP3, M4B, M4R
261	video/webm	Мультимедийный контейнер в формате WEBM	WEBM
258	video/3gpp	Мультимедийный контейнер в формате 3GPP	3GP
259	video/x-m4v	Видеофайл в формате M4V, также известный как видеофайл iTunes	M4V
260	video/x-matroska application/x-matroska	Мультимедийный контейнер в формате MKV	MKV
261	video/webm	Мультимедийный контейнер в формате WEBM	WEBM
257	audio/x-aac	Звукозапись в формате AAC, которая используется для хранения и передачи музыки и звука	AAC
267	audio/x-gsm	Звукозаписи больших объемов для ПК и мобильных устройств	GSM
211	СПИСКИ ВОСПРОИЗВЕДЕНИЯ		
212	audio/x-mpegurl	Список воспроизведения аудио- и видеофайлов	M3U, M3U8

Табл. D.7. MIME-типы, относящиеся к типу файлов «Бизнес»

ID	MIME-тип	Описание	Расширения
ФАЙЛЫ ДАННЫХ			
230	text/csv	Файл данных, разделенных запятыми	CSV
35	text/sgml	Файл данных SGML	SGML, SGM
39	text/xml	Файл данных XML	XML
ИНЖЕНЕРНЫЕ И НАУЧНЫЕ ПАКЕТЫ			
232	application/x-autocad application/x-dwg	Файл AutoCAD	DWG, LIN, CUI, ADT, MVI
235	application/vnd.visio application/vnd.ms-visio.drawing application/vnd.ms-visio.drawing.macroenabled.12 application/vnd.ms-visio.stencil application/vnd.ms-visio.stencil.macroenabled.12 application/vnd.ms-visio.template application/vnd.ms-visio.template.macroenabled.12	Документ MS Visio	VSD, VSDX, VST, VSTX, VSS, VSX, VSW
236	application/x-matlab-binary	Файл MatLab	MAT
234	application/x-AT-mathcad application/vnd.mcd	Файл MathCAD	MCD
233	application/vnd.ms-pki.stl application/x-stl-binary	Формат файла используемый для хранения трехмерных моделей	STL
262	application/x-jt	Формат файла используемый в системах САПР	JT

ID	MIME-тип	Описание	Расширения
47	ФИНАНСЫ		
251	application/x-1c.data	Файл данных 1С	1CD, DT
252	text/x-ptk-pzd	Документ банковской отчетности в формате ПТК ПСД	
262	application/vnd.ms-pki.stl	Файл 3D-моделей	
	application/x-stl-binary		
	application/x-stl-ascii		
263	application/x-jt	Файл САПР	
237	СПРАВОЧНИКИ		
238	application/x-consultant	Файл Консультант Плюс	KUB, DT
242	ЭЛЕКТРОННАЯ ПОЧТА		
246	application/vnd.ms-attachment-tnef	Файл данных MS Exchange	DAT, MS-TNEF, TNEF
	application/vnd.ms-tnef		
244	application/x-pkcs7-mime	Зашифрованное сообщение электронной почты или сертификат	P7M, P7C
249	application/x-sensor-m-box	Почтовый ящик электронной почты	MBOX
248	message/news	Файл почтовых сообщений или новостей Windows Live Mail	NWS
247	application/x-microsoft-rpmsg-message	Сообщение MS Outlook с ограниченным доступом	RPMSG
243	application/vnd.ms-outlook	Файл MS Outlook	DBX, EMAIL, EML, BCMX, DBX, ECF, IDX, MBX, NCH, OFT, PRF, SRS, MSG
250	application/x-pkcs7-signature	Цифровая подпись (без сообщения, которое подписано)	P7A, P7S
245	message/rfc822	Сообщение электронной почты	EML, MHT, MHTML, MIME, NWS
243	application/x-mso.oledata	Отображает вложение Microsoft Word 2000 в электронном письме в виде веб-страницы	MSO
239	УПРАВЛЕНИЕ		
240	application/msproject	Проект MS Project	MPP, MPT
	application/ms-project-2007-workspace		
241	application/x-ibm-requisitepro	Файл IBM Rational Requisite Pro	RQS

Табл. D.8. MIME-типы, относящиеся к типу файлов «Неопределенный тип файлов»

ID	MIME-тип	Описание	Расширения
266	application/octet-stream	Неопределенный тип файлов	

D.3. Язык описания регулярных выражений

При задании MIME-типов могут использоваться регулярные выражения. В регулярных выражениях применяются специальные символы (метасимволы): `$ ^ . * + ? []`.

Табл. D.9. Описание метасимволов

Метасимвол	Назначение
<code>.</code> (точка)	Специальный знак, который соответствует любому одиночному символу, за исключением перевода строки.
<code>*</code> (звездочка)	Постфиксный оператор, который означает, что предыдущее регулярное выражение должно быть повторено столько раз, сколько это возможно. Например, выражение <code>.*</code> соответствует любой последовательности символов, не содержащей переводов строки.
<code>+</code> (плюс)	Оператор, который означает, что стоящее перед ним выражение должно появиться один или более раз. Например, выражение <code>bo+m</code> соответствует <code>boom</code> , <code>booom</code> и т.д.
<code>?</code> (вопрос)	Оператор, который означает, что предыдущий символ или выражение (при использовании группировки) должно появиться один раз или ни одного раза. Выражение <code>file.jpg?g</code> будет соответствовать строкам <code>file.jpg</code> и <code>file.jpeg</code> .
<code>[]</code> (квадратные скобки)	Служат для указания набора знаков, которым может соответствовать символ. Например, <code>[abcd]</code> соответствует любому из символов <code>a</code> , <code>b</code> , <code>c</code> и <code>d</code> . Выражение <code>[ab]*</code> будет соответствовать любой комбинации подряд идущих символов <code>a</code> и <code>b</code> произвольной длины. Кроме того, в скобках могут задаваться интервалы: выражение <code>[a-zA-Z0-9]</code> соответствует любому из символов латинского алфавита в верхнем и нижнем регистре, а также любой десятичной цифре от 0 до 9.
<code>[^]</code>	Конструкция, противоположная предыдущей. Используется для указания того, что не должно содержаться в строке. Выражение <code>[^0-9]</code> соответствует любому символу, кроме цифр от 0 до 9.
<code>^</code>	Символ для обозначения начала строки.
<code>\$</code>	Символ для обозначения конца строки. Таким образом, <code>\$\$</code> соответствует пустой строке, а <code>^HOME\$</code> — строке с единственным словом <code>HOME</code> .
<code>\</code>	Выполняет две функции: отменяет действие специальных символов, превращая их в обычные символы (данная операция называется экранированием символа), и вводит дополнительные специальные конструкции, такие как:
	<ul style="list-style-type: none">• <code>\n</code> — перевод строки;• <code>\r</code> — возврат каретки;• <code>\t</code> — табуляция;• <code>\</code> — установка символа <code>\</code> без функции экранирования символов.
<code> </code>	Означает выбор одного из вариантов. Выражение <code>alpha beta gamma</code> будет соответствовать любой из строк <code>alpha</code> , <code>beta</code> и <code>gamma</code> .

Приложение Е. Аудит действий пользователей Solar webProxy

В таблице приведено подробное описание журналируемых действий пользователя.

Табл. Е.1. Описание действий

Вид действия	Название действия	Атрибут	Описание атрибута	Примеры записей в журнале
Вход и выход из системы	Вход в систему	-	-	-
	Выход из системы	-	-	-
Поиск информации в системе (к поиску относится как непосредственно поиск, так и просмотр любой информации, например, на Рабочем столе)	Поиск	name	Наименование поискового запроса	name: События и инциденты 24 часа;
	Запуск поиска (для расширенного поиска и/или поиска по шаблонам)	obj	Объект поиска: events (события и инциденты)/ messages (сообщения/ нажатия клавиш)/ files (вложенные файлы)/ endpoints (участники переписки)/ chats (беседы)	obj: events;
	Просмотр результатов поиска	type	Тип поиска: quick (быстрый поиск)/ template (шаблоны поиска)/ extended (расширенный поиск)	type: quick;
Управление учетными записями пользователей системы	Создание пользователя	login	Логин пользователя системы	login: lexey;
		name	Имя пользователя системы	name: Кравцев Иван Петрович;
	Изменение пользователя	login	Логин пользователя системы	login: lub_ta;
		name	Имя пользователя системы	name: Любушкина Татьяна Валерьевна;
	Удаление пользователя	login	Логин пользователя системы	login: admin;
		name	Имя пользователя системы	name: Администратор;
Управление ролями пользователей системы	Создание роли пользователей	role	Роль пользователей (при выполнении действия "Импорт ролей" возможно множество значений)	role: Администраторы;
	Изменение роли пользователей			
	Удаление роли пользователей			
	Импорт ролей			
Настройка набора правил политики	Создание набора правил политики	name	Наименование набора правил политики	name: Внутренняя передача;
	Изменение набора правил политики			
	Удаление набора правил политики			
Настройка набора условий политики	Создание набора условий политики	name	Наименование набора условий политики	name: Временная передача;

Вид действия	Название действия	Атрибут	Описание атрибута	Примеры записей в журнале
	Изменение набора условий политики			
	Удаление набора условий политики			
Управление инструментами политики	Создание инструмента политики	name	Наименование инструмента политики	name : template_note_for_admin;
		type	Тип инструмента политики	type : rec-template;
	Изменение инструмента политики	name	Наименование инструмента политики	name : Правило из досье;
		type	Тип инструмента политики	type : monitored-group-rule;
	Удаление инструмента политики	name	Наименование инструмента политики	name : Поиск работы;
		type	Тип инструмента политики	type : ban-text;
Управление шаблонами и профилями	Создание шаблона/профиля	name	Наименование шаблона/профиля	name : icap-шаблон;
		type	Тип шаблона/профиля	type : icap-block-template;
	Изменение шаблона/профиля	name	Наименование шаблона/профиля	name : Шаблон уведомления;
		type	Тип шаблона/профиля	type : mail-template;
	Удаление шаблона/профиля	name	Наименование шаблона/профиля	name : Шаблон каталога;
		type	Тип шаблона/профиля	type : directory-template;
Применение политики	Применение политики	-	-	-
Импорт политики в систему	Импорт политики	name	Наименование импортируемого файла	name : Временная передача;
Управление справочниками	Создание элемента справочника	name	Наименование элемента справочника	name : Запретная переписка;
		type	Тип элемента справочника	type : label-types;
	Изменение элемента справочника	name	Наименование элемента справочника	name : Авария-отказ;
		type	Тип элемента справочника	type : event-category;
	Удаление элемента справочника	name	Наименование элемента справочника	name : Приложения;
		type	Тип элемента справочника	type : apps;
Изменение конфигурации системы	Изменение конфигурации системы	type	Название сервиса, в который внесено изменение	type : incident-daemon;

Приложение F. Описание назначения и форматов сообщений Solar webProxy

F.1. Файлы access-log

В файлах **access-log** содержится информация о доступе пользователей к внешним ресурсам, результатах работы политики, сформированной на прокси-сервере, и результатах выполнения запросов пользователей. Обработка информации выполняется компонентом **skvt-wizor**. В **access-log** регистрируются все события политики (запреты и разрешения доступа) и передаются в **БД Clickhouse** для сбора и хранения журналов доступа.

Файлы **access-log** хранятся в каталоге **/data/spool/skvt/access_log/** с расширением **current**. После обработки службой **log-streamer** файлы отправляются в базу данных и удаляются из каталога.

Пример содержимого файлов, создаваемых **skvt-wizor**, в каталоге **/data/spool/skvt/access_log/**:

```
{"acclp":"10.201.31.90","accld":"00000000-0000-0000-0000-000000000000","accName":"10.201.31.90","accGroupIds":["00000000-0000-0000-0000-000000000000"],"accDomain":"","accLogin":"10.201.31.90","accPort":57059,"reqMethod":"POST","reqProtocol":"https","reqHostname":"ya.ru","reqPort":443,"reqPathname":"/clck/click","reqBodySize":3525,"reqDatatype":"text/plain","reqTime":1692863811743,"reqReferer":"https://ya.ru/","resDatatype":"image/gif","resBodySize":919,"resStatus":200,"resIp":"10.201.31.123","fltTime":26,"fltHost":"main","fltCodes":[11,0,0,0,0,0],"fltStatus":200,"fltLayers":["Decryption","Decryption","Icap Request","Filter req","Icap Response","Filter resps"], "fltRules":["Вскрывать все","Переход к слою Icap Request","Переход к слою Filter req","Переход к слою Icap Response","Переход к слою Filter resps","Переход к слою Завершение обработки политики"], "fltReason":"","fltPolicy":"Завершение обработки политики","fltCategories":[21104],"fltExtension":"","sysTime":1692863811770,"trajType":1,"trajMode":"forward","fltPort":50224,"fltpIp":"10.201.31.164","reqUserAgent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134","reqProxyIp":"10.201.31.164","reqProxyPort":2270,"logMark":[],"resComment":""}
```

Для записи событий доступа пользователей к внешним ресурсам через прокси-сервер в каталог **/var/log/messages** в разделе **Система > Настройки > Журналирование > Фильтрация и анализ трафика пользователей** установите флагшки **Запись журнала (формат access-log)** и/или **Запись журнала (формат SIEM)**.

Каждый сервис записывает в файл **access-log** информацию об определенных действиях. Запись состоит из набора параметров. Общие параметры файлов **access-log** представлены в таблице ниже.

Табл. F.1. Общие параметры файлов access-log

Вид параметра в файле	Параметр в JAVA-свойствах	Описание
acc-domain	accDomain	Домен источника запроса. Для пользователя без домена поле пустое
accGroupIds	accGroupIds	Перечень идентификаторов групп Персоны
acc-groups	accGroupNames	Список имен групп, к которым относится пользователь
accld	accld	Идентификатор Персоны в БД abook
acc-ip	acclp	IP-адрес источника запроса

accLogin	accLogin	Логин пользователя – источника запроса или IP-адрес для неаутентифицированных пользователей
acc-name	accName	Имя персоны, соответствующее идентификатору, или IP-адрес неаутентифицированных пользователей
acc-windows-login	accWindowsLogin	Логин пользователя в формате WINLogin (или WinLogin или UPN)
acc-upn	accUpn	Логин пользователя в формате UPN
acc-port	accPort	SRC-Port на источнике запроса
bytes-out-body	reqBodySize	Размер исходящего тела запроса (передаваемого файла/сообщения)
flt-categories	fltCategories	Категории ресурса из запроса, определенные категоризатором
flt-codes	fltCodes	<p>Массив выполненных действий.</p> <p>Возможные варианты:</p> <p>NOTAUTHORIZED, BLOCKED_ACCOUNT, BAD_NETWORK, ALLOW, DENY, REDIRECT, ARCHIVE, CONFIRM, NOTIFY, DETECT_DATATYPE, MODIFY_HEADERS, NOLOG, MITM, CHECK_CERTIFICATE, MESSAGE, LIMIT_SPEED, PROXY, BIND, DSCP_SETUP, WS_BLOCKING_NOTIFICATION</p>
flt-host	fltHost	Имя узла, обработавшего запрос пользователя
flt-ip	fltIp	Адрес узла фильтрации
flt-layers	fltLayers	Перечень слоев политики, которые были применены к трафику (запросу и ответу)
flt-policy	fltPolicy	Правило или слой, на котором завершилась обработка запроса политикой
flt-port	fltPort	SRC-port на узле фильтрации
flt-reason	fltReason	<p>Причина срабатывания правила. Может принимать значения вида:</p> <p>CATEGORY_BODY – категория содержимого;</p> <p>CATEGORY_HEADERS – категория заголовка;</p> <p>CATEGORY_PREVIEW – категория контента;</p> <p>CATEGORY_URL – категория URL;</p> <p>DESTINATION_IP – IP-адрес назначения;</p> <p>DATATYPE – тип данных;</p> <p>FILE_ATTRIBUTE – атрибут файла URL;</p> <p>GROUP – группа пользователя;</p> <p>HEADER – заголовок;</p> <p>IP – адрес источника/назначения;</p> <p>KEYPHRASE_BODY – ключевое слово в содержимом;</p> <p>KEYPHRASE_URL – ключевое слово в URL;</p> <p>METHOD – метод HTTP;</p> <p>NODE – узел, который выполняет обработку запроса;</p> <p>PORT – порт;</p>

		PROTOCOL – протокол доступа; SIZE – размер файла; TIME – расписание доступа; TRAFFIC – лимит трафика; VIRUS – вирус; USER – логин пользователя; URL – URL
flt-routing-actions	fltRoutingActions	События слоя Маршрутизация соединений
flt-rules	fltRules	Название выполненного правила
flt-status	fltStatus	Результат фильтрации. Соответствует HTTP-коду ответа
flt-time	fltTime	Время выполнения фильтрации политикой
log-mark	logMark	Маркер, добавляемый в журнал при срабатывании правила политики. Может использоваться для отбора событий в разделе Статистика > По узлам фильтрации
bytes-out	reqBodySize	Размер тела запроса в байтах
req-datatype	reqDatatype	Тип данных в запросе
bytes-out	reqHeaderSize	Объем запроса в байтах
req-hostname	reqHostname	Полное имя запрошенного ресурса
req-keywords-report	reqKeyWordsReport	Отчет по найденным ключевым словам и имени файла <u>Примечание</u> <i>Если при загрузке файла на облачное хранилище у запроса отсутствует заголовок content-disposition, будет отображаться бинарное название файла.</i>
req-method	reqMethod	Использованный в запросе метод протокола HTTP
req-pathname	reqPathname	Путь к запрошенному элементу относительно корня
req-port	reqPort	Порт сервера назначения
req-protocol	reqProtocol	Использованный при запросе протокол (HTTP, HTTPS)
req-proxyip	reqProxyIp	IP-адрес вышестоящего прокси (может быть пуст при его отсутствии)
req-proxyport	reqProxyPort	Порт на вышестоящем прокси, на который направлялся запрос
req-query	reqQuery	Query-строка запроса с GET-параметрами
req-referer	reqReferer	Путь для перенаправления к запрошенному ресурсу. В некоторых случаях может быть пуст
req-time	reqTime	Время обработки запроса
req-url	reqUrl	URL-адрес назначения
req-user-agent	reqUserAgent	Значение поля UserAgent , передаваемое приложением (браузером) в заголовке
res-bodysize	resBodySize	Размер тела ответа от сервера
res-comment	resComment	Комментарий к ресурсу (если он содержится в справочнике и ему был присвоен комментарий администратором)
res-datatype	resDatatype	Тип данных в ответе сервера

bytes-in	resHeaderSize resHeaderSize	+ Объем ответа в байтах
res-ip	resIp	IP-адрес сервера, который предоставил ответ. В случае использования вышестоящего прокси будет указан его IP
res-status	resStatus	Статус выполнения запроса/ответа. Код 200 – успешное получение ответа от ресурса
sys-time	sysTime	Время поступления запроса на фильтр
traj-mode	trajMode	Режим трафика (forward для прямого, reverse для обратного прокси)
x-virus-id	virusId	Название вируса

F.2. Файлы audit-log

Файл **audit.log** содержит информацию о действиях администраторов системы в интерфейсе и дополнительных сообщениях о выполнении автоматических действий системными утилитами и скриптами. В перечень регистрируемых действий входят сообщения о:

- Получении администратором доступа к интерфейсу при успешном входе в систему;
- Неуспешных попытках входа в систему;
- Загрузке файла лицензии и результате загрузки;
- Получении администратором сведений об объектах разделов интерфейса;
- Создании администратором новых объектов в разделах интерфейса;
- Внесении администратором изменений в объекты разделов (обновлении их характеристик);
- Удалении объектов в разделах интерфейса;
- Изменении состояния некоторых объектов (сигнатур, других отключаемых объектов) в разделах интерфейса (включение/выключение);
- Изменении состояния правил/исключений в разделе **Политика**;
- Сохранении изменений, внесенных в разделы **Система** и **Политика**;
- Применении администратором политики вручную из интерфейса управления;
- Чтении администратором журнальных сообщений в интерфейсе системы.

Дополнительно, в файл **audit.log** записываются сообщения о выполнении системой таких действий и их результатов, как:

- Успешное/неуспешное применение текущей конфигурации для узлов кластера;
- Загрузка и применение текущей политики в автоматическом режиме;
- Ошибки при выполнении загрузки конфигурации и политики;
- Выполнение задач/скриптов по расписанию системного планировщика.

Файлы **audit.log** хранятся в каталоге **/var/log/audit/**.

Каждое сообщение в файле обязательно начинается с символа @ и имеет уникальный идентификатор, дату и тип сообщения. Все журнальные сообщения содержат различное количество обязательных и необязательных полей, однако порядок их следования определен достаточно строго. Базовым разделителем полей является пробел.

В журнале используется несколько форматов записей:

```
@4000000064c89d991bbc170c INFO s.a.LocalAuthenticator - User 'admin' login
```

```
@4000000064c89d8f1c25cd8c [11347] Hook done: /opt/dozor/policy/hooks/tc-limit.sh (2023-08-01 08:52:05)
```

```
@4000000064c89e540f9e2d34 INFO r.s.d.s.AuthClientActor - Received 0 requests; attempted 0 requests
```

```
@4000000064c89d9b1704d85c INFO f.RequestSlowLogFilter - Request /api/access-log/grafana/public/build/app.17c6ddc5361653e652bc.js total 1370ms (headers 19ms content 1351ms)
```

```
@4000000064c89ebb18436ef4 [5094] Hook done: /opt/dozor/policy/hooks/wizor-force-reload.sh (2023-08-01 08:57:05)
```

Общие параметры файлов **audit.log** представлены в таблице.

Табл. F.2. Общие параметры файлов audit.log

Параметр	Описание
c.a.AuthController	События аутентификации на клиенте
s.a.LocalAuthenticator	Маркер события аутентификации на стороне сервера
s.p.IPSRuleService	Сообщения о событии IPS
s.c.ActionLoggerImpl	Основной маркер действий пользователя в конфигурации и политике
c.p.PolicyController	События о применении политики и его результате
c.r.ReportsController	События от подсистемы отчетности и статистики
f.RequestSlowLogFilter	События от подсистемы фильтрации прокси
r.s.d.s.AuthClientActor	Сообщения о попытках аутентификации внешних клиентов (пользователей) и результатах
LockService	Служебные сообщения/загрузка конфигурации/загрузка политики
PolicyGenerator	Служебные сообщения/загрузка политики
s.a.AbookRealtimeService	События от подсистемы Досье
c.t.s.s.AlgorithmChecker	Сообщения подсистемы внутреннего контроля состояния
r.s.p.c.ConfigApiFacadeB	Сообщения подсистемы интерфейса пользователя
Success	Сообщения об успешном применении конфигурации/политики
LockService	Сообщения о блокировке файлов конфигурации при применении политики
INFO	Тип сообщения
s.c.ActionLoggerImpl	Подсистема, которая создала событие
admin@/0.0.0.0	Имя пользователя и SRC_IP, с которого выполнялось подключение

Action	<p>Действие, которое было выполнено пользователем с объектом раздела интерфейса, правилом или параметром. Может принимать значения вида:</p> <p>Create instruction – создание нового правила или объекта политики;</p> <p>Update instruction – изменение элемента слоя, правила или объекта политики</p>
Changes	<p>Изменения состояния правила. Принимает значения:</p> <p>move rule – изменение порядка следования правил в слое/подслое политики;</p> <p>delete instruction – удаление правила, элемента или объекта политики;</p> <p>read layer – обращение к объектам слоя политики для их отображения;</p> <p>getting policy items – отображение раздела Политика и элементов его блоков;</p> <p>get proxy servers – обращение к блоку описания доступных вышестоящих прокси-серверов для их отображения;</p> <p>get icap servers – обращение к описанию доступных в системе серверов ICAP для их отображения;</p> <p>get list of all categories – отображение списка категорий для ресурсов при настройке правил политики</p>

Приложение G. API Solar webProxy

API Gateway – сервис, предоставляющий API для интеграции Solar webProxy со сторонними приложениями. Сервис является единственной точкой входа для сторонних приложений и выполняет их аутентификацию и авторизацию, а после выполнение запросов с участием внутренних сервисов Solar webProxy.

G.1. Конфигурирование API Solar webProxy

Управлять настройками API Solar webProxy можно в разделе **Система > Основные настройки > Интеграция**.

Примечание

Раздел Система > Основные настройки > Интеграция доступен только при наличии роли Сервер интеграции.

Вы можете задать значения параметров:

- **Порт сервиса интеграции** – значение параметра может быть от 1 до 65535. По умолчанию – 9033.
- **Путь к сертификату межсервисного взаимодействия**.
- **Пароль для сертификата**.
- **Идентификатор клиента** – уникальное имя, которое будет использоваться при журналировании запросов.
- **Тип доступа** – возможны значения **Read-write** (просмотр и чтение, доступ ко всем API Solar webProxy) или **Read-only** (только просмотр, доступ только к тем API, которые не модифицируют работу Solar webProxy).
- **API токен** – создается автоматически при нажатии кнопки **Добавить**. В дальнейшем его можно отредактировать. Длина API токена может быть от 32 до 96 символов.
- **Срок действия API токена** – параметр управления сроком действия API токена:
 - Чтобы API токен работал бессрочно, выберите значение **Не ограничен**.
 - Чтобы ограничить работу API токена, выберите значение **Ограничен** и укажите необходимую дату (ближайшая доступная дата – следующий день). API токен будет работать до указанной даты включительно.

G.2. Работа со справочниками и объектами политик с помощью API Solar webProxy

Примечание

Работа с API Solar webProxy доступна только при назначеннной роли Сервер интеграции.

Для работы с API Solar webProxy передайте свой уникальный API токен в заголовке:

Authorization: App \${token}

где **<\${token}>** – индивидуальный API токен.

При отсутствии заголовка или при неизвестном токене ответ на запрос будет с кодом **401 Unauthorized**. Если клиент с типом доступа **Read-only** пытается воспользоваться API, меняющим данные, будет отображен код ошибки **403 Forbidden**.

Подробнее ознакомиться с API Solar webProxy можно с помощью инструмента Swagger. Это интерактивная документация для API, с помощью которой можно посмотреть методы, примеры запросов, а так же запустить их выполнение. По умолчанию Swagger будет доступен по адресу <https://<ip>:9033/api/>. Порт для доступа к API можно посмотреть в разделе **Система > Основные настройки > Интеграция > Сервис интеграции** в поле **Порт сервиса интеграции**.

Все запросы журналируются в раздел **Система > Журналы**.

URL справочника строится по схеме **/api/policy/item/:typee/:id**, где **:typee** – тип объекта политики, **:id** – его идентификатор.

Табл. G.1. Методы при работе со словарями политики

Метод	Описание
GET /api/policy/item/:typee/	Возвращает JSON-объект, содержащий массив с идентификаторами всех существующих элементов (списков).
GET /api/policy/item/:typee/:id	Возвращает содержимое списка (JSON). Головной объект содержит название списка и список с его содержимым.
PUT /api/policy/item/:typee/:id	При отсутствии списка создает новый список с переданным содержимым. При наличии – замещает содержимое. Элементы списка (unit) в данном методе не передаются.
PUT /api/policy/unit/:typee/:id	При отсутствии элемента списка создает новый элемент с переданным содержимым. При наличии – замещает содержимое.
PATCH /api/policy/item/:typee/:id	Модифицирует существующий список. Элементы списка (unit) в данном методе не передаются.
PATCH /api/policy/unit/:typee/:id	Модифицирует существующий элемент списка. Содержит JSON Patch к содержимому списка в формате rfc6902 (использует библиотеку diffson).
DELETE /api/policy/item/:typee/:id	Удаляет существующий список.
DELETE /api/policy/unit/:typee/:id	Удаляет существующий элемент списка.

Поля, содержащие дату создания и изменения элемента, а также имя изменявшего их, вычисляются автоматически.

После выполнения вызова API, который модифицировал данные, необходимо вручную применить политику.

Лист контроля версий

03/09/2025-15:36