

RedCheck

СРЕДСТВО АНАЛИЗА
ЗАЩИЩЕННОСТИ



Руководство
администратора

АЛМЮ.501410.RC02-01.РА

Версия документа 2.12.ru



Содержание

Аннотация	5
1 Знакомство с RedCheck.....	7
1.1 Основные сведения	8
1.2 Репозиторий OVALdb.....	12
1.3 Архитектура RedCheck.....	13
1.4 Функциональные возможности.....	15
1.5 Ролевая модель RedCheck	22
1.6 Редакции RedCheck	25
1.7 Лицензирование.....	28
1.8 Как получить тестовую версию?	29
1.9 Перечень поддерживаемых платформ	31
1.10 Перечень интегрируемых систем.....	37
1.11 Служба технической поддержки.....	38
2 Системные требования	39
2.1 Требования к аппаратному обеспечению.....	40
2.2 Требования к программному обеспечению.....	44
2.3 Требования к сетевой инфраструктуре.....	45
3 Установка RedCheck Nix	49
3.1 Astra Linux 1.7	50
Установка СУБД	51
Инсталляция RedCheck	55
Конфигурация RedCheck.....	57
3.2 Astra Linux 1.8	66
Установка СУБД	67
Инсталляция RedCheck	70
Конфигурация RedCheck.....	72
3.3 Debian 12.....	81
Установка СУБД	82
Инсталляция RedCheck	86
Конфигурация RedCheck.....	88
3.4 РЕД ОС 7.3	97
Установка СУБД	98

Инсталляция RedCheck	101
Конфигурация RedCheck.....	103
3.5 Установка агента RedCheck (Windows).....	112
3.5.1 Установка на сканируемом хосте в ручном режиме.....	113
3.5.2 Установка через групповые политики домена	118
3.6 Раздельная установка.....	141
3.7 Добавление собственных сертификатов для https	142
3.8 Подключение репозитория совместимости	145
4 Сопровождение Системы	147
4.1 Настройка ролевой модели.....	148
4.2. Сброс активации лицензии	150
4.3 Обновление контента информационной безопасности.....	152
4.3.1 Синхронизация через сеть Интернет	153
4.3.2 Офлайн-синхронизация.....	155
4.3.3 Синхронизация через прокси-сервер.....	160
4.4 Настройка учетных записей для сканирования	162
4.4.1 Сканирование Windows-систем	163
Транспорт Агент RedCheck.....	170
Транспорт WinRM.....	171
Транспорт WinRM (Kerberos).....	186
4.4.2 Сканирование Linux-систем.....	188
Учетная запись суперпользователя (root).....	193
Учетная запись привилегированного пользователя (sudo).....	195
Учетная запись непривилегированного пользователя	197
4.4.3 Сканирование FreeBSD	198
4.4.4 Сканирование Solaris	200
4.4.5 Сканирование Check Point	201
4.4.6 Сканирование Cisco IOS / NX-OS.....	202
4.4.7 Сканирование Huawei	207
4.4.8 Сканирование FortiOS.....	209
4.4.9 Сканирование UserGate.....	211
4.4.10 Сканирование VMware.....	212
Настройка VMware ESXi Server	214
Настройка VMware vCenter Server	219

Настройка VMware NSX Data Center	220
4.4.11 Сканирование Microsoft SQL Server	222
4.4.12 Сканирование MySQL	224
4.4.13 Сканирование PostgreSQL.....	226
4.4.14 Сканирование Oracle.....	228
4.4.15 Сканирование MongoDB.....	232
4.4.16 Сканирование Eltex.....	233
4.4.17 Сканирование Docker	235
4.4.18 Сканирование OpenShift.....	237
4.5 Смена ключа шифрования	238
4.6 Обслуживание БД.....	240
4.7 Резервное копирование и восстановление БД	242
4.7.1 Резервное копирование PostgreSQL.....	243
4.7.2 Восстановление PostgreSQL.....	244
4.8 Обновление RedCheck Nix	245
4.9 Смена лицензионного ключа	249
4.10 Офлайн активация лицензии.....	254
4.11 Изменение порта для Агента сканирования.....	258
4.12 Журнал событий (логи)	262
4.12.1 Примеры регистрации событий.....	264
4.12.2 Настройка логирования компонентов RedCheck	267
4.13 Настройка сервиса доставки отчетов.....	270
4.14 Исключения для средств защиты (САЗ, СЗИ).....	272
4.15 Настройка Windows-аутентификации (Kerberos).....	274
4.16 Дополнительные настройки для сканирования	285
4.17 Удаление RedCheck.....	288
5 Термины и сокращения	290

Аннотация

Данное руководство является помощником для системных администраторов и администраторов ИБ, осуществляющих установку, настройку и эксплуатацию программного средства анализа защищенности RedCheck Nix (далее – RedCheck, Система).

Для пользователей RedCheck рекомендуется ознакомиться с [Руководством Пользователя RedCheck Nix](#).

Для обновления с предыдущих версий используйте инструкцию [4.8 Обновление RedCheck Nix](#).

Что нового в RedCheck Nix 2.12

- Добавлена возможность отправки логов по syslog
- Расширены настройки сервиса доставки на электронную почту
- Расширены возможности по настройке сканирования
- Добавлено единообразное определение ОС во всех заданиях белого ящика
- Расширен список поддерживаемых AD для импорта хостов: ALDPro, Альт Домен, РЕД АДМ
- Добавлены новые атрибуты уязвимости: исправление, смягчение, последствия эксплуатации
- Добавлена возможность выполнения задания типа Фиксация по WinRM

Данное Руководство состоит из следующих разделов:

- [1 Знакомство с RedCheck](#)
- [2 Системные требования](#)
- [3 Установка RedCheck Nix](#)
- [4 Сопровождение Системы](#)
- [5 Термины и сокращения](#)

Производитель может вносить в Руководство изменения, связанные с улучшением ПО. Актуальная версия документации для новой редакции Руководства находится на [сайте](#) компании.

Производитель:	АО «АЛТЭКС-СОФТ»
Почтовый адрес:	ул. Маяковского, д. 10, пом. VII, мкр. Болшево, г. Королев, Московская обл., 141090
Электронная почта:	info@altx-soft.ru / support@altx-soft.ru
Телефон:	+7(495) 543-31-01
Адрес сайта производителя:	altx-soft.ru
Адрес сайта товара:	redcheck.ru

1 Знакомство с RedCheck

Содержание

- [1.1 Основные сведения](#)
- [1.2 Репозиторий OVALdb](#)
- [1.3 Архитектура RedCheck](#)
- [1.4 Функциональные возможности](#)
- [1.5 Ролевая модель RedCheck](#)
- [1.6 Редакции RedCheck](#)
- [1.7 Лицензирование](#)
- [1.8 Как получить тестовую версию?](#)
- [1.9 Перечень поддерживаемых платформ](#)
- [1.10 Перечень интегрируемых систем](#)
- [1.11 Служба технической поддержки](#)

1.1 Основные сведения

RedCheck представляет собой комплексное решение для анализа защищённости и управления ИБ для предприятий любого масштаба (без технических ограничений количества сканируемых хостов).

Система предназначена для использования ИТ-специалистами, службами ИБ, а также органами по аттестации объектов информатизации.

Система применима для решения следующих задач:

- централизованное сетевое или локальное определение уязвимостей системного и прикладного ПО, аппаратных платформ;
- контроль настроек параметров безопасности, соблюдения требований политик и стандартов ИБ;
- инвентаризация оборудования и ПО;
- контроль целостности файлов и каталогов;
- создание отчетов по результатам аудитов.

Объектами сканирования для RedCheck являются:

- ОС Microsoft Windows и Linux, в том числе отечественные;
- сетевое оборудование;
- протоколы АСУ ТП;
- средства виртуализации;
- средства контейнеризации и оркестрации;
- СУБД;
- офисные пакеты и другое прикладное ПО;

Система может использоваться для реализации мер защиты информации в ИС и АСУ, а также для обеспечения безопасности персональных данных в соответствии с приказами ФСТЭК России:

- № [17](#) от 11 февраля 2013 г.;

- № [21](#) от 18 февраля 2013 г.;
- № [31](#) от 14 марта 2014 г.;
- № [239](#) от 25 декабря 2017 г.;

в части:

1. ограничения программной среды (ОПС):

- управление установкой (инсталляцией) компонентов ПО, в том числе:
 - определение компонентов, подлежащих установке;
 - настройка параметров установки компонентов;
 - контроль за установкой компонентов ПО;

2. регистрации событий безопасности (РСБ):

- сбор, запись и хранение информации о событиях безопасности в течении установленного времени хранения;
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них;

3. контроля (анализа) защищенности информации (АНЗ):

- выявление, анализ уязвимостей ИС и оперативное устранение вновь выявленных уязвимостей;
- контроль установки обновлений ПО, включая обновление ПО средств защиты информации;
- контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ;
- контроль состава технических средств, ПО и СЗИ;

4. обеспечения целостности ИС и информации (ОЦЛ):

- контроль целостности ПО, включая ПО СЗИ;

5. защиты среды виртуализации (ЗСВ):

- контроль целостности виртуальной инфраструктуры и её конфигураций;

6. управления конфигурацией ИС и системы защиты персональных данных (УКФ):

- управление изменениями конфигурации ИС и системы защиты персональных данных;
- документирование информации (данных) об изменениях в конфигурации ИС и системы защиты персональных данных.

Система может использоваться для реализации мер по обеспечению безопасности значимых объектов критической информационной инфраструктуры в соответствии с приказом ФСТЭК России № [239](#) от 25 декабря 2017 г., в части:

1. идентификация и аутентификация (ИАФ):

- инвентаризация информационных ресурсов;
- анализ уязвимостей и их устранение;
- регистрация событий безопасности;
- мониторинг безопасности;
- проведение внутренних аудитов;
- проведение внешних аудитов;

2. обеспечение целостности (ОЦЛ):

- контроль целостности ПО;
- контроль целостности информации;

3. управление конфигурацией (УКФ):

- идентификация объектов управления конфигурацией;
- управление изменениями;
- контроль действий по внесению изменений;

4. управление обновлениями ПО (ОПО):

- поиск, получение обновлений ПО от доверенного источника;
- контроль целостности обновлений ПО;
- установка обновлений ПО.

1.2 Репозиторий OVALdb

Информационной базой Системы является Репозиторий проблем безопасности OVALdb (далее – Репозиторий, OVALdb), разработанный и сопровождаемый АО «АЛТЭКС-СОФТ».

Репозиторий OVALdb является открытым и размещен на сайте <https://ovaldb.ru.altx-soft.ru/>.

Информация в Репозитории представлена на основе языков и классификаторов, входящих в Протокол Автоматизации Контента Безопасности (SCAP, Security Content Automation Protocol). Определения уязвимостей выполнены на языке OVAL (Open Vulnerability and Assessment Language).

Кроме контента, разработанного компанией АЛТЭКС-СОФТ, его содержание синхронизировано с экспертными ресурсами, такими как БДУ ФСТЭК России, НКЦКИ, бюллетени производителей и ряд других международных экспертных справочников. Периодичность публикации новых определений составляет 2-3 дня в соответствии с публикациями экспертных ресурсов и производителей. В случае обнаружения критической и распространенной уязвимости, информация в репозитории появляется в тот же день.

Информация является общедоступной и может свободно использоваться любым заинтересованным частным или юридическим лицом в исследовательских или собственных целях, исключая коммерческое использование, в том числе встраивание в виде компонентов в другие программные продукты.

1.3 Архитектура RedCheck

RedCheck состоит из перечня компонентов, разработанных АО «АЛТЭК-СОФТ» в рамках единой платформы, которые рекомендуется устанавливать на одном сервере. RedCheck состоит из следующих компонентов:

- RedCheck Api (REST API компонент)
- RedCheck Web (Веб-консоль)
- RedCheck Sync Service (служба синхронизации контента безопасности)
- RedCheck Scan Service (служба сканирования)
- RedCheck Cleanup Service (служба очистки базы данных)
- RedCheck LDAP Import Tools (утилита импорта хостов из AD –

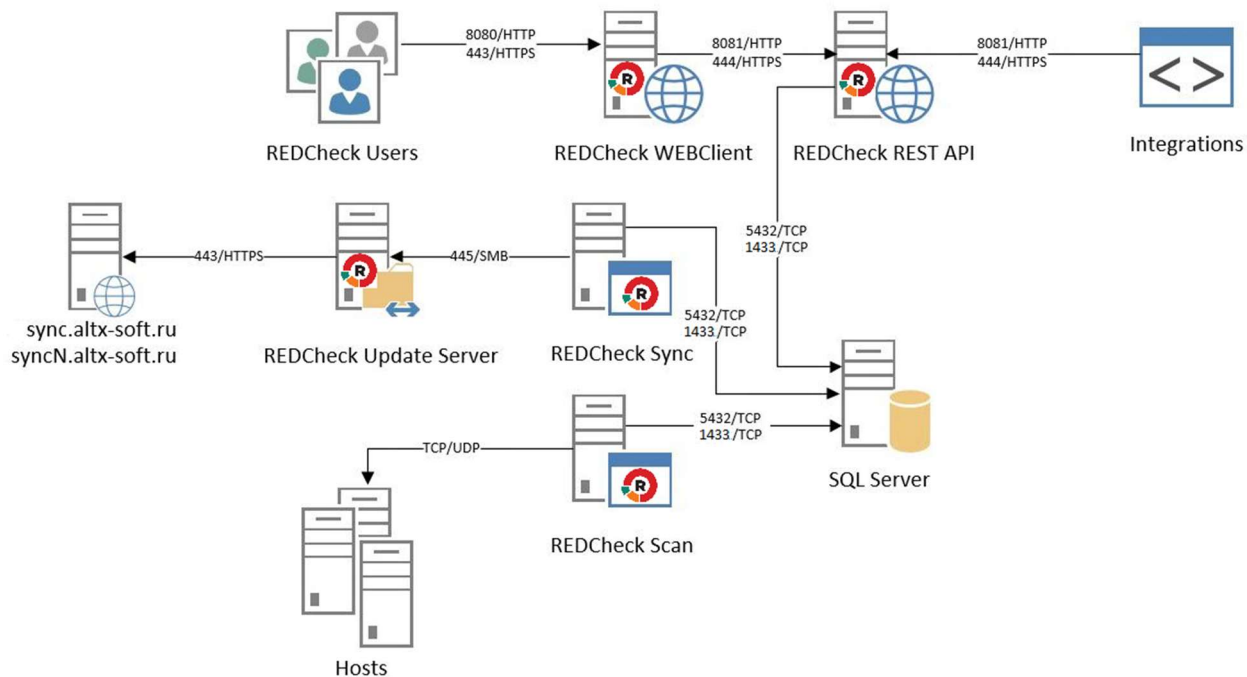
[Руководство](#))

RedCheck может использовать несколько служб сканирования (RedCheck Scan Service), в соответствии с используемой лицензией.

RedCheck также поддерживает распределенное расположения компонентов.

Схема взаимодействия компонентов между собой при такой установке

приведена на рисунке ниже:



RedCheck Update Server является необязательным компонентом и лицензируется отдельно. Установка RedCheck Update Server производится в DMZ-сегменте сети для обновления контента безопасности без доступа к сети Интернет со стороны компонента RedCheck Sync.

1.4 Функциональные возможности

В процессе выполнения всех типов заданий не требуется остановка или перезапуск сервисов на конечных хостах.

Обнаружение хостов

RedCheck выполняет поиск активных хостов и контроль целостности сети по заданному пулу сетевых адресов. Для обнаруженных в сети хостов определяется их IP-адрес, DNS, FQDN, NetBIOS, тип операционной системы. Также имеется возможность определить наличие агента RedCheck. По результатам выполнения задания впервые выявленные хосты могут быть импортированы в одну из существующих групп Системы, или экспортированы во внешний файл.

Сканирование выполняется без привилегий в режиме Черного ящика.

Аудит в режиме «Пентест»

В рамках данного аудита RedCheck позволяет выполнить сетевое сканирование без привилегий в режиме Черного ящика. Аудит в режиме «Пентест» может выполнить следующие типы сканирований в рамках одного задания:

- Сканирование портов — проведение сетевой инвентаризации без привилегий для опубликованных служб каждого хоста, выявление ПО и его версии;
- Поиск уязвимостей — проведение аудита уязвимостей без привилегий с выполнением дополнительных скриптов для выявленного по итогам сетевой инвентаризации ПО.
- Подбор паролей — выполнение подбора паролей на основе указанных словарей для требуемых сетевых служб.

Аудит уязвимостей

RedCheck выполняет централизованное сетевое или локальное сканирование хостов на наличие уязвимостей ОС, общесистемного и прикладного ПО, а также сетевого оборудования. Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик). Во время сканирования сопоставляется состояние параметров системы сигнатурам уязвимостей, содержащихся в открытом Репозитории OVALdb и описанных в формате SCAP.

Аудит обновлений

RedCheck позволяет обнаружить неустановленные обновления безопасности на узлах сети и сформировать необходимые ссылки для загрузки недостающих обновлений. Объектами аудита являются актуальные клиентские и серверные Windows и Linux операционные системы, а также широкий перечень другого общесистемного и прикладного ПО или сетевого оборудования ([1.9 Перечень поддерживаемых платформ](#)). Результат аудита обновлений содержит: наименования обновлений, сведения о рисках, связанных с отсутствием недостающего обновления на узле сети, ссылку на производителя, заявившего о выходе обновления, ссылку на репозиторий (базу), где хранятся доступные для загрузки обновления.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

В RedCheck реализован механизм управления обновлениями совместно со службой WSUS.

Аудит конфигураций

RedCheck позволяет автоматизировать процесс контроля параметров безопасности и осуществлять оценку соответствия информационных систем, ее отдельных компонентов или хостов, стандартам, политикам безопасности,

рекомендациям вендоров или другим «признанным практикам» (best practices). RedCheck содержит большое количество готовых конфигураций, разработанных на основе требований международных стандартов и рекомендаций. Поддержка стандартизированного формата SCAP позволяет пользователям загружать сторонние конфигурации, или использовать собственные.

Также Аудит конфигураций позволяет проводить проверку СУБД на соответствие параметров конфигурации или политике безопасности, например:

- требованию к парольной политике;
- требованию к методам аутентификации;
- требованию к разграничению доступа БД;
- требованию к резервному копированию и восстановлению БД.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Инвентаризация

RedCheck позволяет получать детальную информацию об аппаратных и программных средствах сканируемых хостов, включая: типы и описание оборудования, версии и редакции операционных систем, установленные пакеты обновлений и исправлений, установленное ПО, запущенные службы, пользователей и групп, сведения об общих папках. Глубокая детализация отчетов и использование функции Контроль позволяет отслеживать самые незначительные изменения в составе программного и аппаратного обеспечения сети. Реализована возможность инвентаризации образов Docker.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Фиксация (контроль целостности)

RedCheck может обнаружить и оповестить о несанкционированных изменениях целостности в конфигурационных файлах, папках, ветках реестра (автозагрузка, файл hosts, файл конфигурации межсетевого экрана). Включение режима Контроль позволяет с заданной периодичностью осуществлять проверку целостности эталонных файлов.

Контроль целостности папок и файлов осуществляется по выбранной маске наименования методом контрольного суммирования по алгоритмам MD5, SHA1, SHA256, SHA512, ГОСТ 34.11-2012.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Аудит систем контейнеризации

RedCheck позволяет проводить комплексный аудит безопасности для образов и контейнеров, реализованных на базе платформы контейнеризации Docker, а также системы оркестрации и масштабирования Kubernetes. В рамках данной функции доступны проверки на уязвимости, критичные неустановленные обновления безопасности, неверные настройки параметров конфигураций, инвентаризация, фиксация и контроль целостности. В рамках штатных функциональных возможностей доступна отдельная задача проверки уязвимостей файлов-образов Docker с учетом архитектуры слоев.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Аудит уязвимостей АСУ ТП

Аудит уязвимостей АСУ ТП предназначен для проведения проверок на наличие уязвимостей протоколов АСУ ТП.

Выявление уязвимостей проводится путем сопоставления сигнатур, хранящихся в БД RedCheck, с идентификационными сведениями о запущенном и опубликованном на сканируемом хосте ПО.

Сканирование выполняется на сетевом уровне, без использования привилегий или учетных записей (Черный ящик).

Проверка доступности

RedCheck обладает возможностью проверки доступности добавленных хостов для любых системных режимов сканирования с привилегиями (Белый ящик), учитывая настроенные транспорты/протоколы доступа и учетные записи RedCheck для сканирования.

Результатом выполнения задания является информация о доступности хоста для выполнения сканирования с привилегиями (Белый ящик), либо конкретный отсутствующий параметр настройки.

Сканирование выполняется либо с использованием агента RedCheck, либо на основе безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Сканирование YARA правил

RedCheck позволяет автоматизировать обнаружение вредоносных объектов за счет применения сигнатурного анализа на основе набора пользовательских YARA правил.

Результатом выполнения задания является список успешно обработанных правил и информация о файлах, в которых было обнаружено сигнатурное совпадение.

Сканирование выполняется по безагентной технологии с использованием привилегированных учетных записей (Белый ящик).

Задания могут выполняться как по расписанию, так и по требованию.

Документирование результатов аудита (Отчеты)

Функция Документирование результатов аудита позволяет по итогу проверок сформировать отчет в Системе и сохранить его в файл формата HTML, PDF, MHT, CSV или XML.

Система позволяет осуществлять отправку отчетов по электронной почте, а также экспортировать результаты проверок в программы сторонних организаций.

Функция Контроль

Данная опция позволяет выбрать результат сканирования необходимого задания для сравнения с последующими результатами того же задания (эталон). Контроль работает с заданиями Аудит уязвимостей, Аудит конфигураций, Инвентаризация и Фиксация. Сравнение новых отчетов с эталоном позволяет увидеть произошедшие изменения на хосте.

Компонент Аналитики

Данная функция необходима для контроля сканирования инфраструктуры, анализа и устранения уязвимостей и соответствия конфигурациям безопасности. Инструмент позволяет точно определить, как проблемы доступа к хостам, так и анализ их сканирования в регламент.

Анализ уязвимостей позволяет определить появление новых угроз, количество не устраненных, а также отдельный список по закрытым проблемам безопасности, в указанный пользователем регламент (срок анализа в днях).

Данный функционал приближает классический сканер безопасности RedCheck к возможностям мощных VM-решений без необходимости проводить интеграции и управлять уязвимостями по результатам сканирования в едином интерфейсе.

1.5 Ролевая модель RedCheck

Сегментная ролевая модель

В RedCheck реализована сегментная ролевая модель. Это позволяет разбивать инфраструктуру на непересекающиеся между собой сегменты. К каждому сегменту администратор (суперпользователь) привязывает пользователей RedCheck. Каждый пользователь может взаимодействовать с объектами только своего сегмента, а именно:

- группы;
- хосты;
- задания;
- отчеты;
- результаты сканирования.

После установки RedCheck создается сегмент по умолчанию (Default).

Про управление сегментами читайте в [4.1 Настройка ролевой модели](#).

Разграничение прав доступа

В RedCheck для разграничения прав доступа реализована ролевая модель. Пользователями Системы могут быть доменные учетные записи ОС, а также локальные пользователи RedCheck ([4.1 Настройка ролевой модели](#)). Роль пользователя в Системе определяется его принадлежностью к одной из четырех групп безопасности RedCheck:

- **REDCHECK_ADMINS** – Суперпользователь;
- **REDCHECK_ADMINIS** – Администратор ИБ;
- **REDCHECK_SYSTEMS** – Системный Администратор;
- **REDCHECK_USERS** – Пользователь ИБ.

Перечень возможностей ролей пользователей RedCheck

Управление – возможность создавать, просматривать, изменять и удалять.

Название роли	Перечень возможностей
Суперпользователь (RedCheck_Admins)	<ul style="list-style-type: none">▪ Обладает всеми возможностями в рамках работы с консолью управления RedCheck
Администратор ИБ (Redcheck_Adminis)	<ul style="list-style-type: none">▪ Управление хостами (+импорт / экспорт хостов);▪ Управление группами;▪ Просмотр учетных записей;▪ Управление заданиями;▪ Просмотр и удаление результатов сканирования;▪ Управление функцией Контроль для выполненного задания▪ Управление отчетами;▪ Управление профилями для Аудита уязвимостей / конфигураций;▪ Просмотр пользователями для работы с RedCheck▪ Запуск синхронизации контента безопасности и импортирование OVAL-сигнатур;▪ Просмотр журнала событий и справки о программе;
Системный администратор (RedCheck_Systems)	<ul style="list-style-type: none">▪ Управление хостами (+импорт / экспорт хостов);▪ Управление группами;▪ Управление учетными записями;▪ Просмотр свойств заданий;▪ Управление профилями для Аудита уязвимостей / конфигураций (допустимо удаление только пользовательских профилей);▪ Изменять настройки RedCheck (+ смена лицензионного ключа);▪ Запуск и настройка синхронизации контента безопасности;

	<ul style="list-style-type: none">▪ Просмотр журнала событий и справки о программе;
Пользователь ИБ (RedCheck_Users)	<ul style="list-style-type: none">▪ Просмотр свойств хостов;▪ Просмотр свойств групп;▪ Просмотр учетных записей;▪ Просмотр свойств заданий;▪ Просмотр результатов сканирования;▪ Просмотр работы функции Контроль для отчета выполненного задания▪ Просмотр отчетов;▪ Просмотр профилей для Аудита уязвимостей / конфигураций;▪ Просмотр справки о программе;▪ Запуск синхронизации контента безопасности;

1.6 Редакции RedCheck

RedCheck доступен в четырех редакциях:

Base – предоставляет необходимые инструменты для аудита уязвимостей и обновлений Windows и Linux систем при повседневном контроле защищённости ИС.

Professional – включает в себя основной набор возможностей Системы для мониторинга и управления защищённостью сетей корпоративного уровня.

Expert – включает все функции и сканируемые платформы, позволяет проводить комплексный аудит безопасности образов на базе платформы контейнеризации Docker.

Enterprise – обладает всеми имеющимися функциональными возможностями Системы. Редакция ориентирована на крупные и распределённые ИС и обладает возможностью подключения дополнительных модулей сканирования.

Функциональные возможности	Base	Professional	Expert	Enterprise
ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ				
Обнаружение хостов	+	+	+	+
Аудит в режиме «Пентест»	+	+	+	+
Аудит уязвимостей	+	+	+	+
Аудит обновлений	+	+	+	+
Аудит конфигураций	–	+	+	+

Инвентаризация	+	+	+	+
Фиксация и контроль	+	+	+	+
Аудит СУБД	–	+	+	+
Аудит уязвимостей АСУ ТП	–	за дополнительную плату (по количеству хостов)		
Аудит уязвимостей образов Docker	–	–	+	+
Проверка доступности	+	+	+	+
Отчеты по результатам аудитов	+	+	+	+
Компонент Аналитики	–	–	+	+
ОБЪЕКТЫ СКАНИРОВАНИЯ				
ОС Windows и Linux	+	+	+	+
Сетевое оборудование	–	+	+	+
Протоколы АСУ ТП	–	за дополнительную плату (по количеству хостов)		
Средства виртуализации	–	+	+	+
Средства контейнеризации и оркестрации	–	–	+	+
СУБД	–	+	+	+
ДОПОЛНИТЕЛЬНЫЙ СЕРВИС				
Сертифицированная версия	+	+	+	+

Системы				
Адаптация конфигураций	за дополнительную плату			+
Разработка индивидуальных конфигураций безопасности	–	за дополнительную плату		
Расширенная поддержка	за дополнительную плату			+
АРХИТЕКТУРА И МАСШТАБИРУЕМОСТЬ				
Подключение дополнительных служб сканирования (лицензируются отдельно)	–	–	+	+
Многопоточное сканирование Белым ящиком	+	+	+	+
Многопоточное сканирование Черным ящиком («Пентест»)	+	+	+	+
Возможность интеграции с помощью RestAPI	–	+	+	+
Web-консоль управления	+	+	+	+

Информация о версии и установленных службах программы, а также об ограничениях используемой редакции RedCheck, находится в пункте **Справка** → **О программе**.

1.7 Лицензирование

Система лицензируется согласно редакциям, указанным в [1.6 Редакции RedCheck](#)

Система лицензирования не накладывает ограничений на количество проводимых аудитов, их повтор, а также количество сканируемых хостов в каждом аудите в пределах используемой лицензии.

Срок действия лицензии составляет 1-3 года, возможно приобретение RedCheck на 2 года или более. В период действия лицензии пользователю RedCheck бесплатно предоставляется базовая техническая поддержка, доступ к актуальному контенту безопасности и обновления версий RedCheck.

Сведения об актуальных лицензиях на САЗ RedCheck и ценах приведены в официальном [прайс-листе](#), опубликованном сайте продукта <https://www.redcheck.ru> и официальном [сайте компании](#)

[ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ REDCHECK \(EULA\)](#)

1.8 Как получить тестовую версию?

Для приобретения лицензии RedCheck необходимо обратиться в отдел продаж АО «АЛТЭК-СОФТ» в свободной форме – sales@altx-soft.ru или к партнерам в вашем регионе - https://www.altx-soft.ru/company/partner_net/

Чтобы получить тестовую версию RedCheck, необходимо:

Шаг 1. Перейти на сайт [RedCheck](#) → Скачать тестовую версию.

Шаг 2. Через [форму обратной](#) связи заполнить обязательные поля для выдачи тестовой лицензии.

Шаг 3. В течение рабочего дня на электронную почту, указанную при запросе, будет отправлено сообщение с тестовым лицензионным ключом и краткой инструкцией по использованию.

RedCheck доступен в следующих версиях:

- Сертифицированная ФСТЭК России версия (для других государств могут быть доступны сертифицированные версии по требованиям собственного регулятора, информацию о доступности можно получить у соответствующего дистрибьютора);
- Несертифицированная старшая версия (обладает новыми функциями и находится на сертификации).

Сертифицированная ФСТЭК России версия RedCheck поставляется в течении 5-10 рабочих дней. В поставку входят:

- сертифицированная версия дистрибутива на USB-носителе;
- лицензия на бланке с уникальным ключом;
- комплект сопроводительной и эксплуатационной документации (на USB-носителе);
- копия Сертификата соответствия ФСТЭК России;
- абонемент на расширенную техническую поддержку (при заказе).

При необходимости [обновления контента ИБ](#) в офлайн режиме используется пара логин/пароль для доступа к Центру сертифицированных обновлений.

Несертифицированная версия RedCheck поставляется в электронном виде в течении 1-3 рабочих дней. В поставку входят:

- лицензия/ии на бланке с уникальным ключом (электронно, pdf);
- абонемент на расширенную техническую поддержку (при заказе, электронно).

1.9 Перечень поддерживаемых платформ

Microsoft Windows

- XP¹ / XP Embedded / Vista / 7 / 8 / 8.1 / 10 / 11
- Server 2003² / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019 / 2022

Linux

- AlmaLinux 8.x / 9.x
- Amazon Linux 2 / AMI / 2023
- Alpine 3.9 – 3.22 / edge
- CentOS Linux 5 / 6 / 7 / 8
- CentOS Stream 8 / 9
- Debian 6.0 / 7 / 8 / 9 / 10 / 11 / 12
- Debian GNU/kFreeBSD 6 / 7
- Debian GNU/Linux 2.2 / 3.0 / 3.1 / 4.0 / 5.0 / 6.0 / 7
- Fedora CoreOS 34
- FreeBSD 10 / 11 / 12
- Linux Mint 17 / 18 / 19 / 20
- Mageia 4 / 5 / 6 / 7 / 8 / 9
- openSUSE 10.2 / 10.3 / 11.0 / 11.1 / 11.2 / 11.3 / 11.4 / 12.1 / 12.2 / 12.3 / 13.1 / 13.2
- openSUSE Leap 15.0 / 15.1 / 15.3 / 15.4 / 42.1 / 42.2 / 42.3
- Oracle Solaris 10 / 11 / 11.1 / 11.2 / 11.3 / 11.4
- Oracle Linux 4 / 5 / 6 / 7 / 8 / 9
- Red Hat Enterprise Linux 3 / 4 / 5 / 6.x / 7.x / 8.x / 9.x
- Red Hat CoreOS 4
- Rocky Linux 8 / 9
- Solaris 10 / 11
- SUSE CaaS Platform 3 / 4
- SUSE Linux Enterprise Desktop 10 / 11 / 12 / 15
- SUSE Linux Enterprise Server 10 / 11 / 12 / 15
- SUSE Linux Enterprise Server for SAP 11 / 12 / 15
- SUSE Linux Enterprise Point of Service 11
- SUSE Linux Enterprise Real Time 11 / 15
- SUSE Linux Enterprise High Performance Computing 15
- Ubuntu 4.10 / 5.04 / 5.10 / 6.06 / 6.10 / 7.04 / 7.10 / 8.04 / 8.10 / 9.04 / 9.10 / 10.04 / 10.10 / 11.04 / 11.10 / 12.04 / 12.10 / 13.04 / 13.10 / 14.04 / 14.10 / 15.04 / 15.10 / 16.04 / 16.10 / 17.04 / 17.10 / 18.04 / 18.10 / 19.04 / 19.10 / 20.04 / 20.10 / 21.04 / 21.10 / 22.04 / 22.10 / 23.04 / 23.10 / 24.04 / 24.10 /

25.04

- VMware Photon OS 1.0 / 2.0 / 3.0 / 4.0

Отечественные ОС

- ALT Linux SPT 6 / 7
- ALT 8 SP / 10 SP
- ALT 9 / 10
- Astra Linux CE (Орёл) 2.12
- Astra Linux SE 1.5 / 1.6 / 1.7 / 1.8 Орел / Воронеж / Смоленск
- RED OS MUROM 7.1 / 7.2 / 7.3
- ROSA DX COBALT 1.0
- ROSA SX COBALT 1.0
- ROSA Cobalt 7.9
- ROSA Enterprise Linux Desktop 7.3
- ROSA Enterprise Linux Server 7.3
- SberLinux OS Server
- SberLinux CoreOS

Сетевое оборудование

- Check Point GAiA
- Cisco IOS
- Cisco NX-OS
- Eltex серии ESR / MES
- FortiGate FortiOS 5.0 и выше
- Huawei VRP
- UserGate UTM 6.1.0.10123F / 6.1.5.11134R и выше

Виртуализация

- Astra Linux "Брест"
- Microsoft Hyper-V Server 2008 / Hyper-V Server 2008 R2 / Hyper-V Server 2012 / Hyper-V Server 2012 R2
- как роль Windows Server 2008 / Windows Server 2008R2 / Windows Server 2012 / Windows Server 2012 R2
- ROSA Virtualization 2.1
- VMware ESXi Server 5.0 / 5.1 / 5.5 / 6.0 / 6.5 / 6.7 / 7
- VMware vCenter Server 5.1 / 5.5 / 6.0 / 6.5 / 6.7 / 7
- VMware NSX

СУБД

- Microsoft SQL Server 2005 / 2008 / 2008 R2 / 2012 / 2014 / 2016 / 2017 / 2019 / 2022
- MySQL Server 4.1 / 5.0 / 5.1 / 5.5 / 5.6 / 5.7 / 6.0 / 8.0 / 8.1 / 8.2
- Oracle Database Server 11 / 12 / 18 / 19
- Pangolin
- PostgreSQL 8 / 9 / 10 / 11 / 12 / 13 / 14 / 15 / 16

АСУ ТП

- Codesys V2 / V3
- Citect SCADA
- Iconics GENESIS (32/64)
- IGSS
- Siemens Automation License Manager
- Siemens SICAM PAS
- Siemens Simatic WinCC
- Siemens Simatic WinCC flexible
- Siemens STEP7
- Wonderware InTouch

ПЛК

- ПЛК Агава
- ПЛК Кастом
- ПЛК Овен
- ПЛК Элси
- ПЛК Advantech APAX-xxxxKW, ADAM-xxxxKW
- ПЛК Ergon
- ПЛК Fastwel
- ПЛК Omron
- ПЛК RealLab!
- ПЛК Rockwell Automation
- ПЛК Siemens Simatic S7
- ПЛК Schneider Electric Modicon
- ПЛК Yokogawa FCN

Контейнеризация

- Docker 1.13.0 и выше (Storage Driver overlay2)
- Kubernetes 1.18 / 1.19 / 1.20 / 1.21 / 1.22 / 1.23 / 1.24

¹RedCheck не поддерживает сканирование Windows XP при помощи WinRm-туннеля;

²RedCheck не поддерживает сканирование Windows Server 2003 при помощи агента;

Полный перечень поддерживаемого ПО доступен [по ссылке](#).

В Таблицах 1-3 представлены возможные режимы сканирования для соответствующих типов заданий.

Таблица 1 Операционные системы

Цели сканирований/Типы заданий	Windows	Linux	FreeBSD	Solaris
Аудит уязвимостей	A/RE	AL	AL	AL
Аудит обновлений	A/RE	AL	NA	NA
Аудит конфигураций	A/RE	AL	NA	AL
Инвентаризация	A/RE	AL	NA	NA
Фиксация	A/RE	AL	NA	NA
Аудит в режиме Пентест	BB	BB	BB	BB

Таблица 2 Сетевое оборудование

Цели сканирований/Типы заданий	Huawei	Check Point	Cisco	FortiOS	UserGate	Eltex
Аудит уязвимостей	NA	AL	AL	AL	AL	AL
Аудит обновлений	NA	NA	NA	NA	NA	NA
Аудит конфигураций	AL	AL	AL	AL	AL	AL
Инвентаризация	NA	AL	AL	AL	AL	AL
Фиксация	NA	NA	NA	NA	NA	NA
Аудит в режиме Пентест	BB	BB	BB	BB	BB	BB

Таблица 3 Системы виртуализации и контейнеризации

Цели сканирований/Типы заданий	VMWare	Docker
Аудит уязвимостей	AL	AL
Аудит обновлений	AL	NA
Аудит конфигураций	AL	AL
Инвентаризация	AL	AL
Фиксация	AL	NA
Аудит в режиме Пентест	BB	BB

Условные обозначения

«A» – агент;

«AL» – безагент (SSH);

«RE» – безагент (WinRM);

«NA» – режим сканирования и тип задания не применимы;

«BB» – аудит методом черного ящика.

1.10 Перечень интегрируемых систем

RedCheck имеет действующие интеграции со следующими SIEM-системами:

- Kaspersky KUMA ([официальный сайт](#));
- Neurodat SIEM ([официальный сайт](#));
- R-Vision ([официальный сайт](#));
- Security Vision; ([официальный сайт](#))

Инструкцию по интеграции и конфигурации можно найти на сайте разработчика SIEM-системы или при обращении к ним в техническую поддержку.

1.11 Служба технической поддержки

Технические вопросы, связанные с использованием сканера безопасности RedCheck, можно задать нашей службе технической поддержки удобным для Вас способом:

- Web-портал: portal.altx-soft.ru
- Электронная почта: support@altx-soft.ru
- Web-сайт продукта: redcheck.ru

При обращении в службу технической поддержки необходимо указать:

- номер лицензии;
- номер купона для расширенной технической поддержки;
- наименование представляемой организации;
- прикрепить полные скриншоты окна консоли, где зафиксирована проблема и описать действия, которые приводят к такому результату
- в случае ошибок в работе Системы, прикрепить файл журнала событий соответствующей службы, в котором зафиксирована проблема.

С Регламентом оказания технической поддержки можно ознакомиться на [сайте](#) производителя.

2 Системные требования

Содержание

- [2.1 Требования к аппаратному обеспечению](#)
- [2.2 Требования к программному обеспечению](#)
- [2.3 Требования к сетевой инфраструктуре](#)

2.1 Требования к аппаратному обеспечению

Допускается установка компонентов RedCheck на виртуальные машины. При этом система виртуализации должна быть совместима с ОС, представленными в пункте [2.2 Требования к программному обеспечению](#)

Требования к аппаратным ресурсам, которые необходимы для корректной работы RedCheck:

Компоненты	Аппаратные требования
Совместная установка	
Серверный компонент (redcheck-api) Консоль управления (redcheck-client) Служба сканирования (redcheck-scan-service) Служба синхронизации (redcheck-sync-service)	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 4 ядер ОЗУ не менее 12 ГБ ПЗУ не менее 2 ГБ
Раздельная установка	
Серверный компонент (redcheck-api) Консоль управления (redcheck-client)	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ

Служба сканирования (redcheck-scan-service)	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ
Служба синхронизации (redcheck-sync-service)	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 4 ГБ ПЗУ не менее 1 ГБ
Сервер СУБД ¹	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 10 ГБ (рекомендации по расчету объема БД приведены ниже)
Дополнительные компоненты	
Дополнительный модуль сканирования	ЦП Xeon, частота не ниже 1,86 ГГц, не менее 2 ядер ОЗУ не менее 6 ГБ ПЗУ не менее 1 ГБ

Требования к объему HDD представлены без учета размещения на ЭВМ операционных систем, СУБД и другого системного и прикладного ПО.

¹ - В случае размещения сервера СУБД совместно с компонентами RedCheck аппаратные требования складываются.

Значения в таблице являются рекомендуемыми, реальное потребление может отличаться в зависимости от сценариев использования Системы. Рекомендуется выполнять мониторинг потребления CPU и памяти на хостах для оптимизации потребления ресурсов.

Выделяемый объем HDD на сервере БД предназначен для хранения контента ИБ и результатов сканирования. При определении необходимого объема HDD следует учитывать следующие факторы:

- количество сканируемых хостов + количество типов аудитов для каждого хоста;
- частота проводимых сканирований;
- период хранения результатов сканирования в БД.

Ориентировочно необходимый объем HDD (для одного типа аудита) можно определить по следующей формуле:

$$V_{HDD} \approx V_{ср} NT$$

где V_{HDD} – необходимый объем HDD, ГБ; $V_{ср}$ – средний объем результатов сканирования одного хоста,

$V_{ср} \approx 2$ МБ; N – количество сканируемых хостов, ед.

T – период хранения результатов сканирования в БД, нед.

Так, для хранения результатов еженедельного сканирования 100 хостов в течение полугода, необходимо выделить $0,002 \cdot 100 \cdot 26 = 5,2$ ГБ свободного дискового пространства.

Значения выделяемого объема HDD на сервере БД в зависимости от количества сканируемых хостов (для одного типа аудита) представлены в таблице.

Количество сканируемых хостов	Частота сканирования	HDD*, ГБ
Не более 200	1 раз в квартал	3

	1 раз в месяц	6
	1 раз в неделю	22
От 200 до 500	1 раз в квартал	5
	1 раз в месяц	13
	1 раз в неделю	53
От 500 до 2000	1 раз в квартал	20
	1 раз в месяц	52
	1 раз в неделю	212
2000**	1 раз в квартал	35
	1 раз в месяц	100
	1 раз в неделю	400

* Значения представлены из условия хранения результатов сканирования в течении одного года.

** Для обеспечения быстродействия и уменьшения временных интервалов выполняемых операций с БД рекомендуется СУБД располагать на SSD. Использование SSD должно применяться совместно с выполнением работ по оптимизации и тонкой настройке СУБД.

2.2 Требования к программному обеспечению

Требования к ПО для корректного функционирования основных компонентов RedCheck:

- ОС:
 - Astra Linux 1.7.6 SE (Смоленск / Воронеж / Орел);
 - Astra Linux 1.8.1 SE (Смоленск / Воронеж);
 - Debian 12;
 - РЕД ОС 7.3;
 - SberLinux 9;
- СУБД:
 - [PostgreSQL](#) версия 12.5 – 16;
 - [Postgres Pro](#) версия 14 / 15;
 - [Jatoba](#) 4.13.2 / 5.8.2 / 6.6.1
 - Platform V Pangolin;
- Браузер на основе ядра Chromium;
- Командная оболочка Bash;
- Статическая строка приглашения (динамическая строка приглашения не поддерживается).

2.3 Требования к сетевой инфраструктуре

Взаимодействие осуществляется по протоколам стека сетевых протоколов TCP/IP. Инициация сетевых взаимодействий осуществляется Источником с использованием динамических портов, определенных в ОС.

Все порты назначения могут быть переопределены, кроме получения обновлений с официального репозитория производителя (Сервис синхронизации - <https://syncn.altx-soft.ru>).

Таблица 1 – перечень сетевых портов взаимодействия компонентов RedCheck

Источник	Назначение	Порт назначения	Прикладной протокол/комментарий
Веб-консоль RedCheck	Веб-консоль RedCheck	8080/TCP	HTTP/Взаимодействие с веб-консолью (рекомендуется установить SSL-сертификат и переопределить порт)
Служба REST RedCheck	Служба REST RedCheck	8081/TCP	HTTP/Взаимодействие со службой REST RedCheck (рекомендуется установить SSL-сертификат и переопределить порт)
Веб-консоль RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен
Служба REST RedCheck	База данных	5432/TCP	Взаимодействие с базой данных
Служба REST RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен

Веб-консоль / Служба REST	Сервис электронных почтовых сообщений, e- mail	25/TCP	SMTP/Отправка почтовых уведомлений о результатах работы службы
Служба сканирования RedCheck	База данных	5432/TCP	Взаимодействие с базой данных
Служба сканирования RedCheck	Агент RedCheck на сканируемом объекте сети	8732/TCP	Взаимодействие с агентом сканирования RedCheck
Служба сканирования RedCheck	Агент RedCheck Update на сканируемом объекте сети	8733/TCP	Взаимодействие с агентом обновлений RedCheck
Служба сканирования RedCheck	Безагентное сканирование объектов сети	22/TCP	SSH/Безагентное сканирование Linux
		80, 443/TCP	HTTP/HTTPS/Безагентное сканирование объектов с веб-доступом
		1433/TCP	Сканирование баз данных Microsoft SQL Server
		3306/TCP	Сканирование баз данных MySQL
		5432/TCP	Сканирование баз данных Postgres SQL
		1521/TCP	Сканирование баз данных Oracle Database
		50000/TCP	Сканирование баз данных IBM DB2

		39015/TCP	Сканирование баз данных SAP HANA
Служба сканирования RedCheck	Сканирование в режиме «Пентест»	0-65535/UDP-TCP	Сканирование объектов сети в режиме Пентест
Служба сканирования RedCheck	Сетевой каталог	445/TCP	SMB/Взаимодействие с каталогом в сетевом размещении для хранения отчетов о результатах сканирования
Служба сканирования RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен
Служба синхронизации RedCheck	База данных	5432/TCP	Взаимодействие с базой данных
Служба синхронизации RedCheck	Сетевой каталог	445/TCP	SMB/Взаимодействие с каталогом обновлений в сетевом размещении с офлайн-контентом
Служба синхронизации RedCheck	Сервер обновлений RedCheck	445/TCP	SMB/Взаимодействие с каталогом обновлений на сервере обновлений RedCheck
Служба синхронизации RedCheck	Прокси-сервер	3128/TCP (порт зависит от службы прокси)	HTTPS/Доступ к сервису синхронизации производителя через прокси-сервер (https://syncn.altx-soft.ru)
Служба синхронизации RedCheck	Сервис синхронизации (https://syncn.altx-	443/TCP	HTTPS/Доступ к сервису синхронизации производителя

	soft.ru)		https://syncn.altx-soft.ru
Служба синхронизации RedCheck	Сервис электронных почтовых сообщений, e-mail	25/TCP	SMTP/Отправка почтовых уведомлений о результатах работы службы
Служба синхронизации RedCheck	Сервис DNS	53/TCP	DNS/Запросы в службу разрешения имен

Для обеспечения стабильной работы RedCheck, сетевая инфраструктура организации должна обеспечивать пропускную способность линий передачи, не ниже приведенной в таблице.

	Сканирование посредством SSH	Сканирование посредством Агента сканирования
Скорость передачи данных, Кбит/с	160	121
Суммарный объем трафика на узел, КБ	5 000	8 400

Приведенные в таблице значения рассчитаны для выполнения наиболее ресурсоемкого задания Аудит уязвимостей (полное сканирование).

3 Установка RedCheck Nix

Содержание

- [3.1 Astra Linux 1.7](#)
- [3.2 Astra Linux 1.8](#)
- [3.3 Debian 12](#)
- [3.4 РЕД ОС 7.3](#)
- [3.5 SberLinux](#)
- [3.6 Установка RedCheck Update Server \(Windows\)](#)
- [3.7 Установка агента RedCheck \(Windows\)](#)
- [3.8 Раздельная установка](#)
- [3.9 Добавление собственных сертификатов для https](#)

3.1 Astra Linux 1.7

Содержание

- [Установка СУБД](#)
- [Инсталляция RedCheck](#)
- [Конфигурация RedCheck](#)

Установка СУБД

Установка СУБД PostgreSQL с репозитория Astra Linux

Шаг 1. Откройте терминал комбинацией **Alt + T**;

Если хост без подключения к сети Интернет, скачайте репозитории в личном кабинете Astra Linux – [Подключение репозитория в Astra Linux без доступа к сети Интернет](#)

Шаг 2. Добавьте адрес репозитория в файл **/etc/apt/sources.list**:

Bash (оболочка Unix)

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

Для добавления репозитория в файл рекомендуем использовать текстовый редактор **nano**.

Шаг 1. Откройте файл с помощью команды;

Bash (оболочка Unix)

```
sudo nano /etc/apt/sources.list
```

Шаг 2. Скопируйте репозитории и вставьте их с помощью комбинации **Ctrl + U** (**Shift + Insert** или **Правка → Вставить**);

Шаг 3. Сохраните файл с помощью комбинации **Ctrl + O**; Для выхода используйте **Ctrl + X**;

Шаг 3. Обновите пакеты;

Bash (оболочка Unix)

```
sudo apt -y update
```

Шаг 4. Установите PostgreSQL;

Bash (оболочка Unix)

```
sudo apt -y install postgresql
```

Настройка PostgreSQL

Шаг 5. Добавьте службу **postgresql** в автозапуск;

Bash (оболочка Unix)

```
sudo systemctl enable postgresql
```

```
root@astra-db:/etc/apt# systemctl enable postgresql
Synchronizing state of postgresql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable postgresql
```

Шаг 6. Создайте пользователя для администрирования СУБД;

PostgreSQL по умолчанию создает суперпользователя **postgres**.

Bash (оболочка Unix)

```
sudo su postgres
```

Bash (оболочка Unix)

```
psql -U postgres
```

Bash (оболочка Unix)

```
CREATE ROLE redcheck WITH PASSWORD '12345' LOGIN CREATEDB SUPERUSER;
```

```

root@astra-db:/etc/apt# sudo su - postgres
postgres@astra-db:~$ psql -U postgres
psql (14.5 (Debian 14.5-1.pgdg90+1))
Введите "help", чтобы получить справку.

postgres=# CREATE ROLE redcheck WITH PASSWORD '12345' SUPERUSER LOGIN CREATEDB;
CREATE ROLE
postgres=# \q
postgres@astra-db:~$ exit
Выход
root@astra-db:/etc/apt# █

```

Для выхода из базы данных postgres введите `\q`

Шаг 7. Завершите сессию командой **exit**

Шаг 8. Откройте доступ по сети для серверов, на которых планируется установка REST-компонента и служб сканирования и синхронизации RedCheck;

Bash (оболочка Unix)

```

sudo echo "listen_addresses = 'ip_СУБД'" >>
/etc/postgresql/14/main/postgresql.conf

```

Bash (оболочка Unix)

```

sudo echo host all имя_пользователя_СУБД имя_сети/маска scram-sha-256
>> /etc/postgresql/14/main/pg_hba.conf

```

ip_СУБД – IP-адреса хостов, на которых установлена СУБД, службы сканирования, служба синхронизации и серверный компонент RedCheck,
имя_базы_данных – имя базы данных, которая создается при установке RedCheck (по умолчанию RedCheck),
имя_пользователя_СУБД – имя созданного ранее пользователя,
имя_сети/маска – сеть или один адрес, которым разрешается доступ к СУБД. К примеру, 192.168.100.0/24 или 192.168.100.15/32;

```

root@astra-db:/etc/apt# echo "listen_addresses = '192.168.1.8'" >> /etc/postgresql/14/main/postgresql.conf
root@astra-db:/etc/apt# tail -n1 /etc/postgresql/14/main/postgresql.conf
listen_addresses = '192.168.1.8'
root@astra-db:/etc/apt# echo "host all redcheck 192.168.1.0/24 md5" >> /etc/postgresql/14/main/pg_hba.conf
root@astra-db:/etc/apt# tail -n1 /etc/postgresql/14/main/pg_hba.conf
host all redcheck 192.168.1.0/24 md5
root@astra-db:/etc/apt# █

```

Чтобы узнать ip-адрес устройства, используйте команду **ip a**

Шаг 9. Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
sudo systemctl restart postgresql
```

Чтобы проверить работоспособность СУБД, используйте команду:

Bash (оболочка Unix)

```
systemctl status postgresql
```

При необходимости разрешите доступ к сетевому порту postgresql. Для установки брандмауэра ufw используйте команду:

Bash (оболочка Unix)

```
sudo apt install ufw
```

Bash (оболочка Unix)

```
sudo ufw allow 5432/tcp
```

Инсталляция RedCheck

Для обновления RedCheck – [4.8 Обновление RedCheck Nix](#)

Перед началом установки RedCheck в системе не должно быть пользователя с именем redcheck. Данное имя пользователя является служебным. Не допускается вносить изменения в права доступа, а также использовать в заданиях сканирования.

Шаг 1. Смонтируйте установочный диск и добавьте репозиторий в пакетный менеджер;

Bash (оболочка Unix)

```
sudo apt-cdrom add
```

Перед следующими шагами подключение репозиторий совместимости (3.10 Подключение репозитория совместимости)

Репозиторий совместимости расширяет список поддерживаемых версий Astra Linux 1.7 ([2.2 Требования к программному обеспечению](#))

Шаг 2. Разархивируйте скачанный архив redcheck-astra1.7-repo-2.12.0.20663.tar.gz в директорию /usr/local/src;

Bash (оболочка Unix)

```
sudo tar -xvf /home/имя_пользователя/Загрузки/redcheck-astra1.7-repo-2.12.0.20663.tar.gz -C /usr/local/src
```

Шаг 3. Добавьте GPG-ключ, который находится в только что разархивированном каталоге;

Bash (оболочка Unix)

```
sudo apt-key add /usr/local/src/redcheck-astra-repo/PUBLIC-GPG-KEY-
```

```
redcheck
```

Шаг 4. Создайте файл **redcheck.list** и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
echo "deb file:/usr/local/src/redcheck-astra-repo/ 1.7_x86-64 non-free" | sudo tee /etc/apt/sources.list.d/redcheck.list
```

Шаг 5. Обновите пакеты;

Bash (оболочка Unix)

```
sudo apt -y update
```

Шаг 6. Установите компоненты RedCheck;

Bash (оболочка Unix)

```
sudo apt -y install redcheck-api redcheck-client redcheck-scan-service redcheck-sync-service redcheck-cleanup-service
```

Конфигурация RedCheck

Содержание

- [Конфигурация всех компонентов](#)
- [Выборочная настройка компонентов](#)
- [Дополнительные параметры](#)

Если хост не подключен к сети Интернет, сначала получите файл лицензии. Если подключен, начните с шага 6.

Шаг 1. Сгенерируйте код активации командой:

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный - критичное сообщение либо ошибка выполнения команды
желтый  - важное замечание требующее действия от пользователя
зеленый - успешное выполнение команды либо статус выполнения конфигурации
[*]     - диапазон допустимых значений
(*)     - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

Выберите пункт **Получение кода активации** и введите ключ лицензии:

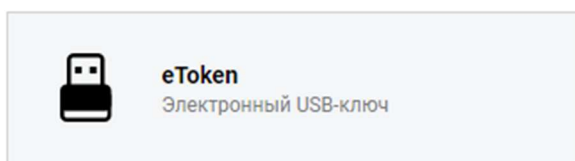
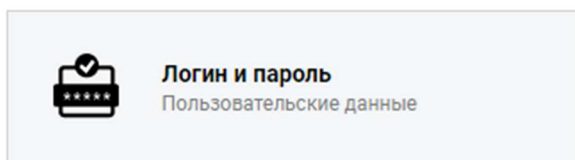
```
=====
Получение кода активации
=====
Введите ключ лицензии:
Код активации: BEE856C323A62FABFB6307CC01BFECDF85B035FEA71185B9284F3C78255CE7DC
Окончание получения кода активации
=====
```

Шаг 2. Авторизуйтесь в [Центре сертифицированных обновлений](#) с помощью логина и пароля;

Логин/пароль поставляется всем коммерческим клиентам в [Формуляре, раздел 15, «Особые отметки»](#) (начиная с 18.05.2022).

Центр сертифицированных обновлений

Для получения обновлений необходимо выбрать способ входа



Шаг 3. Раскройте **RedCheck лицензии** → выберите интересующий Вас номер лицензионного ключа;

Справка по конфигуратору вызывается командой **redcheck-bootstrap help**

Логи инсталлятора располагаются в **/var/opt/redcheck-common/log/configuration.log**

Перед повторной конфигурацией **рекомендуем [сделать резервную копию](#)** базы данных.

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

Выберите пункт **Настроить все сразу**, чтобы настроить все компоненты на одном сервере.

Первым шагом конфигуратор предложит ввести данные для подключения к базе данных:

```
Выберите действие [1-9]: 8
=====
Настройка подключения к БД
=====
Сервер СУБД [IP]: 192.168.80.129
Введите порт (5432):
Логин: redcheck
Пароль:
Введите имя БД: RedCheck
Настройка подключения к БД успешно
=====
```

Далее укажите пользовательский ключ шифрования для повышения безопасности данных в БД (по желанию):

```
=====
Настройка redcheck-api
=====
Проверяется версия сервера PostgreSQL..
Версия сервера PostgreSQL соответствует минимально необходимой
Проверяется наличие указанной БД на сервере..
БД с таким именем не найдена
Хотите создать новую БД? [Y/N] (Y): y
Создание БД..
Внимание! В случае использования пользовательского ключа шифрования – сохраните его и используйте при установке и переустановке всех компонентов программы. Утрата или неправильный ввод ключей при переустановке или обновлении компонентов программы на последующие версии при сохранении БД программы приведет к неработоспособности программы и отсутствию возможности использования сохранённых в БД учетных записей. Вы можете не использовать пользовательский ключ шифрования, при этом учетные данные, использованные программой, будут шифроваться, но с меньшим уровнем криптографической стойкости.
Введите пользовательский ключ шифрования: |
```

Выберите способ активации лицензии: онлайн (К - ключ) или офлайн (Ф - лицензионный файл):

```
проверка лицензии/активация продукта
=====
Выберите тип работы с лицензией – ключ лицензии или файл лицензии? (К/Ф,F): К
Введите ключ лицензии: |
```

При офлайн активации укажите путь к лицензионному файлу.

Следующим шагом выберите протокол и IP для работы redcheck-api. При выборе https инсталлятор сгенерирует самоподписанный сертификат. Аналогичная настройка и для redcheck-client.

```

Конфигурация redcheck-api новым подключением..
Новое подключение сохранено в конфигурационный файл redcheck-api
Обновление БД..
БД обновлена и готова к работе
Доступные протоколы:
[1] : https
[2] : http
Выберите протокол взаимодействия [1-2]: 1
Доступные интерфейсы:
[1] : 192.168.218.144
[2] : 192.168.80.32
Выберите интерфейс из списка доступных [1-2]: 2
Введите порт (445):
Сформировать сертификат на:
[1] : ip
[2] : dns
Выберите тип генерации сертификата [1-2]: 1
prepare gencert: redcheck-api 192.168.80.32 192.168.80.32
Генерация сертификата..
Generating a RSA private key
.....++++
.....++++
writing new private key to '/var/opt/redcheck-api/ssl/redcheck-api.key'
-----
Сертификат сформирован
(отсутствует переменная)
Nothing to do
libsemanage.map_file: Unable to open my-httpd.pp
(No such file or directory).
libsemanage.semanage_direct_install_file: Unable to read file my-httpd.pp
(No such file or directory).
semodule: Failed on my-httpd.pp!
Настройка redcheck-api успешна
=====

```

Далее укажите имя для службы сканирования и дождитесь настройки служб сканирования и синхронизации:

```

=====
Настройка redcheck-scan-service
=====
Проверка БД на соответствие требованиям для установки службы сканирования..
Выполняется проверка подключения к БД для redcheck-scan-service
Подключение к БД установлено
Конфигурация redcheck-scan-service новым подключением..
Новое подключение сохранено в конфигурационный файл redcheck-scan-service
Введите имя службы: scan
Проверка прошла успешно. Служба сканирования может быть установлена к указанной БД
Служба сканирования обновлена
Настройка redcheck-scan-service успешна
=====
Настройка redcheck-sync-service
=====
Выполняется проверка подключения к БД для redcheck-sync-service
Подключение к БД установлено
Конфигурация redcheck-sync-service новым подключением..
Новое подключение сохранено в конфигурационный файл redcheck-sync-service
Проверка БД на соответствие требованиям для установки службы синхронизации..
Проверка прошла успешно. Служба синхронизации может быть установлена к указанной БД
Служба синхронизации обновлена
Настройка redcheck-sync-service успешно
=====

```

Если вы установили пакет компонента redcheck-cleanup-service, то инсталлятор предложит его настроить. Укажите логин и пароль от учетной записи RedCheck с ролью RedCheck_Admins.

```

=====
Настройка redcheck-cleanup-service
=====
Выберите имя хоста для web службы redcheck-cleanup-service
Найдены имена хоста:
[1] : localhost
Выберите DNS имя [1]: 1
Укажите существующую учетную запись с правами Администратора:
Логин: admin
Пароль:

Повторите ввод:

Генерация сертификата..
Generating a RSA private key
.....++++
.....++++
writing new private key to '/var/opt/redcheck-cleanup-service/ssl/redcheck-cleanup-service.key'
-----
Сертификат сформирован
Введите порт (446):
(отсутствует переменная)
Строка подключения службы очистки сохранена в конфигурационном файле
Настройка redcheck-cleanup-service успешно
=====

```

Выборочная настройка компонентов

Конфигуратор позволяет выборочно настроить компоненты RedCheck.

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-API
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

1. **Обновить структуру БД.** После обновления RedCheck структура используемой БД может измениться, но не всегда необходимо изменять настройки ранее сконфигурированных компонентов. Выбрав данное действие, вы обновите структуру БД, не перенастраивая другие компоненты.
2. **Настройка RedCheck-API / RedCheck-Client.** Позволяет изменить протокол и DNS-имя / IP-адрес для компонентов RedCheck-API и RedCheck-Client.
3. **Настройка RedCheck-Scan-Service.** Настраивает службу сканирования для работы с БД. Данное действие может использоваться для конфигурирования дополнительной службы сканирования.
4. **Настройка RedCheck-Sync-Service.** Настраивает службу синхронизации для работы с БД.
5. **Настройка RedCheck-Cleanup-Service.** Настраивает службу очистки БД для работы с БД.

Дополнительные параметры

secret_save – вводимые в процессе конфигурации пароли будут сохраняться в лог.

advanced_setup – конфигурактор запросит расширенные параметры при настройке подключения к БД.

При необходимости продолжите конфигурацию RedCheck и настройте:

- [Сканирование с помощью WinRM](#)
- [Доменную аутентификацию в RedCheck \(Kerberos\)](#)
- [Руководство по компоненту RedCheck LDAP Import Tools \(для импорта хостов из AD\)](#)
- [Руководство по эксплуатации сервера обновлений](#)

3.2 Astra Linux 1.8

Содержание

- [Установка СУБД](#)
- [Инсталляция RedCheck](#)
- [Конфигурация RedCheck](#)

Установка СУБД

Установка СУБД PostgreSQL с репозитория Astra Linux

Шаг 1. Откройте терминал комбинацией **Alt + T**;

Шаг 2. Обновите пакеты;

Bash (оболочка Unix)

```
sudo apt -y update
```

Для установки достаточно репозитория с установочного диска.

Шаг 3. Установите PostgreSQL;

Bash (оболочка Unix)

```
sudo apt -y install postgresql
```

Настройка PostgreSQL

Шаг 4. Добавьте службу **postgresql** в автозапуск;

Bash (оболочка Unix)

```
sudo systemctl enable postgresql
```

```
root@astra-db:/etc/apt# systemctl enable postgresql
Synchronizing state of postgresql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable postgresql
```

Шаг 5. Создайте пользователя для администрирования СУБД;

PostgreSQL по умолчанию создает суперпользователя **postgres**.

Bash (оболочка Unix)

```
sudo su postgres
```

Bash (оболочка Unix)

```
psql -U postgres
```

Bash (оболочка Unix)

```
CREATE ROLE redcheck WITH PASSWORD '12345' LOGIN CREATEDB SUPERUSER;
```

```
root@astra-db:/etc/apt# sudo su - postgres
postgres@astra-db:~$ psql -U postgres
psql (14.5 (Debian 14.5-1.pgdg90+1))
Введите "help", чтобы получить справку.

postgres=# CREATE ROLE redcheck WITH PASSWORD '12345' SUPERUSER LOGIN CREATEDB;
CREATE ROLE
postgres=# \q
postgres@astra-db:~$ exit
Выход
root@astra-db:/etc/apt#
```

Для выхода из базы данных postgres введите `\q`

Шаг 6. Завершите сессию командой **exit**

Шаг 7. Откройте доступ по сети для серверов, на которых планируется установка REST-компонента и служб сканирования и синхронизации RedCheck;

Bash (оболочка Unix)

```
sudo echo "listen_addresses = 'ip_СУБД'" >>
/etc/postgresql/15/main/postgresql.conf
```

Bash (оболочка Unix)

```
sudo echo host all имя_пользователя_СУБД имя_сети/маска scram-sha-256
>> /etc/postgresql/15/main/pg_hba.conf
```

ip_СУБД – IP-адреса хостов, на которых установлена СУБД, службы сканирования, служба синхронизации и серверный компонент RedCheck,
имя_базы_данных – имя базы данных, которая создается при установке RedCheck (по умолчанию RedCheck),
имя_пользователя_СУБД – имя созданного ранее пользователя,

имя_сети/маска – сеть или один адрес, которым разрешается доступ к СУБД. К примеру, 192.168.100.0/24 или 192.168.100.15/32;

```
root@astra-db:/etc/apt# echo "listen_addresses = '192.168.1.8'" >> /etc/postgresql/14/main/postgresql.conf
root@astra-db:/etc/apt# tail -n1 /etc/postgresql/14/main/postgresql.conf
listen_addresses = '192.168.1.8'
root@astra-db:/etc/apt# echo "host all redcheck 192.168.1.0/24 md5" >> /etc/postgresql/14/main/pg_hba.conf
root@astra-db:/etc/apt# tail -n1 /etc/postgresql/14/main/pg_hba.conf
host all redcheck 192.168.1.0/24 md5
root@astra-db:/etc/apt# █
```

Чтобы узнать ip-адрес устройства, используйте команду **ip a**

Шаг 8. Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
sudo systemctl restart postgresql
```

Чтобы проверить работоспособность СУБД, используйте команду:

Bash (оболочка Unix)

```
systemctl status postgresql
```

При необходимости разрешите доступ к сетевому порту postgresql. Для установки брандмауэра ufw используйте команду:

Bash (оболочка Unix)

```
sudo apt install ufw
```

Bash (оболочка Unix)

```
sudo ufw allow 5432/tcp
```

Инсталляция RedCheck

Для обновления RedCheck – [4.8 Обновление RedCheck Nix](#)

Перед началом установки RedCheck в системе не должно быть пользователя с именем redcheck. Данное имя пользователя является служебным. Не допускается вносить изменения в права доступа, а также использовать в заданиях сканирования.

Шаг 1. Смонтируйте установочный диск и добавьте репозиторий в пакетный менеджер;

Bash (оболочка Unix)

```
sudo apt-cdrom add
```

Перед следующими шагами подключение репозиторий совместимости (3.10 Подключение репозитория совместимости)

Репозиторий совместимости расширяет список поддерживаемых версий Astra Linux 1.7 ([2.2 Требования к программному обеспечению](#))

Шаг 2. Разархивируйте скачанный архив redcheck-astra1.8-repo-2.12.0.20659.tar.gz в директорию /usr/local/src;

Bash (оболочка Unix)

```
sudo tar -xvf /home/имя_пользователя/Загрузки/redcheck-astra1.8-repo-2.12.0.20659.tar.gz -C /usr/local/src
```

Шаг 3. Добавьте GPG-ключ, который находится в только что разархивированном каталоге;

Bash (оболочка Unix)

```
sudo apt-key add /usr/local/src/redcheck-astra-repo/PUBLIC-GPG-KEY-  
redcheck
```

Шаг 4. Создайте файл **redcheck.list** и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
echo "deb [signed-by=/etc/apt/keyrings/redcheck-keyring.gpg]  
file:/usr/local/src/redcheck-astra-repo/ 1.8_x86-64 non-free" | sudo  
tee /etc/apt/sources.list.d/redcheck.list
```

Шаг 5. Обновите пакеты;

Bash (оболочка Unix)

```
sudo apt -y update
```

Шаг 6. Установите компоненты RedCheck;

Bash (оболочка Unix)

```
sudo apt -y install redcheck-api redcheck-client redcheck-scan-  
service redcheck-sync-service redcheck-cleanup-service
```

Конфигурация RedCheck

Содержание

- [Конфигурация всех компонентов](#)
- [Выборочная настройка компонентов](#)
- [Дополнительные параметры](#)

Если хост не подключен к сети Интернет, сначала получите файл лицензии. Если подключен, начните с шага 6.

Шаг 1. Сгенерируйте код активации командой:

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

Выберите пункт **Получение кода активации** и введите ключ лицензии:

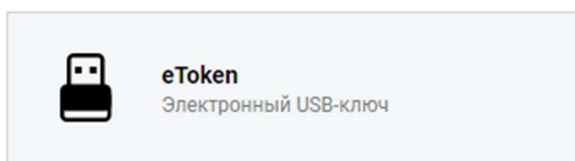
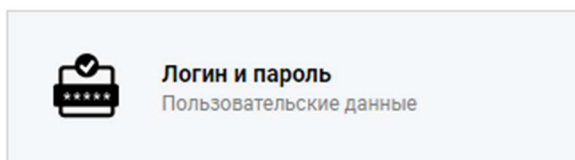
```
=====
Получение кода активации
=====
Введите ключ лицензии:
Код активации: BEE856C323A62FABFB6307CC01BFECDF85B035FEA71185B9284F3C78255CE7DC
Окончание получения кода активации
=====
```

Шаг 2. Авторизуйтесь в [Центре сертифицированных обновлений](#) с помощью логина и пароля;

Логин/пароль поставляется всем коммерческим клиентам в [Формуляре, раздел 15, «Особые отметки»](#) (начиная с 18.05.2022).

Центр сертифицированных обновлений

Для получения обновлений необходимо выбрать способ входа



Шаг 3. Раскройте **RedCheck лицензии** → выберите интересующий Вас номер лицензионного ключа;

Справка по конфигуратору вызывается командой **redcheck-bootstrap help**

Логи инсталлятора располагаются в **/var/opt/redcheck-common/log/configuration.log**

Перед повторной конфигурацией **рекомендуем [сделать резервную копию](#)** базы данных.

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

Выберите пункт **Настроить все сразу**, чтобы настроить все компоненты на одном сервере.

Первым шагом конфигуратор предложит ввести данные для подключения к базе данных:

```
Выберите действие [1-9]: 8
=====
Настройка подключения к БД
=====
Сервер СУБД [IP]: 192.168.80.129
Введите порт (5432):
Логин: redcheck
Пароль:
Введите имя БД: RedCheck
Настройка подключения к БД успешно
=====
```

Далее укажите пользовательский ключ шифрования для повышения безопасности данных в БД (по желанию):

```
=====
Настройка redcheck-api
=====
Проверяется версия сервера PostgreSQL..
Версия сервера PostgreSQL соответствует минимально необходимой
Проверяется наличие указанной БД на сервере..
БД с таким именем не найдена
Хотите создать новую БД? [Y/N] (Y): y
Создание БД..
Внимание! В случае использования пользовательского ключа шифрования – сохраните его и используйте при установке и переустановке всех компонентов программы. Утрата или неправильный ввод ключей при переустановке или обновлении компонентов программы на последующие версии при сохранении БД программы приведет к неработоспособности программы и отсутствию возможности использования сохранённых в БД учетных записей. Вы можете не использовать пользовательский ключ шифрования, при этом учетные данные, использованные программой, будут шифроваться, но с меньшим уровнем криптографической стойкости.
Введите пользовательский ключ шифрования: |
```

Выберите способ активации лицензии: онлайн (К - ключ) или офлайн (Ф - лицензионный файл):

```
проверка лицензии/активация продукта
=====
Выберите тип работы с лицензией – ключ лицензии или файл лицензии? (К/Ф,F): К
Введите ключ лицензии: |
```

При офлайн активации укажите путь к лицензионному файлу.

Следующим шагом выберите протокол и IP для работы redcheck-api. При выборе https инсталлятор сгенерирует самоподписанный сертификат. Аналогичная настройка и для redcheck-client.

```

Конфигурация redcheck-api новым подключением..
Новое подключение сохранено в конфигурационный файл redcheck-api
Обновление БД..
БД обновлена и готова к работе
Доступные протоколы:
[1] : https
[2] : http
Выберите протокол взаимодействия [1-2]: 1
Доступные интерфейсы:
[1] : 192.168.218.144
[2] : 192.168.80.32
Выберите интерфейс из списка доступных [1-2]: 2
Введите порт (445):
Сформировать сертификат на:
[1] : ip
[2] : dns
Выберите тип генерации сертификата [1-2]: 1
prepare gencert: redcheck-api 192.168.80.32 192.168.80.32
Генерация сертификата..
Generating a RSA private key
.....++++
.....++++
writing new private key to '/var/opt/redcheck-api/ssl/redcheck-api.key'
-----
Сертификат сформирован
(отсутствует переменная)
Nothing to do
libsemanage.map_file: Unable to open my-httpd.pp
(No such file or directory).
libsemanage.semanage_direct_install_file: Unable to read file my-httpd.pp
(No such file or directory).
semodule: Failed on my-httpd.pp!
Настройка redcheck-api успешна
=====

```

Далее укажите имя для службы сканирования и дождитесь настройки служб сканирования и синхронизации:

```
=====  
Настройка redcheck-scan-service  
=====  
Проверка БД на соответствие требованиям для установки службы сканирования..  
Выполняется проверка подключения к БД для redcheck-scan-service  
Подключение к БД установлено  
Конфигурация redcheck-scan-service новым подключением..  
Новое подключение сохранено в конфигурационный файл redcheck-scan-service  
Введите имя службы: scan  
Проверка прошла успешно. Служба сканирования может быть установлена к указанной БД  
Служба сканирования обновлена  
Настройка redcheck-scan-service успешна  
=====  
Настройка redcheck-sync-service  
=====  
Выполняется проверка подключения к БД для redcheck-sync-service  
Подключение к БД установлено  
Конфигурация redcheck-sync-service новым подключением..  
Новое подключение сохранено в конфигурационный файл redcheck-sync-service  
Проверка БД на соответствие требованиям для установки службы синхронизации..  
Проверка прошла успешно. Служба синхронизации может быть установлена к указанной БД  
Служба синхронизации обновлена  
Настройка redcheck-sync-service успешно  
=====
```

Если вы установили пакет компонента redcheck-cleanup-service, то инсталлятор предложит его настроить. Укажите логин и пароль от учетной записи RedCheck с ролью RedCheck_Admins.

```
=====  
Настройка redcheck-cleanup-service  
=====  
Выберите имя хоста для web службы redcheck-cleanup-service  
Найдены имена хоста:  
[1] : localhost  
Выберите DNS имя [1]: 1  
Укажите существующую учетную запись с правами Администратора:  
Логин: admin  
Пароль:  
  
Повторите ввод:  
  
Генерация сертификата..  
Generating a RSA private key  
.....++++  
.....++++  
writing new private key to '/var/opt/redcheck-cleanup-service/ssl/redcheck-cleanup-service.key'  
-----  
Сертификат сформирован  
Введите порт (446):  
(отсутствует переменная)  
Строка подключения службы очистки сохранена в конфигурационном файле  
Настройка redcheck-cleanup-service успешно  
=====
```

Выборочная настройка компонентов

Конфигуратор позволяет выборочно настроить компоненты RedCheck.

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

1. **Обновить структуру БД.** После обновления RedCheck структура используемой БД может измениться, но не всегда необходимо изменять настройки ранее сконфигурированных компонентов. Выбрав данное действие, вы обновите структуру БД, не перенастраивая другие компоненты.
2. **Настройка RedCheck-Api / RedCheck-Client.** Позволяет изменить протокол и DNS-имя / IP-адрес для компонентов RedCheck-Api и RedCheck-Client.
3. **Настройка RedCheck-Scan-Service.** Настраивает службу сканирования для работы с БД. Данное действие может использоваться для конфигурирования дополнительной службы сканирования.
4. **Настройка RedCheck-Sync-Service.** Настраивает службу синхронизации для работы с БД.
5. **Настройка RedCheck-Cleanup-Service.** Настраивает службу очистки БД для работы с БД.

Дополнительные параметры

secret_save – вводимые в процессе конфигурации пароли будут сохраняться в лог.

advanced_setup – конфигурактор запросит расширенные параметры при настройке подключения к БД.

При необходимости продолжите конфигурацию RedCheck и настройте:

- [Сканирование с помощью WinRM](#)
- [Доменную аутентификацию в RedCheck \(Kerberos\)](#)
- [Руководство по компоненту RedCheck LDAP Import Tools \(для импорта хостов из AD\)](#)
- [Руководство по эксплуатации сервера обновлений](#)

3.3 Debian 12

Содержание

- [Установка СУБД](#)
- [Инсталляция RedCheck](#)
- [Конфигурация RedCheck](#)

Установка СУБД

Установка СУБД PostgreSQL

Добавьте официальный репозиторий PostgreSQL. Для этого выполните следующие шаги:

Шаг 1. Откройте терминал и выполните следующие команды;

Bash (оболочка Unix)

```
sudo apt install curl ca-certificates
```

Bash (оболочка Unix)

```
sudo install -d /usr/share/postgresql-common/pgdg
```

Bash (оболочка Unix)

```
sudo curl -o /usr/share/postgresql-common/pgdg/apt.postgresql.org.asc  
--fail https://www.postgresql.org/media/keys/ACCC4CF8.asc
```

Bash (оболочка Unix)

```
sudo sh -c 'echo "deb [signed-by=/usr/share/postgresql-  
common/pgdg/apt.postgresql.org.asc]  
https://apt.postgresql.org/pub/repos/apt $(lsb_release -cs)-pgdg  
main" > /etc/apt/sources.list.d/pgdg.list'
```

Шаг 2. Обновите пакеты;

Bash (оболочка Unix)

```
sudo apt update
```

Шаг 3. Установите PostgreSQL;

Устанавливать можно версию postgresql, имеющуюся в репозитории, согласно [требованиям к программному обеспечению](#).

Bash (оболочка Unix)

```
sudo apt -y install postgresql-16
```

Настройка PostgreSQL

Шаг 4. Добавьте службу **postgresql** в автозапуск;

Bash (оболочка Unix)

```
sudo systemctl enable postgresql
```

```
root@astra-db:/etc/apt# systemctl enable postgresql
Synchronizing state of postgresql.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable postgresql
```

Шаг 5. Создайте пользователя для администрирования СУБД;

PostgreSQL по умолчанию создает суперпользователя **postgres**.

Bash (оболочка Unix)

```
sudo su postgres
```

Bash (оболочка Unix)

```
psql -U postgres
```

Bash (оболочка Unix)

```
CREATE ROLE redcheck WITH PASSWORD '12345' LOGIN CREATEDB SUPERUSER;
```

```

root@astra-db:/etc/apt# sudo su - postgres
postgres@astra-db:~$ psql -U postgres
psql (14.5 (Debian 14.5-1.pgdg90+1))
Введите "help", чтобы получить справку.

postgres=# CREATE ROLE redcheck WITH PASSWORD '12345' SUPERUSER LOGIN CREATEDB;
CREATE ROLE
postgres=# \q
postgres@astra-db:~$ exit
Выход
root@astra-db:/etc/apt# █

```

Для выхода из базы данных postgres введите `\q`

Шаг 6. Завершите сессию командой **exit**

Шаг 7. Откройте доступ по сети для серверов, на которых планируется установка REST-компонента и служб сканирования и синхронизации RedCheck;

Bash (оболочка Unix)

```

sudo echo "listen_addresses = 'ip_СУБД'" >>
/etc/postgresql/16/main/postgresql.conf

```

Bash (оболочка Unix)

```

sudo echo host all имя_пользователя_СУБД имя_сети/маска scram-sha-256
>> /etc/postgresql/16/main/pg_hba.conf

```

ip_СУБД – IP-адреса хостов, на которых установлена СУБД, службы сканирования, служба синхронизации и серверный компонент RedCheck,
имя_базы_данных – имя базы данных, которая создается при установке RedCheck (по умолчанию RedCheck),
имя_пользователя_СУБД – имя созданного ранее пользователя,
имя_сети/маска – сеть или один адрес, которым разрешается доступ к СУБД. К примеру, 192.168.100.0/24 или 192.168.100.15/32;

```

root@astra-db:/etc/apt# echo "listen_addresses = '192.168.1.8'" >> /etc/postgresql/14/main/postgresql.conf
root@astra-db:/etc/apt# tail -n1 /etc/postgresql/14/main/postgresql.conf
listen_addresses = '192.168.1.8'
root@astra-db:/etc/apt# echo "host all redcheck 192.168.1.0/24 md5" >> /etc/postgresql/14/main/pg_hba.conf
root@astra-db:/etc/apt# tail -n1 /etc/postgresql/14/main/pg_hba.conf
host all redcheck 192.168.1.0/24 md5
root@astra-db:/etc/apt# █

```

Чтобы узнать ip-адрес устройства, используйте команду **ip a**

Шаг 8. Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
sudo systemctl restart postgresql
```

Чтобы проверить работоспособность СУБД, используйте команду:

Bash (оболочка Unix)

```
systemctl status postgresql
```

При необходимости разрешите доступ к сетевому порту postgresql. Для установки брандмауэра ufw используйте команду:

Bash (оболочка Unix)

```
sudo apt install ufw
```

Bash (оболочка Unix)

```
sudo ufw allow 5432/tcp
```

```
root@astra-db:/etc/apt# ufw allow 5432/tcp
Rules updated
Rules updated (v6)
root@astra-db:/etc/apt# █
```

Инсталляция RedCheck

Для обновления RedCheck – [4.8 Обновление RedCheck Nix](#)

Перед началом установки RedCheck в системе не должно быть пользователя с именем redcheck. Данное имя пользователя является служебным. Не допускается вносить изменения в права доступа, а также использовать в заданиях сканирования.

Шаг 1. Разархивируйте скачанный архив redcheck-debian12-repo-2.12.0.20660.tar.gz в директорию /usr/local/src;

Bash (оболочка Unix)

```
sudo tar -xvf /home/имя_пользователя/Загрузки/redcheck-debian12-repo-2.12.0.20660.tar.gz -C /usr/local/src
```

Шаг 2. Добавьте GPG-ключ, который находится в только что разархивированном каталоге;

Bash (оболочка Unix)

```
sudo gpg --no-default-keyring --keyring /etc/apt/keyrings/redcheck-keyring.gpg --import /usr/local/src/redcheck-debian-repo/PUBLIC-GPG-KEY-redcheck
```

Шаг 3. Создайте файл **redcheck.list** и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
echo "deb [signed-by=/etc/apt/keyrings/redcheck-keyring.gpg] file:/usr/local/src/redcheck-debian-repo/ bookworm non-free" | sudo tee /etc/apt/sources.list.d/redcheck.list
```

Шаг 4. Обновите пакеты;

Bash (оболочка Unix)

```
sudo apt -y update
```

Шаг 5. Установите компоненты RedCheck;

Bash (оболочка Unix)

```
sudo apt -y install redcheck-api redcheck-client redcheck-scan-  
service redcheck-sync-service redcheck-cleanup-service
```

Конфигурация RedCheck

Содержание

- [Конфигурация всех компонентов](#)
- [Выборочная настройка компонентов](#)
- [Дополнительные параметры](#)

Если хост не подключен к сети Интернет, сначала получите файл лицензии. Если подключен, начните с шага 6.

Шаг 1. Сгенерируйте код активации командой:

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

Выберите пункт **Получение кода активации** и введите ключ лицензии:

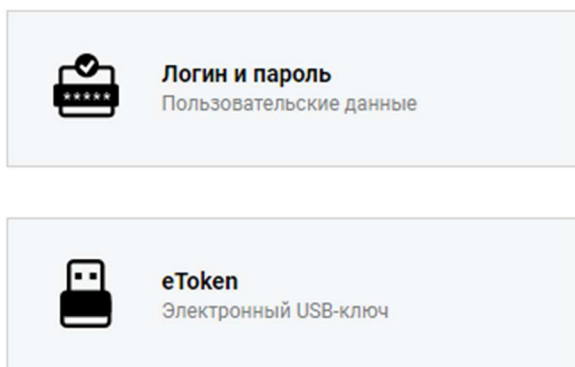
```
=====
Получение кода активации
=====
Введите ключ лицензии:
Код активации: BEE856C323A62FABFB6307CC01BFECDF85B035FEA71185B9284F3C78255CE7DC
Окончание получения кода активации
=====
```

Шаг 2. Авторизуйтесь в [Центре сертифицированных обновлений](#) с помощью логина и пароля;

Логин/пароль поставляется всем коммерческим клиентам в [Формуляре, раздел 15, «Особые отметки»](#) (начиная с 18.05.2022).

Центр сертифицированных обновлений

Для получения обновлений необходимо выбрать способ входа



Шаг 3. Раскройте **RedCheck лицензии** → выберите интересующий Вас номер лицензионного ключа;

Справка по конфигуратору вызывается командой **redcheck-bootstrap help**

Логи инсталлятора располагаются в **/var/opt/redcheck-common/log/configuration.log**

Перед повторной конфигурацией **рекомендуем [сделать резервную копию](#)** базы данных.

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

Выберите пункт **Настроить все сразу**, чтобы настроить все компоненты на одном сервере.

Первым шагом конфигуратор предложит ввести данные для подключения к базе данных:

```
Выберите действие [1-9]: 8
=====
Настройка подключения к БД
=====
Сервер СУБД [IP]: 192.168.80.129
Введите порт (5432):
Логин: redcheck
Пароль:
Введите имя БД: RedCheck
Настройка подключения к БД успешно
=====
```

Далее укажите пользовательский ключ шифрования для повышения безопасности данных в БД (по желанию):

```
=====
Настройка redcheck-api
=====
Проверяется версия сервера PostgreSQL..
Версия сервера PostgreSQL соответствует минимально необходимой
Проверяется наличие указанной БД на сервере..
БД с таким именем не найдена
Хотите создать новую БД? [Y/N] (Y): y
Создание БД..
Внимание! В случае использования пользовательского ключа шифрования – сохраните его и используйте при установке и переустановке всех компонентов программы. Утрата или неправильный ввод ключей при переустановке или обновлении компонентов программы на последующие версии при сохранении БД программы приведет к неработоспособности программы и отсутствию возможности использования сохранённых в БД учетных записей. Вы можете не использовать пользовательский ключ шифрования, при этом учетные данные, использованные программой, будут шифроваться, но с меньшим уровнем криптографической стойкости.
Введите пользовательский ключ шифрования: |
```

Выберите способ активации лицензии: онлайн (К - ключ) или офлайн (Ф - лицензионный файл):

```
проверка лицензии/активация продукта
=====
Выберите тип работы с лицензией – ключ лицензии или файл лицензии? (К/Ф, F): К
Введите ключ лицензии: |
```

При офлайн активации укажите путь к лицензионному файлу.

Следующим шагом выберите протокол и IP для работы redcheck-api. При выборе https инсталлятор сгенерирует самоподписанный сертификат. Аналогичная настройка и для redcheck-client.

```

Конфигурация redcheck-api новым подключением..
Новое подключение сохранено в конфигурационный файл redcheck-api
Обновление БД..
БД обновлена и готова к работе
Доступные протоколы:
[1] : https
[2] : http
Выберите протокол взаимодействия [1-2]: 1
Доступные интерфейсы:
[1] : 192.168.218.144
[2] : 192.168.80.32
Выберите интерфейс из списка доступных [1-2]: 2
Введите порт (445):
Сформировать сертификат на:
[1] : ip
[2] : dns
Выберите тип генерации сертификата [1-2]: 1
prepare gencert: redcheck-api 192.168.80.32 192.168.80.32
Генерация сертификата..
Generating a RSA private key
.....++++
.....++++
writing new private key to '/var/opt/redcheck-api/ssl/redcheck-api.key'
-----
Сертификат сформирован
(отсутствует переменная)
Nothing to do
libsemanage.map_file: Unable to open my-httpd.pp
(No such file or directory).
libsemanage.semanage_direct_install_file: Unable to read file my-httpd.pp
(No such file or directory).
semodule: Failed on my-httpd.pp!
Настройка redcheck-api успешна
=====

```

Далее укажите имя для службы сканирования и дождитесь настройки служб сканирования и синхронизации:

```
=====  
Настройка redcheck-scan-service  
=====  
Проверка БД на соответствие требованиям для установки службы сканирования..  
Выполняется проверка подключения к БД для redcheck-scan-service  
Подключение к БД установлено  
Конфигурация redcheck-scan-service новым подключением..  
Новое подключение сохранено в конфигурационный файл redcheck-scan-service  
Введите имя службы: scan  
Проверка прошла успешно. Служба сканирования может быть установлена к указанной БД  
Служба сканирования обновлена  
Настройка redcheck-scan-service успешна  
=====  
Настройка redcheck-sync-service  
=====  
Выполняется проверка подключения к БД для redcheck-sync-service  
Подключение к БД установлено  
Конфигурация redcheck-sync-service новым подключением..  
Новое подключение сохранено в конфигурационный файл redcheck-sync-service  
Проверка БД на соответствие требованиям для установки службы синхронизации..  
Проверка прошла успешно. Служба синхронизации может быть установлена к указанной БД  
Служба синхронизации обновлена  
Настройка redcheck-sync-service успешно  
=====
```

Если вы установили пакет компонента redcheck-cleanup-service, то инсталлятор предложит его настроить. Укажите логин и пароль от учетной записи RedCheck с ролью RedCheck_Admins.

```
=====  
Настройка redcheck-cleanup-service  
=====  
Выберите имя хоста для web службы redcheck-cleanup-service  
Найдены имена хоста:  
[1] : localhost  
Выберите DNS имя [1]: 1  
Укажите существующую учетную запись с правами Администратора:  
Логин: admin  
Пароль:  
  
Повторите ввод:  
  
Генерация сертификата..  
Generating a RSA private key  
.....++++  
.....++++  
writing new private key to '/var/opt/redcheck-cleanup-service/ssl/redcheck-cleanup-service.key'  
-----  
Сертификат сформирован  
Введите порт (446):  
(отсутствует переменная)  
Строка подключения службы очистки сохранена в конфигурационном файле  
Настройка redcheck-cleanup-service успешно  
=====
```

Выборочная настройка компонентов

Конфигуратор позволяет выборочно настроить компоненты RedCheck.

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

1. **Обновить структуру БД.** После обновления RedCheck структура используемой БД может измениться, но не всегда необходимо изменять настройки ранее сконфигурированных компонентов. Выбрав данное действие, вы обновите структуру БД, не перенастраивая другие компоненты.
2. **Настройка RedCheck-Api / RedCheck-Client.** Позволяет изменить протокол и DNS-имя / IP-адрес для компонентов RedCheck-Api и RedCheck-Client.
3. **Настройка RedCheck-Scan-Service.** Настраивает службу сканирования для работы с БД. Данное действие может использоваться для конфигурирования дополнительной службы сканирования.
4. **Настройка RedCheck-Sync-Service.** Настраивает службу синхронизации для работы с БД.
5. **Настройка RedCheck-Cleanup-Service.** Настраивает службу очистки БД для работы с БД.

Дополнительные параметры

secret_save – вводимые в процессе конфигурации пароли будут сохраняться в лог.

advanced_setup – конфигурактор запросит расширенные параметры при настройке подключения к БД.

При необходимости продолжите конфигурацию RedCheck и настройте:

- [Сканирование с помощью WinRM](#)
- [Доменную аутентификацию в RedCheck \(Kerberos\)](#)
- [Руководство по компоненту RedCheck LDAP Import Tools \(для импорта хостов из AD\)](#)
- [Руководство по эксплуатации сервера обновлений](#)

3.4 РЕД ОС 7.3

Содержание

- Установка СУБД
- Инсталляция RedCheck
- Конфигурация RedCheck

Установка СУБД

Установка СУБД PostgreSQL с репозитория РЕД ОС

Шаг 1. Откройте терминал комбинацией **Ctrl + Alt + T**;

Шаг 2. Установите PostgreSQL следующей командой;

Устанавливать можно любую версию postgresql, имеющуюся в репозиториях РЕД ОС;

Bash (оболочка Unix)

```
sudo dnf -y install postgresql15-server postgresql15-contrib
```

Шаг 3. Произведите инициализацию базы данных postgresql;

Bash (оболочка Unix)

```
sudo postgresql-15-setup initdb
```

Шаг 4. Запустите службу postgresql и добавьте ее в автозагрузку;

Bash (оболочка Unix)

```
sudo systemctl enable postgresql-15 --now
```

Для проверки статуса службы используйте команду **systemctl status postgresql-15**

Настройка СУБД

Шаг 5. Создайте пользователя для администрирования СУБД;

PostgreSQL по умолчанию создает суперпользователя **postgres**.

Bash (оболочка Unix)

```
sudo su postgres
```

Bash (оболочка Unix)

```
psql -U postgres
```

Bash (оболочка Unix)

```
CREATE ROLE redcheck WITH PASSWORD '12345' LOGIN CREATEDB SUPERUSER;
```

Для выхода из базы данных postgres введите **\q**

Шаг 6. Завершите сессию командой **exit**

Шаг 7. Откройте доступ по сети для серверов, на которых планируется установка серверного-компонента и служб сканирования и синхронизации RedCheck;

Bash (оболочка Unix)

```
sudo echo "listen_addresses = 'ip_СУБД'" >>  
/var/lib/pgsql/15/data/postgresql.conf
```

Bash (оболочка Unix)

```
sudo echo host all имя_пользователя_СУБД имя_сети/маска scram-sha-256  
>> /var/lib/pgsql/15/data/pg_hba.conf
```

ip_СУБД – IP-адреса хостов, на которых установлена СУБД, службы сканирования, служба синхронизации и серверный компонент RedCheck, **имя_базы_данных** – имя базы данных, которая создается при установке RedCheck (по умолчанию RedCheck),

имя_пользователя_СУБД – имя созданного ранее пользователя,
имя_сети/маска – сеть или один адрес, которым разрешается доступ к СУБД. К примеру, 192.168.100.0/24 или 192.168.100.15/32;

Чтобы узнать ip-адрес устройства, используйте команду **ip a**

Шаг 8. Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
sudo systemctl restart postgresql-15
```

Для установки firewall используйте команду:

Bash (оболочка Unix)

```
dnf -y install firewalld
```

Запустите firewall:

Bash (оболочка Unix)

```
systemctl start firewalld
```

Добавьте исключение для порта, на котором работает postgresql:

Bash (оболочка Unix)

```
firewall-cmd --permanent --add-port=5432/tcp
```

```
firewall-cmd --reload
```

Инсталляция RedCheck

Для обновления RedCheck – [4.8 Обновление RedCheck Nix](#)

Перед началом установки RedCheck в системе не должно быть пользователя с именем redcheck. Данное имя пользователя является служебным. Не допускается вносить изменения в права доступа, а также использовать в заданиях сканирования.

Шаг 1. Откройте терминал комбинацией **Ctrl + Alt + T**;

Перед следующими шагами подключение репозиторий совместимости ([3.10 Подключение репозиторий совместимости](#))

Репозиторий совместимости расширяет список поддерживаемых версий Astra Linux 1.8 ([2.2 Требования к программному обеспечению](#))

Шаг 2. Смонтируйте установочный диск и создайте файл cd.repo:

Bash (оболочка Unix)

```
echo -e "[cd]
name=CD
baseurl=file:///run/media/user/redos-DVD-x86_64-MUROM-7.3
gpgcheck=0
enabled=1" | sudo tee /etc/yum.repos.d/cd.repo
```

Если нет установочного диска, подключите сетевой репозиторий

Bash (оболочка Unix)

```
echo -e "[base]
name=RedOS - Base
baseurl=https://repo1.red-soft.ru/redos/7.3c/$basearch/os,https://mirror.yandex.ru/redos/7.3c/$basearch/os,http://repo.red-soft.ru/redos/7.3c/$basearch/os
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg-RPM-GPG-KEY-RED-SOFT
enabled=1" | sudo tee /etc/yum.repos.d/RedOS-Base.repo
```

Шаг 3. Разархивируйте скачанный архив `redcheck-redos7.3-repo-2.12.0.20662.tar.gz` в директорию `/usr/local/src`;

Bash (оболочка Unix)

```
sudo tar -xvf /home/имя_пользователя/Загрузки/ redcheck-redos7.3-repo-2.12.0.20662.tar.gz -C /usr/local/src
```

Шаг 4. Создайте файл `redcheck.repo` и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
echo -e "[redcheck-repo]
name=RedCheck
baseurl=file:/usr/local/src/redcheck-redos-repo/redcheck-base
enabled=1
gpgcheck=0
gpgkey=file:/usr/local/src/redcheck-redos-repo/redcheck-base/PUBLIC-
GPG-KEY-redcheck" | sudo tee /etc/yum.repos.d/redcheck.repo
```

Шаг 5. Обновите пакеты;

Bash (оболочка Unix)

```
sudo dnf makecache
```

Шаг 6. Установите компоненты RedCheck;

Bash (оболочка Unix)

```
sudo dnf -y install redcheck-api redcheck-client redcheck-scan-
service redcheck-sync-service redcheck-cleanup-service
```

Конфигурация RedCheck

Содержание

- [Конфигурация всех компонентов](#)
- [Выборочная настройка компонентов](#)
- [Дополнительные параметры](#)

Если хост не подключен к сети Интернет, сначала получите файл лицензии. Если подключен, начните с шага 6.

Шаг 1. Сгенерируйте код активации командой:

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

Выберите пункт **Получение кода активации** и введите ключ лицензии:

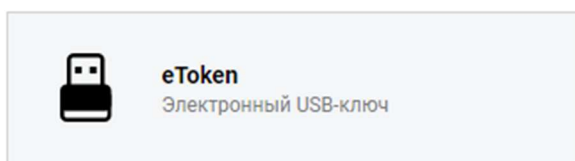
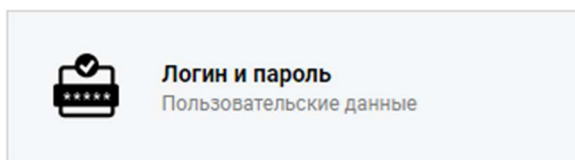
```
=====
Получение кода активации
=====
Введите ключ лицензии:
Код активации: BEE856C323A62FABFB6307CC01BFECDF85B035FEA71185B9284F3C78255CE7DC
Окончание получения кода активации
=====
```

Шаг 2. Авторизуйтесь в [Центре сертифицированных обновлений](#) с помощью логина и пароля;

Логин/пароль поставляется всем коммерческим клиентам в [Формуляре, раздел 15, «Особые отметки»](#) (начиная с 18.05.2022).

Центр сертифицированных обновлений

Для получения обновлений необходимо выбрать способ входа



Шаг 3. Раскройте **RedCheck лицензии** → выберите интересующий Вас номер лицензионного ключа;

Справка по конфигуратору вызывается командой **redcheck-bootstrap help**

Логи инсталлятора располагаются в **/var/opt/redcheck-common/log/configuration.log**

Перед повторной конфигурацией **рекомендуем [сделать резервную копию](#)** базы данных.

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

Выберите пункт **Настроить все сразу**, чтобы настроить все компоненты на одном сервере.

Первым шагом конфигуратор предложит ввести данные для подключения к базе данных:

```
Выберите действие [1-9]: 8
=====
Настройка подключения к БД
=====
Сервер СУБД [IP]: 192.168.80.129
Введите порт (5432):
Логин: redcheck
Пароль:
Введите имя БД: RedCheck
Настройка подключения к БД успешно
=====
```

Далее укажите пользовательский ключ шифрования для повышения безопасности данных в БД (по желанию):

```
=====
Настройка redcheck-api
=====
Проверяется версия сервера PostgreSQL..
Версия сервера PostgreSQL соответствует минимально необходимой
Проверяется наличие указанной БД на сервере..
БД с таким именем не найдена
Хотите создать новую БД? [Y/N] (Y): y
Создание БД..
Внимание! В случае использования пользовательского ключа шифрования – сохраните его и используйте при установке и переустановке всех компонентов программы. Утрата или неправильный ввод ключей при переустановке или обновлении компонентов программы на последующие версии при сохранении БД программы приведет к неработоспособности программы и отсутствию возможности использования сохранённых в БД учетных записей. Вы можете не использовать пользовательский ключ шифрования, при этом учетные данные, использованные программой, будут шифроваться, но с меньшим уровнем криптографической стойкости.
Введите пользовательский ключ шифрования: |
```

Выберите способ активации лицензии: онлайн (К - ключ) или офлайн (Ф - лицензионный файл):

```
проверка лицензии/активация продукта
=====
Выберите тип работы с лицензией – ключ лицензии или файл лицензии? (К/Ф, F): К
Введите ключ лицензии: |
```

При офлайн активации укажите путь к лицензионному файлу.

Следующим шагом выберите протокол и IP для работы redcheck-api. При выборе https инсталлятор сгенерирует самоподписанный сертификат. Аналогичная настройка и для redcheck-client.

```

Конфигурация redcheck-api новым подключением..
Новое подключение сохранено в конфигурационный файл redcheck-api
Обновление БД..
БД обновлена и готова к работе
Доступные протоколы:
[1] : https
[2] : http
Выберите протокол взаимодействия [1-2]: 1
Доступные интерфейсы:
[1] : 192.168.218.144
[2] : 192.168.80.32
Выберите интерфейс из списка доступных [1-2]: 2
Введите порт (445):
Сформировать сертификат на:
[1] : ip
[2] : dns
Выберите тип генерации сертификата [1-2]: 1
prepare gencert: redcheck-api 192.168.80.32 192.168.80.32
Генерация сертификата..
Generating a RSA private key
.....++++
.....++++
writing new private key to '/var/opt/redcheck-api/ssl/redcheck-api.key'
-----
Сертификат сформирован
(отсутствует переменная)
Nothing to do
libsemanage.map_file: Unable to open my-httpd.pp
(No such file or directory).
libsemanage.semanage_direct_install_file: Unable to read file my-httpd.pp
(No such file or directory).
semodule: Failed on my-httpd.pp!
Настройка redcheck-api успешна
=====

```

Далее укажите имя для службы сканирования и дождитесь настройки служб сканирования и синхронизации:

```

=====
Настройка redcheck-scan-service
=====
Проверка БД на соответствие требованиям для установки службы сканирования..
Выполняется проверка подключения к БД для redcheck-scan-service
Подключение к БД установлено
Конфигурация redcheck-scan-service новым подключением..
Новое подключение сохранено в конфигурационный файл redcheck-scan-service
Введите имя службы: scan
Проверка прошла успешно. Служба сканирования может быть установлена к указанной БД
Служба сканирования обновлена
Настройка redcheck-scan-service успешна
=====
Настройка redcheck-sync-service
=====
Выполняется проверка подключения к БД для redcheck-sync-service
Подключение к БД установлено
Конфигурация redcheck-sync-service новым подключением..
Новое подключение сохранено в конфигурационный файл redcheck-sync-service
Проверка БД на соответствие требованиям для установки службы синхронизации..
Проверка прошла успешно. Служба синхронизации может быть установлена к указанной БД
Служба синхронизации обновлена
Настройка redcheck-sync-service успешно
=====

```

Если вы установили пакет компонента redcheck-cleanup-service, то инсталлятор предложит его настроить. Укажите логин и пароль от учетной записи RedCheck с ролью RedCheck_Admins.

```

=====
Настройка redcheck-cleanup-service
=====
Выберите имя хоста для web службы redcheck-cleanup-service
Найдены имена хоста:
[1] : localhost
Выберите DNS имя [1]: 1
Укажите существующую учетную запись с правами Администратора:
Логин: admin
Пароль:

Повторите ввод:

Генерация сертификата..
Generating a RSA private key
.....++++
.....++++
writing new private key to '/var/opt/redcheck-cleanup-service/ssl/redcheck-cleanup-service.key'
-----
Сертификат сформирован
Введите порт (446):
(отсутствует переменная)
Строка подключения службы очистки сохранена в конфигурационном файле
Настройка redcheck-cleanup-service успешно
=====

```

Выборочная настройка компонентов

Конфигуратор позволяет выборочно настроить компоненты RedCheck.

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный  - критичное сообщение либо ошибка выполнения команды
желтый   - важное замечание требующее действия от пользователя
зеленый  - успешное выполнение команды либо статус выполнения конфигурации
[*]      - диапазон допустимых значений
(*)      - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

1. **Обновить структуру БД.** После обновления RedCheck структура используемой БД может измениться, но не всегда необходимо изменять настройки ранее сконфигурированных компонентов. Выбрав данное действие, вы обновите структуру БД, не перенастраивая другие компоненты.
2. **Настройка RedCheck-Api / RedCheck-Client.** Позволяет изменить протокол и DNS-имя / IP-адрес для компонентов RedCheck-Api и RedCheck-Client.
3. **Настройка RedCheck-Scan-Service.** Настраивает службу сканирования для работы с БД. Данное действие может использоваться для конфигурирования дополнительной службы сканирования.
4. **Настройка RedCheck-Sync-Service.** Настраивает службу синхронизации для работы с БД.
5. **Настройка RedCheck-Cleanup-Service.** Настраивает службу очистки БД для работы с БД.

Дополнительные параметры

secret_save – вводимые в процессе конфигурации пароли будут сохраняться в лог.

advanced_setup – конфигурактор запросит расширенные параметры при настройке подключения к БД.

При необходимости продолжите конфигурацию RedCheck и настройте:

- [Сканирование с помощью WinRM](#)
- [Доменную аутентификацию в RedCheck \(Kerberos\)](#)
- [Руководство по компоненту RedCheck LDAP Import Tools \(для импорта хостов из AD\)](#)
- [Руководство по эксплуатации сервера обновлений](#)

3.5 Установка агента RedCheck (Windows)

Агент сканирования – компонент RedCheck, предназначенный для сканирования хостов, ограниченных политикой ИБ организации (например, запрет или ограничение использования WMI, WinRM, отсутствие возможности использовать УЗ администратора), а также для обеспечения быстродействия и повышенной надёжности сканирования.

Данный компонент работает только по запросу от сервера сканирования в рамках назначенной задачи аудита.

Содержание

- [3.5.1 Установка на сканируемом хосте в ручном режиме](#)
- [3.5.2 Установка через групповые политики домена](#)

3.5.1 Установка на сканируемом хосте в ручном режиме

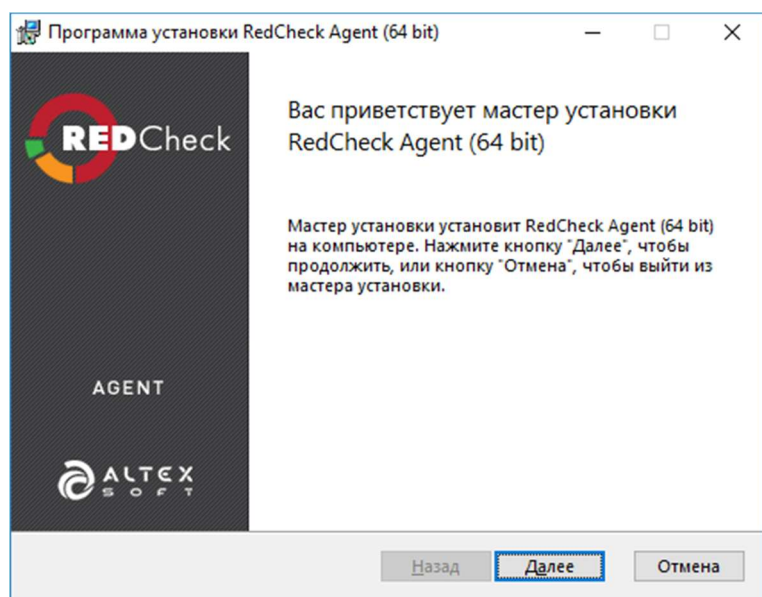
Агент сканирования входит в состав дистрибутива RedCheck 2.6.9

Перед установкой убедитесь, что на компьютере есть все необходимые компоненты:

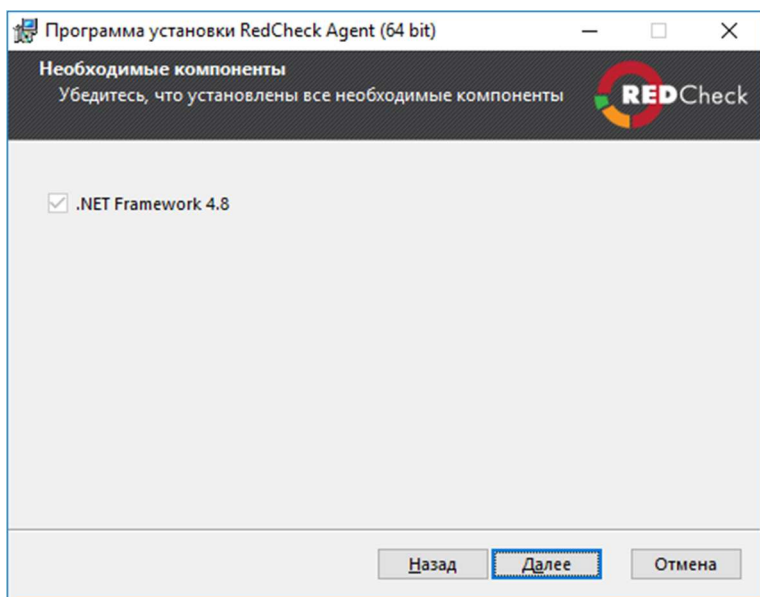
- Microsoft .NET Framework 4.8 ([4.3.2 Установка Microsoft .NET Framework](#)).

Возможна автоматическая установка через командную строку ([4.6.3 Агент RedCheck](#))

Шаг 1. Запустите установочный файл RedCheckAgent.msi на сканируемом хосте → **Далее**;

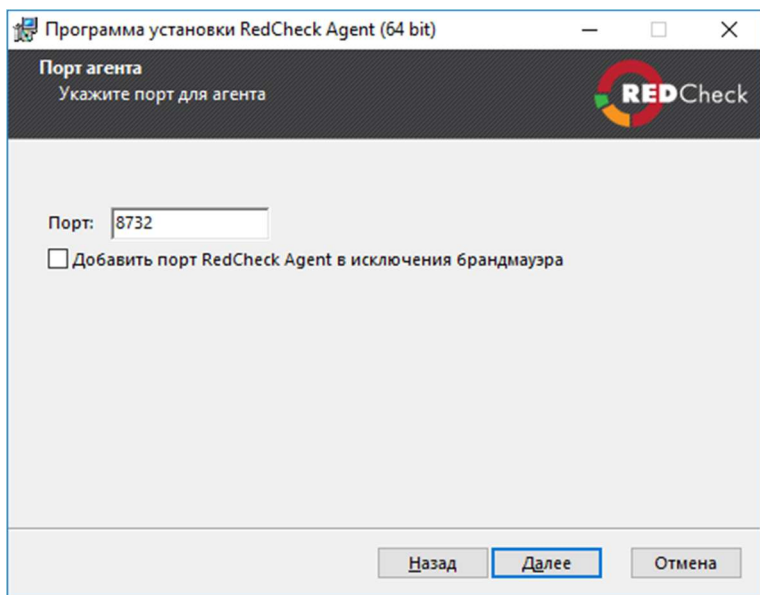


Шаг 2. Инсталлятор проверит наличие всех необходимых компонентов → **Далее**;

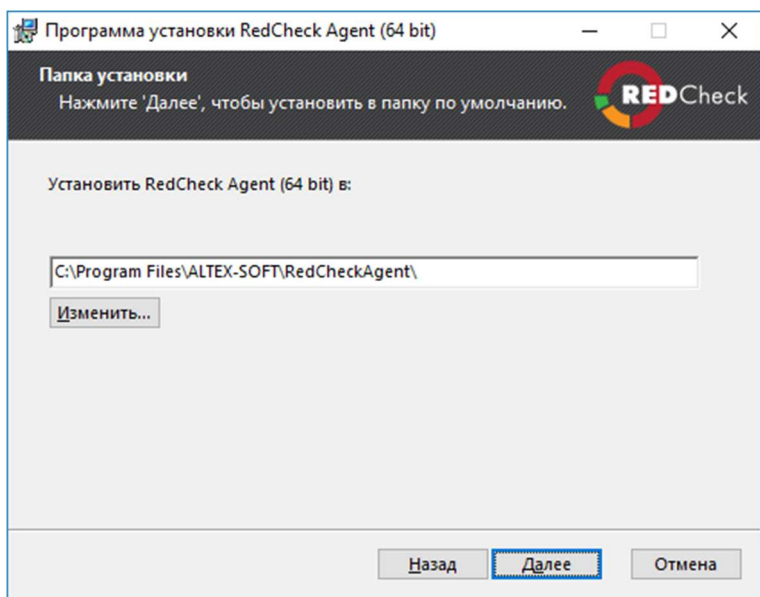


Шаг 3. Задайте порт агента (по умолчанию 8732) и отметьте поле **Добавить порт... в исключение брандмауэра** → **Далее;**

Изменить порт можно после установки ([4.11.2 Изменение порта для агента RedCheck](#)).

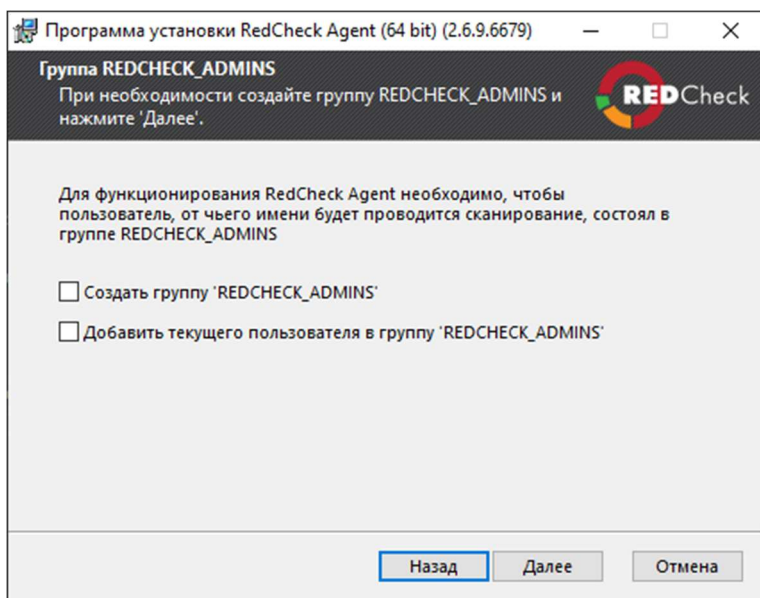


Шаг 4. Укажите директорию для установки агента → **Далее;**



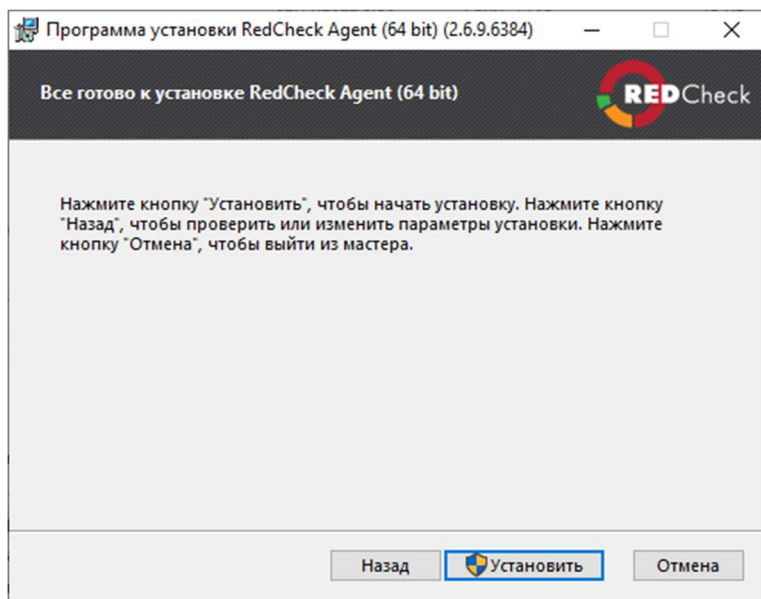
Шаг 5. По необходимости отметьте создание локальной группы безопасности REDCHECK_ADMINS и добавление в нее пользователя, из под которого производится установка агента → **Далее;**

Членство в группе безопасности REDCHECK_ADMINS требуется для корректной работы агента.



Если хост находится в домене или на нем уже имеется группа безопасности REDCHECK_ADMINS, данный раздел будет пропущен при установке.

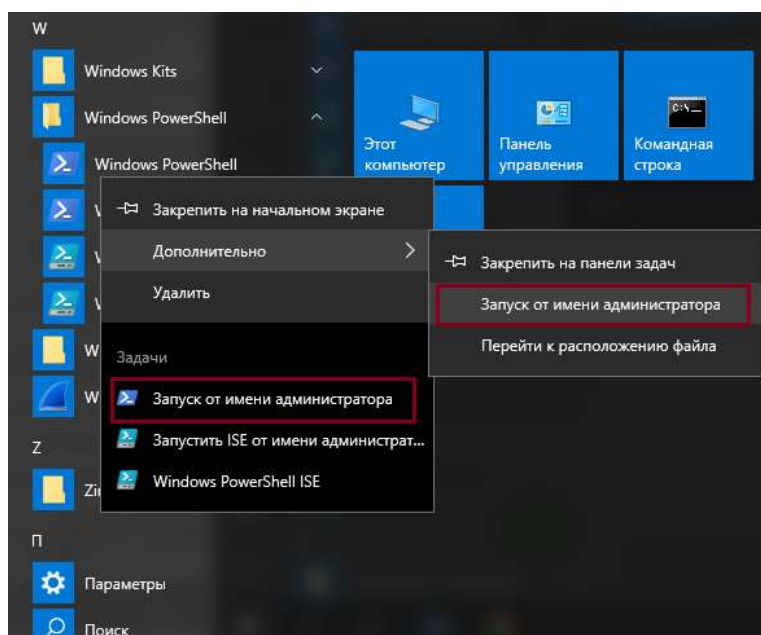
Шаг 6. Нажмите **Установить**;



После окончания установки нажмите **Готово**;

Добавление порта в исключения брандмауэра

Шаг 1. Откройте консоль **PowerShell**: **Пуск** → **Windows PowerShell** → ПКМ по **Windows PowerShell** → **Запуск от имени администратора**;



Шаг 7. Выполните следующую команду:

Код

```
netsh advfirewall firewall add rule name="RedCheck Agent port" dir=in  
action=allow protocol=TCP localport=8732
```

3.5.2 Установка через групповые политики домена

Агент сканирования входит в состав дистрибутива RedCheck 2.6.9

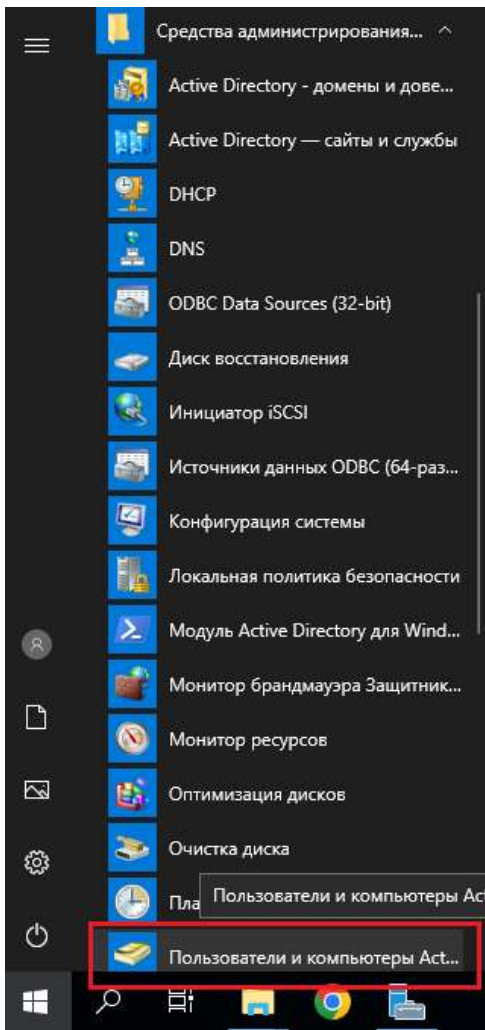
Инсталляция агента сканирования RedCheck в доменном окружении осуществляется посредством групповых политик в несколько этапов:

- [Создание и настройка группы безопасности](#)
- [Создание и настройка сетевой папки](#)
- [Настройка групповой политики](#)

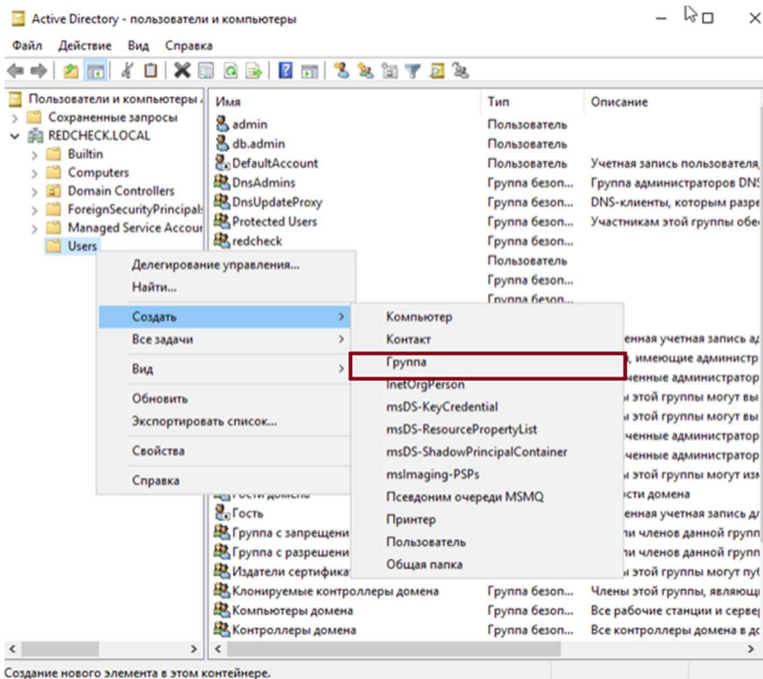
Для обеспечения большей безопасности и контроля за установкой Агента, создайте группу безопасности, в которой определите, какие устройства подлежат установке, а какие нет. Если такой ГБ не требуется, начните с шага 8.

Создание и настройка группы безопасности

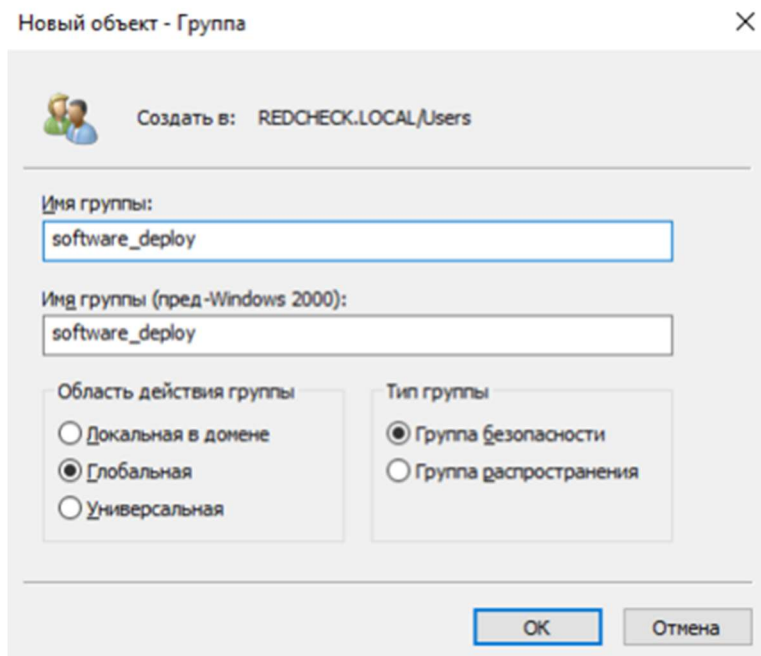
Шаг 1. Пуск → Средства администрирования Windows → Пользователи и компьютеры Active Directory;



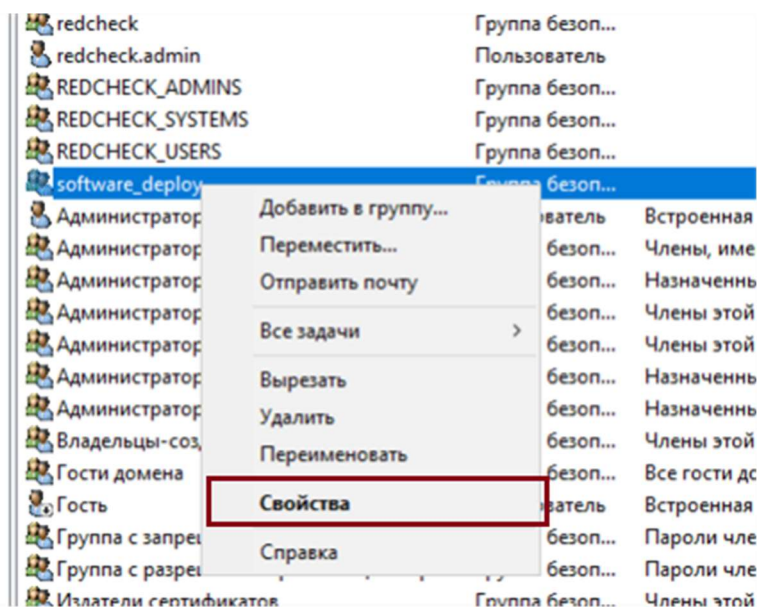
Шаг 2. ПКМ по Users → Создать → Группа;



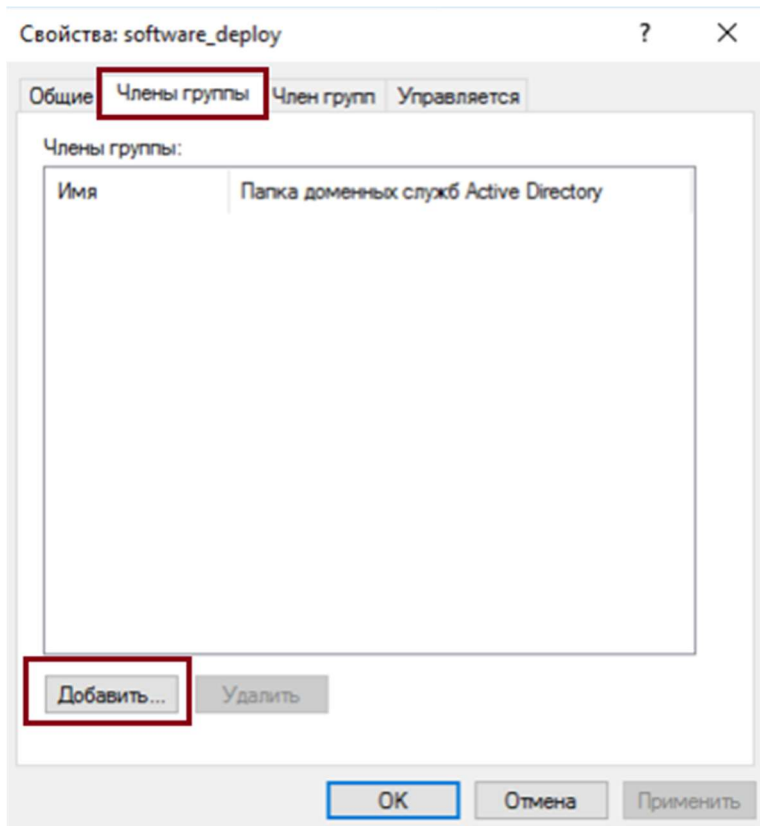
Шаг 3. В поле **Имя группы** укажите название группы (в примере **software_deploy**). Область действия группы **Глобальная**; тип группы **Группа безопасности** → **ОК**.



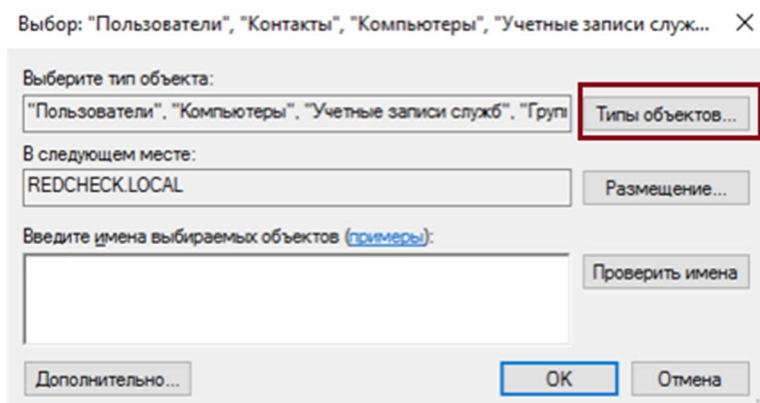
Шаг 4. ПКМ по **software_deploy** → **Свойства**;



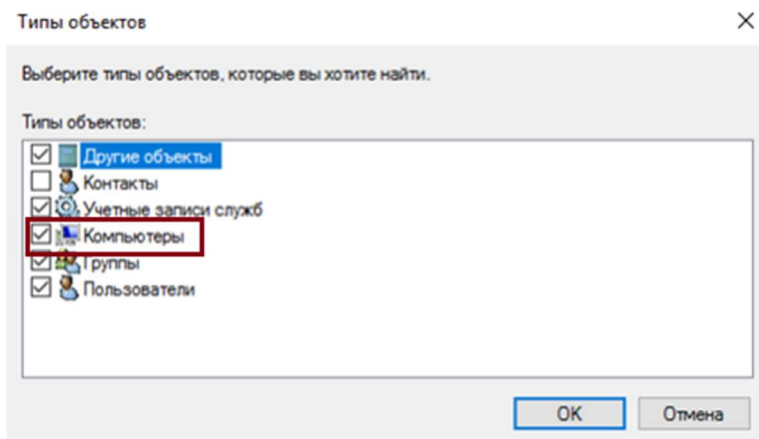
Шаг 5. Выберите **Члены группы** → **Добавить**;



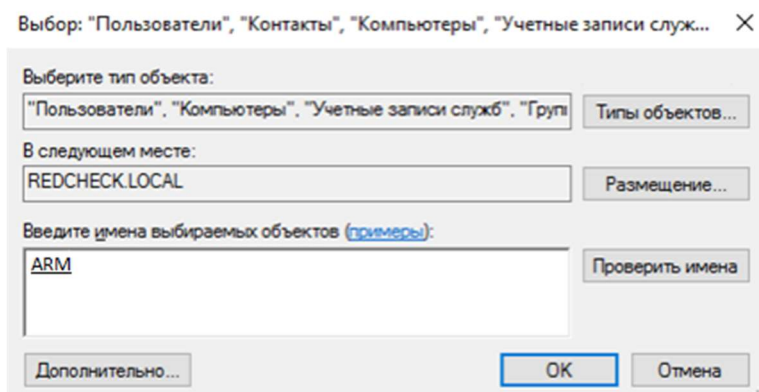
Шаг 6. Нажмите **Типы объектов**



Отметьте **Компьютеры**;

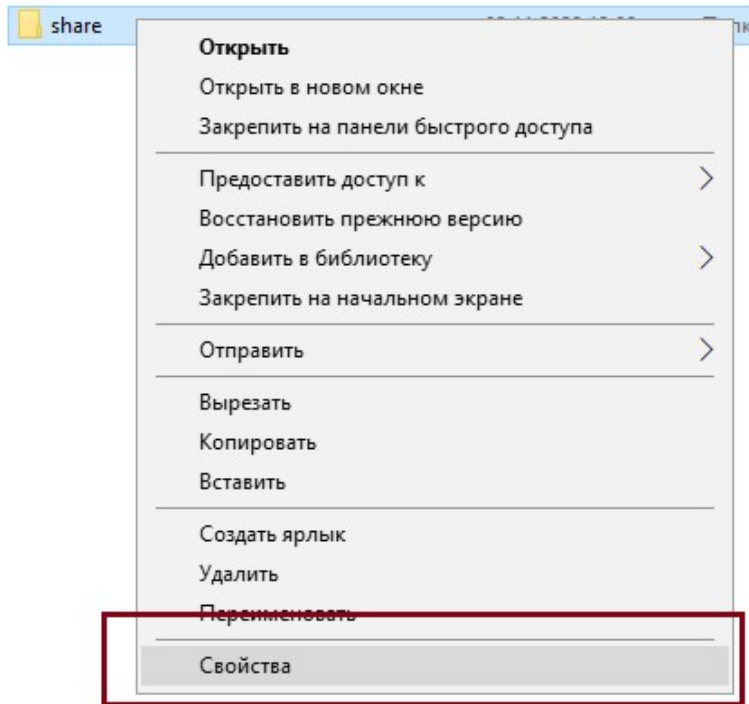


Шаг 7. Укажите имя компьютера, на котором планируется установка агента → **Проверить имена** → **OK**.

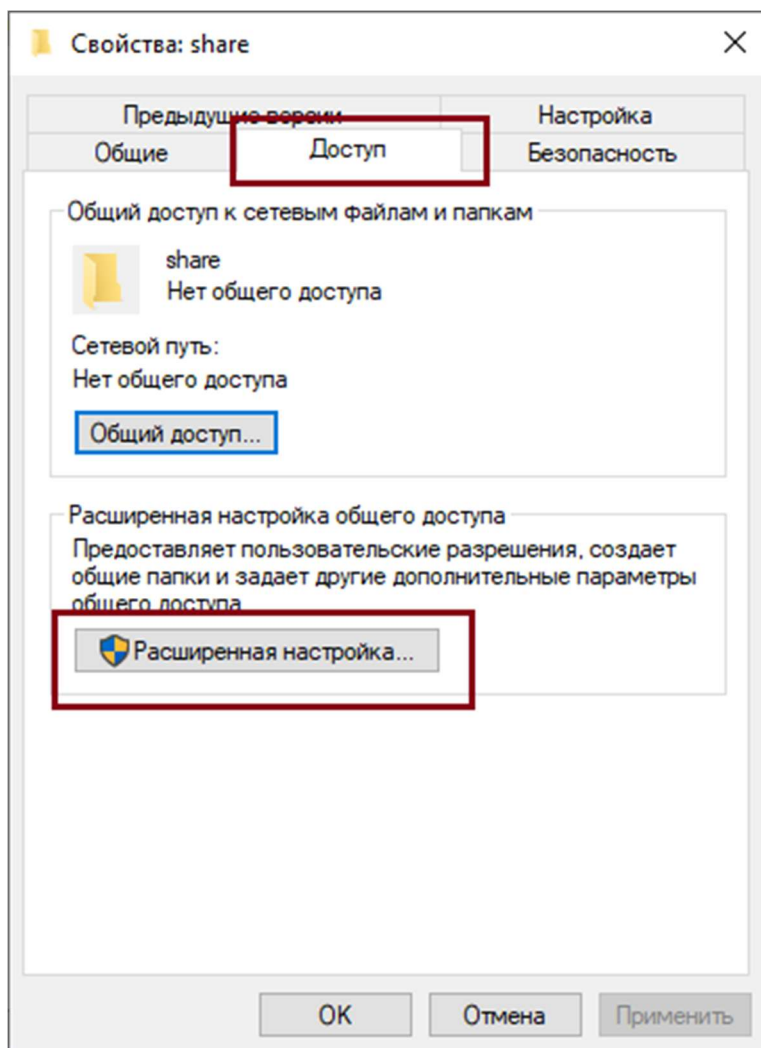


Создание и настройка сетевой папки

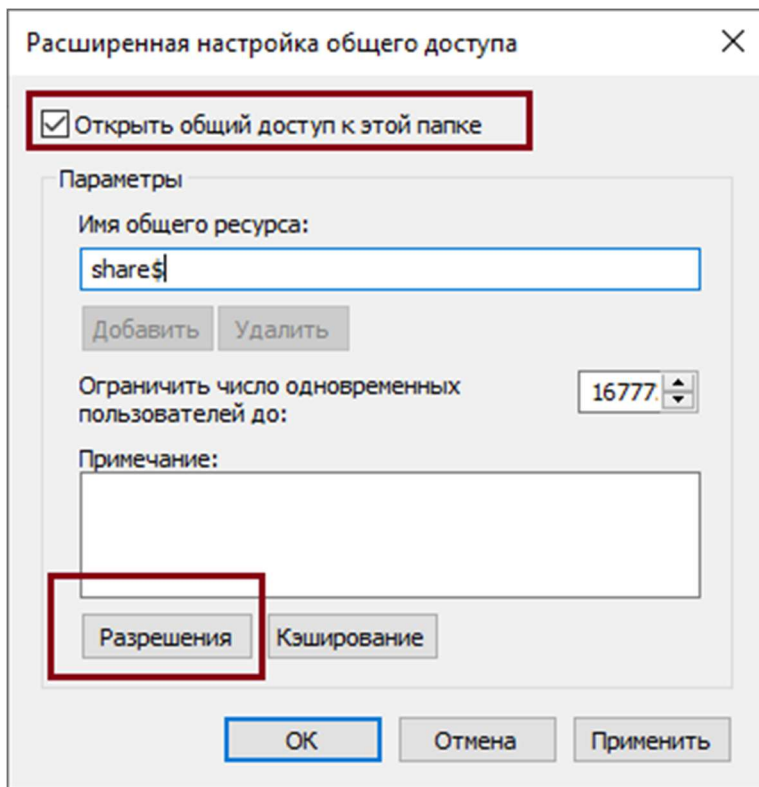
Шаг 8. Создайте директорию с произвольным названием (например, C:\share) → ПКМ по созданной директории → **Свойства**;



Шаг 9. Перейдите в **Доступ** → **Расширенная настройка**;

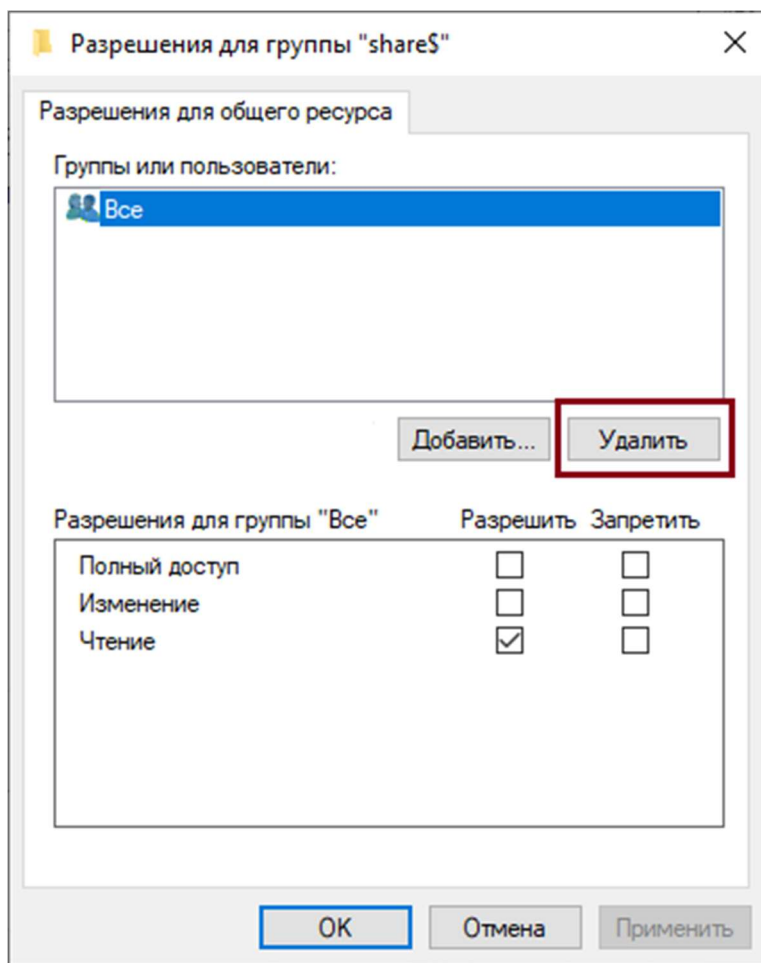


Шаг 10. Отметьте **Открыть общий доступ** → **Разрешения**;

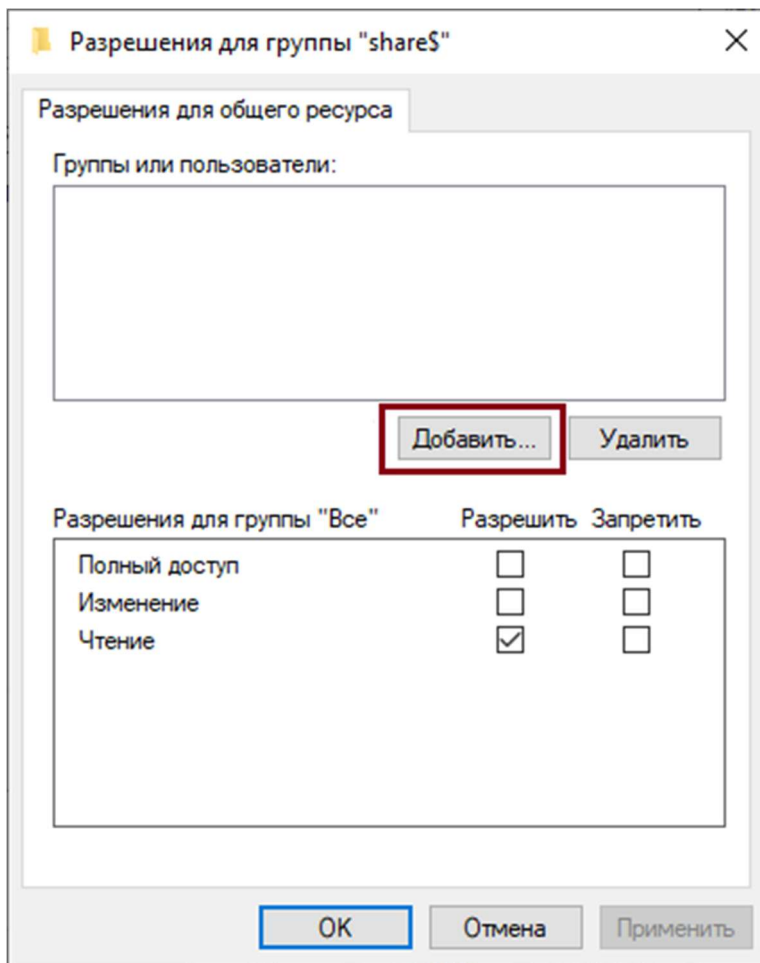


Символ \$ на конце имени папки позволяет скрыть её из сетевого окружения пользователей.

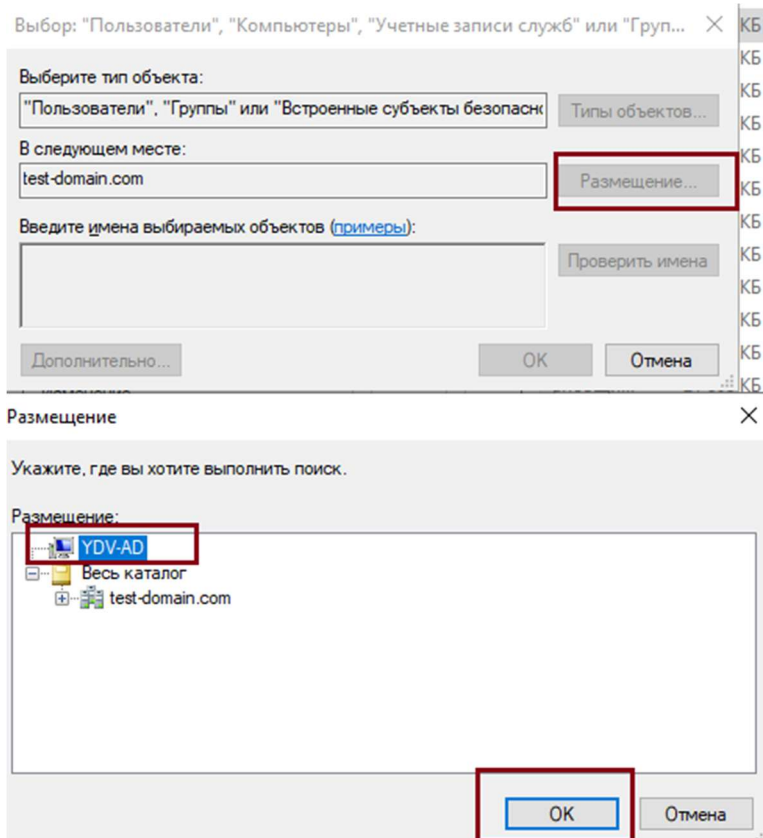
Шаг 11. Удалите группу **Все**;



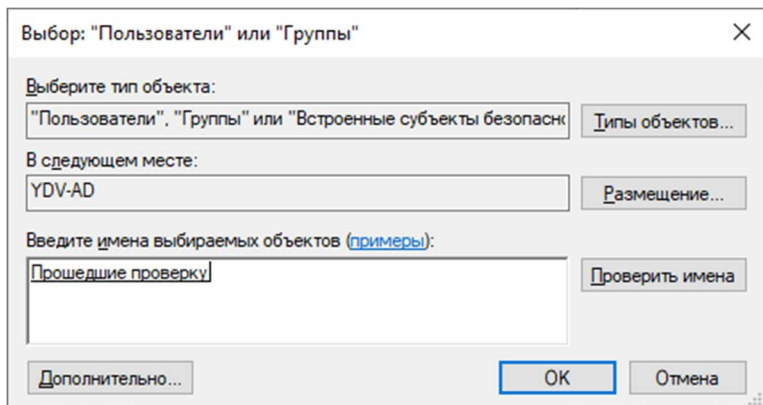
Нажмите **Добавить**;



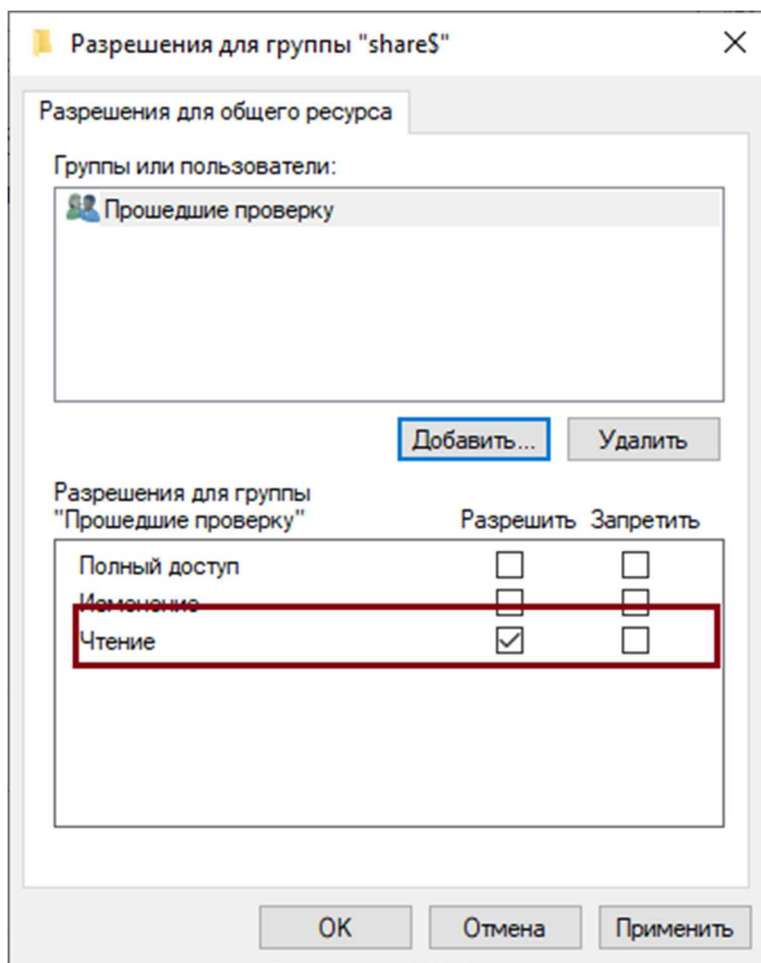
Шаг 12. Нажмите **Размещение** → выберите локальный компьютер → **OK**;



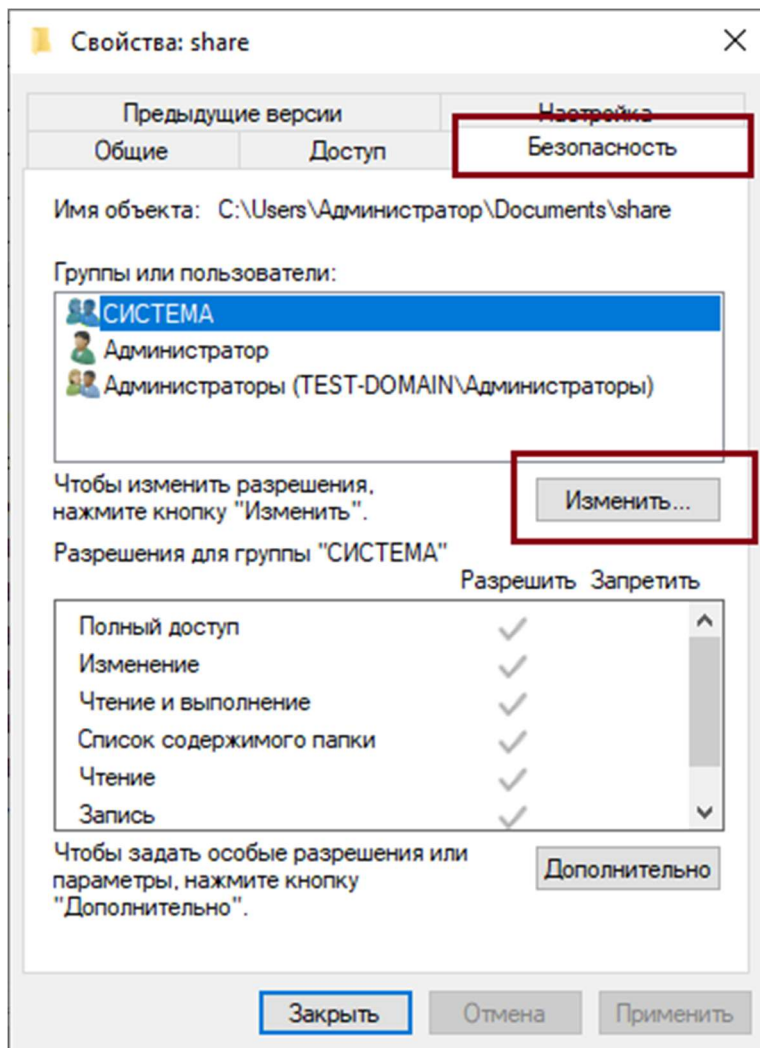
Шаг 13. Введите имя **Прошедшие проверку** → **Проверить имена** → **OK**;



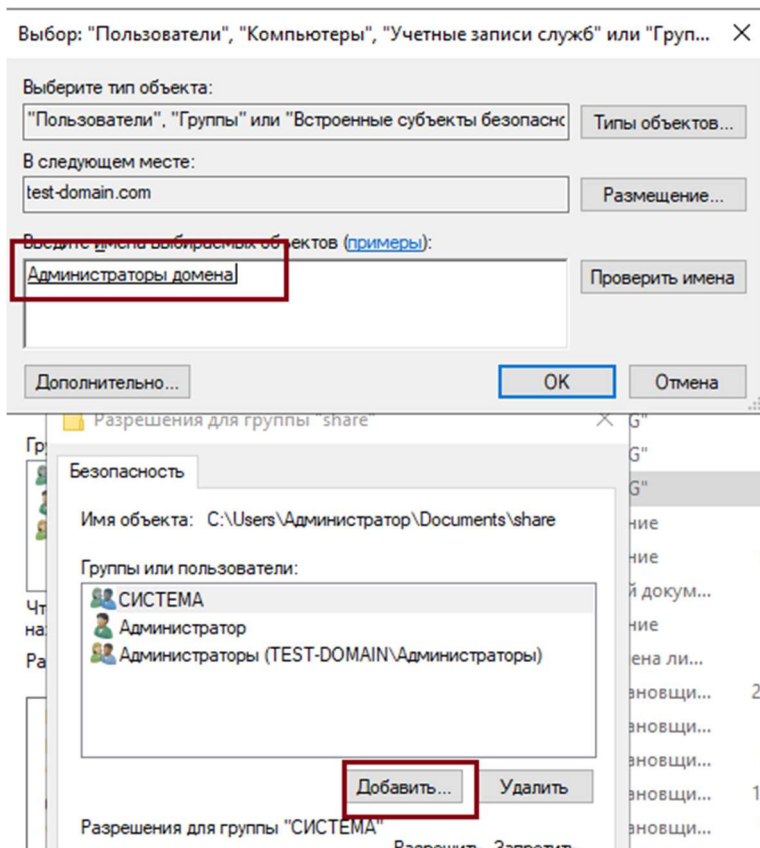
Предоставьте разрешение на **Чтение**;



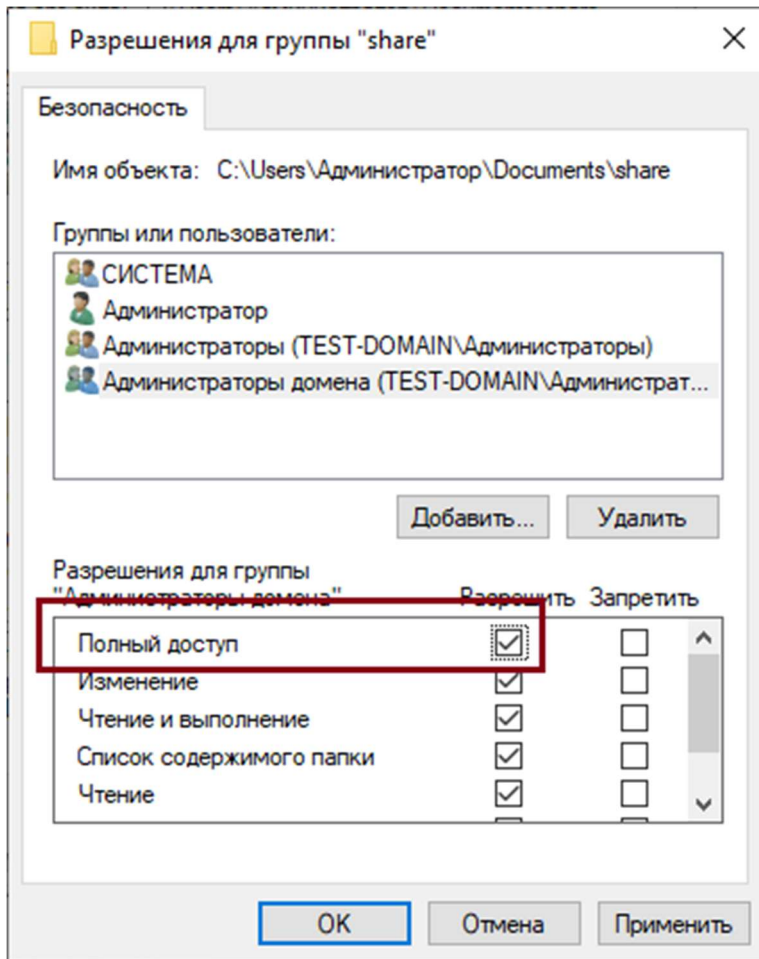
Шаг 14. В свойствах директории перейдите в **Безопасность** → **Изменить**;



Шаг 15. Нажмите **Добавить** → введите **Администраторы домена** → **ОК**;



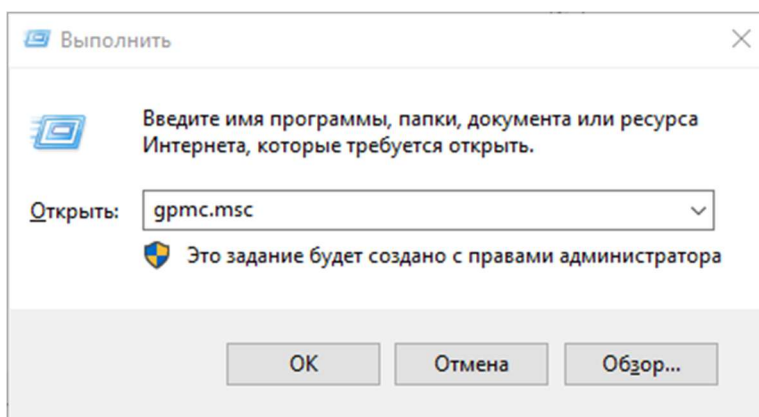
Шаг 16. Для **Администраторы домена** отметьте **Полный доступ** → **ОК**;



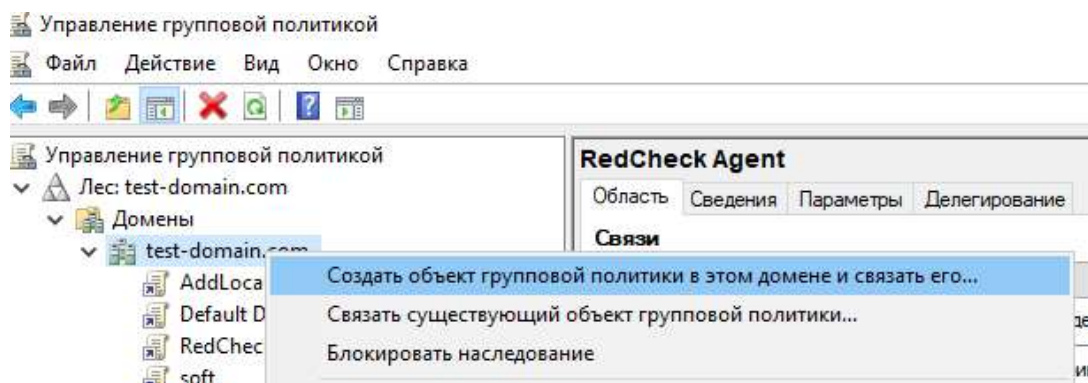
Шаг 17. Скопируйте в созданную директорию установочный файл Агента.

Настройка групповой политики

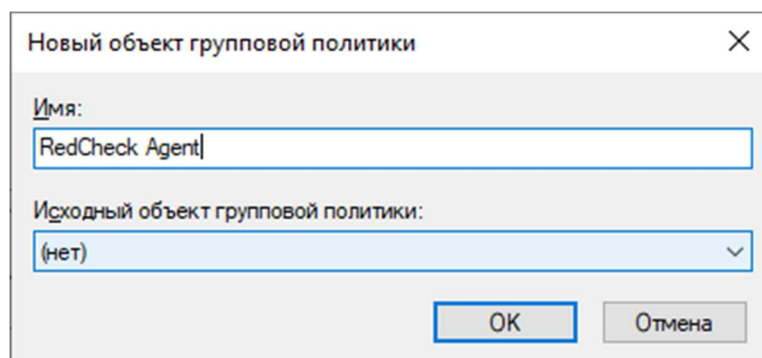
Шаг 18. Нажмите **Win + R** → введите **gpms.msc**;



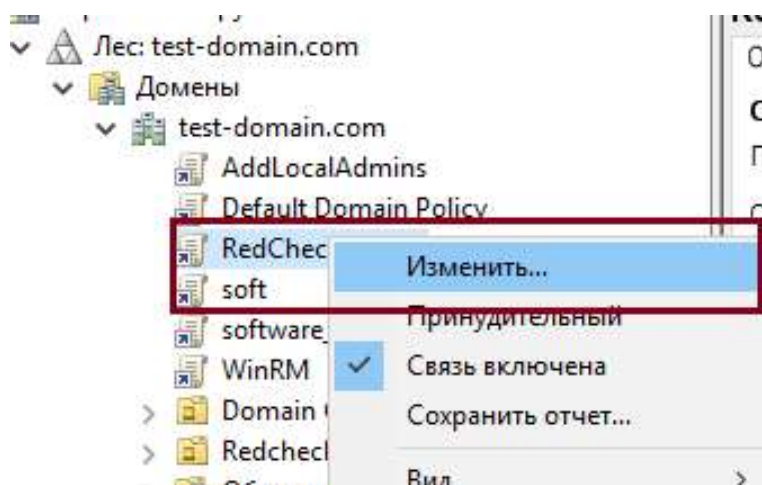
Шаг 19. Раскройте **Домены** → ПКМ по домену → **Создать объект групповой политики в этом домене...**;



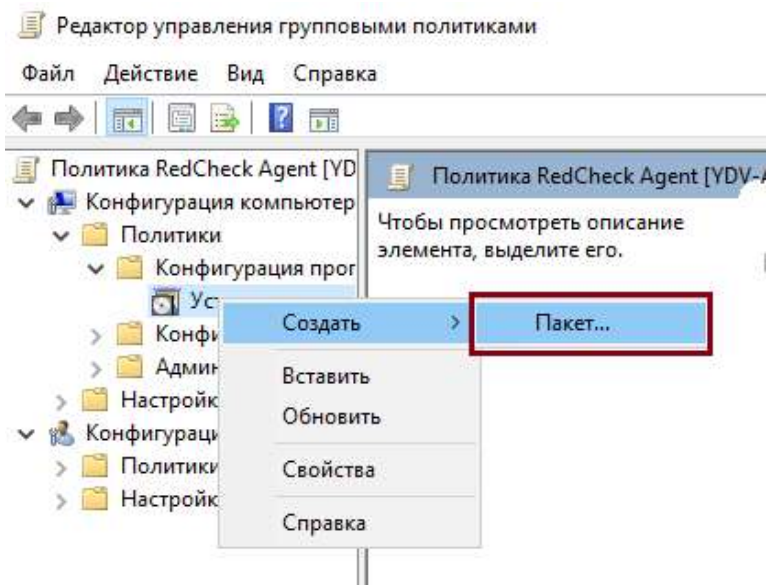
Введите имя для групповой политики → **ОК**;



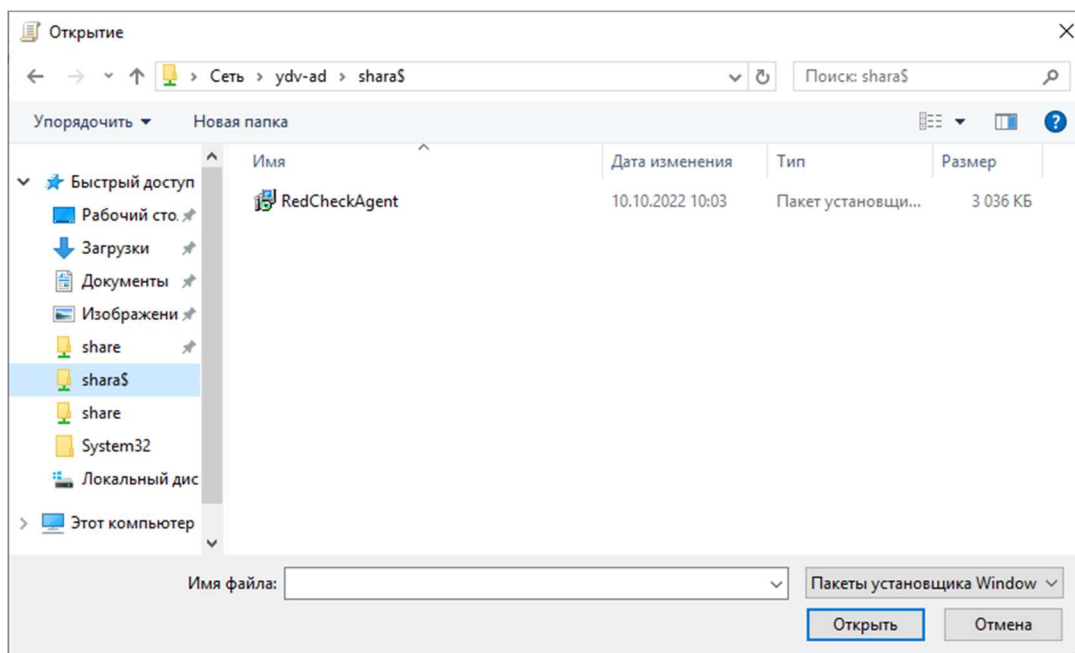
Шаг 20. ПКМ по созданной политике → **Изменить**;



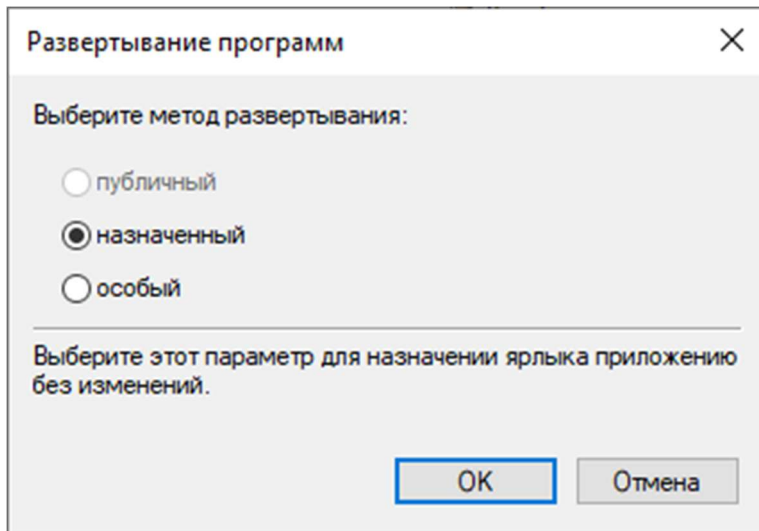
Шаг 21. Раскройте **Конфигурация компьютера** → **Политики** → **Конфигурация программ** → ПКМ по **Установка программ** → **Создать** → **Пакет**;



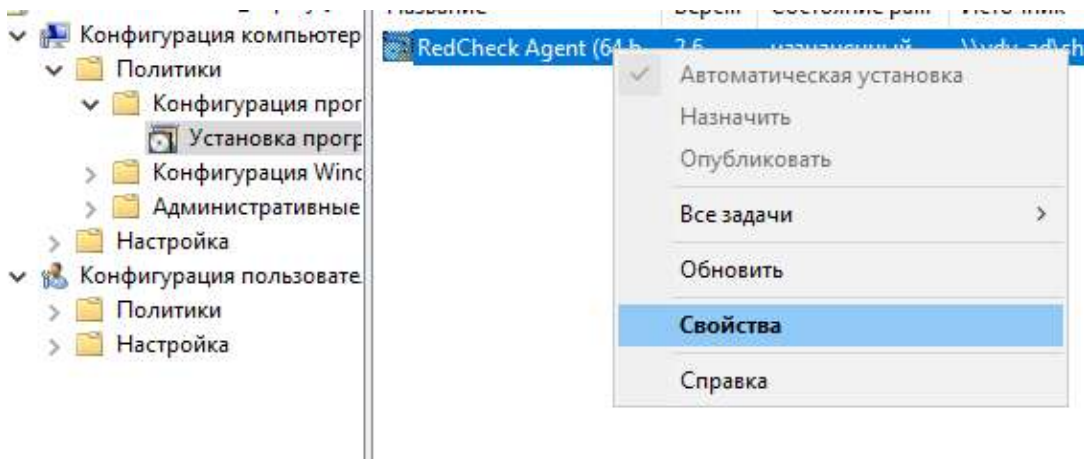
Шаг 22. Введите в адресной строке путь к сетевой папке: \\<имя_компьютера>\<имя_папки>\$ → выберите установочный файл Агента;



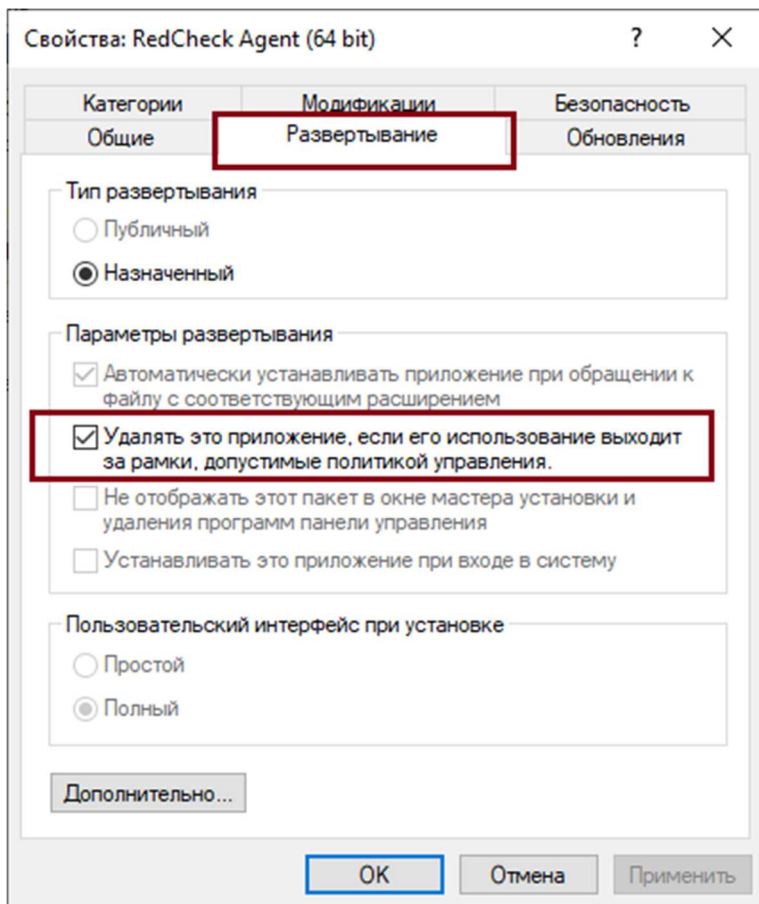
Метод развертывания – **назначенный**;



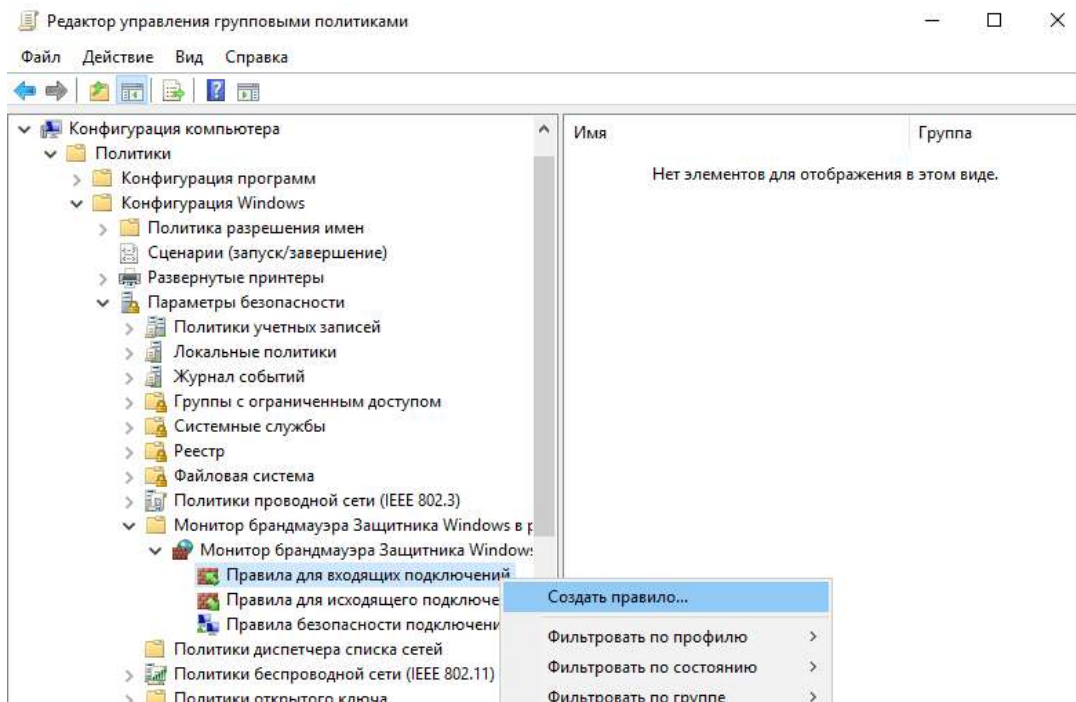
Шаг 23. ПКМ по появившемуся установочному файлу → **Свойства**;



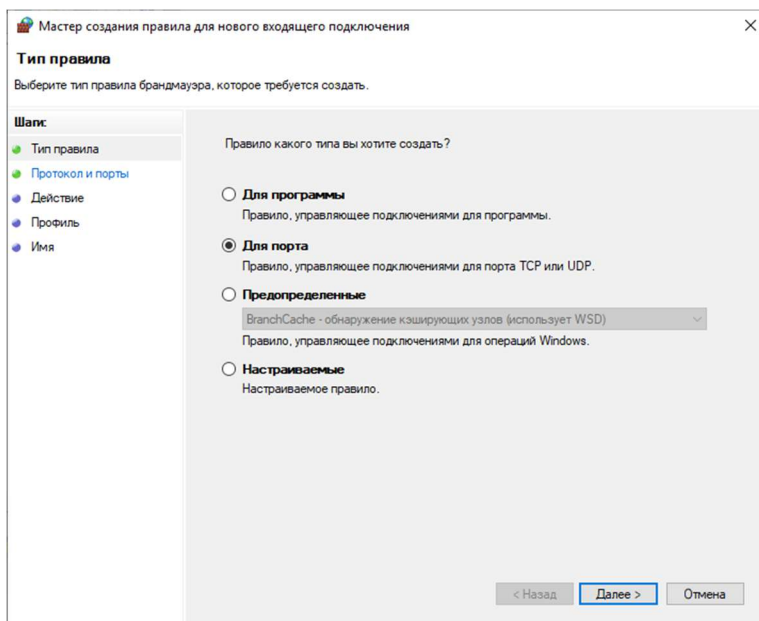
Шаг 24. В **Развертывание** отметьте **Удалить это приложение, если его использование...** → **ОК**;



Шаг 25. Перейдите в **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Монитор брандмауэра Защитника Windows...** → ПКМ по **Правила для входящих подключений** → **Создать правило...**;

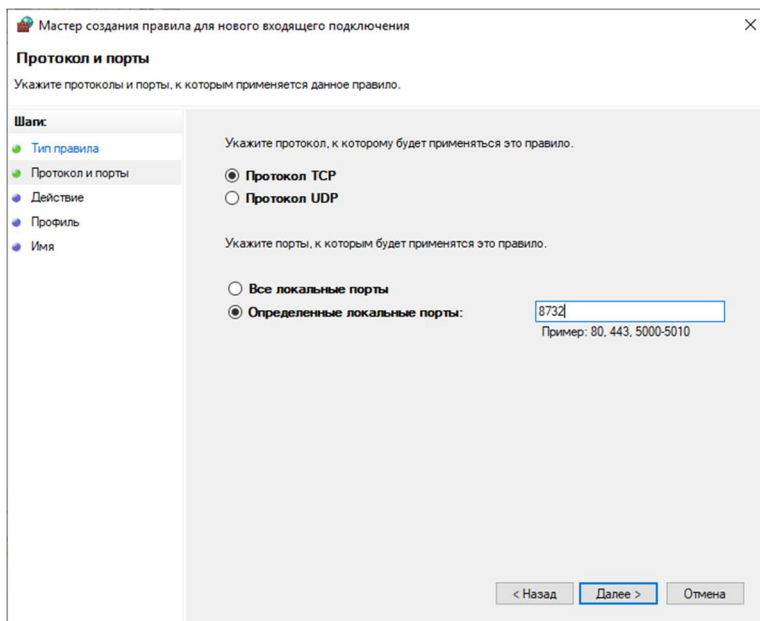


Шаг 26. Укажите тип правила **Для порта** → **Далее**;

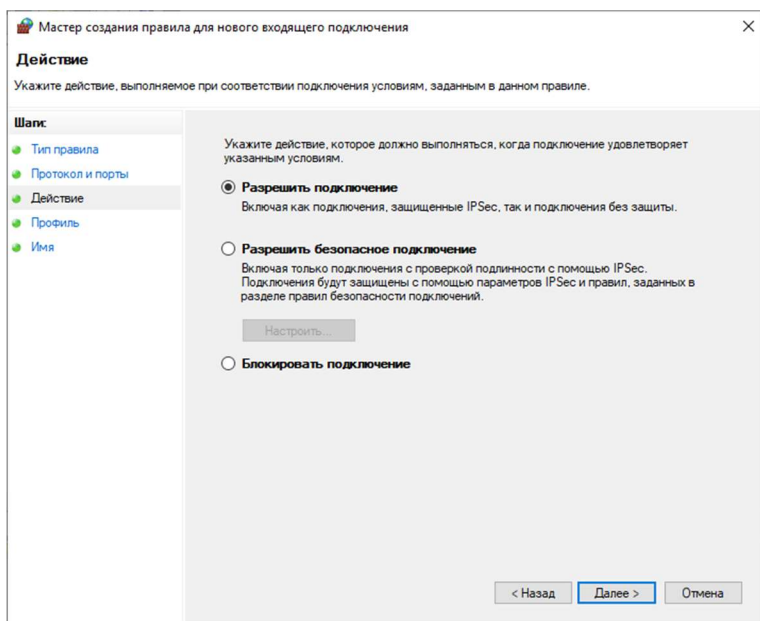


Отметьте **Протокол TCP** → укажите порт Агента (по умолчанию **8732**) → **Далее**;

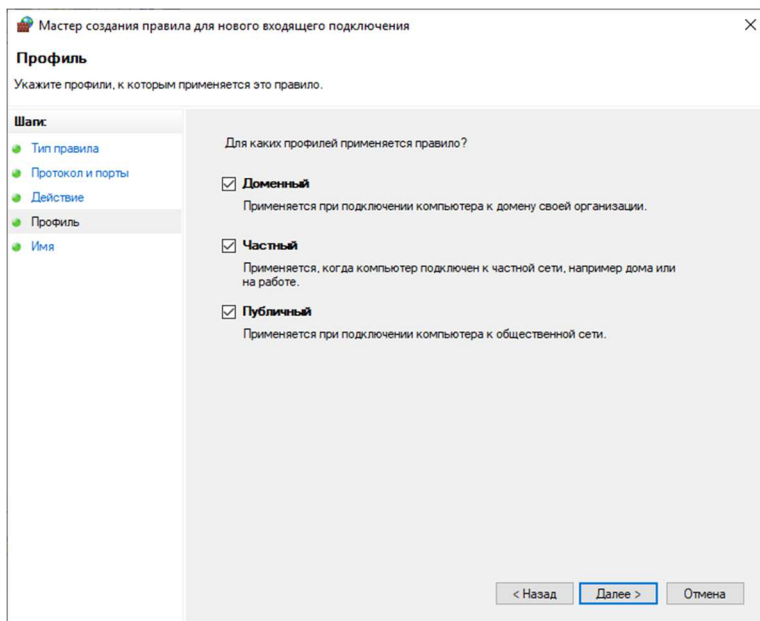
Можно, но не рекомендуется использовать другой порт Агента.



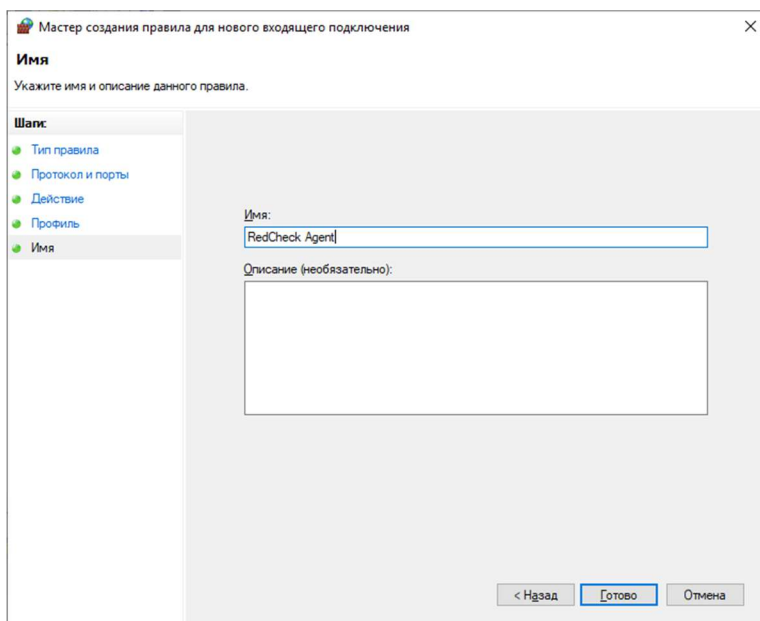
Выберите **Разрешить подключение** → **Далее**;



Выберите профили для применения правила (рекомендуется оставить по умолчанию) → **Далее**;



Задайте имя → **Готово**.



После установки Агента появится директория **RedCheckAgent** по адресу C:\Program Files\ALTEX-SOFT, а служба Агента будет отображаться в **Процессах** в **Диспетчере задач**.

Имя	Состояние	3%	42%	1%	0%
		ЦП	Память	Диск	Сеть
Application Frame Host		0%	4,3 МБ	0 МБ/с	0 Мбит/с
COM Surrogate		0%	1,9 МБ	0,1 МБ/с	0 Мбит/с
CTF-загрузчик		0%	3,1 МБ	0 МБ/с	0 Мбит/с
Microsoft Edge Update (32 бита)		0%	0,5 МБ	0 МБ/с	0 Мбит/с
> Microsoft Network Realtime Ins...		0%	2,8 МБ	0 МБ/с	0 Мбит/с
Microsoft OneDrive		0%	15,4 МБ	0,1 МБ/с	0 Мбит/с
> Microsoft Text Input Application		0%	5,4 МБ	0 МБ/с	0 Мбит/с
> Microsoft Update Health Service		0%	0,9 МБ	0 МБ/с	0 Мбит/с
MoUSO Core Worker Process		0%	2,1 МБ	0 МБ/с	0 Мбит/с
▼ RedCheck Agent		0%	9,5 МБ	0 МБ/с	0 Мбит/с
RedCheck Agent					
> Runtime Broker		0%	1,1 МБ	0 МБ/с	0 Мбит/с
> Runtime Broker		0%	2,3 МБ	0 МБ/с	0 Мбит/с
> Runtime Broker		0%	2,3 МБ	0 МБ/с	0 Мбит/с

Для ускорения применения групповой политики воспользуйтесь командой **gpupdate /force**. Данная команда выполняется от имени администратора домена на контроллере домена и на хосте, где производилась установка Агента RedCheck.

3.6 Раздельная установка

RedCheck также поддерживает распределенное расположения компонентов. Например, для установки службы сканирования отдельно от остальных компонентов выполните следующие шаги:

Шаг 1. Установите пакет **redcheck-scan-service**;

Шаг 2. Проведите конфигурирование, выбрав пункт **Настройка RedCheck-Scan-Service**;

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный - критичное сообщение либо ошибка выполнения команды
желтый  - важное замечание требующее действия от пользователя
зеленый - успешное выполнение команды либо статус выполнения конфигурации
[*] - диапазон допустимых значений
(*) - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Настройка RedCheck-Scan-Service
[3] : Выход
Выберите действие [1-3]:
```

3.7 Добавление собственных сертификатов для https

Шаг 1. Скопируйте сертификаты в следующие директории:

Astra Linux / Debian: **/usr/local/share/ca-certificates**

РЕД ОС / SberLinux: **/etc/pki/tls/certs**

Для РЕД ОС / SberLinux дополнительно нужно скопировать **.key** файлы в директорию **/etc/pki/tls/private**

Для всех ОС: **/var/opt/redcheck-api/ssl** и **/var/opt/redcheck-client/ssl**

Шаг 2. Обновите хранилище сертификатов:

Astra Linux / Debian:

Bash (оболочка Unix)

```
update-ca-certificates
```

РЕД ОС / SberLinux:

Bash (оболочка Unix)

```
update-ca-trust
```

Шаг 3. Отредактируйте конфигурационные файлы Apache:

Astra Linux / Debian:

Конфигурационные файлы для redcheck-api и redcheck-client находятся в **/etc/apache2/sites-available**

Пропишите актуальный адрес в VirtualHost согласно сертификату (<**VirtualHost имя:порт**>)

Измените значение для настройки **ServerName** согласно сертификату.

РЕД ОС / SberLinux:

Измените значение для **SSLCertificateKeyFile** на **/etc/pki/tls/private/cert.key** (вместо cert может быть другое название вашего файла).

Измените значение для **SSLCertificateFile** на **/etc/pki/tls/certs/cert.crt** (вместо cert может быть другое название вашего файла).

Шаг 4. Активируйте новые конфигурации:

Astra Linux / Debian:

Активируйте новые сайты:

Bash (оболочка Unix)

```
a2ensite -q redcheck-api-ssl.conf
```

Bash (оболочка Unix)

```
a2ensite -q redcheck-client-ssl.conf
```

Деактивируйте старые (HTTP), если нужно:

Bash (оболочка Unix)

```
a2ensite -q redcheck-api.conf
```

Bash (оболочка Unix)

```
a2dissite -q redcheck-client.conf
```

РЕД ОС / SberLinux:

Скопируйте конфигурационные файлы redcheck-client-ssl.conf и redcheck-api-ssl.conf:

Bash (оболочка Unix)

```
sudo cp /etc/httpd/redcheck/redcheck-api-ssl.conf /etc/httpd/conf.d/
```

Bash (оболочка Unix)

```
sudo cp /etc/httpd/redcheck/redcheck-client-ssl.conf  
/etc/httpd/conf.d/
```

Удалите из /etc/httpd/conf.d старые конфигурационные файлы, если они там есть:

Bash (оболочка Unix)

```
sudo rm /etc/httpd/conf.d/redcheck-api.conf
```

Bash (оболочка Unix)

```
sudo rm /etc/httpd/conf.d/redcheck-client.conf
```

Шаг 5. Отредактируйте значение **RestUrl** в конфигурационном файле **/var/opt/redcheck-client/conf/redcheck-client.dll.config**, указав имя сервера согласно сертификату:

Шаг 6. Перезапустите apache:

Astra Linux / Debian:

Bash (оболочка Unix)

```
sudo systemctl restart apache2
```

РЕД ОС / SberLinux:

Bash (оболочка Unix)

```
sudo systemctl restart httpd
```

3.8 Подключение репозитория совместимости

Шаг 1. Скачайте последнюю актуальную версию репозитория совместимости для необходимой ОС с [официального сайта](#);

Шаг 2. Разархивируйте скачанный архив:

Bash (оболочка Unix)

```
sudo tar -xvf /путь_к_архиву -C /usr/local/src
```

Шаг 3. Добавьте репозиторий в пакетный менеджер:

Astra Linux 1.7:

Bash (оболочка Unix)

```
sudo apt-key add /usr/local/src/redcheck-compatibility/PUBLIC-GPG-KEY-redcheck
```

Bash (оболочка Unix)

```
echo "deb file:/usr/local/src/redcheck-compatibility/ 1.7_x86-64 non-free" | sudo tee -a /etc/apt/sources.list.d/redcheck.list
```

Astra Linux 1.8:

Bash (оболочка Unix)

```
sudo apt-key add /usr/local/src/redcheck-compatibility/PUBLIC-GPG-KEY-redcheck
```

Bash (оболочка Unix)

```
echo "deb file:/usr/local/src/redcheck-compatibility/ 1.8_x86-64 non-free" | sudo tee -a /etc/apt/sources.list.d/redcheck.list
```

РЕД ОС:

Bash (оболочка Unix)

```
echo -e "[redcheck-compatibility]
name=RedCheck compatibility repo
baseurl=file:/usr/local/src/redcheck-compatibility
enabled=1
gpgcheck=0
gpgkey=file:/usr/local/src/redcheck-compatibility/PUBLIC-GPG-KEY-
redcheck" | sudo tee /etc/yum.repos.d/redcheck-compatibility.repo
```

Продолжайте установку RedCheck / обновление ОС.

4 Сопровождение Системы

Содержание

- [4.1 Настройка ролевой модели](#)
- [4.2. Сброс активации лицензии](#)
- [4.3 Обновление контента информационной безопасности](#)
- [4.4 Настройка учетных записей для сканирования](#)
- [4.5 Смена ключа шифрования](#)
- [4.6 Обслуживание БД](#)
- [4.7 Резервное копирование и восстановление БД](#)
- [4.8 Обновление RedCheck Nix](#)
- [4.9 Смена лицензионного ключа](#)
- [4.10 Офлайн активация лицензии](#)
- [4.11 Изменение порта для Агента сканирования](#)
- [4.12 Журнал событий \(логи\)](#)
- [4.13 Настройка сервиса доставки отчетов](#)
- [4.14 Исключения для средств защиты \(САЗ, СЗИ\)](#)
- [4.15 Настройка Windows-аутентификации \(Kerberos\)](#)
- [4.16 Дополнительные настройки для сканирования](#)
- [4.17 Удаление RedCheck](#)

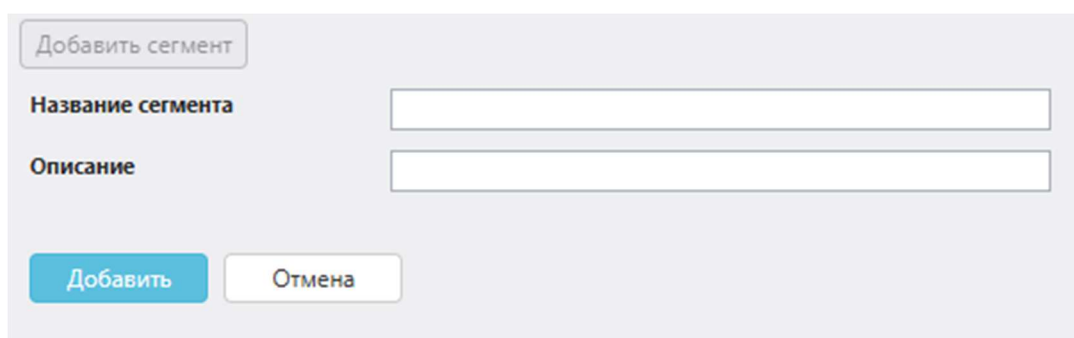
4.1 Настройка ролевой модели

Сегментная ролевая модель

Создание сегмента: Создать сегмент может только пользователь с ролью Admins и правом на управление сегментами.

Шаг 1. Откройте консоль управления → **Сегменты**;

Шаг 2. Нажмите **Добавить сегмент** → укажите название и описание для нового сегмента → **Добавить**;



Редактирование: нажмите  → **Редактировать**.

Удаление: нажмите  → **Удалить**;

Разграничение прав доступа

Для корректного разграничения прав доступа ознакомьтесь с перечнем возможностей каждой из ролей ([1.4 Полевая модель RedCheck](#)).

Создание пользователя: Добавить пользователя может только пользователь с ролью Admins.

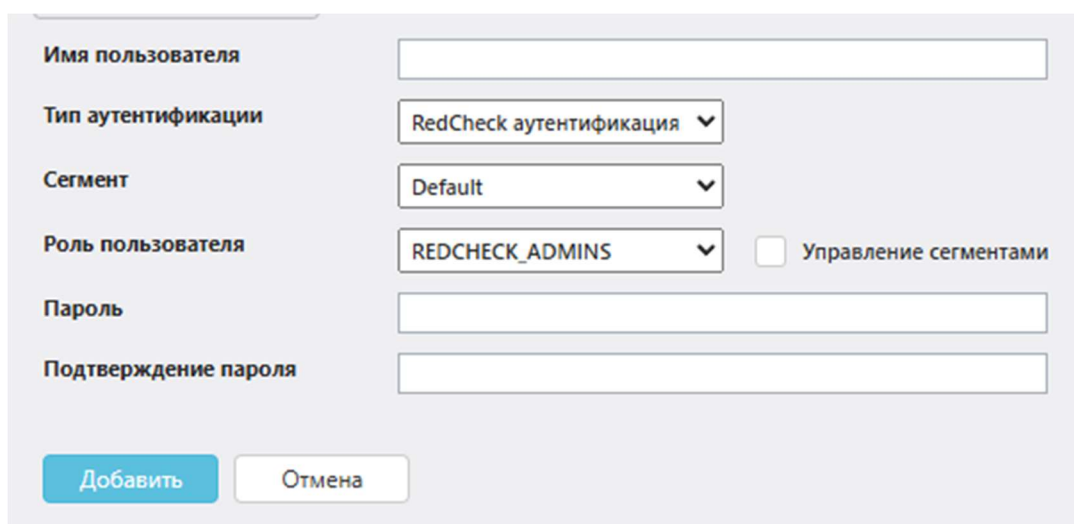
Шаг 1. Откройте консоль управления → **Пользователи**;

Шаг 2. Нажмите **Добавить пользователя** → укажите учетные данные для нового пользователя → **Добавить**;

Есть два типа аутентификации:

- RedCheck аутентификация – локальные пользователи;
- Windows аутентификация – доменный пользователь (AD). Используется для [аутентификации по Kerberos](#)

Параметр **Управление сегментами** позволяет пользователю создавать, редактировать и удалять сегменты.



Имя пользователя	<input type="text"/>
Тип аутентификации	RedCheck аутентификация ▾
Сегмент	Default ▾
Роль пользователя	REDCHECK_ADMINS ▾ <input type="checkbox"/> Управление сегментами
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>

Редактирование: нажмите  → **Редактировать**.

Удаление: нажмите  → **Удалить**;

4.2. Сброс активации лицензии

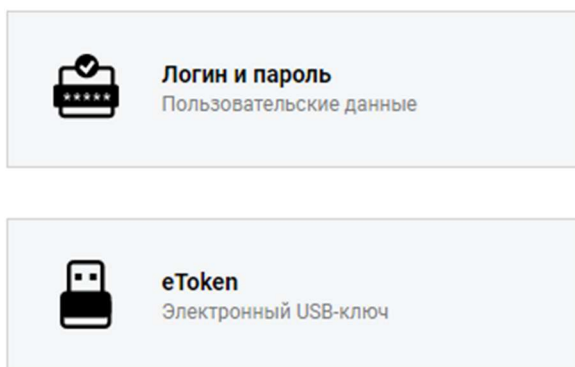
Для сброса активации лицензии необходимо выполнить следующие шаги:

Шаг 1. Авторизуйтесь в [Центре сертифицированных обновлений](#) с помощью логина и пароля;

Логин/пароль поставляется всем коммерческим клиентам в [Формуляре, раздел 15, «Особые отметки»](#) (начиная с 18.05.2022).

Центр сертифицированных обновлений

Для получения обновлений необходимо выбрать способ входа



Шаг 2. Раскройте **RedCheck лицензии** → нажмите на интересующий Вас номер ключа RedCheck;

АЛТЭКС
СОФТ

Обновления

Выберите тему:
Стекло

Пользователь

Учётная запись: s30363
Организация: АЛТЭКС-СОФТ тест 2

Предыдущий вход:
08.11.2022, 11:01:41
IP: 194.190.48.111

Выйти

Загрузить

Бюллетень изменений РС
3172

Система сертификации

Обновления для сертифицированного ПО (92)

Файлы (28)

Руководства (6)

Материалы по сертифицированному ПО (5)

Обновления Media Kit (21)

Обновления VmWare (11)

Обновления контента (4)

Net Check лицензии (2)

RedCheck лицензии (2)

Лицензионный ключ	Редакция	Дата окончания
☞ [REDACTED]	RedCheck Enterprise	17.04.2025 14:03:06

Шаг 3. Нажмите **Сбросить** в столбце **Действия**;

Активен	Дата активации	Действия
True	09.09.2022 17:41:42	Сбросить Скачать
True	07.07.2022 12:48:09	Сбросить Скачать
True	01.07.2022 17:02:32	Сбросить Скачать
True	19.05.2022 12:41:20	Сбросить Скачать
True	19.05.2022 12:41:13	Сбросить Скачать
True	19.05.2022 12:41:04	Сбросить Скачать
True	19.05.2022 12:40:28	Сбросить Скачать
False	19.04.2022 12:17:22	

Шаг 4. Нажмите **ОК**.

4.3 Обновление контента информационной безопасности

Перед началом работы в RedCheck необходимо обновить контент ИБ. Загрузка обновлений осуществляется посредством синхронизации с внешним сервером обновлений АО «АЛТЭКС-СОФТ».

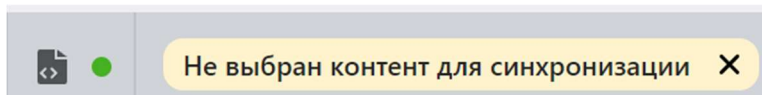
Содержание

- [4.3.1 Синхронизация через сеть Интернет](#)
- [4.3.2 Офлайн-синхронизация](#)
- [4.3.3 Синхронизация через прокси-сервер](#)

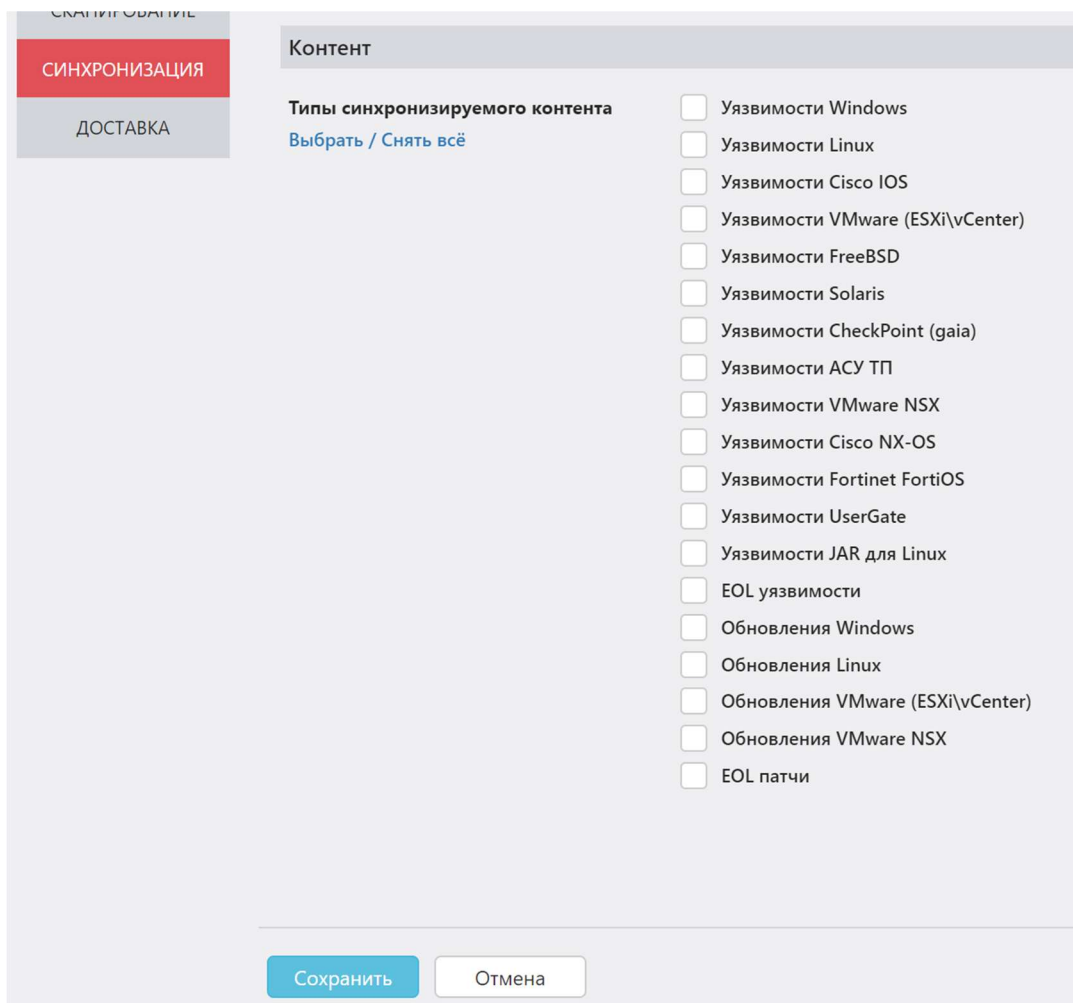
4.3.1 Синхронизация через сеть Интернет

Данный способ является предпочтительным и осуществляется по умолчанию.

Адрес сервиса синхронизации – <https://syncn.altx-soft.ru>
[Руководство по эксплуатации сервера обновлений \(Windows\)](#)

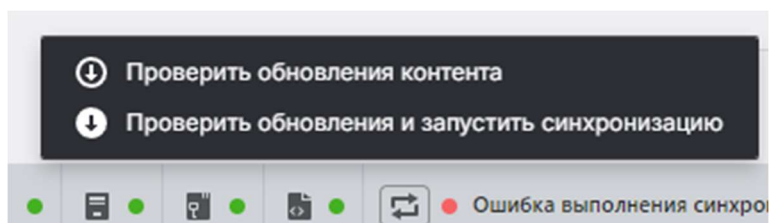


Шаг 1. После установки RedCheck необходимо выбрать контент, который будет синхронизироваться. Для этого нажмите на подсказку **Не выбран контент для синхронизации** (или нажмите **Инструменты** → **Настройки** → **Синхронизация**);



Выберите нужный контент и нажмите **Сохранить**;

Шаг 2. Откройте консоль управления RedCheck → нажмите на статусной панели кнопку синхронизации → **Проверить обновления и запустить синхронизацию**;



Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.



4.3.2 Офлайн-синхронизация

Автоматический режим

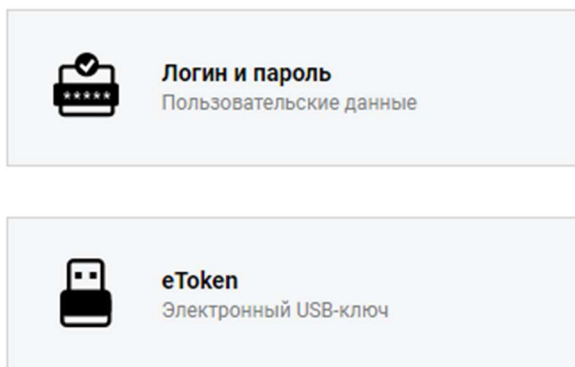
В случае отсутствия доступа к сети Интернет обновление контента ИБ осуществляется посредством архива с необходимым контентом.

Шаг 1. Авторизуйтесь в [Центре сертифицированных обновлений](#) с помощью логина и пароля;

Логин/пароль поставляется всем коммерческим клиентам в [Формуляре, раздел 15, «Особые отметки»](#) (начиная с 18.05.2022).

Центр сертифицированных обновлений

Для получения обновлений необходимо выбрать способ входа



Шаг 2. Раскройте **Обновления** → **Файлы** → скачайте архив **RedCheck_OfflineData (Актуальный контент для синхронизации RedCheck (без файла лицензии) для версии 2.8+)**, нажав **Скачать**;

Система сертифицированных обновлений

#	Название	Описание	Видимость	Дата создания	Дата модификации	Продукты	Скачать
Edit New Delete	Документация на КриттоПро CSP 3.6		<input checked="" type="checkbox"/>	10.09.2014 18:45:23	10.09.2014 18:47:07	Показать	Скачать
Edit New Delete	Документация на КриттоПро CSP 3.9		<input checked="" type="checkbox"/>	24.12.2015 11:02:45	24.12.2015 11:03:01	Показать	Скачать
Edit New Delete	RedCheck_OfflineData	Актуальный контент для синхронизации RedCheck (без файла лицензии) для версии 2.8+	<input checked="" type="checkbox"/>	01.10.2024 10:41:20	22.11.2024 21:00:02	Показать	Скачать
Edit New Delete	RedCheck_OfflineData	Актуальный контент для синхронизации RedCheck (без файла лицензии) для версии 2.7	<input checked="" type="checkbox"/>	25.11.2024 16:26:13	25.11.2024 16:26:13	Показать	Скачать

Шаг 3. Распакуйте архив в директорию для офлайн-синхронизации (по умолчанию **/var/opt/redcheck-sync-service/data**);

Директория может находиться в произвольном месте в инфраструктуре сети и должна быть доступна для чтения хостом, на котором установлена служба синхронизации. В случае сетевой папки указывается учетная запись RedCheck, пользователь которой имеет разрешение на чтение.

Шаг 4. На панели навигации выберите **Инструменты** → **Настройки** → **Синхронизация**:

- Выберите **Офлайн** и отметьте **Запускать по расписанию**, указав по необходимости время;
- Укажите путь, куда был распакован архив с контентом;
- Выберите ранее созданную учетную запись;

Общие настройки

Тип синхронизации

Онлайн

Офлайн

Путь к папке офлайн-синхронизации

\\

Учётные данные для доступа к папке

Учётная запись ...

Расписание

Запускать по расписанию

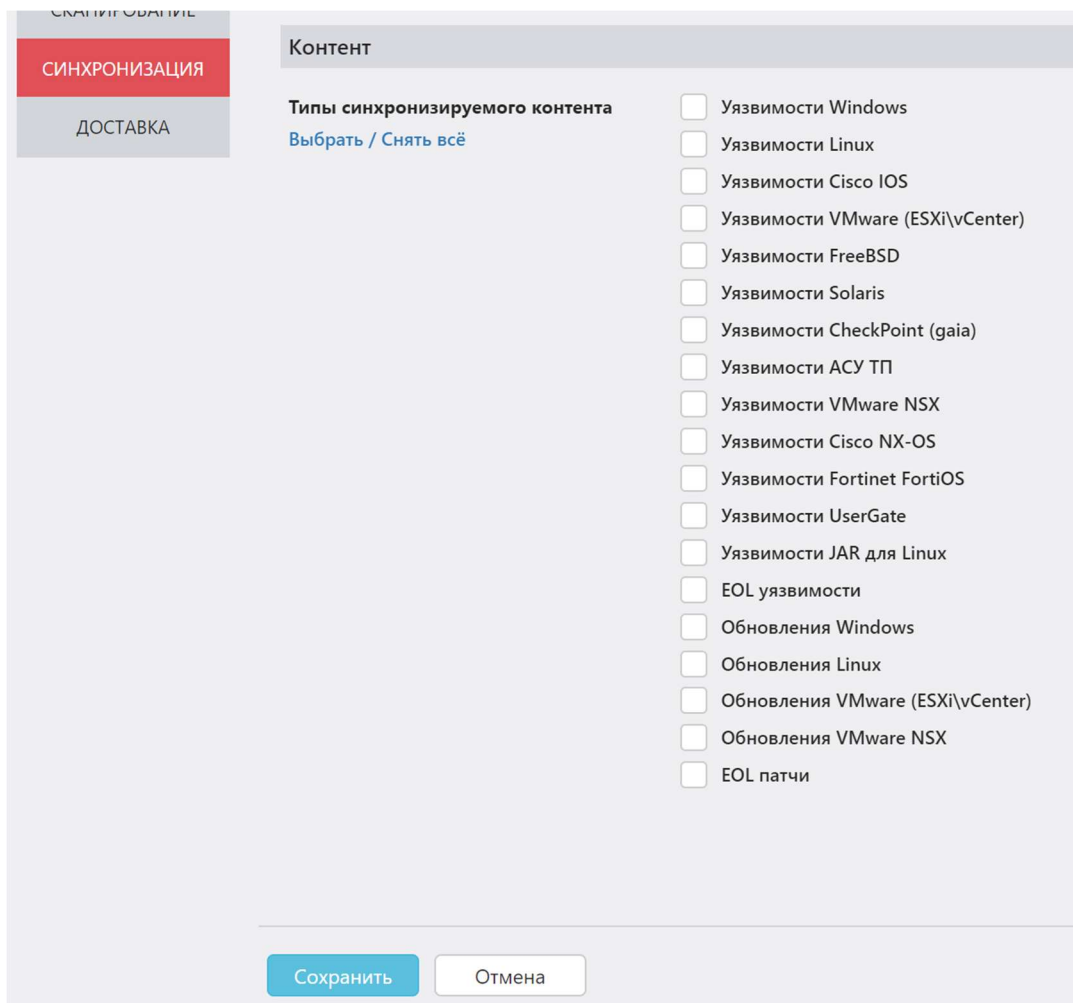
Время

12 00

Отчётность

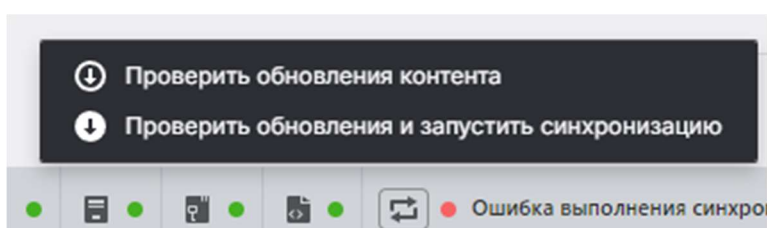
По завершении синхронизации отправлять e-mail

Тут же можно выбрать нужный контент для синхронизации;



Шаг 5. Нажмите **Сохранить** для внесения изменений;

Шаг 6. Нажмите на статусной панели кнопку синхронизации → **Проверить обновления и запустить синхронизацию**;



После завершения процесса синхронизации директория с контентом будет очищена. Не рекомендуется хранить в ней важные файлы.

Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.

Ручной режим

RedCheck позволяет загрузить архив с контентом ИБ, скачанным с личного кабинета [Центра сертифицированных обновлений](#).

Шаг 1. На панели навигации выберите **Инструменты**

→ **Настройки** → **Синхронизация**. Выберите **Офлайн** тип синхронизации;

Общие настройки

Тип синхронизации Онлайн Офлайн

Путь к папке офлайн-синхронизации

Учётные данные для доступа к папке

Учётная запись

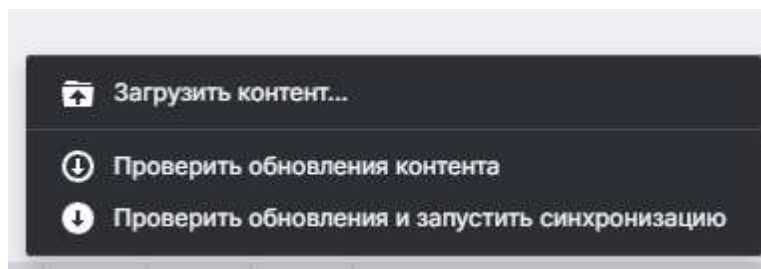
Расписание Запускать по расписанию

Время

Отчётность По завершении синхронизации отправлять e-mail

Шаг 2. Нажмите **Сохранить** для внесения изменений;

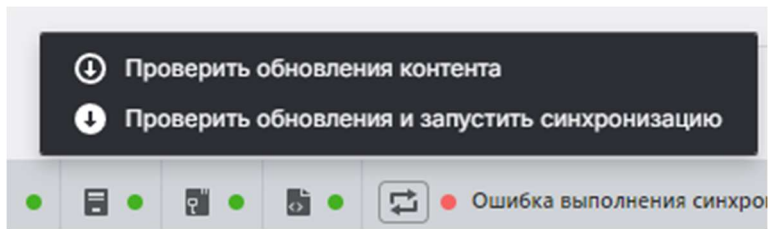
Шаг 3. Нажмите на статусной панели кнопку синхронизации → **Загрузить контент**;



Шаг 4. Выберите архив с контентом;



Шаг 5. Нажмите на статусной панели кнопку синхронизации → **Проверить обновления и запустить синхронизацию**;



Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.

4.3.3 Синхронизация через прокси-сервер

Для проведения синхронизации через прокси-сервер необходимо выполнить следующие шаги.

Адрес сервиса синхронизации – <https://syncn.altx-soft.ru>
[Руководство по эксплуатации сервера обновлений \(Windows\)](#)

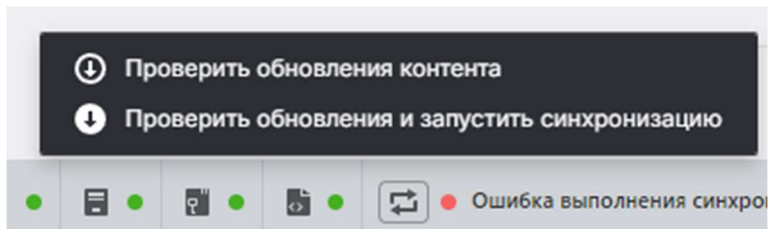
Шаг 1. Нажмите **Инструменты** → **Настройки** → **Общие** → в разделе **Прокси-сервер** выберите в соответствующем списке нужный параметр;

Шаг 2. Введите адрес и порт прокси-сервера, укажите при необходимости учетные данные для аутентификации;

Отметьте **Не использовать прокси службой сканирования**, если нет такой необходимости. По умолчанию функция включена.

Шаг 3. Нажмите **Сохранить**;

Шаг 4. Нажмите на статусной панели кнопку синхронизации → **Проверить обновления и запустить синхронизацию**;



Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.



4.4 Настройка учетных записей для сканирования

Рекомендуется:

- Не ограничивать срок действия пароля для сервисной учетной записи, если таких требований не предъявляет политика безопасности;
- Запретить учетной записи изменять свой пароль.

Содержание

- [4.4.1 Сканирование Windows-систем](#)
- [4.4.2 Сканирование Linux-систем](#)
- [4.4.3 Сканирование FreeBSD](#)
- [4.4.4 Сканирование Solaris](#)
- [4.4.5 Сканирование Check Point](#)
- [4.4.6 Сканирование Cisco IOS / NX-OS](#)
- [4.4.7 Сканирование Huawei](#)
- [4.4.8 Сканирование FortiOS](#)
- [4.4.9 Сканирование UserGate](#)
- [4.4.10 Сканирование VMware](#)
- [4.4.11 Сканирование Microsoft SQL Server](#)
- [4.4.12 Сканирование MySQL](#)
- [4.4.13 Сканирование PostgreSQL](#)
- [4.4.14 Сканирование Oracle](#)
- [4.4.15 Сканирование MongoDB](#)
- [4.4.16 Сканирование Eltex](#)
- [4.4.17 Сканирование Docker](#)
- [4.4.18 Сканирование OpenShift](#)

4.4.1 Сканирование Windows-систем

В RedCheck для сканирования удаленного хоста требуется создать учётную запись, **Тип учётной записи – Windows**.

Новая / Редактируемая учётная запись

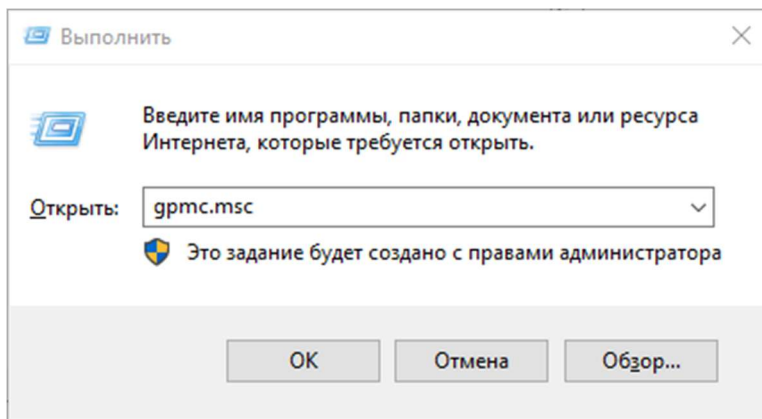
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text" value="windows"/>
Тип учётной записи	<input type="text" value="Windows"/>
<hr/>	
Имя пользователя	<input type="text"/>
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
Домен	<input type="text"/>
WinRM порт	<input type="checkbox"/> Указать WinRM порт <input type="text" value="5985"/>
	<input type="checkbox"/> WinRM через HTTPS
	<input type="checkbox"/> Указать порт RedCheck Agent
Порт RedCheck Agent	<input type="text" value="8732"/>
	<input type="checkbox"/> Указать порт RedCheck Update Agent
Порт RedCheck Update Agent	<input type="text" value="8733"/>

Для сканирования удаленных хостов необходимо их заранее настроить. Это можно сделать как локально на каждом компьютере, так и через групповые политики, если хосты находятся в домене.

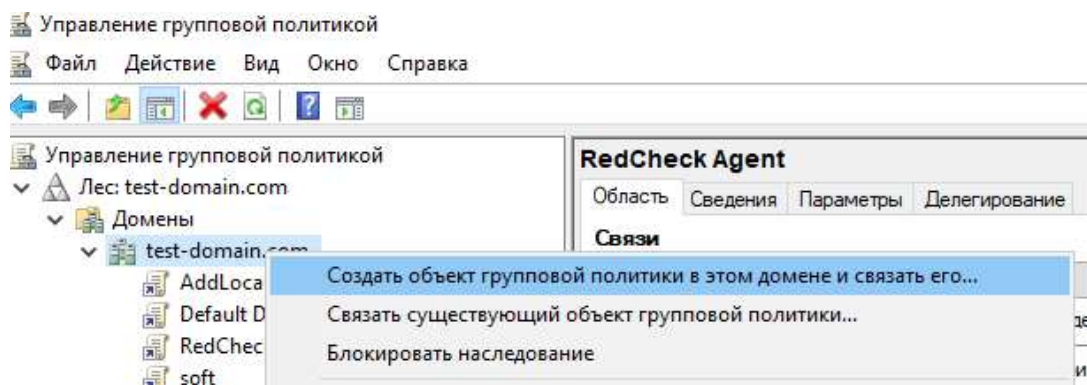
Создание групповой политики

Шаг 1. Нажмите **Win + R** → введите **gpmmc.msc**;

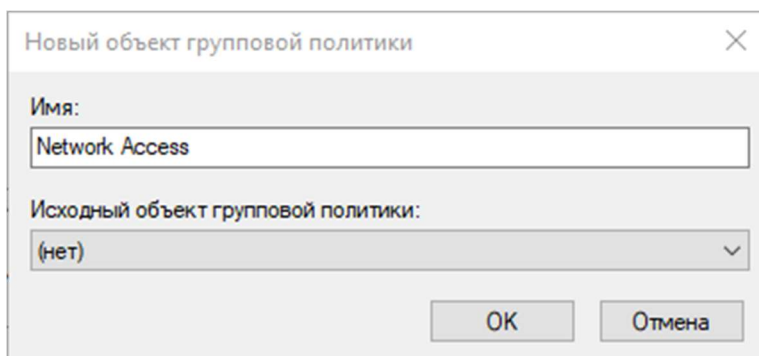


При локальной настройке нажмите **Win + R** → введите **gpedit.msc**;

Шаг 2. Раскройте **Домены** → ПКМ по **Создать объект групповой политики в этом домене...**

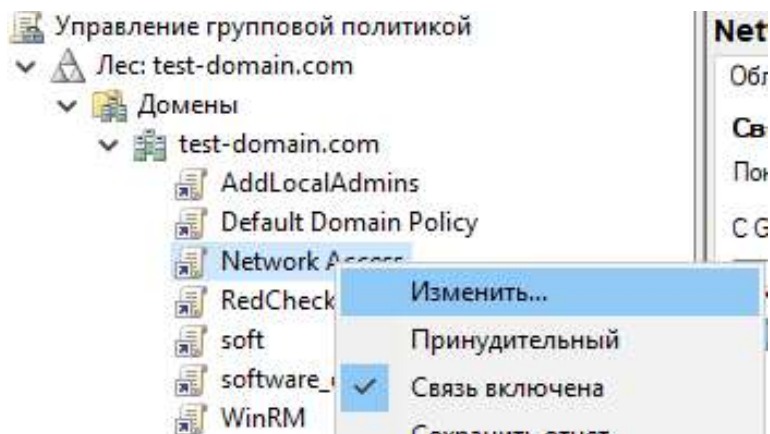


Введите название новой групповой политики;

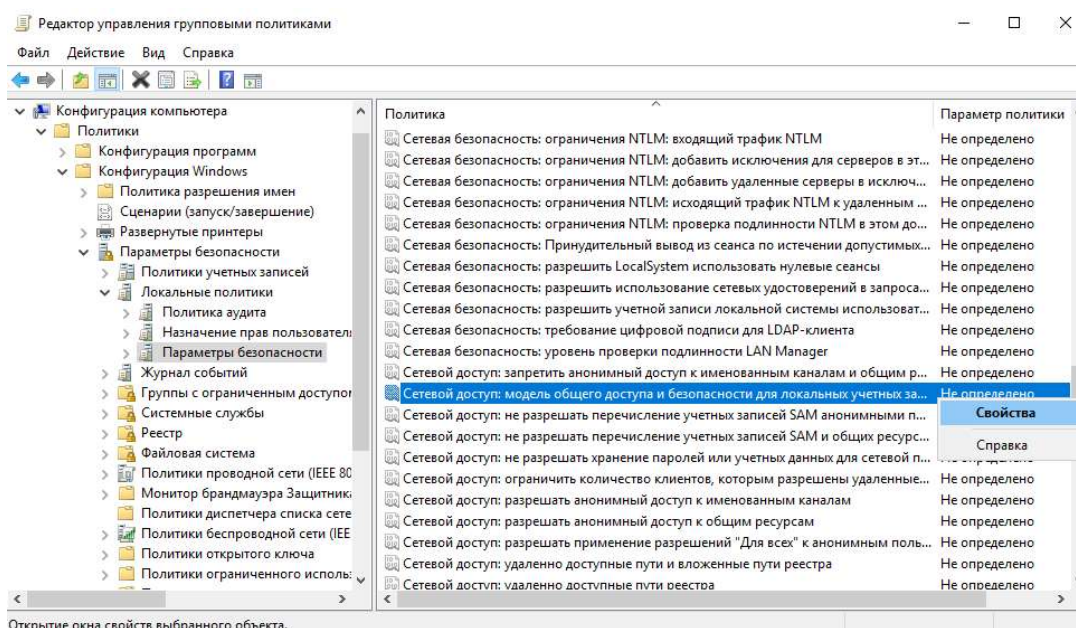


Настройка сетевого доступа

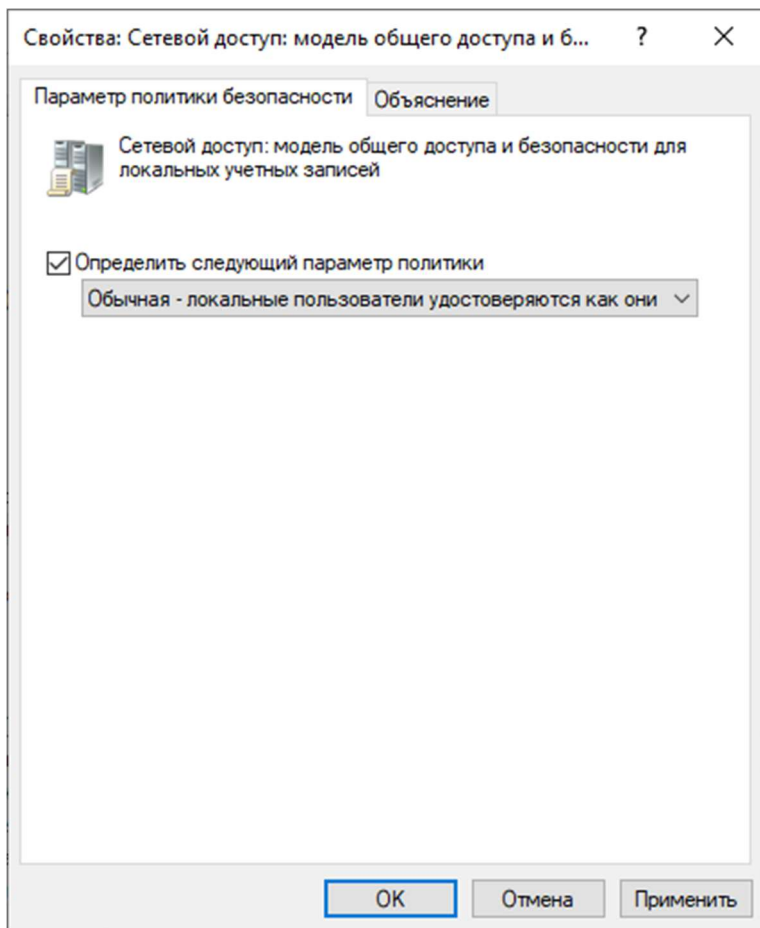
Шаг 3. ПКМ по созданной групповой политике → **Изменить**;



Шаг 4. Раскройте **Конфигурация компьютера** → **Политика** → **Конфигурация Windows** → **Параметры безопасности** → **Локальные политики** → **Параметры безопасности** → ПКМ по **Сетевой доступ: модель общего доступа и безопасности для локальных учетных записей** → **Свойства**;



Шаг 5. Отметьте **Определить следующий параметр политики** → выберите **Обычная – локальные пользователи...**

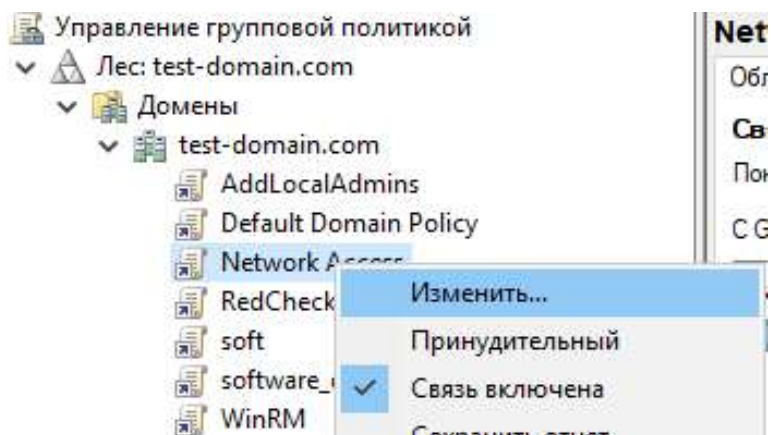


Настройка контроля учетных записей пользователей

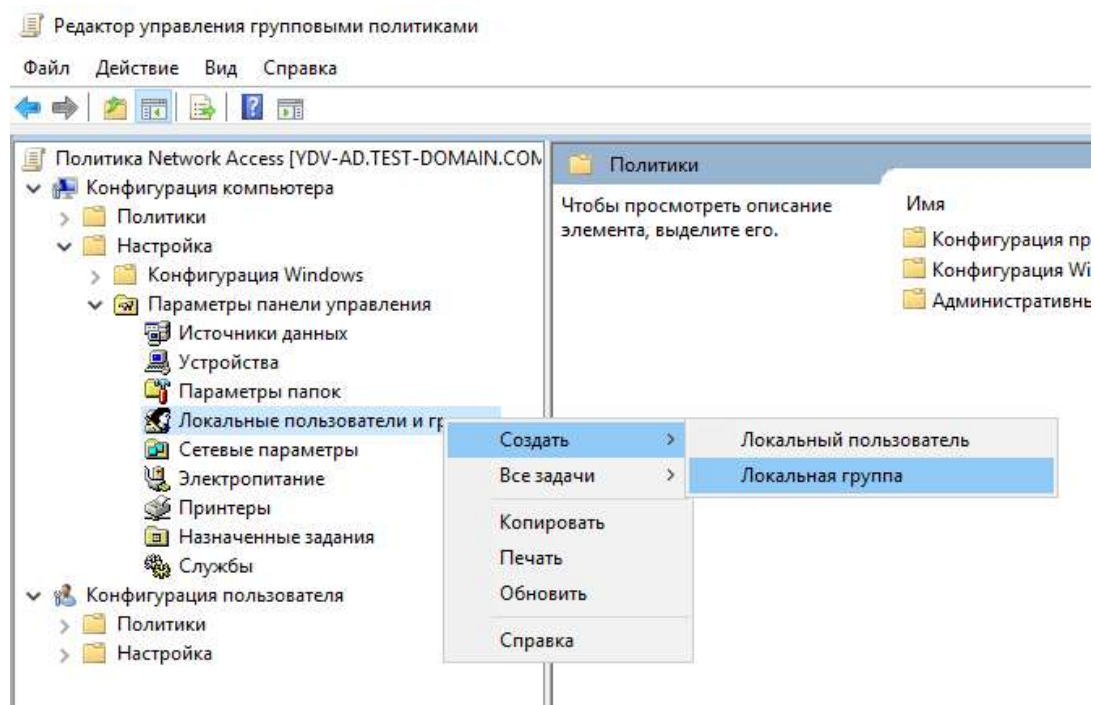
Рекомендуется использовать доменную УЗ для отключения функции UAC.

Шаг 1. Создайте доменную учетную запись, которая будет предназначена для сканирования;

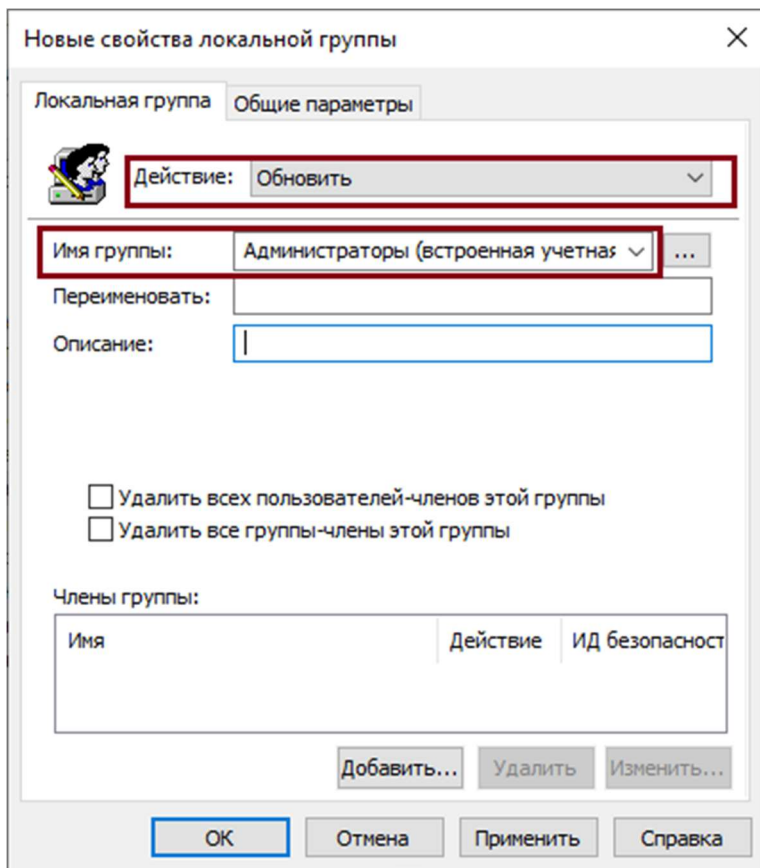
Шаг 2. ПКМ по необходимой групповой политике → **Изменить**;



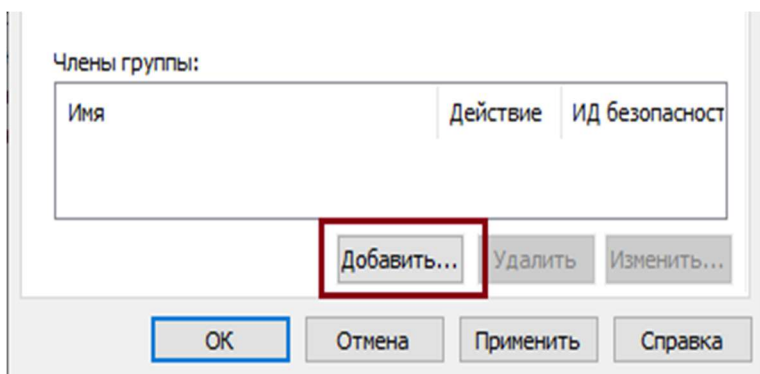
Шаг 3. Добавьте пользователя в группу локальных администраторов сканируемого хоста: **Конфигурация компьютера** → **Настройки** → **Параметры панели управления** → ПКМ по **Локальные пользователи и группы** → **Создать** → **Локальная группа**;



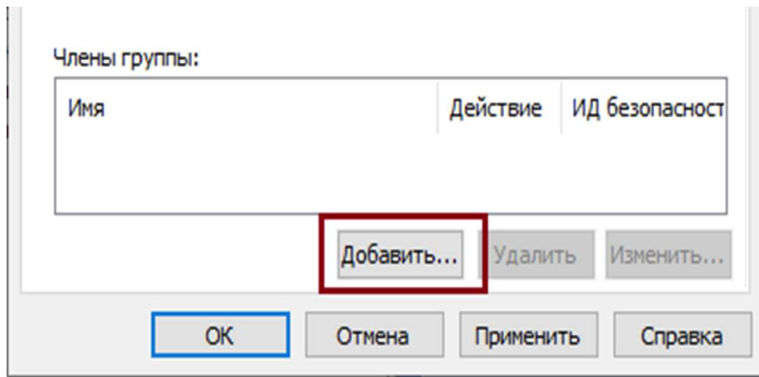
Шаг 4. В **Действие** выберите **Обновить**, в **Имя группы** – **Администраторы (встроенная учетная запись)**;



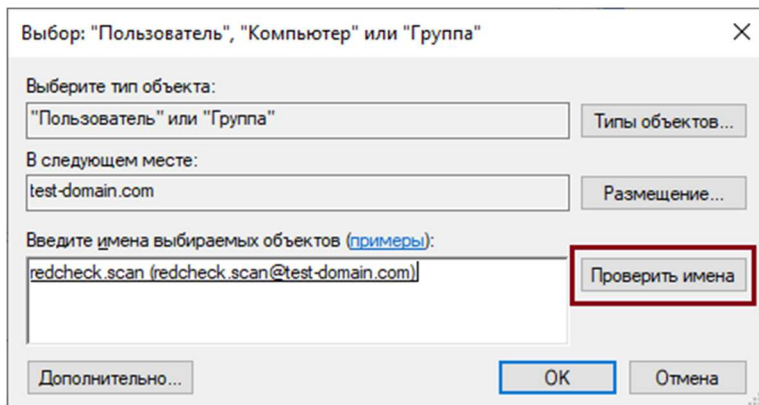
Нажмите **Добавить**;



Нажмите на троеточие справа от строки **Имя**;



Укажите имя созданного ранее пользователя → **Проверить имена** → **ОК**;



Шаг 5. Дождитесь обновления групповой политики на устройствах.

При использовании такой учётной записи настройки UAC не будут влиять на сканирование.

Дальнейшая настройка

- Транспорт Агент RedCheck
- Транспорт WinRM
- Транспорт WinRM (Kerberos)

Транспорт Агент RedCheck

Для агентского сканирования на целевых хостах должен быть установлен компонент Microsoft .NET Framework 4.8.

- Должна быть запущена служба Агента, открыт порт для входящих соединений TCP (по умолчанию 8732) ([3.6 Установка агента сканирования RedCheck](#));

Агент сканирования входит в состав дистрибутива RedCheck 2.6.9

- В одноранговой сети пользователь, от имени которого происходит обращение к агенту, должен находиться в локальной группе безопасности **REDCHECK_***. В случае доменной сети пользователь должен находиться в доменной группе безопасности **REDCHECK_*** ([5.1.2 Создание групп безопасности для Windows аутентификации](#));

Для повышения безопасности в сети предприятия рекомендуется, чтобы пользователь имел роль с минимальными правами доступа в ролевой модели RedCheck ([1..4 Ролевая модель RedCheck](#)).

- Пропускная способность канала между Агентом и службой сканирования должна быть не менее 128 Кбит/с.

Привилегии учетной записи, необходимые для взаимодействия:

- Локальный пользователь сканируемого хоста или пользователь домена;
- Пользователь с параметрами групповой политики **Вход в качестве службы** и **Доступ к компьютеру из сети**;
- Пользователь с правами на чтение списка состава групп REDCHECK_* и списка компьютеров в сети.

Транспорт WinRM

Для обеспечения сканирования хостов без применения агента сканирования RedCheck используется технология Remote Engine, которая осуществляется посредством службы удалённого управления Windows **Remote Management (WinRM)**. Данная служба для своей работы требует настройку службы сканирования и сканируемых узлов.

Содержание

- [Настройка WinRM \(SberLinux\)](#)
- [Настройка сканируемого узла \(локально\)](#)
- [Настройка сканируемых хостов через групповые политики](#)

WinRM на стороне службы сканирования настраивается конфигуратором автоматически (кроме SberLinux).

Настройка транспорта WinRM на стороне службы сканирования (SberLinux)

Шаг 1. Установите необходимые зависимости:

Bash (оболочка Unix)

```
sudo dnf install -y python38 python38-pip
```

Bash (оболочка Unix)

```
sudo dnf install -y gcc python38-devel krb5-devel
```

Bash (оболочка Unix)

```
sudo dnf install -y gssntlmssp
```

Шаг 2. Скачайте tar.gz архив ([ссылка на скачивание](#)) с необходимыми компонентами, поместите на хост с установленной службой сканирования (`/var/opt/redcheck-scan-service/pypsrp`) и разархивируйте;

Bash (оболочка Unix)

```
sudo tar -xf /var/opt/redcheck-scan-service/pypsrp/pypsrp-krb-SberLinux.tar.gz
```

Шаг 3. Установите python-пакеты:

Bash (оболочка Unix)

```
sudo pip3.8 install setuptools wheel Cython --no-index -f /var/opt/redcheck-scan-service/pypsrp/
```

Bash (оболочка Unix)

```
sudo pip3.8 install krb5 gssapi pypsrp[kerberos] --no-index -f /var/opt/redcheck-scan-service/pypsrp/
```

Шаг 4. Внесите правки в конфигурационный файл службы сканирования `/var/opt/redcheck-scan-service/conf/appsettings.json`;

Bash (оболочка Unix)

```
sudo nano /var/opt/redcheck-scan-service/conf/appsettings.json
```

Для параметра **PythonDll** установите значение `/usr/lib64/libpython3.8.so.1.0`

```
},
  "DbOperationTimeout": 3000,
  "Sckd": "",
  "Service": {
    "ServiceId": "48660376-fb93-488f-a57b-0dd216e43211",
    "Language": "Ru"
  },
},
  "Polling": {
    "PollingIntervalSec": 1
  },
},
  "PythonRuntime": {
    "PythonDll": "/usr/lib64/libpython3.8.so.1.0"
  }
}
```

Шаг 5. Перезапустите службу сканирования;

Bash (оболочка Unix)

```
sudo systemctl restart redcheck-scan-service
```

Если в вашем домене настроена Kerberos-аутентификация, выполните [дополнительную настройку](#) на хосте с установленной службой сканирования.

Настройка сканируемого узла

Windows Remote Management присутствует в составе Windows Vista\Windows Server 2008 и более поздних версий Windows. Для более ранних версий Windows необходимо отдельно скачать и установить пакет Windows Management Framework.

Для сканирования транспортом WinRM на конечных хостах должен быть установлен .NET Framework 4.0 и выше

Шаг 1. Откройте PowerShell и включите службу Windows Remote Management (WS-managment) командой:

Code

```
winrm qc
```

Команда изменит тип запуска службы WinRM на автоматический, задаст стандартные настройки WinRM и добавит исключения для WinRM портов (HTTP – 5985, HTTPS - 5986) в брандмауэр Windows.

Шаг 2. Добавьте в доверенные хосты ip-адрес службы сканирования:

Code

```
winrm set winrm/config/client '@{TrustedHosts="IP"}'
```

Шаг 3. Для стабильной работы RedCheck в режиме Remote Engine необходимо расширить квоту по использованию памяти с 150 Мб (по умолчанию) до рекомендованных 2 Гб. Для этого в оболочке PowerShell введите команду:

Code

```
Set-Item wsman:localhost\Shell\MaxMemoryPerShellMB 2048
```

Для проверки подключения выполните задание **Проверка доступности**, выбрав вид транспорта WinRM и учетную запись Windows.

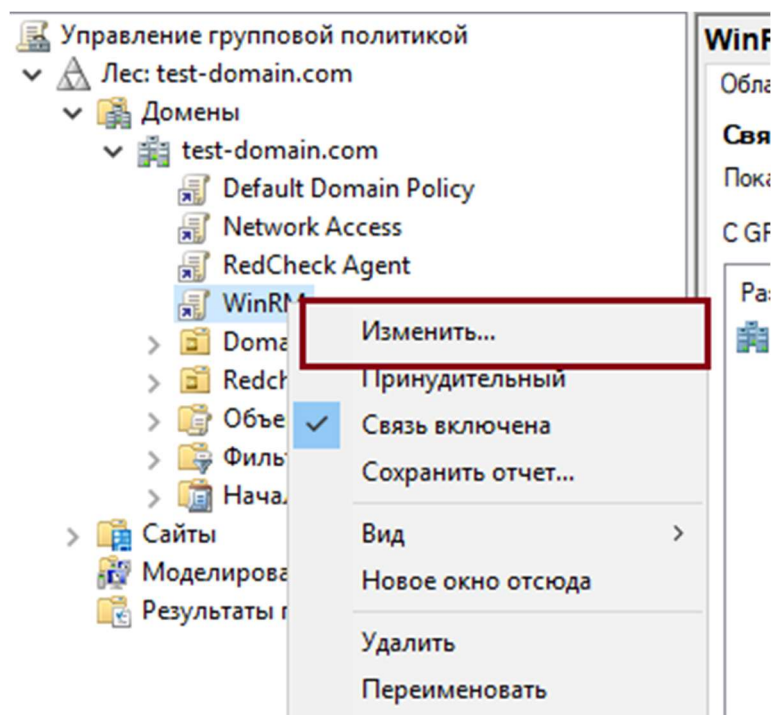
В случае возникновения проблем с подключением рекомендуется следовать [руководству](#).

Настройка WinRM через групповые политики [Настройка сканируемого узла \(локально\)](#)

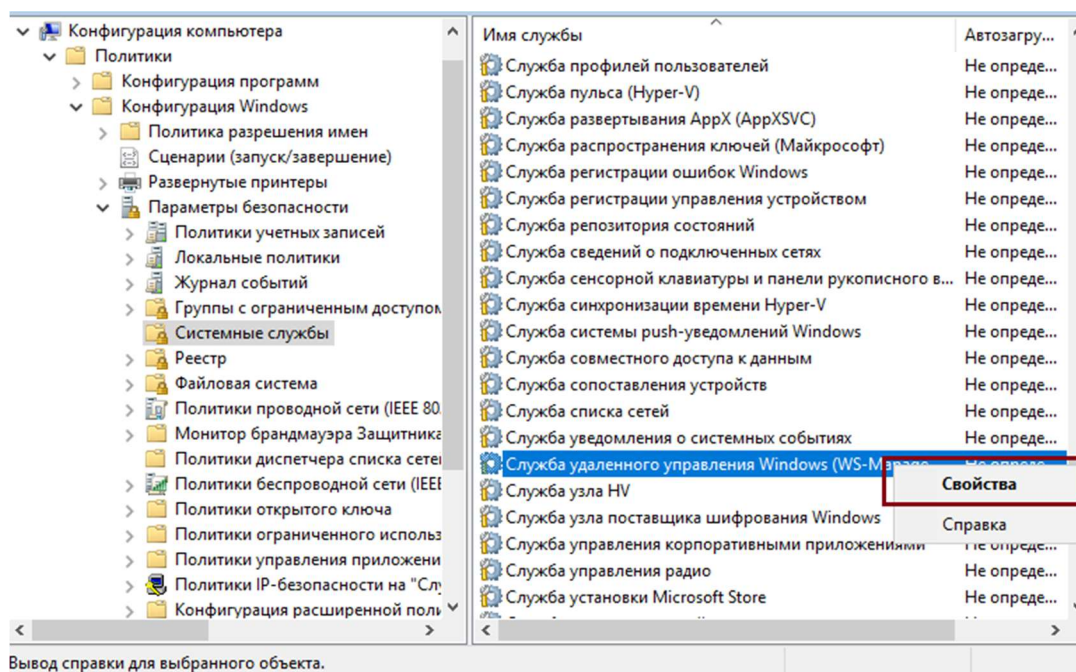
Для сканирования транспортом WinRM на конечных хостах должен быть установлен .NET Framework 4.0 и выше

Для настройки WinRM потребуется две групповые политики: одна для сервера сканирования, другая для сканируемых хостов. Их настройка идентична.

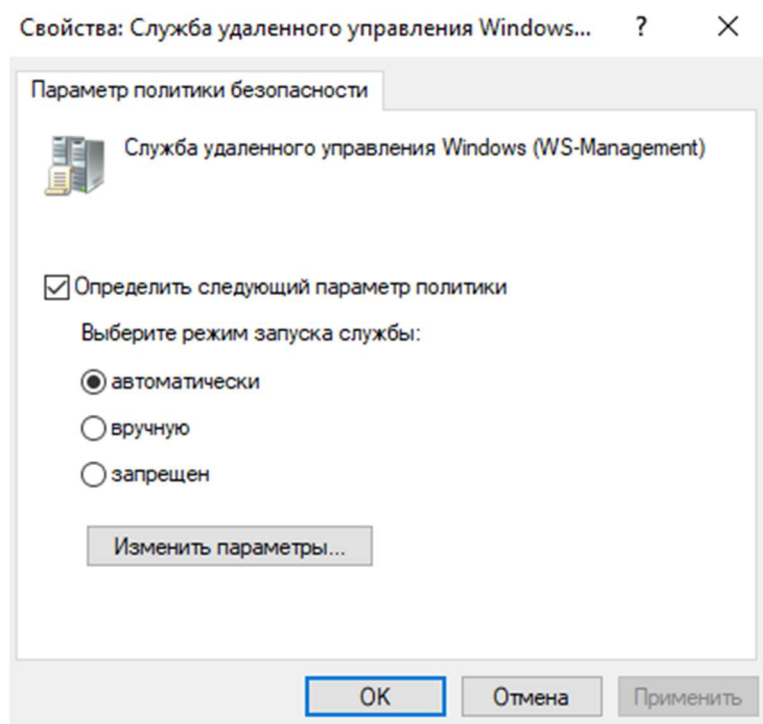
Шаг 1. ПКМ по групповой политике → **Изменить**;



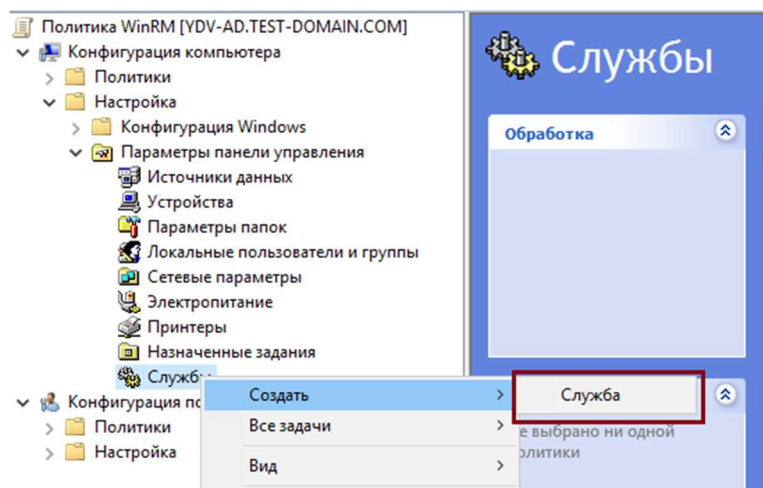
Шаг 2. Перейдите в **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Системные службы** → ПКМ по **Служба удаленного управления Windows (WS-Management)** → **Свойства**;



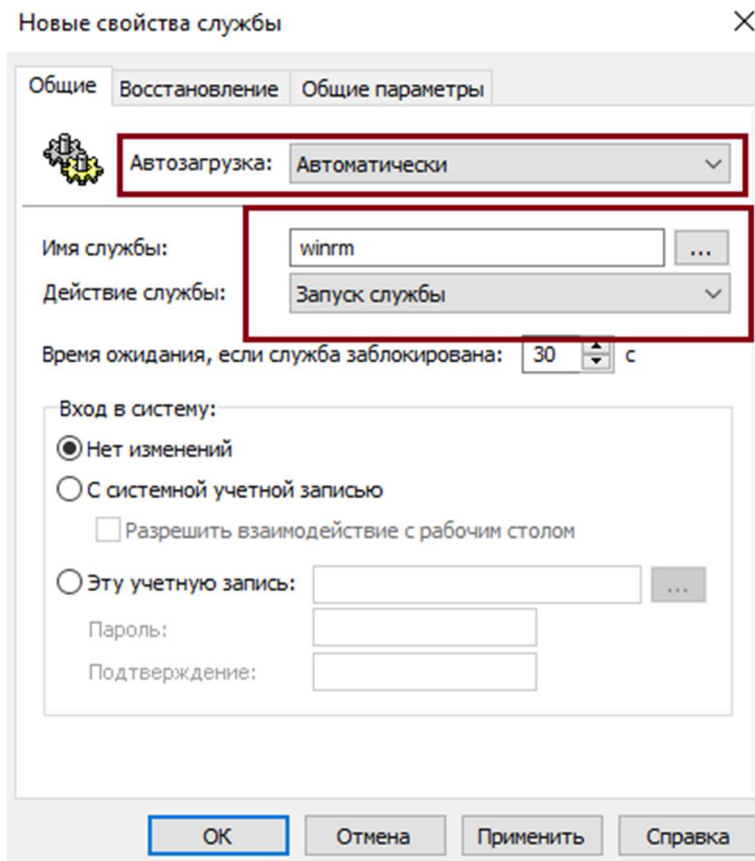
Отметьте **Определить следующий параметр политики**, режим запуска службы – **автоматически** → **ОК**;



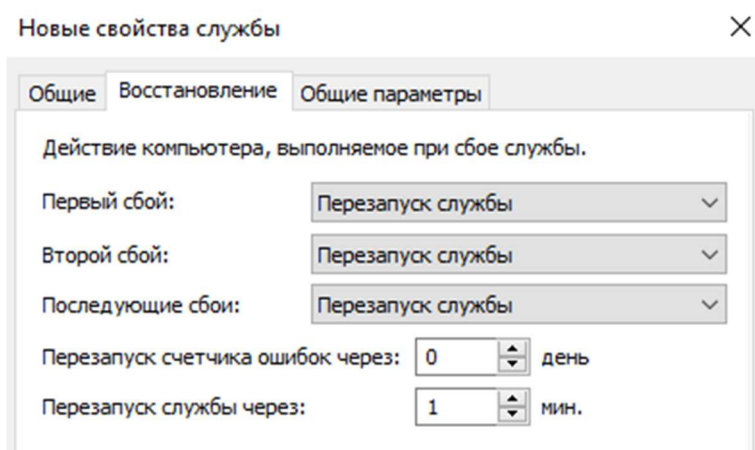
Шаг 3. Перейдите в **Конфигурация компьютера** → **Настройка** → **Параметры панели управления** → ПКМ по **Службы** → **Создать** → **Служба**;



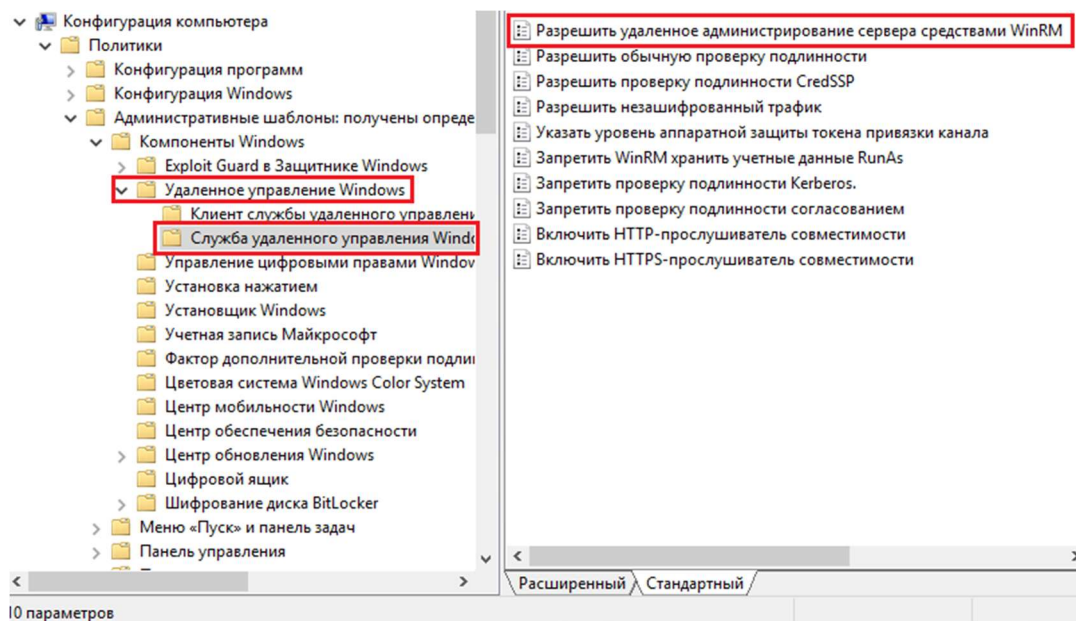
Шаг 4. Имя службы – **winrm**. В **Действия** выберите **Запуск службы**;



В разделе **Восстановление** укажите для трех параметров значение **Перезапуск службы**;

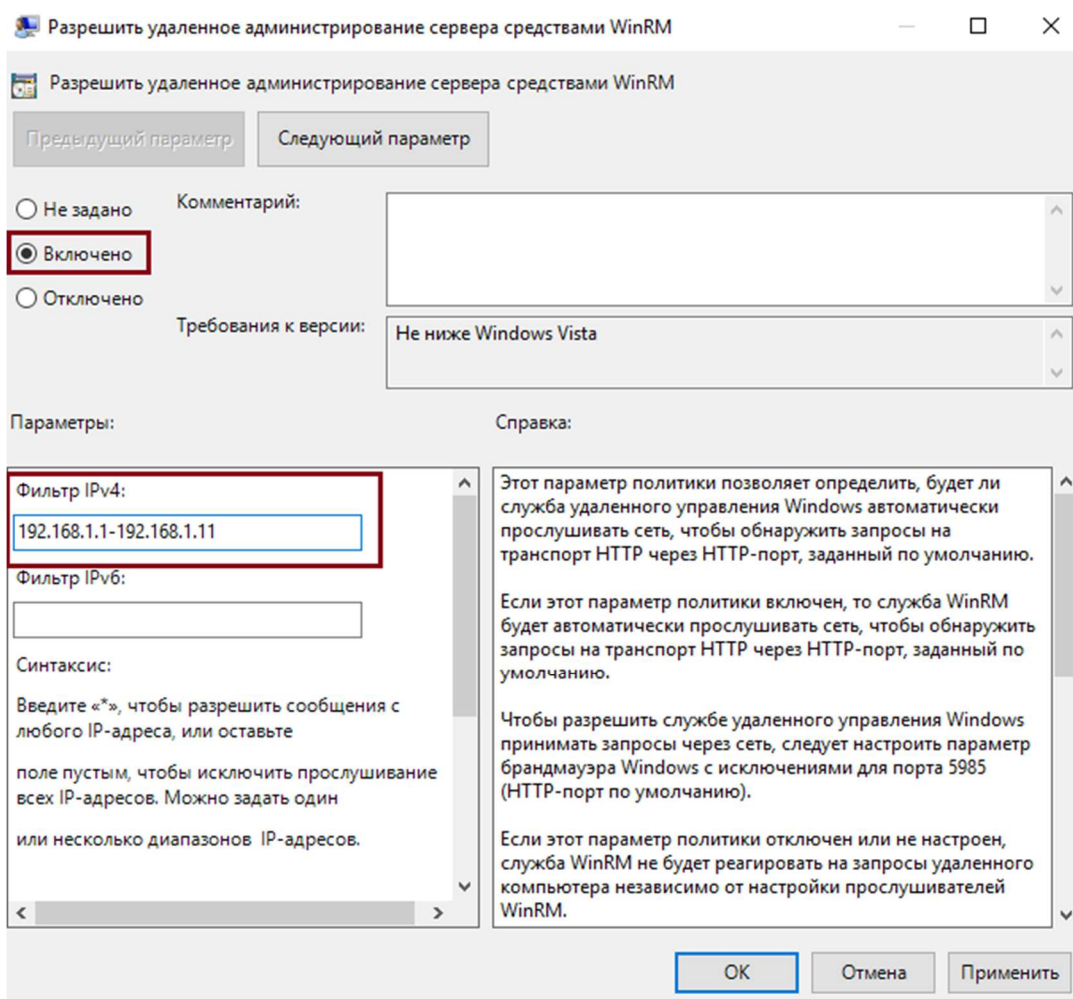


Шаг 5. Перейдите в **Конфигурация компьютера** → **Политики** → **Административные шаблоны...** → **Компоненты Windows** → **Удаленное управление Windows** → **Служба удаленного управления Windows** → откройте **Разрешить удаленное администрирование сервера...**;

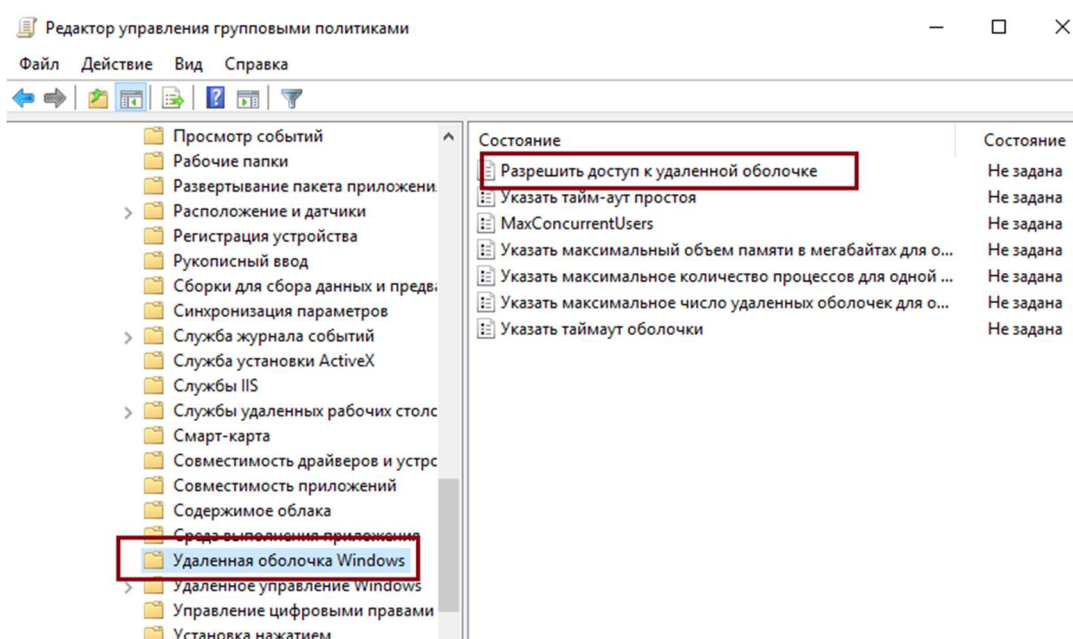


Укажите **Включено** → укажите в **Фильтр IPv4** IP-адреса:

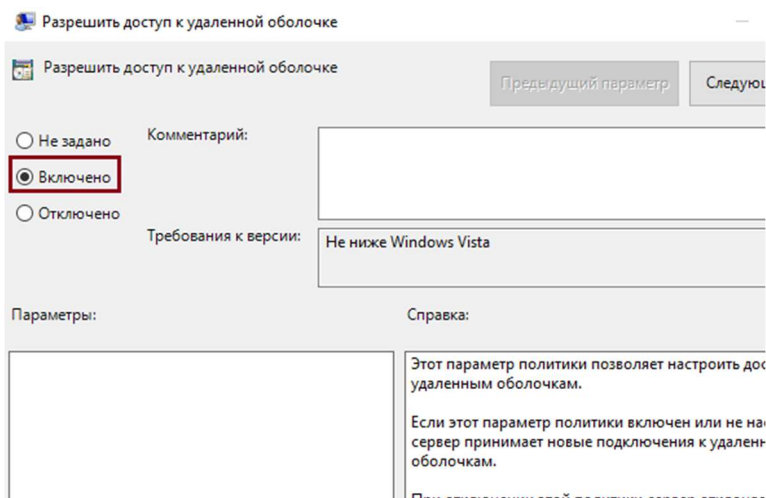
- **Для групповой политики для хоста службы сканирования:** ip-адрес хоста службы сканирования;
- **Для групповой политики для сканируемых узлов:** диапазон ip-адресов.



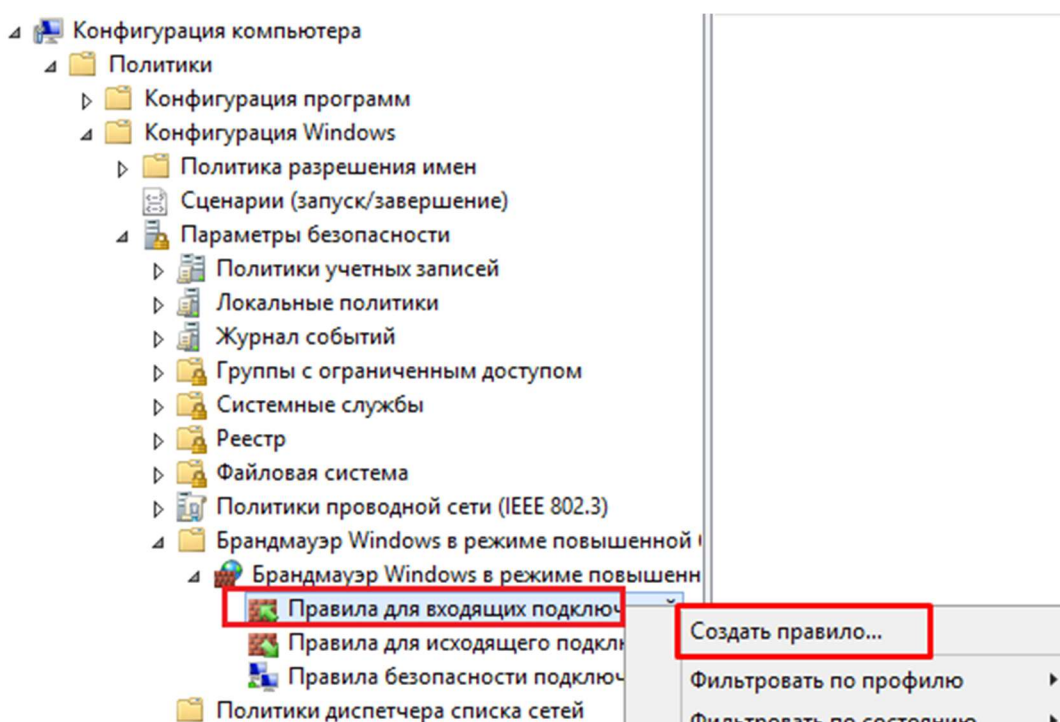
Шаг 6. Перейдите в **Компоненты Windows → Удаленная оболочка Windows** → откройте **Разрешить доступ к удаленной оболочке**;



Укажите **Включено**;



Шаг 7. Перейдите в **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Монитор брандмауэра Защитника Windows** → ПКМ по **Правила для входящих подключений** → **Создать правило**;



Шаг 8. Отметьте **Предопределенные** → выберите **Удаленное управление Windows** → **Далее**;

Тип правила

Выберите тип правила брандмауэра, которое требуется создать.

Шаги:

- Тип правила
- Предопред. правила
- Действие

Правило какого типа вы хотите создать?

Для программы
Правило, управляющее подключениями для программы.

Для порта
Правило, управляющее подключениями для порта TCP или UDP.

Предопределенные
Удаленное управление Windows
Правило, управляющее подключениями для операций Windows.

Настраиваемые
Настраиваемое правило.

< Назад **Далее >** Отмена

Отметьте два правила **Удаленное управление Windows...** → **Далее**;

Предопред. правила

Выберите правила, создаваемые для данной ситуации.

Шаги:

- Тип правила
- Предопред. правила**
- Действие

Какие правила вы хотите создать?

Следующие правила определяют требования сетевого подключения для выбранных предопределенных групп. Будут созданы правила, отмеченные флажком. Если отмеченное флажком правило уже существует, его содержимое будет заменено.

Правила:

Имя	Профиль	Прот...	Локал
<input checked="" type="checkbox"/> Удаленное управление Windows (HTTP - вход...	Общий	TCP	5985
<input checked="" type="checkbox"/> Удаленное управление Windows (HTTP - вход...	Домен, Частный	TCP	5985

< III >

< Назад **Далее >** Отмена

Укажите **Разрешить подключение** → **Готово**;

Действие

Укажите действие, выполняемое при соответствии подключения условиям, заданным в данном правиле.

Шаг:

- Тип правила
- Предопред. правила
- Действие**

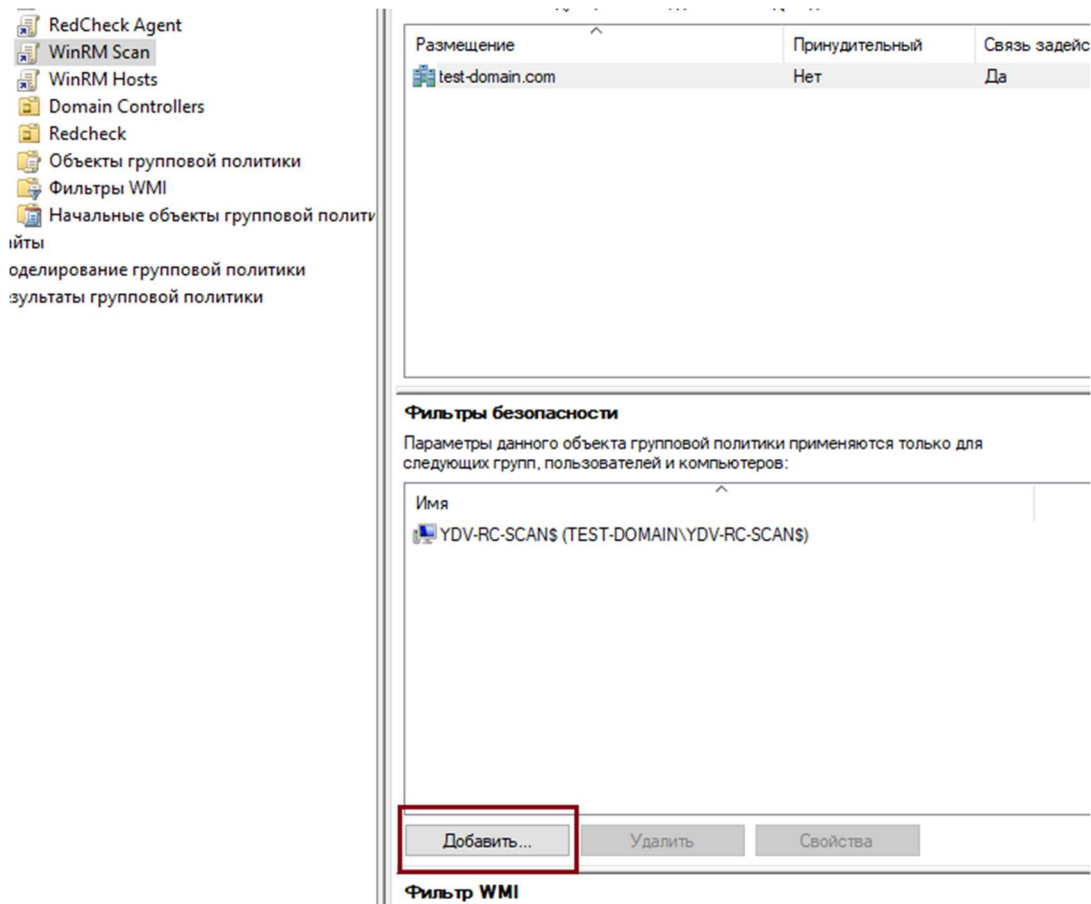
Укажите действие, которое должно выполняться, когда подключение удовлетворяет указанным условиям.

Разрешить подключение
Включая как подключения, защищенные IPSec, так и подключения без защиты.

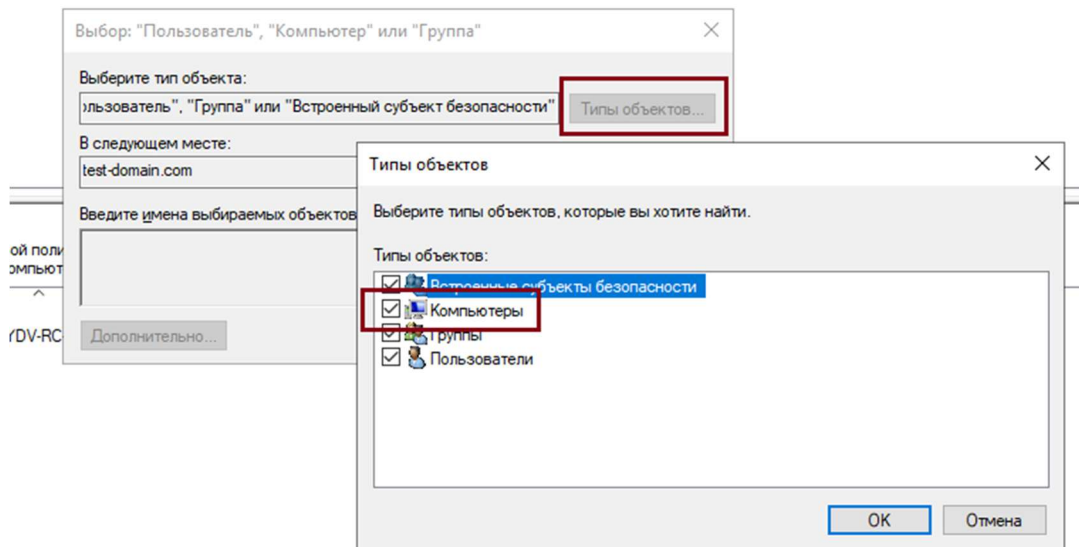
Разрешить безопасное подключение
Включая только подключения с проверкой подлинности с помощью IPSec. Подключения будут защищены с помощью параметров IPSec и правил, заданных в разделе правил безопасности подключений.

Блокировать подключение

Шаг 9. Укажите каждой групповой политике хосты, для которых эти политики будут применяться. Для хоста службы сканирования удалите группу **Прошедшие проверку** → **Добавить**;



Нажмите **Типы объектов** → отметьте **Компьютеры**;



Укажите имя компьютера, на котором установлена служба сканирования → **OK**;

Выбор: "Пользователь", "Компьютер" или "Группа" ×

Выберите тип объекта:

"Пользователь", "Компьютер", "Группа" или "Встроенный субъект"

Типы объектов...

В следующем месте:

test-domain.com

Размещение...

Введите имена выбираемых объектов ([примеры](#)):

YDV-RC-SCAN

Проверить имена

Дополнительно...

OK

Отмена

Транспорт WinRM (Kerberos)

Для сканирования хостов по протоколу WinRM с использованием доменных учетных записей по протоколу аутентификации Kerberos необходимо настроить конфигурационный файл /etc/krb5.conf, находящийся на хосте с установленной службой сканирования.

Содержимое файла **регистрозависимо**

Свойства (файлы .properties)

```
includedir /etc/krb5.conf.d/

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

[libdefaults]
dns_lookup_realm = false
dns_lookup_kdc = false
rdns = false
ticket_lifetime = 24h
renew_lifetime = 7d
pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
spake_preauth_groups = edwards25519
default_ccache_name = KEYRING:persistent:%{uid}
permitted_enctypes = aes256-cts arcfour-hmac-md5 aes128-cts rc4-
hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
default_tgs_enctypes = aes256-cts arcfour-hmac-md5 aes128-cts
rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc
default_tkt_enctypes = aes256-cts arcfour-hmac-md5 aes128-cts
rc4-hmac des3-cbc-sha1 des-cbc-md5 des-cbc-crc

[realms]
NAME-DOMAIN.COM = {
    kdc = dnsname.name-domain.com
    admin_server = dnsname.name-domain.com
}

[domain_realm]
.name-domain.com = NAME-DOMAIN.COM
name-domain.com = NAME-DOMAIN.COM
```

[libdefaults]

- **rdns** – если этот флаг установлен, то обратный поиск по имени будет использоваться в дополнение к прямому поиску по имени для

канонизации имен хостов для использования в именах участников службы;

- Параметры **permitted_enctypes**, **default_tgs_enctypes**, **default_tkt_enctypes** необходимы для корректного определения алгоритма шифрования во время сканирования.

[realms]

- **kdc** – имя или адрес хоста, на котором запущен KDC для этой области (может быть указано несколько адресов);
- **admin_server** – определяет хост, на котором запущен сервер администрирования. Как правило, это главный сервер Kerberos;

Раздел **[domain_realm]** предоставляет преобразование доменного имени или имени хоста в имя области Kerberos.

Подробную документацию по настройке конфигурационного файла можно найти по ссылке – https://web.mit.edu/kerberos/krb5-1.16/doc/admin/conf_files/krb5_conf.html

4.4.2 Сканирование Linux-систем

При сканировании Linux-систем (сканирование осуществляется по безагентской технологии) в качестве транспорта используется SSH-протокол не ниже версии 2.0 с включенным модулем поддержки протокола SFTP. Для сканирования удаленного хоста требуется создать учётную запись с возможностью подключения к удалённой системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.

В RedCheck для сканирования удаленного хоста требуется создать учётную запись, **Тип учетной записи – SSH**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	SSH <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
SSH порт	<input type="text" value="22"/>
Настройка привилегий	Sudo <input type="button" value="v"/> <input type="checkbox"/> Указать пароль привилегий
Пароль привилегий	<input type="password"/>
Подтверждение пароля привилегий	<input type="password"/>
	<input type="checkbox"/> Разделитель
Разделитель терминального пейджера	<input type="text" value="--More--"/>

Для сканирования удалённой системы могут использоваться следующие типы учётных записей:

- Учетная запись суперпользователя (root)
- Учетная запись привилегированного пользователя (sudo)

- Учетная запись непривилегированного пользователя

Установка openssh-server и sftp

Перед настройкой учетных записей необходимо установить пакет openssh-server, если его нет в системе по умолчанию.

Шаг 1. Выполните команду:

```
Bash (Unix Shell)
```

```
apt-get -y install openssh-server
```

Шаг 2. Запустите сервис:

```
Bash (Unix Shell)
```

```
/etc/init.d/ssh start
```

или

```
Bash (Unix Shell)
```

```
/etc/init.d/sshd start
```

Для проверки статуса работы сервиса введите команду: **systemctl status sshd** (или **systemctl status ssh**).

```
root@astra:~# systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2022-11-08 14:52:28 MSK; 1 months 4 days ago
     Process: 16216 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
     Process: 3486 ExecReload=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
     Process: 3523 ExecReload=/bin/kill -HUP $MAINPID (code=exited, status=0/SUCCESS)
    Main PID: 16228 (sshd)
      Tasks: 1 (limit: 1020)
     Memory: 1.0M
    CGroup: /system.slice/ssh.service
           └─16228 /usr/sbin/sshd -D

Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable.
root@astra:~#
```

Шаг 3. Протокол sftp включается добавлением специальной строки в файл `/etc/ssh/sshd_config` (или `/etc/openssh/sshd_config`). Проверьте наличие необходимой строки командой:

Bash (Unix Shell)

```
cat /etc/ssh/sshd_config | grep Subsystem
```

или

Bash (Unix Shell)

```
cat /etc/openssh/sshd_config | grep Subsystem
```

```
redcheck-scan@astra:~$ cat /etc/ssh/sshd_config | grep Subsystem
Subsystem sftp /usr/lib/openssh/sftp-server
redcheck-scan@astra:~$
```

Если результат команды оказался пустым, откройте файл любым текстовым редактором и добавьте следующую строку:

```
Subsystem sftp /usr/lib/openssh/sftp-server
```

```
# override default of no subsystems
Subsystem sftp /usr/lib/openssh/sftp-server
```

Необходимо отключить SELinux для корректного сканирования с использованием привилегированной учетной записи (sudo).

Требования к пользователю в системе:

- Командная оболочка Bash;
- Статическая строка приглашения (рекомендуемая длина – не менее 8 символов, как минимум 2 спецсимвола);

Требования к ключам шифрования:

- Минимальная длина ключа RSA - 1024;

- Минимальная длина ключа DiffieHellman - 1024;

Поддерживаемые алгоритмы обмена ключами:

- Diffie-Hellman (Oakley Group 2) with SHA-1
- Diffie-Hellman (Oakley Group 14) with SHA-1
- Diffie-Hellman (Group Exchange) with SHA-1
- Diffie-Hellman (Group Exchange) with SHA-256
- Diffie-Hellman (Oakley Group 14) with SHA-256
- Diffie-Hellman (Oakley Group 15 or 16) with SHA-512

Поддерживаемые алгоритмы шифрования:

- aes256-gcm@openssh.com
- aes128-gcm@openssh.com
- chacha20-poly1305@openssh.com
- aes256-ctr
- aes192-ctr
- aes128-ctr
- aes256-cbc
- aes192-cbc
- aes128-cbc
- ed25519
- 3des-ctr
- 3des-cbc
- twofish256-ctr
- twofish192-ctr
- twofish128-ctr
- twofish256-cbc
- twofish192-cbc
- twofish128-cbc
- twofish-cbc

Поддерживаемые алгоритмы имитовставки:

- MD5
- SHA1
- SHA256
- SHA512

Поддерживаемые методы аутентификации:

- Password
- KeyboardInteractive
- PublicKey

Поддерживаемые форматы закрытого ключа:

- PKCS #8 (RFC 5208)
- PuTTY .ppk
- OpenSSH/OpenSSL (SSLeay) for RSA/DSA
- New OpenSSH for EcDSA

Поддерживаемые алгоритмы открытого ключа и ключа хоста:

- RSA
- DSS
- ECDsaNistP256
- ECDsaNistP384
- ECDsaNistP521

Список используемых команд при сканировании динамичен и зависит от конфигурации конкретного хоста.

Учетная запись суперпользователя (root)

Данный тип учётной записи используется, чтобы получить все доступные данные и провести глубокий анализ параметров безопасности удалённой системы, и/или в случаях, когда невозможно использовать другие типы учётных записей.

По умолчанию в Linux-системах учётная запись суперпользователя имеет имя root.

RedCheck не накладывает ограничений на использование в качестве учетной записи суперпользователя root. Допустимо использовать любую другую учётную запись суперпользователя с отличным от root именем, если таковые существуют на удалённой системе.

По умолчанию на некоторых Linux-системах учетная запись суперпользователя root может быть неактивна. Чтобы активировать учетную запись суперпользователя root, выполните команду смены пароля:

```
Bash (Unix Shell)
```

```
passwd root
```

На некоторых Linux-системах для учетной записи суперпользователя root запрещен удаленный вход по протоколу SSH. Чтобы разрешить учетной записи суперпользователя root выполнять вход по протоколу SSH, выполните настройку SSH-сервера:

Шаг 1. Откройте текстовым редактором файл **/etc/ssh/sshd_config** или **/etc/openssh/sshd_config**

Шаг 2. Добавьте строку

```
Code
```

```
PermitRootLogin yes
```

Шаг 3. Перезапустите сервис **ssh** командой:

```
Bash (Unix Shell)
```

```
/etc/init.d/ssh restart
```

или

```
Bash (Unix Shell)
```

```
/etc/init.d/sshd restart
```

Конфигурационный файл SSH-сервера уже может содержать директиву **PermitRootLogin**. В таком случае измените значение директивы на **yes** с помощью текстового редактора.

Проверьте, что порт 22 открыт для входящих подключений.

Учетная запись привилегированного пользователя (sudo)

Для сканирования удалённой системы с помощью данного типа учётной записи у пользователя требуется наличие прав для выполнения sudo на удалённой системе. При создании учетной записи RedCheck необходимо указать **Sudo** для параметра **Настройка привилегий**.

По умолчанию на большинстве Linux-систем уже установлена программа sudo. Для проверки наличия программы sudo на удалённой системе выполните команду: **sudo -V**
Если программа sudo отсутствует на удалённой машине, необходимо выполнить её установку или воспользоваться другими типами учётных записей.

Шаг 1. Создайте учётную запись привилегированного пользователя (в примере ниже указано имя rc-scan-user) на удалённой системе:

Bash (Unix Shell)

```
adduser rc-scan-user
```

Шаг 2. Задайте пароль для созданной учётной записи пользователя:

Bash (Unix Shell)

```
passwd rc-scan-user
```

Шаг 3. Наделите пользователя правами для выполнения sudo:

Bash (оболочка Unix)

```
sudo visudo
```

Добавьте запись для нового пользователя, предоставив доступ к необходимым командам (в инструкции предоставляется доступ ко всем командам):

Код

```
rc-scan-user ALL=(ALL:ALL) ALL
```

Учетная запись непривилегированного пользователя

Данный тип учётной записи предназначен для получения данных, не требующих для своего доступа повышения прав, и не может применяться для полной оценки защищенности удалённой системы.

Шаг 1. Создайте учётную запись непривилегированного пользователя (в примере ниже указано имя `rc-scan-user`) на удалённой системе:

Bash (Unix Shell)

```
adduser rc-scan-user
```

Шаг 2. Задайте пароль для созданной учётной записи пользователя:

Bash (Unix Shell)

```
passwd rc-scan-user
```

4.4.3 Сканирование FreeBSD

Для сканирования удалённого хоста требуется создать учётную запись, **Тип** – **FreeBSD**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	FreeBSD <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
Настройка привилегий	Sudo <input type="button" value="v"/> <input type="checkbox"/> Указать пароль привилегий
Пароль привилегий	<input type="text"/>
Подтверждение пароля привилегий	<input type="text"/>

Для сканирования FreeBSD (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется SSH-протокол (по умолчанию используется порт 22) с включенным модулем поддержки протокола SFTP.

Перечень выполняемых команд в момент сканирования:

- sudo
- echo
- bind
- printf
- grep
- test
- file
- mktemp
- command
- cat
- find
- getfacl
- stat
- uname
- chmod
- base64

- rm
- basename
- dirname
- which
- openssl
- ls
- pkg

4.4.4 Сканирование Solaris

Для сканирования удалённого хоста требуется создать учётную запись, **Тип** – **Solaris**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	Solaris <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
Настройка привилегий	Sudo <input type="button" value="v"/> <input type="checkbox"/> Указать пароль привилегий
Пароль привилегий	<input type="text"/>
Подтверждение пароля привилегий	<input type="text"/>

Для сканирования удалённой системы в качестве основного транспорта используется протокол SSH. Убедитесь, что SSH-сервер установлен и настроен, а выбранная учётная запись пользователя имеет возможность подключения к удалённой системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.

Для сканирования удалённой системы, допускается использовать существующую учётную запись пользователя Solaris (привилегированного - sudo и rfxes; непривилегированного), или создать отдельную.

4.4.5 Сканирование Check Point

Для сканирования удалённого хоста требуется создать учетную запись, **Тип** – **Check Point Gaia**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	<input type="text" value="Check Point Gaia"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль
	<input type="radio"/> Указать ключ
	<input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
	<input type="checkbox"/> Разделитель
Разделитель терминального пейджера	<input type="text" value="-- More --"/>

Для сканирования Check Point (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется SSH-протокол (по умолчанию используется порт 22).

Перечень выполняемых команд в момент сканирования:

- show version all
- show software-version
- show interfaces
- show asset all
- cpinfo -y all
- cpstat os

4.4.6 Сканирование Cisco IOS / NX-OS

Для сканирования Cisco IOS / NX-OS (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется SSH-протокол (по умолчанию используется порт 22). Перед проведением сканирования необходимо убедиться, что служба SSH включена и настроена, а выбранная учётная запись пользователя имеет возможность подключения к удалённой системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.

Для сканирования удалённого хоста требуется создать учётную запись, **Тип** – **Cisco IOS / Cisco NX-OS**

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	Cisco IOS <input type="button" value="v"/>
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	22 <input type="text"/>
Настройка привилегий	None <input type="button" value="v"/> <input type="checkbox"/> Разделитель
Разделитель терминального пейджера	<input type="text" value="^\s*--\s*more\s*--\s*\$"/>

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	Cisco NX-OS <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
	<input type="checkbox"/> Разделитель
Разделитель терминального пейджера	<input type="text" value="^\s*--\s*more\s*--\s*\$"/>

Cisco IOS. Для сканирования должна использоваться учётная запись пользователя с возможностью входа в привилегированный режим с использованием команды **enable**

Требования к ключам и алгоритмам шифрования:

- Минимальная длина ключа RSA - 1024
- Минимальная длина ключа DiffieHellman - 1024

Поддерживаемые алгоритмы обмена ключами:

- DiffieHellmanGroup1SHA1
- DiffieHellmanGroup14SHA1
- DiffieHellmanGroupExchangeSHA1
- DiffieHellmanGroupExchangeSHA256
- ECDiffieHellmanNistP256
- ECDiffieHellmanNistP384
- ECDiffieHellmanNistP521
- Curve25519
- DiffieHellmanOakleyGroupSHA256

- DiffieHellmanOakleyGroupSHA512

Поддерживаемые алгоритмы шифрования:

- RC4
- TripleDES
- AES
- Blowfish
- Twofish

Поддерживаемые алгоритмы ключа хоста:

- RSA
- DSS
- ED25519
- ECDsaNistP256
- ECDsaNistP384
- ECDsaNistP521

Поддерживаемые алгоритмы имитовставки:

- MD5
- SHA1
- SHA256
- SHA512

Поддерживаемые методы аутентификации:

- Password
- KeyboardInteractive
- PublicKey

Поддерживаемые форматы закрытого ключа:

- PKCS #8 (RFC 5208)
- PuTTY .ppk

- OpenSSH/OpenSSL (SSLeay) for RSA/DSA
- New OpenSSH for EcDSA/Ed25519

Поддерживаемые алгоритмы открытого ключа:

- RSA
- DSS
- ED25519
- ECDsaNistP256
- ECDsaNistP384
- ECDsaNistP521

Для сканирования оборудования Cisco существует возможность использовать учётную запись без возможности перехода в привилегированный режим. Для реализации такого типа сканирования необходимо дополнительно настроить разрешающие правила для учётной записи.

Для такой учётной записи необходимо добавить разрешение на выполнение команд, указанных ниже:

- terminal length 0
- show
- show access-lists
- show arp
- show cdp
- show clock
- show file systems
- show interfaces
- show inventory
- show ip interface brief
- show ip ssh
- show privilege
- show snmp user
- show version

- more
- dir
- tclsh
- exit

Указанные ниже команды выполняются в привилегированном режиме:

- show file information
- show running-config all
- show logging
- show snmp group
- show startup-config

4.4.7 Сканирование Huawei

Для сканирования Huawei VRP (сканирование осуществляется по безагентской технологии) в качестве транспорта для сканирования используется протокол SSH (по умолчанию используется порт 22). Для сканирования необходима учётная запись пользователя с возможностью перехода в привилегированный режим с вводом пароля «super» и указанием уровня доступа данного пользователя, используемого для конкретного типа оборудования (не ниже 3-го).

Перед проведением сканирования необходимо убедиться, что служба SSH включена и настроена, а выбранная учётная запись пользователя имеет возможность подключения к удалённой системе по протоколу SSH.

Осуществить проверку подключения можно с помощью любого удобного SSH-клиента.

Для сканирования удаленного хоста требуется создать учётную запись, **Тип – Huawei VRP**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	<input type="text" value="Huawei VRP"/>
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
Настройка привилегий	<input type="text" value="None"/>
	<input type="checkbox"/> Разделитель
Разделитель терминального пейджера	<input type="text" value="^\s*--\s*more\s*--\s*\$"/>

Аналогичные настройки учётных записей производятся и для сетевого

оборудования «Булат».

Перечень команд, выполняемых при сканировании Huawei:

- screen-length 0 temporary
- display version
- display current-configuration
- display patch-information
- display authentication-scheme
- display aaa authentication-scheme
- display authorization-scheme
- display aaa authorization-scheme
- display accounting-scheme
- display aaa accounting-scheme
- display domain name
- display aaa domain
- display domain
- display elabel backplane
- display interface

4.4.8 Сканирование FortiOS

Для сканирования удаленного хоста требуется создать учётную запись, **Тип** – **FortiOS**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	Fortinet FortiOS <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
	<input type="checkbox"/> Разделитель
Разделитель терминального пейджера	<input type="text" value="--More--"/>

При сканировании FortiOS (сканирование осуществляется по безагентской технологии) в качестве транспорта используется SSH-протокол не ниже версии 2.0 с включенным модулем поддержки протокола SFTP.

Требования к УЗ:

- Разделитель по умолчанию: "--**More**-- ", без пробела внутри, пробел в конце строки;

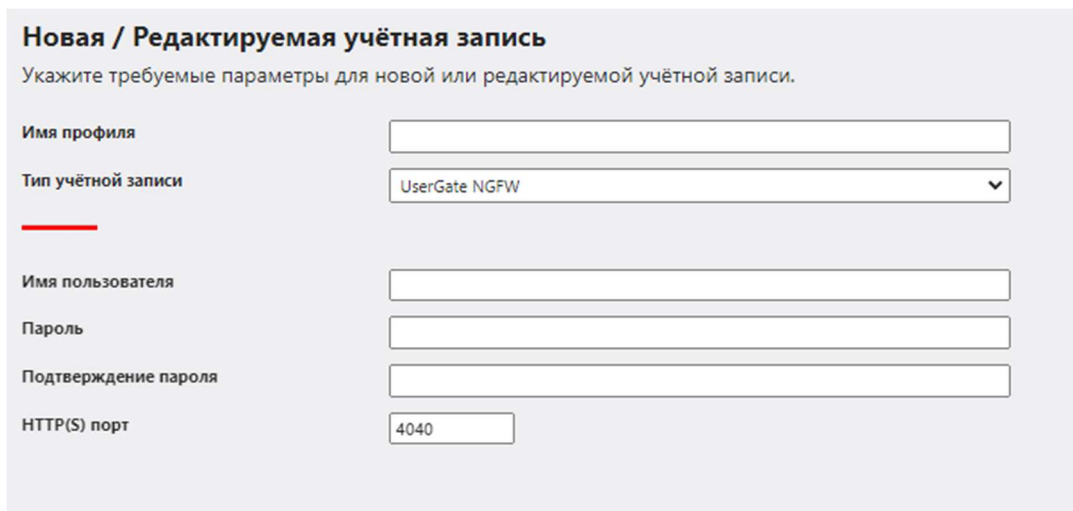
Настройки сканирования на стороне инфраструктуры:

- Создать профиль администрирования (System → Admin Profiles) с правами Read (Access Control);
- Создать УЗ администратора (System → Administrators);
- Привязать созданный профиль к УЗ;

- Отключить баннеры входа (pre-login-banner/post-login-banner).

4.4.9 Сканирование UserGate

Для сканирования удаленного хоста требуется создать учётную запись, **Тип** – **UserGate**.



Новая / Редактируемая учётная запись
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля

Тип учётной записи

Имя пользователя

Пароль

Подтверждение пароля

HTTP(S) порт

При сканировании UserGate (сканирование осуществляется по безагентской технологии) в качестве транспорта используется HTTP-протокол, номер порта 4040.

Настройки сканирования на стороне инфраструктуры

- Создать профиль администрирования (Настройки → UserGate → Администраторы → Профили администраторов);
- Указать для созданного профиля разрешения на чтение для всех объектов API (Настройки профиля → Разрешения для API);
- Создать УЗ администратора (Настройки → UserGate → Администраторы → Администраторы);
- Привязать созданный профиль к УЗ (Свойства администратора → Профиль администратора).

4.4.10 Сканирование VMware

Поддерживаются все редакции, указанные в [1.8 Перечень поддерживаемых платформ](#), лицензии для которых активируют feature vSphere API.

При сканировании VMware ESXi Server и VMware vCenter Server (кроме задания типа **Фиксация**) в качестве транспорта используются протоколы SOAP+HTTPS. При сканировании VMware ESXi Server и VMware vCenter Server заданием типа **Фиксация** в качестве транспорта используется SSH-протокол не ниже версии 2.0 с включенным модулем поддержки протокола SFTP.

Используемая технология доступа к данным – VMware Infrastructure Management (VIM).

Общий перечень команд, выполняемых при сканировании VMware ESXi Server и vCenter Server:

- Login
- Logout
- RetrieveServiceContent
- ContinueRetrievePropertiesEx
- RetrievePropertiesEx
- CreateContainerView
- DestroyView
- HostImageConfigGetAcceptance
- HostImageConfigGetProfile
- QueryLockdownExceptions
- RetrieveHostAccessControlEntries

Команда, выполняемая при сканировании VMware ESXi Server:

- VimEsxCllsoftwareviblist

Содержание

- [Настройка VMware ESXi Server](#)
- [Настройка VMware vCenter Server](#)
- [Настройка VMware NSX Data Center](#)

Настройка VMware ESXi Server

Для сканирования удаленного хоста требуется создать учетную запись, **Тип – VMware ESXi.**

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	VMware ESXi <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
HTTP(S) порт	<input type="text" value="443"/>
	<input type="checkbox"/> Проверка сертификата

Для выполнения заданий Аудит уязвимостей / обновлений, Аудит конфигураций и Инвентаризация, необходимо:

- активированная лицензия на продукт с включенной в нее feature vSphere API;
- наличие учётной записи пользователя VMware ESXi Server;
- присутствие учётной записи пользователя, состоящей в группе Администраторы, а также добавленной в список исключений Lockdown Mode;

Для выполнения задания Фиксации необходимо:

- активированная лицензия на продукт с включенной в нее feature vSphere API;
- наличие учетной записи пользователя Linux;
- присутствие учетной записи пользователя, состоящей в группе Администраторы, а также добавленной в список исключений Lockdown Mode;
- включенная служба SSH;

- включенная служба ESXi Shell;
- настроенные правила брандмауэра для доступа к SSH серверу;
- наличие параметра **PermitRootLogin yes** в настройках SSH сервера;
- наличие параметра **MaxSession 10** в настройках SSH сервера;

При использовании авторизации по ключам для выполнения задания типа **Фиксация** необходим ключ, сгенерированный утилитой **ssh-keygen**. Ключ, сгенерированный утилитой **puttygen**, не применим для данного задания.

По умолчанию на серверах ESXi доступ по протоколу SSH отключен. Включить доступ по SSH можно следующими способами:

- Включение SSH через DCUI;
- Включение SSH при помощи Web-клиента vSphere.

Включение SSH через DCUI

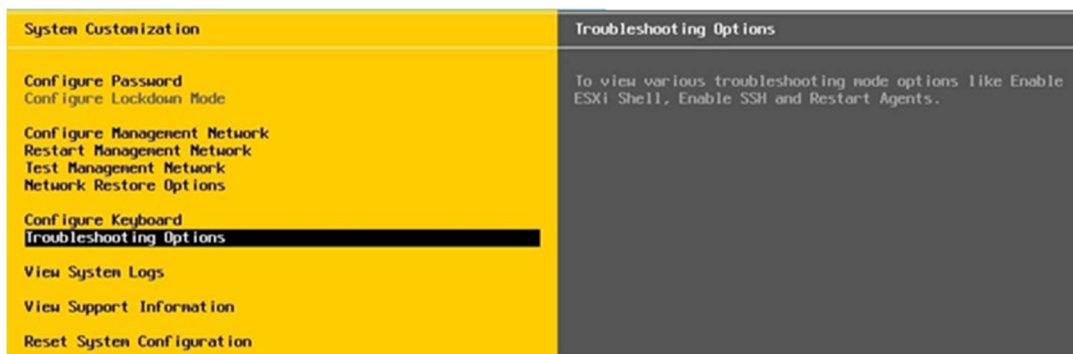
Direct Console User Interface (DCUI) – это интерфейс сервера ESXi, который выводится на монитор при прямом подключении к серверу.



Шаг 1. На сервере ESXi нажмите **F2** и авторизуйтесь при помощи учётной записи root;



Шаг 2. В меню **System Customization** выберите **Troubleshooting Options**;



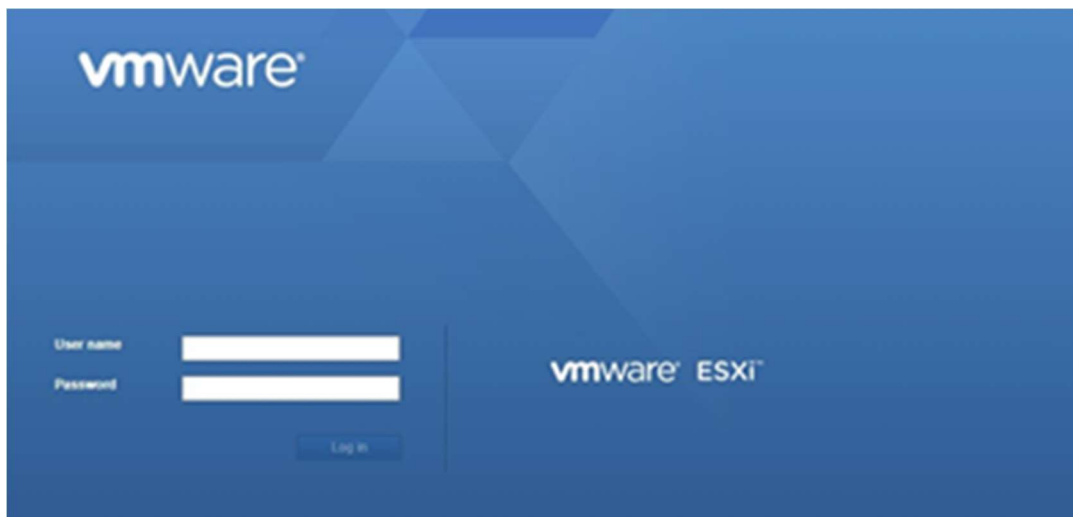
Шаг 3. В **Troubleshooting Mode Options** включите **Enable SSH**;



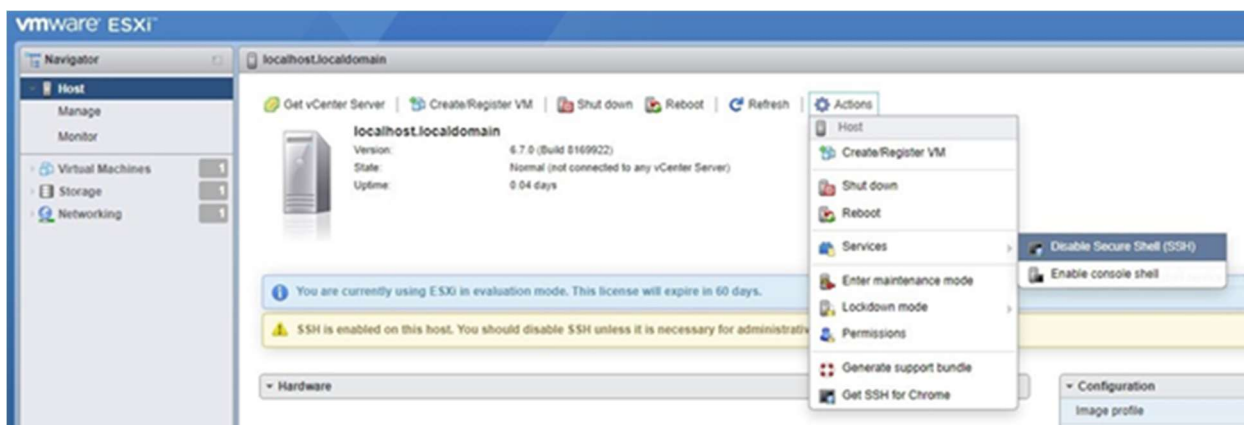
Для возврата в основное меню нажмите ESC.

Включение SSH при помощи Web-клиента vSphere

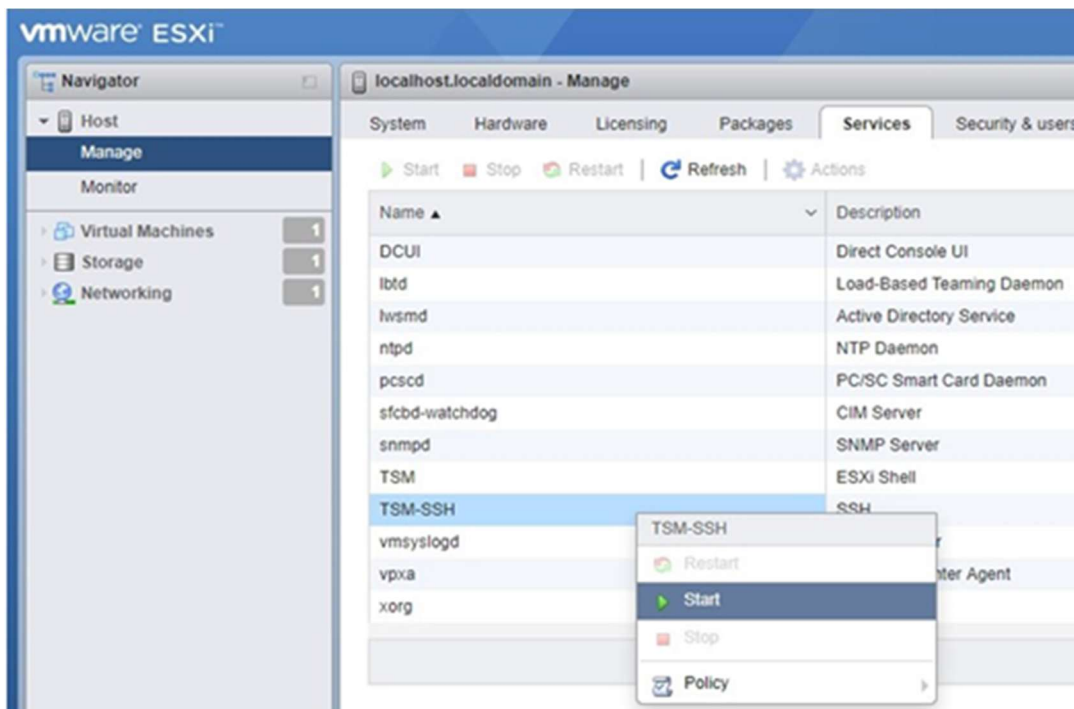
Шаг 1. Запустите браузер → введите в адресной строке адрес VMware сервера → авторизуйтесь на сервере ESXi через интерфейс vSphere Web Client;



Шаг 2. Выберите **Actions** → **Services** → **Enable Secure Shell (SSH)**;



Также активировать SSH можно в разделе **Manage** → **Services** → ПКМ по службе **TSM-SSH** → **Start**



Настройка SSH-туннеля завершена.

Настройка VMware vCenter Server

Для сканирования удаленного хоста требуется создать учётную запись, **Тип** – **VMware vCenter**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	VMware vCenter
Имя пользователя	<input type="text"/>
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
HTTP(S) порт	<input type="text" value="443"/>
	<input type="checkbox"/> Проверка сертификата

Для выполнения заданий Аудит уязвимостей / обновлений, Аудит конфигураций и Инвентаризация, необходимо:

- активированная лицензия на продукт с включенной в нее feature vSphere API;
- наличие учётной записи с ролью Administrator;

Для выполнения задания Фиксации необходимо:

- активированная лицензия на продукт с включенной в нее feature vSphere API;
- наличие учётной записи пользователя Linux;
- включенная служба SSH;
- включенная служба ESXi Shell;
- настроенные правила брандмауэра для доступа к SSH серверу;
- наличие параметра **PermitRootLogin yes** в настройках SSH сервера;
- наличие параметра **MaxSession 10** в настройках SSH сервера;
- наличие BASH в качестве shell по умолчанию;

Настройка VMware NSX Data Center

Для сканирования удаленного хоста требуется создать учётную запись, **Тип – VMware NSX.**

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	VMware NSX <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
Пароль	<input type="password"/>
Подтверждение пароля	<input type="password"/>
HTTP(S) порт	<input type="text" value="443"/>
	<input type="checkbox"/> Проверка сертификата

При сканировании VMware NSX Data Center for vSphere в качестве транспорта используется протокол HTTPS.

Для выполнения всех типов заданий RedCheck, кроме Фиксации, требуются:

- наличие включенной учётной записи Auditor;
- проверка доступности транспорта внешними средствами (например, Postman);

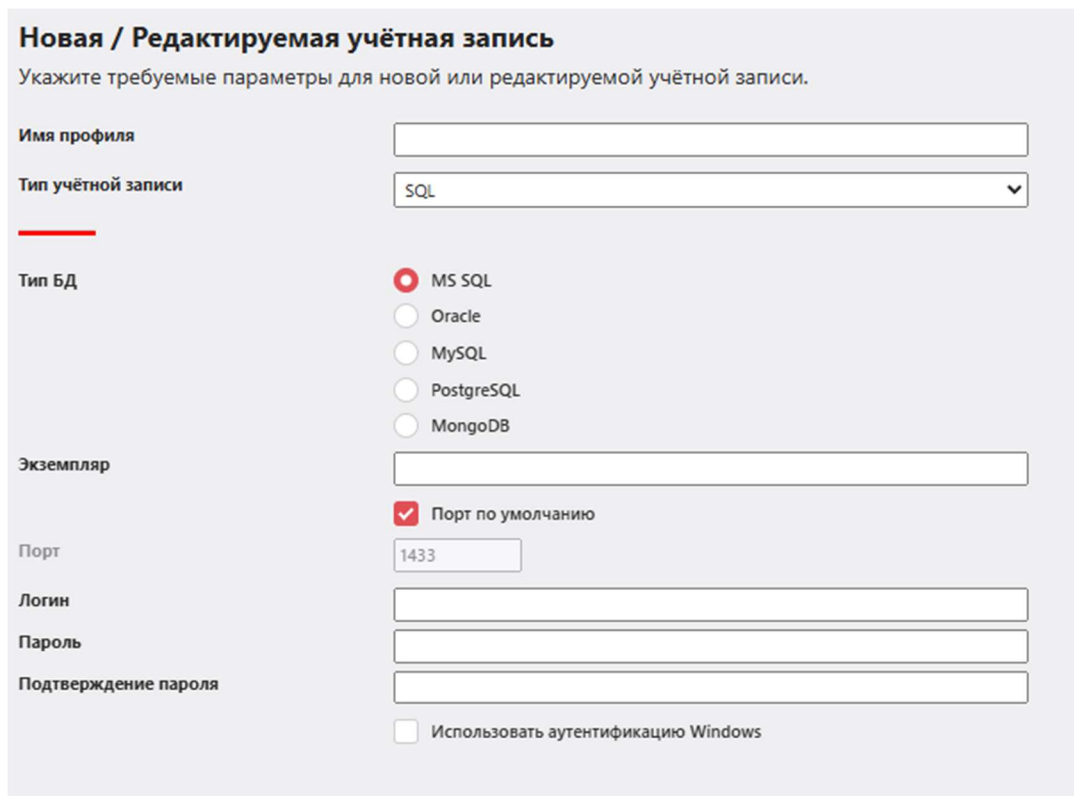
Перечень команд, выполняемых при сканировании VMware NSX Data Center for vSphere:

- api/1.0/appliance-management/backuprestore/backupsettings
- api/1.0/appliance-management/system/network
- api/1.0/appliance-management/components
- api/1.0/appliance-management/system/timesettings
- api/1.0/appliance-management/system/syslogserver

- `api/2.0/vdn/controller/node`

4.4.11 Сканирование Microsoft SQL Server

Для сканирования БД Microsoft SQL Server требуется создать учётную запись, **Тип – SQL, Тип БД – MS SQL.**



Новая / Редактируемая учётная запись
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля

Тип учётной записи

Тип БД MS SQL
 Oracle
 MySQL
 PostgreSQL
 MongoDB

Экземпляр

Порт Порт по умолчанию

Логин

Пароль

Подтверждение пароля

Использовать аутентификацию Windows

Для сканирования СУБД Microsoft SQL Server в экземпляре СУБД может использоваться режим доменной и смешанной авторизации.

По умолчанию, для сканирования СУБД MS SQL используется порт 1433. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

Минимальные требования для учётной записи

- роль сервера – **public**;
- учётная запись должна быть включена для базы данных **master**.

Поддержка TLS 1.2 начинается с версии SQL Server 2016.

Для сканирования Microsoft SQL Server ниже 2016 необходимо изменить версию протокола в /etc/ssl/openssl.cnf на стороне службы сканирования:

Bash (оболочка Unix)

```
MinProtocol = TLSv1  
CipherString = DEFAULT@SECLEVEL=1
```

4.4.12 Сканирование MySQL

Для сканирования БД MySQL требуется создать учётную запись, **Тип – SQL, Тип БД – MySQL.**

Новая / Редактируемая учётная запись
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля

Тип учётной записи

Тип БД

- MS SQL
- Oracle
- MySQL
- PostgreSQL
- MongoDB

Порт по умолчанию

Порт

База данных

Логин

Пароль

Подтверждение пароля

Для сканирования СУБД MySQL в экземпляре СУБД должен использоваться смешанный тип аутентификации (проверка подлинности MySQL).

По умолчанию, для сканирования СУБД MySQL используется порт 3306. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

Минимальные требования для учётной записи

1. Учетная запись должна иметь права на выполнение **SELECT-запросов к перечисленным таблицам:**

- information_schema.plugins
- mysql.user
- mysql.slave_master_info (если есть)

4.4.13 Сканирование PostgreSQL

Для сканирования БД требуется создать учётную запись **Тип – SQL, Тип БД – PostgreSQL**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	SQL <input type="button" value="v"/>
Тип БД	<input type="radio"/> MS SQL <input type="radio"/> Oracle <input type="radio"/> MySQL <input checked="" type="radio"/> PostgreSQL <input type="radio"/> MongoDB
	<input checked="" type="checkbox"/> Порт по умолчанию
Порт	<input type="text" value="5432"/>
База данных	<input type="text"/> <small>Если не указать имя базы данных, подключение будет выполняться к базе данных с тем же именем, что и логин.</small>
Логин	<input type="text"/>
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
Timeout	<input type="text"/>
Command Timeout	<input type="text"/>
Protocol	<input type="button" value="v"/>
SslMode	<input type="button" value="v"/>

По умолчанию для сканирования СУБД PostgreSQL используется порт 5432. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

Настройка учетной записи СУБД

Для СУБД необходимо создать учётную запись (например, `rc_scan_pg`) с правами, достаточными для выполнения запросов.

Шаг 1. Выполните минимальную настройку прав следующими командами (выполняются от привилегированного пользователя в СУБД):

PL/SQL

```
GRANT SELECT ON pg_settings TO rc_scan_pg;  
GRANT SELECT ON pg_roles TO rc_scan_pg;  
GRANT SELECT ON pg_database TO rc_scan_pg;  
GRANT SELECT ON pg_user TO rc_scan_pg;  
GRANT SELECT ON pg_class TO rc_scan_pg;  
GRANT SELECT ON pg_authid TO rc_scan_pg;  
GRANT SELECT ON pg_shadow TO rc_scan_pg;
```

Шаг 2. В файле **pg_hba.conf** необходимо разрешить подключение к СУБД.

Выполните для этого команды:

Для Windows-систем

Code

```
echo host all rc_scan_pg <имя_сети/маска> md5 >> C:\Program  
Files\PostgreSQL\версия\data\pg_hba.conf
```

<имя_сети/маска> - сеть или один адрес, которым разрешается доступ к СУБД.

К примеру, 192.168.100.0/24 или 192.168.100.15/32;

Для Astra Linux

Bash (Unix Shell)

```
echo host all rc_scan_pg <имя_сети/маска> md5 >>  
/etc/postgresql/версия/main/pg_hba.conf
```

Для BaseAlt

Bash (Unix Shell)

```
echo host all rc_scan_pg <имя_сети/маска> md5 >>  
/var/lib/pgsql/data/pg_hba.conf
```

4.4.14 Сканирование Oracle

Для сканирования БД Oracle требуется создать учётную запись, **Тип – SQL**, **Тип БД – Oracle**.

Новая / Редактируемая учётная запись
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	SQL <input type="text"/>
Тип БД	<input type="radio"/> MS SQL <input checked="" type="radio"/> Oracle <input type="radio"/> MySQL <input type="radio"/> PostgreSQL <input type="radio"/> MongoDB <input checked="" type="checkbox"/> Порт по умолчанию
Порт	<input type="text" value="1521"/>
База данных	<input type="text"/>
Логин	<input type="text"/>
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
Привилегии DBA	По умолчанию <input type="text"/>

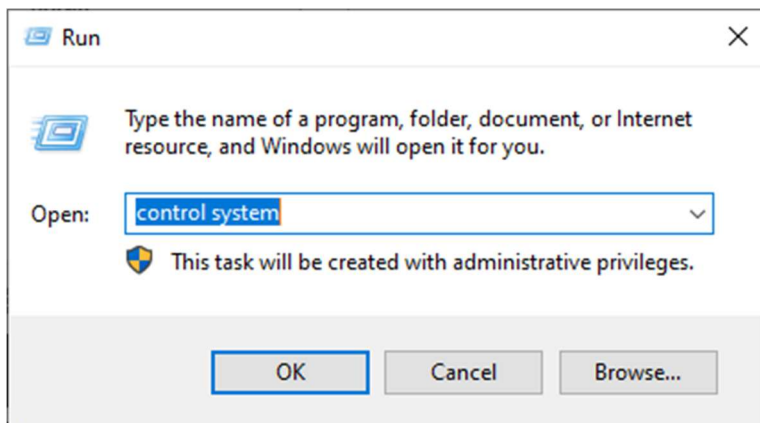
В экземпляре СУБД должен использоваться смешанный тип аутентификации (проверка подлинности Oracle).

По умолчанию для сканирования СУБД Oracle используется порт 1521. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

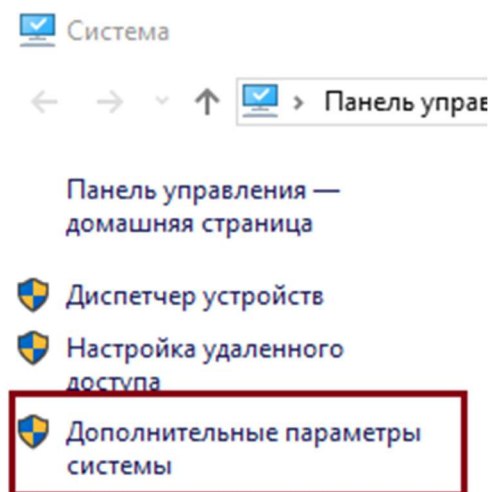
Добавление переменной среды ORACLE_HOME

Для проведения задания **Аудит БД Oracle** на сервере с установленной СУБД необходимо добавить переменную среды ORACLE_HOME.

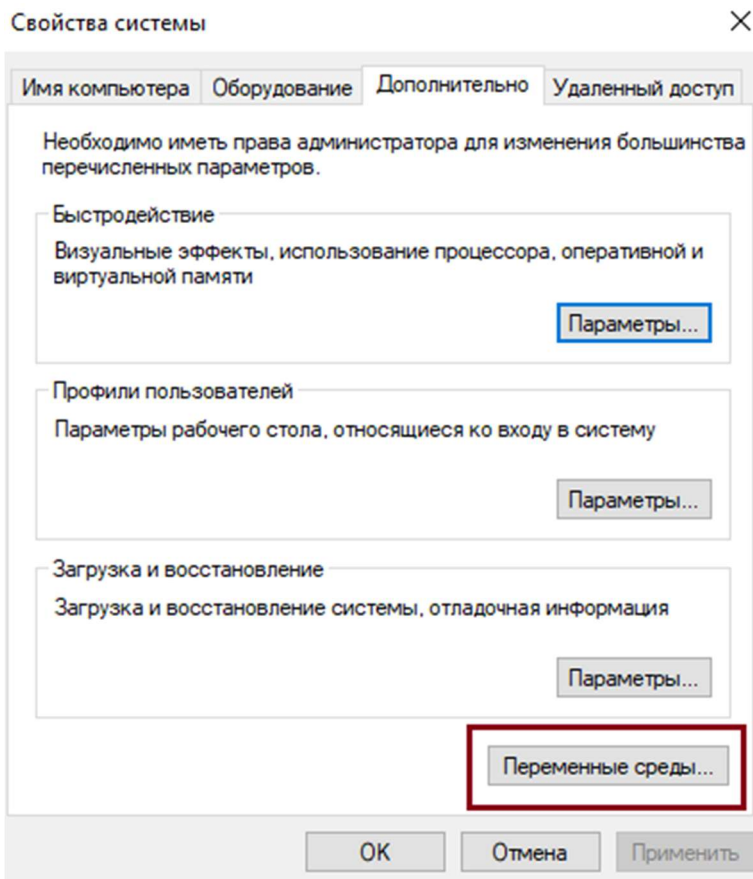
Шаг 1. Нажмите **Win + R** и введите **control system**;



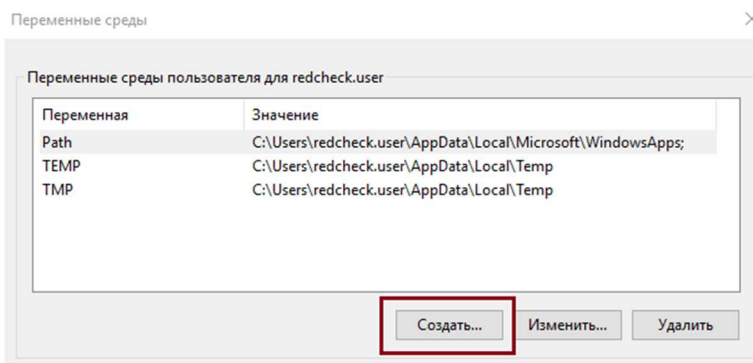
Шаг 2. Перейдите в **Дополнительные параметры системы;**



Перейдите в **Переменные среды;**



Нажмите **Создать**;



Шаг 3. В **Значение переменной** укажите каталог с ПО (по умолчанию каталог расположен по следующему пути: **C:\app\Имя_пользователя\virtual\product\Версия\Имя_БД**)

Необходимые разрешения на выполнение команд

Для сканирования СУБД допускается использование непривилегированной учетной записи. Ей потребуется добавить роль и предоставить необходимые

разрешения, выполнив указанные ниже команды от имени привилегированного пользователя СУБД:

PL/SQL

```
GRANT CONNECT TO <USER NAME>;
GRANT SELECT ON DBA_USERS TO <USER NAME>;
GRANT SELECT ON DBA_USERS_WITH_DEFPWD TO <USER NAME>;
GRANT SELECT ON DBA_TAB_PRIVS TO <USER NAME>;
GRANT SELECT ON DBA_PROFILES TO <USER NAME>;
GRANT SELECT ON DBA_TS_QUOTAS TO <USER NAME>;
GRANT SELECT ON DBA_ROLE_PRIVS TO <USER NAME>;
GRANT SELECT ON DBA_SYS_PRIVS TO <USER NAME>;
GRANT SELECT ON DBA_ROLES TO <USER NAME>;
GRANT SELECT ON DBA_PRIV_AUDIT_OPTS TO <USER NAME>;
GRANT SELECT ON DBA_OBJ_AUDIT_OPTS TO <USER NAME>;
GRANT SELECT ON DBA_STMT_AUDIT_OPTS TO <USER NAME>;
GRANT SELECT ON ALL_SYNONYMS TO <USER NAME>;
GRANT SELECT ON V_$PARAMETER TO <USER NAME>;
GRANT SELECT ON V_$DATABASE TO <USER NAME>;
GRANT SELECT ON V_$INSTANCE TO <USER NAME>;
GRANT SELECT ON V_$SESSION TO <USER NAME>;
```

<USER NAME> – имя непривилегированной учетной записи.

4.4.15 Сканирование MongoDB

Для сканирования БД требуется создать учётную запись **Тип – SQL, Тип БД – MongoDB.**

Новая / Редактируемая учётная запись
Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	SQL <input type="button" value="v"/>
Тип БД	<input type="radio"/> MS SQL <input type="radio"/> Oracle <input type="radio"/> MySQL <input type="radio"/> PostgreSQL <input checked="" type="radio"/> MongoDB <input checked="" type="checkbox"/> Порт по умолчанию
Порт	<input type="text" value="27017"/>
База данных	<input type="text"/>
Логин	<input type="text"/>
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
Параметры строки подключения	<input type="text"/>

По умолчанию для сканирования СУБД MongoDB используется порт 27017. В случае использования в инфраструктуре сети другого порта его необходимо явно указать.

4.4.16 Сканирование Eltex

Для сканирования удаленного хоста требуется создать учётную запись, **Тип** – **Eltex**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	<input type="text" value="Eltex"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
Настройка привилегий	<input type="text" value="None"/>
	<input type="checkbox"/> Разделитель
Разделитель терминального пейджера	<input type="text" value="^[^\n]*more"/>

При сканировании UserGate (сканирование осуществляется по безагентской технологии) в качестве транспорта используется SSH-протокол, порт по умолчанию 22.

Типовая процедура установки

Bash (оболочка Unix)

```
username redcheck password encrypted *** privilege 1
```

Bash (оболочка Unix)

```
enable password level 15 encrypted ***
```

Требования к учетной записи для сканирования

- Разделитель по умолчанию: `^.*[\\-\\]*more`
- Отключить логирование в консоль терминала:
 - **no logging console**
 - **syslog monitor none**

4.4.17 Сканирование Docker

При сканировании образов под управлением Docker выполняется подключение к хосту с клиентом и демоном Docker. В качестве транспорта используется SSH-протокол не ниже версии 2.0 с включенным модулем поддержки протокола SFTP.

Для проведения сканирования требуется, чтобы пользователь, от имени которого выполняется сканирование, имел возможность использовать `sudo` для повышения привилегий.

В RedCheck для сканирования Docker требуется создать учётную запись, **Тип – SSH.**

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

Имя профиля	<input type="text"/>
Тип учётной записи	SSH <input type="button" value="v"/>
<hr/>	
Имя пользователя	<input type="text"/>
	<input checked="" type="radio"/> Указать пароль <input type="radio"/> Указать ключ <input type="radio"/> Указать ключ и проверочную фразу
Пароль	<input type="text"/>
Подтверждение пароля	<input type="text"/>
SSH порт	<input type="text" value="22"/>
Настройка привилегий	Sudo <input type="button" value="v"/>
	<input type="checkbox"/> Указать пароль привилегий
Пароль привилегий	<input type="text"/>
Подтверждение пароля привилегий	<input type="text"/>
	<input type="checkbox"/> Разделитель
Разделитель терминального пейджера	--More-- <input type="text"/>

Требования к сканируемому хосту

- Bash shell;

- Утилита [rc-rpm](#).

Контрольные суммы:

MD5: 3932107273BBC55A9327C545D011B47F

SHA256:

E6588C5FAEBB2D182329D3AF60FCE1DFA071F9922B3E0A002264BD43E4F5CD
E8

Утилита `rc-rpm` устанавливается автоматически во время сканирования. Если автоматическая установка не произошла, необходимо установить утилиту в одну из директорий:

- `/usr/local/bin`
- `/usr/bin`

и выдать права на чтение и исполнение файла тому пользователю, от имени которого будет выполняться сканирование.

Имя файла должно быть строго **`rc-rpm`**.

4.4.18 Сканирование OpenShift

Для сканирования удаленного хоста требуется создать учётную запись, **Тип** – **OpenShift**.

Новая / Редактируемая учётная запись

Укажите требуемые параметры для новой или редактируемой учётной записи.

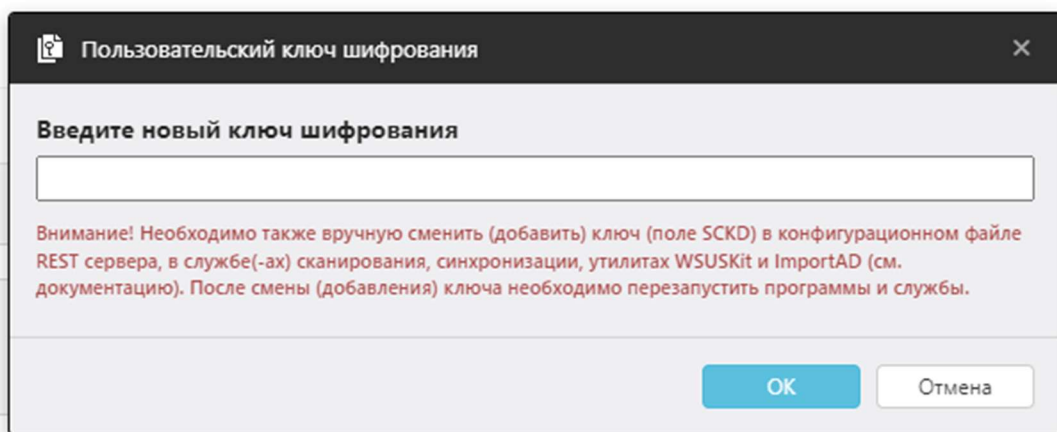
Имя профиля	<input type="text"/>
Тип учётной записи	<input type="text" value="OpenShift"/>
<hr/>	
Токен	<input type="text"/>
HTTP(S) порт	<input type="text" value="6443"/>
	<input type="checkbox"/> Проверка сертификата

При сканировании OpenShift (сканирование осуществляется по безагентской технологии) в качестве транспорта используется HTTP-протокол, порт по умолчанию **6443**.

4.5 Смена ключа шифрования

Шаг 1. Откройте консоль управления RedCheck, авторизовавшись под учетной записью с ролью RedCheck_Admins → **Справка** → **Сменить ключ шифрования**;

Шаг 2. Введите новый ключ шифрования → **ОК**;



Пользовательский ключ шифрования

Введите новый ключ шифрования

Внимание! Необходимо также вручную сменить (добавить) ключ (поле SCKD) в конфигурационном файле REST сервера, в службе(-ах) сканирования, синхронизации, утилитах WSUSKit и ImportAD (см. документацию). После смены (добавления) ключа необходимо перезапустить программы и службы.

ОК Отмена

Шаг 3. Вручную смените ключ шифрования для серверного компонента. На хосте с установленным серверным компонентом необходимо открыть файл **/var/opt/redcheck-api/conf/appsettings.json** и заменить старый ключ на новый для параметра **Sckd**

Шаг 4. На хосте для каждой установленной службы сканирования необходимо открыть файл **/var/opt/redcheck-scan-service/conf/appsettings.json** и заменить старый ключ на новый для параметра **Sckd**

```
{
  "ConnectionStrings": {
    "Default": "CfDJ8JN-D2R9",
  },
  "DbOperationTimeout": 3000,
  "Sckd": "",
  "Service": {
    "ServiceId": "3ba1f3f2-1",
    "Language": "Ru"
  },
  "Polling": {
    "PollingIntervalSec": 1
  },
}
```

Шаг 5. На хосте с установленной службой синхронизации необходимо открыть файл `/var/opt/redcheck-sync-service/conf/appsettings.json` и заменить старый ключ на новый для параметра **Sckd**

Шаг 6. Перезапустите службу сканирования и синхронизации;

Bash (оболочка Unix)

```
sudo systemctl restart redcheck-scan-service
```

Bash (оболочка Unix)

```
sudo systemctl restart redcheck-sync-service
```

4.6 Обслуживание БД

Шаг 1. Откройте консоль управления RedCheck → на панели навигации выберите **Инструменты** → **Настройки**;

Для изменения настроек RedCheck авторизуйтесь под УЗ с ролью **REDCHECK_SYSTEMS** или **REDCHECK_ADMINS**

Шаг 2. Перейдите в **Общие** и дождитесь подключения к службе очистки БД;

The screenshot shows the 'Очистка БД' (Database Cleanup) settings page. The page is divided into several sections:

- Очистка БД:** Служба очистки БД позволяет удалять неактуальные результаты сканирований и отчёты для уменьшения размера БД.
- Адрес службы:** http://192.168.80.8:8741
- Статус:** Свободна (green button). Версия: 2.8.0.9476
- Удаление сканирований:** Сканирования-эталон контролей не удаляются службой очистки. Со статусом "Хост недоступен", Со статусом "Ошибка", Со статусом "Завершено"
- Удаление отчётов:** Удалять отчёты старше 12 мес.
- Очистка сейчас:** Очистка с параметрами выше будет запущена немедленно.
- Очистка по расписанию:** Периодическая очистка позволяет эффективно ограничивать рост размера БД. Запускать очистку ежедневно
- Время запуска:** 00:00
- Уведомления:** Уведомления приходят по расписанию очистки, если оно активно, или после запуска вручную. Уведомлять при превышении размера БД
- Размер БД, Гб:** 0
- Список получателей:** Почта (empty list),

Шаг 3. Выберите какие сканирования и отчеты необходимо удалить;

Удаление сканирований
Сканирования-эталонны контролей не удаляются службой очистки.

Со статусом "Хост недоступен"
 Со статусом "Ошибка"
 Со статусом "Завершено"

Удаление отчётов
 Удалять отчёты старше мес.

Нажмите **Очистить БД**, чтобы назначить службе задачу;

Шаг 4. Для автоматической очистки БД отметьте **Запускать очистку ежедневно** → выберите время запуска службы очистки;

Очистка по расписанию
Периодическая очистка позволяет эффективно ограничивать рост размера БД.

Запускать очистку ежедневно

Время запуска

Шаг 5. При необходимости включите оповещение о превышении БД указанного размера, отметив **Уведомлять при превышении размера БД** и указав почтовые адреса получателей.

Уведомления
Уведомления приходят по расписанию очистки, если оно активно, или после запуска вручную.

Уведомлять при превышении размера БД

Размер БД, Гб

Список получателей

Почта

Нет данных для

4.7 Резервное копирование и восстановление БД

Все данные о хостах, результаты сканирования и настройки RedCheck хранятся в базе данных. Для планового резервного копирования достаточно поддерживать актуальную резервную копию БД.

В системах виртуализации допускается резервное копирование и восстановление виртуальных машин целиком.

Содержание

- [4.7.1 Резервное копирование PostgreSQL](#)
- [4.7.2 Восстановление PostgreSQL](#)

4.7.1 Резервное копирование PostgreSQL

Для создания резервной копии базы данных выполните следующие шаги.

Шаг 1. Создайте резервную копию с помощью утилиты `pg_dump`;

Bash (оболочка Unix)

```
pg_dump -Fc -h 127.0.0.1 -U redcheck RedCheck -f db_dd_mm_yyyy.dump
```

-Fc = пользовательский архивный формат результирующего файла;
-h = listen_address, на котором работает СУБД;
-U = имя пользователя, имеющего права для выполнения операции;
RedCheck = имя БД;
-f = путь для результирующего файла.

4.7.2 Восстановление PostgreSQL

Шаг 1. Войдите под пользователем postgres;

Bash (оболочка Unix)

```
sudo su postgres
```

Шаг 2. Удалите текущую базу данных;

Bash (оболочка Unix)

```
dropdb -U redcheck -f RedCheck
```

-U = имя пользователя, имеющего права для выполнения операции;
-f = принудительный режим удаления БД.

Шаг 3. Создайте новую базу данных;

Bash (оболочка Unix)

```
createdb RedCheck -h 127.0.0.1 -O redcheck -U redcheck
```

-h = listen_address, на котором работает СУБД;
-O = имя владельца БД;
-U = имя пользователя, имеющего права для выполнения операции.

Шаг 4. Восстановите данные;

Bash (оболочка Unix)

```
pg_restore -d RedCheck -h 127.0.0.1 -U redcheck db_dd_mm_yyyy.dump
```

-d = имя базы данных;
-h = listen_address, на котором работает СУБД;
-U = имя пользователя, имеющего права для выполнения операции;
путь к файлу резервной копии.

4.8 Обновление RedCheck Nix

Обновлять службу сканирования необходимо только после окончания всех сканирований. В случае обновления службы, у которой есть не окончившиеся или принудительно остановленные задания, эти задания не смогут запуститься после обновления.

Перед обновлением поддерживаемой российской ОС подключите репозиторий совместимости ([3.8 Подключение репозитория совместимости](#))

Для обновления RedCheck необходимо выполнить следующие шаги:

Если вы ранее разархивировали репозиторий в директорию /mnt, не забудьте удалить репозиторий оттуда.

Шаг 1. Удалите текущий репозиторий из директории /usr/local/src;

Bash (оболочка Unix)

```
sudo rm -R /usr/local/src/название_прошлого_репозитория
```

Шаг 2. Скачайте обновленный архив и разархивируйте его в директорию /usr/local/src;

Bash (оболочка Unix)

```
sudo tar -xvf путь_к_архиву -C /usr/local/src
```

Шаг 3. Обновите пакеты;

Astra Linux 1.7:

Bash (оболочка Unix)

```
sudo apt-key add /usr/local/src/redcheck-astra-repo/PUBLIC-GPG-KEY-
```

```
redcheck
sudo apt -y update
```

Astra Linux 1.8:

Bash (оболочка Unix)

```
sudo gpg --no-default-keyring --keyring /etc/apt/keyrings/redcheck-
keyring.gpg --import /usr/local/src/redcheck-astra-repo/PUBLIC-GPG-
KEY-redcheck
sudo apt -y update
```

Debian:

Bash (оболочка Unix)

```
sudo apt-key add /usr/local/src/redcheck-debian-repo/PUBLIC-GPG-KEY-
redcheck
sudo apt -y update
```

РЕД ОС / SberLinux:

Bash (оболочка Unix)

```
sudo dnf makecache
```

Для обновления с более ранних версий необходимо сначала обновиться до версии 2.9.1

Шаг 4. Обновите компоненты RedCheck;

Astra Linux:

Bash (оболочка Unix)

```
sudo apt install redcheck-api redcheck-client redcheck-scan-service
redcheck-sync-service altxmap redcheck-cleanup-service redcheck-
update-server
```

Debian:

Bash (оболочка Unix)

```
sudo apt install redcheck-api redcheck-client redcheck-scan-service  
redcheck-sync-service altxmap redcheck-cleanup-service redcheck-  
update-server
```

РЕД ОС:

Bash (оболочка Unix)

```
sudo dnf -y upgrade redcheck-api redcheck-client redcheck-scan-  
service redcheck-sync-service altxmap redcheck-cleanup-service  
redcheck-update-server
```

На этапе обновления пакетов введите Y или I для обновления
конфигурационных файлов:

```
Configuration file '/var/opt/redcheck-client/conf/appsettings.json'  
==> Modified (by you or by a script) since installation.  
==> Package distributor has shipped an updated version.  
What would you like to do about it? Your options are:  
Y or I : install the package maintainer's version  
N or O : keep your currently-installed version  
D      : show the differences between the versions  
Z      : start a shell to examine the situation  
The default action is to keep your current version.  
*** appsettings.json (Y/I/N/O/D/Z) [default=N] ? y
```

Шаг 5. Проведите конфигурацию RedCheck-Api и RedCheck-Cleanup-Service;

Сконфигурируйте также RedCheck-Client, если консоль управления была ранее настроена на HTTPS.

Перед повторной конфигурацией **рекомендуем** [сделать резервную копию](#) базы данных.

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный - критичное сообщение либо ошибка выполнения команды
желтый  - важное замечание требующее действия от пользователя
зеленый - успешное выполнение команды либо статус выполнения конфигурации
[*]     - диапазон допустимых значений
(*)     - значение по умолчанию
=====

Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

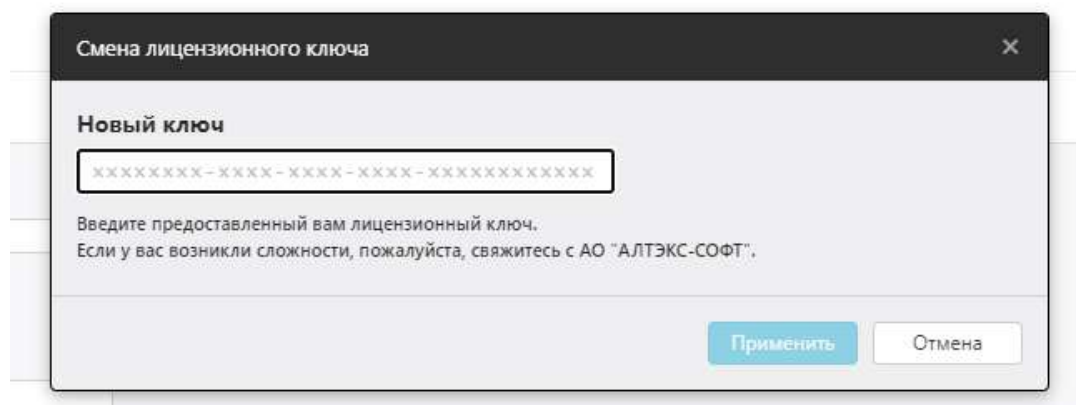
Шаг 6. Перезапустите службы:

Bash (оболочка Unix)

```
sudo systemctl restart redcheck-sync-service
sudo systemctl restart redcheck-scan-service
```

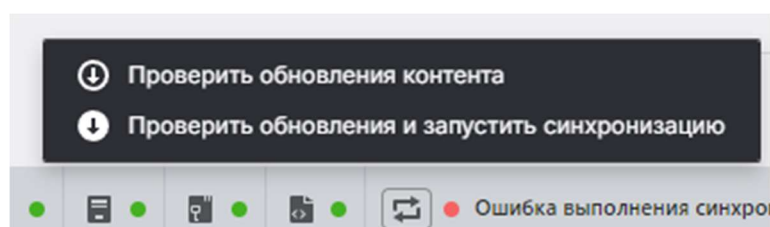
4.9 Смена лицензионного ключа

Откройте консоль управления RedCheck, авторизовавшись под учетной записью с ролью RedCheck_Admins → **Справка** → **Сменить лицензионный ключ** → введите новый лицензионный ключ → **ОК**;



Онлайн смена лицензионного ключа

Нажмите на статусной панели кнопку синхронизации → **Проверить обновления и запустить синхронизацию**;



Смена ключа и его активация осуществляется после завершения синхронизации.

Офлайн смена лицензионного ключа

В случае, если на устройстве нет доступа к сети Интернет, необходимо получить лицензионный файл.

Шаг 1. Сгенерируйте код активации командой:

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

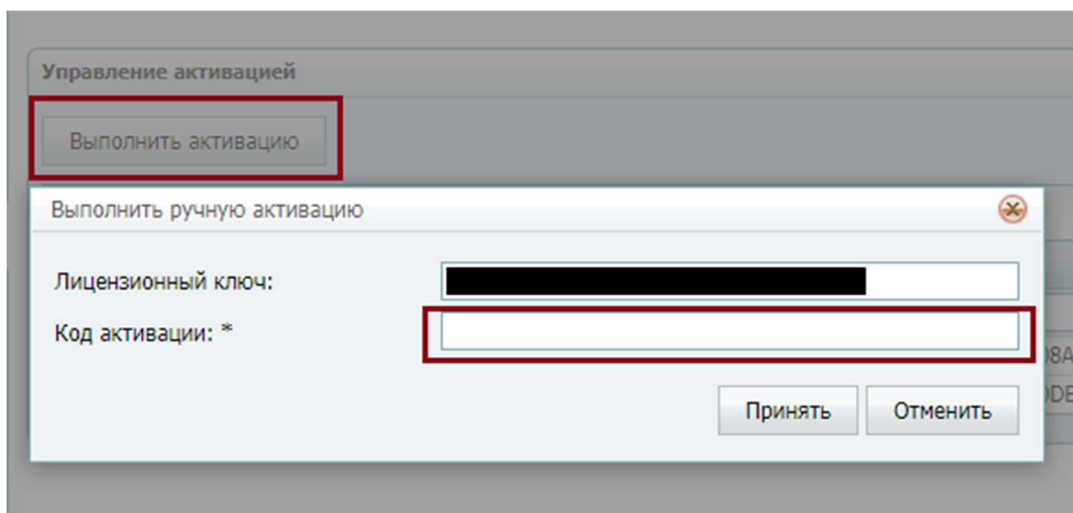
```
Добро пожаловать в мастер конфигурации RedCheck
=====
красный - критичное сообщение либо ошибка выполнения команды
желтый  - важное замечание требующее действия от пользователя
зеленый - успешное выполнение команды либо статус выполнения конфигурации
[*] - диапазон допустимых значений
(*) - значение по умолчанию
=====
Доступные действия:
[1] : Обновить структуру БД
[2] : Получение кода активации
[3] : Настройка RedCheck-Api
[4] : Настройка RedCheck-Client
[5] : Настройка RedCheck-Scan-Service
[6] : Настройка RedCheck-Sync-Service
[7] : Настройка RedCheck-Cleanup-Service
[8] : Настроить все сразу
[9] : Выход
Выберите действие [1-9]: |
```

Выберите пункт **Получение кода активации** и введите ключ лицензии:

```
=====
Получение кода активации
=====
Введите ключ лицензии:
Код активации: BEE856C323A62FABFB6307CC01BFECDF85B035FEA71185B9284F3C78255CE7DC
Окончание получения кода активации
=====
```

Шаг 2. Авторизуйтесь в [Центре сертифицированных обновлений](#) с помощью логина и пароля;

Логин/пароль поставляется всем коммерческим клиентам в [Формуляре, раздел 15, «Особые отметки»](#) (начиная с 18.05.2022).



Шаг 4. Нажмите **Скачать**;

	Активен	Дата активации	Действия
	False	10.12.2021 09:54:44	Скачать
	True	24.09.2020 11:09:35	Скачать

Шаг 5. Сохраните файл **license.xml** в директорию для офлайн синхронизации (по умолчанию **/var/opt/redcheck-sync-service/data**);

Если файл был сохранен в директорию по умолчанию, измените владельца на пользователя redcheck, чтобы служба синхронизации могла удалить данный файл в дальнейшем:

Bash (оболочка Unix)

```
sudo chown redcheck:redcheck /var/opt/redcheck-sync-service/data/license.xml
```

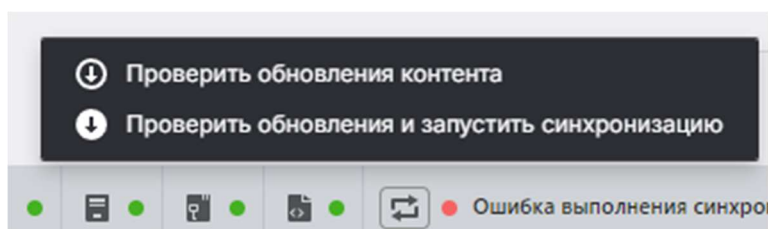
Директория может находиться в произвольном месте в инфраструктуре сети и должна быть доступна для чтения хостом, на котором установлена служба синхронизации. В случае сетевой папки указывается учетная запись RedCheck, пользователь которой имеет разрешение на чтение.

Шаг 6. На панели навигации выберите **Инструменты**

→ **Настройки** → **Синхронизация**:

- Выберите **Офлайн** и отметьте **Запускать по расписанию**, указав по необходимости время;
- Укажите путь, куда был сохранен файл лицензии;
- Выберите ранее созданную учетную запись (если указывается сетевая папка);

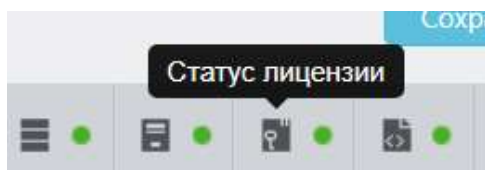
Шаг 7. Нажмите на статусной панели кнопку синхронизации → **Проверить обновления и запустить синхронизацию**;



Смена ключа и его активация осуществляется после завершения синхронизации.

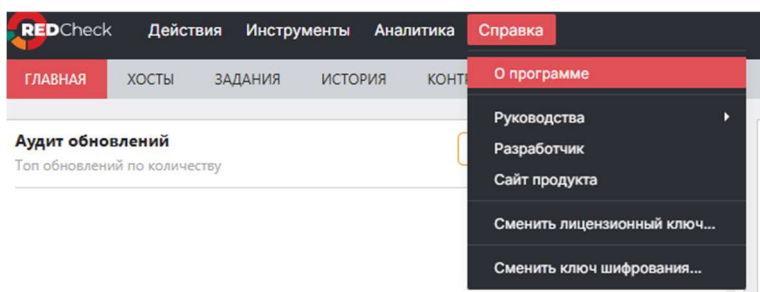
4.10 Офлайн активация лицензии

Статус лицензии отображается на статусной панели:



В случае отсутствия доступа к сети Интернет активация лицензии осуществляется посредством файла лицензии license.xml.

Шаг 1. На панели навигации выберите **Справка** → **О программе**:



Скопируйте код активации в соответствующей строке таблицы;

Средство анализа защищённости RedCheck	
Сведения о программе	
Параметр	Значение
Версия программы	[REDACTED]
Версия сервера	[REDACTED]
Версия REST	0.3
Версия базы данных	266
Версия контента	CVEFULL:1.10.5.9 NIXCOMPL:1.10.5.9 GLA:1.10.5.9 WINCOMPL:1.10.5.8
Уникальный ID программы	48660376-FB93-488F-A57B-0DD216E43211
Лицензионный ключ	[REDACTED]
Код активации	<u>BED340FA43C07EE1983217D3FDC482D4C216B24E6B1E8EDAD58C42186CB114B5</u>



Код активации также можно получить во время установки ([Конфигурация RedCheck](#)).

Шаг 2. Авторизуйтесь в [Центре сертифицированных обновлений](#) с помощью логина и пароля;

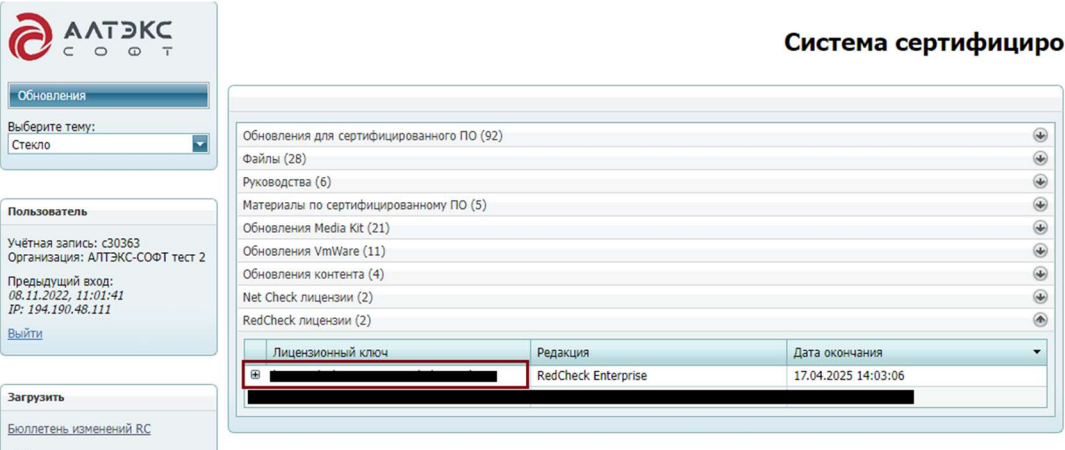
Логин/пароль поставляется всем коммерческим клиентам в разделе 15, «Особые отметки» (начиная с 18.05.2022).

Центр сертифицированных обновлений

Для получения обновлений необходимо выбрать способ входа

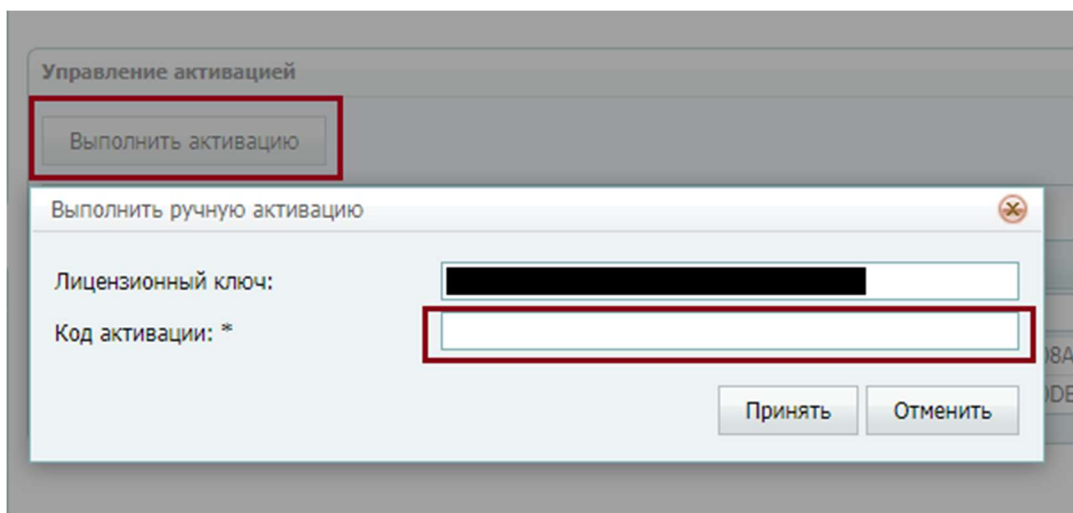
	Логин и пароль Пользовательские данные
	eToken Электронный USB-ключ

Шаг 3. Раскройте **RedCheck лицензии** → выберите нужный ключ RedCheck;



Лицензионный ключ	Редакция	Дата окончания
[Redacted]	RedCheck Enterprise	17.04.2025 14:03:06

Нажмите **Выполнить активацию** → введите ранее скопированный код активации → **Принять**;



Шаг 4. Нажмите **Скачать**;

	Активен	Дата активации	Действия
	False	10.12.2021 09:54:44	Скачать
	True	24.09.2020 11:09:35	Скачать

Шаг 5. Сохраните файл **license.xml** в директорию для офлайн синхронизации (по умолчанию **/var/opt/redcheck-sync-service/data**);

Если файл был сохранен в директорию по умолчанию, измените владельца на пользователя redcheck, чтобы служба синхронизации могла удалить данный файл в дальнейшем:

Bash (оболочка Unix)

```
sudo chown redcheck:redcheck /var/opt/redcheck-sync-service/data/license.xml
```

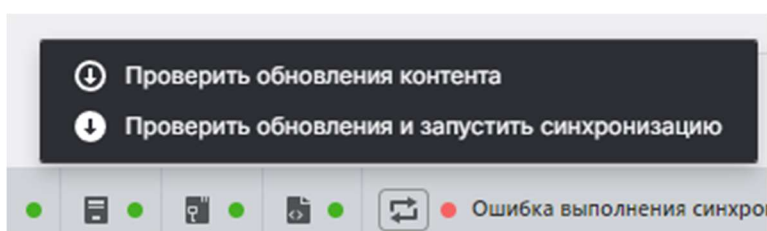
Директория может находиться в произвольном месте в инфраструктуре сети и должна быть доступна для чтения хостом, на котором установлена служба синхронизации. В случае сетевой папки указывается учетная запись RedCheck, пользователь которой имеет разрешение на чтение.

Шаг 6. На панели навигации выберите **Инструменты**

→ **Настройки** → **Синхронизация**:

- Выберите **Офлайн** и отметьте **Запускать по расписанию**, указав по необходимости время;
- Укажите путь, куда был сохранен файл лицензии;
- Выберите ранее созданную учетную запись (если указывается путь к сетевой папке);

Шаг 7. Нажмите на статусной панели кнопку синхронизации → **Проверить обновления и запустить синхронизацию**;



Активация лицензии осуществляется после завершения синхронизации.

После завершения процесса синхронизации директория с контентом будет очищена. Не рекомендуется хранить в ней важные файлы.

Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.



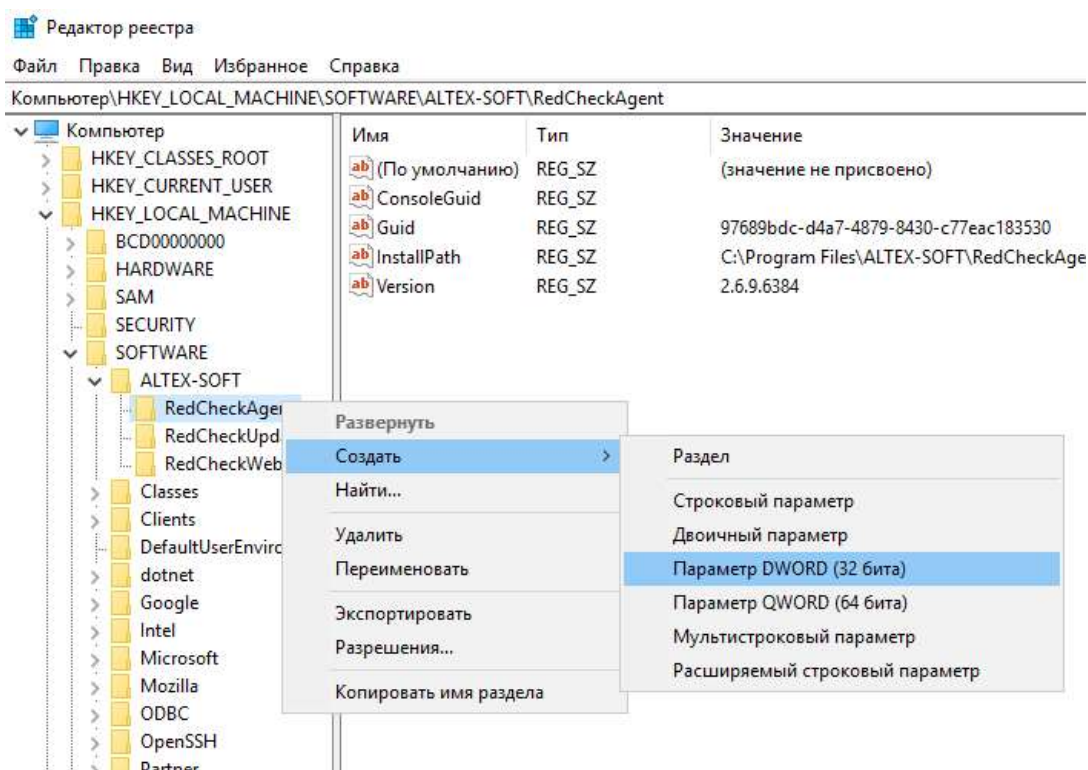
4.11 Изменение порта для Агента сканирования

Стандартный порт Агента **TCP/IP 8732**.

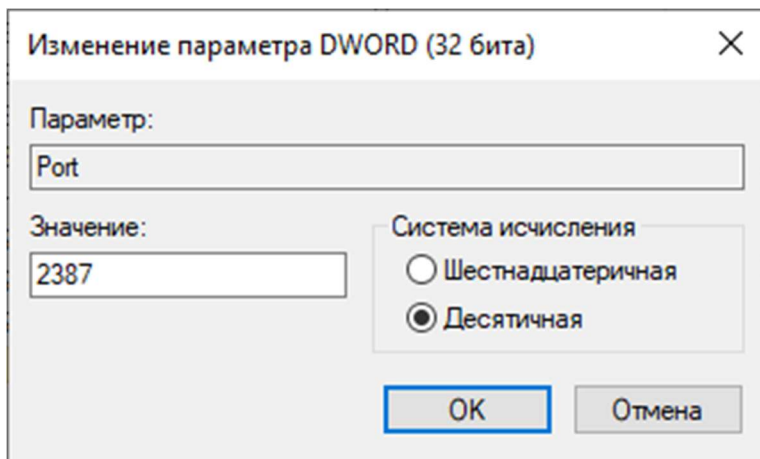
Шаг 1. Зайдите в реестр хоста с установленным агентом и создайте новый параметр **DWORD** с именем **Port**;

Для x-86 разрядных систем: **HKEY_LOCAL_MACHINE\ SOFTWARE\ Wow6432Node\ ALTEX-SOFT\ RedCheckAgent\ Port (DWORD)**

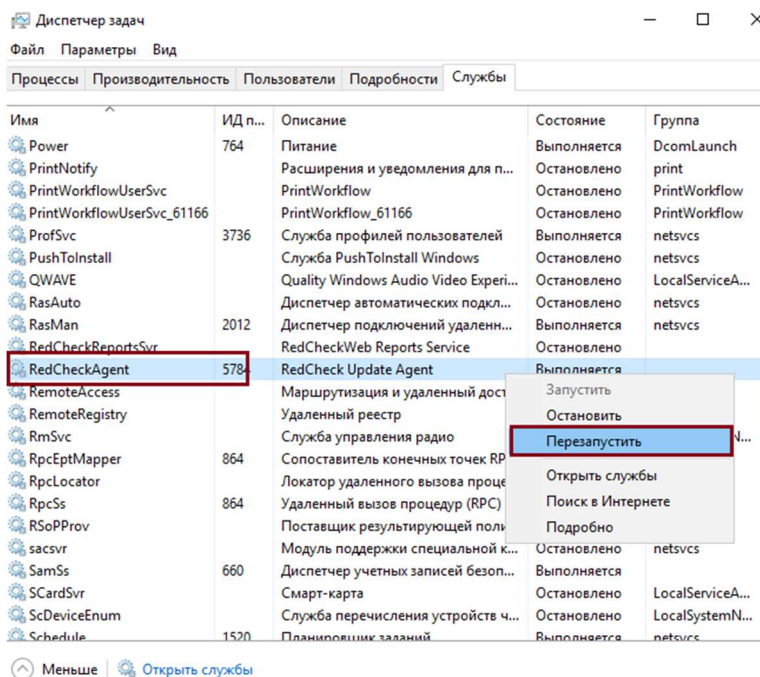
Для x-64 разрядных систем: **HKEY_LOCAL_MACHINE\ SOFTWARE\ ALTEX-SOFT\ RedCheckAgent\ Port (DWORD)**



Присвойте ему необходимое значение → **ОК**;



Шаг 2. Нажмите **Ctrl + Alt + Delete** → **Диспетчер задач**. Перейдите в **Службы** → ПКМ по **RedCheckAgent** → **Перезапустить**;

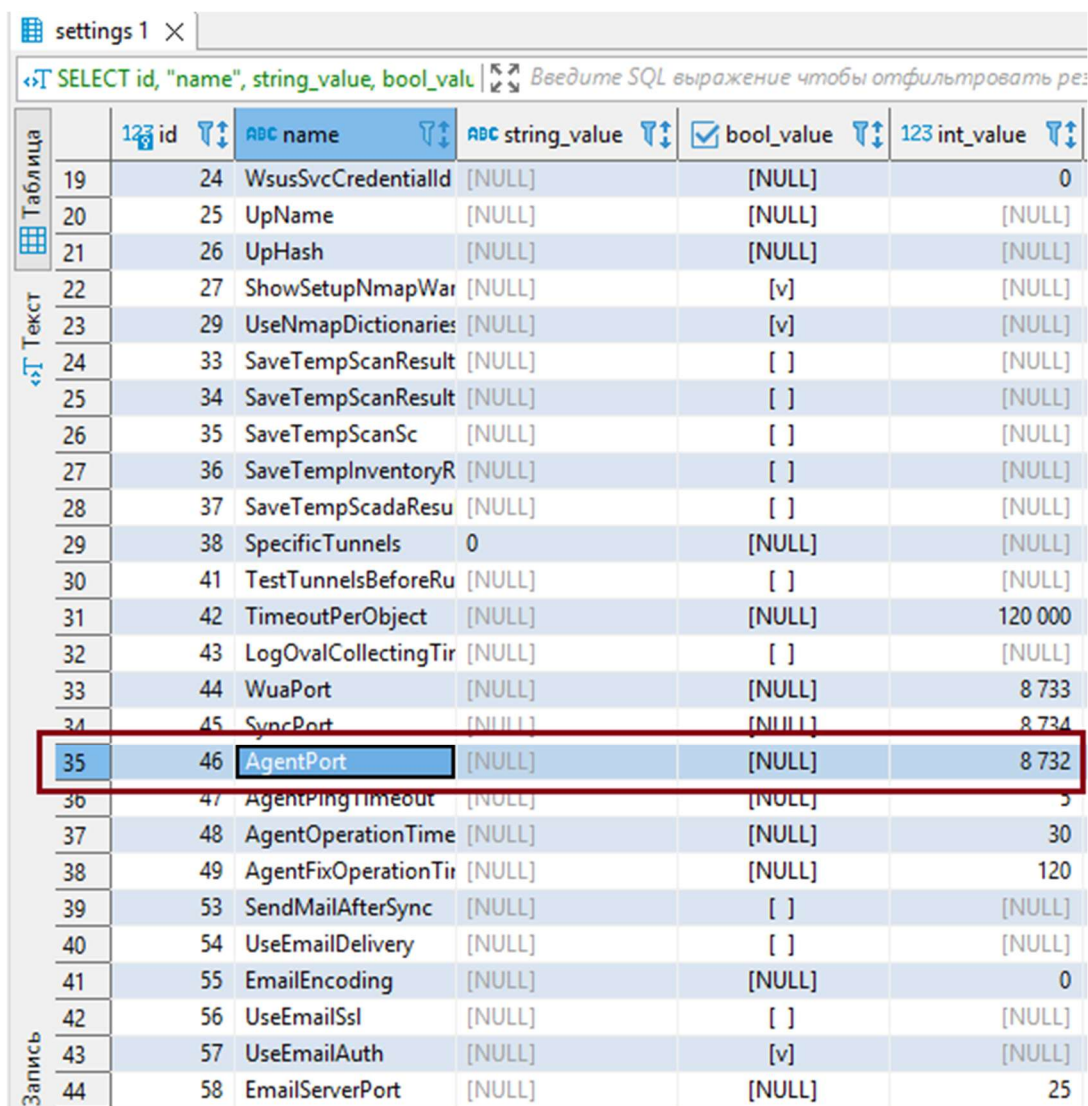


Для сканирования сегмента сети, в которой для Агента установлен альтернативный порт, используется учетная запись RedCheck с указанием переопределенного порта по умолчанию.

Изменение порта по умолчанию

Порт по умолчанию используется для сканирования в тех случаях, когда не указано альтернативное значение в УЗ RedCheck.

Шаг 1. В БД RedCheck найдите таблицу **settings** → в столбце **name** найдите поле **AgentPort** и внесите новое значение порта;



	123 id	ABC name	ABC string_value	<input checked="" type="checkbox"/> bool_value	123 int_value
19	24	WsusSvcCredentialId	[NULL]	[NULL]	0
20	25	UpName	[NULL]	[NULL]	[NULL]
21	26	UpHash	[NULL]	[NULL]	[NULL]
22	27	ShowSetupNmapWar	[NULL]	[v]	[NULL]
23	29	UseNmapDictionaries	[NULL]	[v]	[NULL]
24	33	SaveTempScanResult	[NULL]	[]	[NULL]
25	34	SaveTempScanResult	[NULL]	[]	[NULL]
26	35	SaveTempScanSc	[NULL]	[]	[NULL]
27	36	SaveTempInventoryR	[NULL]	[]	[NULL]
28	37	SaveTempScadaResu	[NULL]	[]	[NULL]
29	38	SpecificTunnels	0	[NULL]	[NULL]
30	41	TestTunnelsBeforeRu	[NULL]	[]	[NULL]
31	42	TimeoutPerObject	[NULL]	[NULL]	120 000
32	43	LogOvalCollectingTir	[NULL]	[]	[NULL]
33	44	WuaPort	[NULL]	[NULL]	8 733
34	45	SyncPort	[NULL]	[NULL]	8 734
35	46	AgentPort	[NULL]	[NULL]	8 732
36	47	AgentPingTimeout	[NULL]	[NULL]	5
37	48	AgentOperationTime	[NULL]	[NULL]	30
38	49	AgentFixOperationTir	[NULL]	[NULL]	120
39	53	SendMailAfterSync	[NULL]	[]	[NULL]
40	54	UseEmailDelivery	[NULL]	[]	[NULL]
41	55	EmailEncoding	[NULL]	[NULL]	0
42	56	UseEmailSsl	[NULL]	[]	[NULL]
43	57	UseEmailAuth	[NULL]	[v]	[NULL]
44	58	EmailServerPort	[NULL]	[NULL]	25

Шаг 2. Нажмите **Ctrl + Alt + Delete** → **Диспетчер задач**. Перейдите в **Службы** → ПКМ по **RedCheckAgent** → **Перезапустить**;

Диспетчер задач

Файл Параметры Вид

Процессы Производительность Пользователи Подробности **Службы**

Имя	ИД п...	Описание	Состояние	Группа
Power	764	Питание	Выполняется	DcomLaunch
PrintNotify		Расширения и уведомления для п...	Остановлено	print
PrintWorkflowUserSvc		PrintWorkflow	Остановлено	PrintWorkflow
PrintWorkflowUserSvc_61166		PrintWorkflow_61166	Остановлено	PrintWorkflow
ProfSvc	3736	Служба профилей пользователей	Выполняется	netsvcs
PushToInstall		Служба PushToInstall Windows	Остановлено	netsvcs
QWAVE		Quality Windows Audio Video Experi...	Остановлено	LocalServiceA...
RasAuto		Диспетчер автоматических подкл...	Остановлено	netsvcs
RasMan	2012	Диспетчер подключений удаленн...	Выполняется	netsvcs
RedCheckReportsSvr		RedCheckWeb Reports Service	Остановлено	
RedCheckAgent	578	RedCheck Update Agent	Выполняется	
RemoteAccess		Маршрутизация и удаленный дост	Запустить	
RemoteRegistry		Удаленный реестр	Остановить	
RmSvc		Служба управления радио	Перезапустить	N...
RpcEptMapper	864	Сопоставитель конечных точек RP		
RpcLocator		Локатор удаленного вызова проце	Открыть службы	
RpcSs	864	Удаленный вызов процедур (RPC)	Поиск в Интернете	
RSoPProv		Поставщик результирующей поли	Подробнее	
sacsvr		Модуль поддержки специальной к...	Остановлено	netsvcs
SamSs	660	Диспетчер учетных записей безоп...	Выполняется	
SCardSvr		Смарт-карта	Остановлено	LocalServiceA...
ScDeviceEnum		Служба перечисления устройств ч...	Остановлено	LocalSystemN...
Schedule	1520	Планировщик заданий	Выполняется	netsvcs

Меньше | Открыть службы

4.12 Журнал событий (логи)

При возникновении ошибок во время сканирования технической поддержке может понадобиться файл с логами работы служб Системы. RedCheck позволяет сохранять два типа логов: обычные и расширенные. По умолчанию расширенные логи отключены.

Параметры логов:

- На каждую уникальную дату (день) будет создан новый файл логов;
- Глубина хранения логов составляет 1 год;
- Архивирование текущего файла логов происходит каждый день;
- Объем логов не превышает 100 Мб

Обычные логи располагаются в каталогах `/var/opt`

- `/redcheck-api/log` – серверный компонент;
- `/redcheck-api/reports-export/log` – служба отчетов;
- `/redcheck-scan-service/log` – служба сканирования;
- `/redcheck-sync-service/log` – служба синхронизации;
- `/redcheck-client/log` – консоль управления;
- `C:\ProgramData\ALTEX-SOFT\RedCheck\Logs\Agent` – агент сканирования;

Расширенные логи

Расширенные логи находятся в каталоге `/var/opt/redcheck-scan-service/jobs/exec_id/host_name/uuid_directory/*.xml`

- `exec_id` – **История** → столбец **E**, обозначающий итерацию выполнения задания;
- `host_name` – IP-адрес или DNS-имя хоста;
- `uuid_directory` – уникальное имя каталога, в котором находятся логи.

Пример и формат записи в журнале

2024-05-16 17:23:56.3938|INFO|Check.R.Rest.Api.Startup|Application start

ГГГГ-ММ-ДД ЧЧ:ММ:СС.МССС|Уровень|Модуль|Сообщение, где

- **ГГГГ** – год в формате четырех цифр;
- **ММ** – месяц в формате двух цифр;
- **ДД** – день в формате двух цифр;
- **ЧЧ** – час в 24-часовом формате;
- **ММ** – минута в 60-минутном формате;
- **СС** – секунда в 60-секундном формате;
- **МССС** – микросекунда в формате четырех цифр;
- **Уровень** – уровень информационного сообщения;
- **Модуль** – наименование модуля службы;
- **Сообщение** – выполняемая команда или информационное сообщение

4.12.1 Примеры регистрации событий

Регистрация событий входа и выхода пользователей (консоль управления)

Событие входа пользователя имеет тип [Authorization], каждое событие имеет дату и время в формате ГГГГ-ММ-ДД ЧЧ:ММ:СС.МССС, в разделе сообщения указывается результат события, в качестве объекта указывается используемая учетная запись:

```
2024-04-02 12:58:16.3963|INFO|altxLogger|[Authorization]|JWT|admin |Successful authorization
```

Событие выхода пользователя имеет тип [Signout], каждое событие имеет дату и время в формате ГГГГ-ММ-ДД ЧЧ:ММ:СС.МССС, в разделе сообщения указывается результат события, в качестве объекта указывается используемая учетная запись

```
2024-04-02 13:15:25.5691|INFO|altxLogger|[Signout]|admin |Successful signout
```

Неудачный вход

```
[2025-03-31 16:47:12.7726 INF] [altxLogger] [Authentication]|JWT|admin 192.168.100.26|Unsuccessful authentication|Wrong username or password
```

Регистрация событий входа и выхода пользователей (серверный компонент)

Удачный вход

```
[2025-03-31 16:41:07.2587 INF] [Check.R.Rest.Api.v1._0.ApiEndpoints.Accounts.CreateBearerToken] [Authentication] Successful authentication | User <name>
```

Неудачный вход

[2025-03-31 16:47:12.7552 INF]

[Check.R.Rest.Api.v1._0.ApiEndpoints.Accounts.CreateBearerToken] [Authentication]
Unsuccessful authentication | No local users | User <name>

Регистрация событий запуска заданий сканирования (журнал службы сканирования)

[2024-04-01 12:12:37.3401 INF]

[RedCheck.Services.Scan.ServerContext.Commands.RunOrResumeLegacyJobCommandDbFinder] [Thread 9] Job 10 with status NeedToRun found. Call "Run" command

Регистрация событий управления учетными записями (консоль управления)

Создание УЗ

2024-05-17 12:11:51.6189|INFO|altxLogger|[RedCheckWebClient Actions]|admin|User has been successfully created: New_user

Редактирование УЗ

2024-05-17 17:01:23.8986|INFO|altxLogger|[RedCheckWebClient Actions]|admin|User has been successfully edited: New_user

Удаление УЗ

2024-05-17 17:12:42.6000|INFO|altxLogger|[RedCheckWebClient Actions]|admin|User has been successfully deleted: 4

Регистрация событий управления учетными записями (серверный компонент)

Создание УЗ

2024-05-17 17:01:23.8715|INFO|ResponseTimeMiddleware||Request POST
http://astra-rc-rests:444/api/v1.0/accounts starting

Редактирование УЗ

2024-05-17 17:01:23.8715|INFO|ResponseTimeMiddleware|Request PUT http://astra-rc-rests:444/api/v1.0/accounts/4 starting

Удаление УЗ

2024-05-17 17:12:42.5992|INFO|ResponseTimeMiddleware|admin|Request DELETE http://astra-rc-rests:444/api/v1.0/accounts/4 finished in 67ms Status 200

Регистрация событий изменения настроек RedCheck

Консоль управления

[2025-03-31 17:08:05.1020 INF] [altxLogger] [RedCheckWebClient Api]|admin|http://192.168.100.26:51000/api/v0.3/settings/0|HttpMethod.Patch|HttpStatusCode.OK

Серверный компонент

[2025-03-31 17:08:05.1018 INF] [ResponseTimeMiddleware] admin|Request PATCH http://192.168.100.26:51000/api/v0.3/settings/0 finished in 16ms Status 200

Регистрация ошибочных событий

[2025-03-31 16:36:13.8770 ERR] [Microsoft.EntityFrameworkCore.Query] <Описание ошибки>

4.12.2 Настройка логирования компонентов RedCheck

В системе предусмотрена возможность изменения каталогов, времени хранения и уровня логирования журналов системных служб RedCheck, с возможностью отправки по syslog.

Для этого необходимо перейти в панель **Инструменты** →

Настройки → **Логирование**;

Компонент	Тип	Путь хранения файловых логов	Общий мин. уровень логирования	Время хранения файловых логов в днях	Сервер Syslog	Мин. уровень логирования для Syslog
API	API	/var/opt/redcheck-api/log	Info	365		
rc-scan-01	Служба сканирования	/var/opt/redcheck-scan-service/log	Info	365		
rc-scan-2	Служба сканирования	/var/opt/redcheck-scan-service/log	Info	365		
rc-scan2	Служба сканирования	/var/opt/redcheck-scan-service/log	Info	365		
SyncService	Служба синхронизации	/var/opt/redcheck-sync-service/log	Info	365		
WebClient	WEB клиент	/var/opt/redcheck-client/log	Info	365		

Всего: 6 Страница 1 из 1

Для для выбранной системной службы предусмотрено изменение следующих параметров:

- Каталог хранения файлов логов;
- Уровень логирования;
- Время хранения логов в днях;
- Сервер Syslog;
- Порт Syslog;
- Минимальный уровень логирования по Syslog.

Выбранный компонент	
Путь хранения файловых логов	<input type="text" value="/var/opt/redcheck-api/log"/>
Общий мин. уровень логирования	Info
Время хранения файловых логов в днях	<input type="text" value="365"/>
Сервер Syslog	<input type="text"/>
Порт Syslog	<input type="text"/>
Мин. уровень логирования для Syslog	
<input type="checkbox"/> Применить настройки для всех служб сканирования	

По умолчанию рекомендуется использовать уровень **info** для отслеживания событий безопасности.

Также есть возможность вручную настроить отправку логов по syslog.

Шаг 1. Добавьте в конфигурационный файл `/var/opt/redcheck-api/conf/nlog.config` новый target (внутри тега targets):

XML

```
<target xsi:type="Network" name="syslog"
  layout="${message}"
  onOverflow="Split"
  newLine="false"
  lineEnding="None"
  maxMessagesSize="65000"
  encoding="utf-8"
  connectionCacheSize="5"
  maxConnections="0"
  maxQueueSize="0"
  keepConnection="true"
  onConnectionOverflow="AllowNewConnection"
  address="udp://address:port" />
```

Укажите в параметре **address** IP и порт syslog сервера.

Шаг 2. Добавьте rule (внутри тега rules):

XML

```
<logger name="*" minLevel="Info" writeTo="syslog" />
```

Можно повысить минимальный уровень логирования:

- Info – отслеживание выполнения всех запросов;
- Warn – потенциально опасные события, которые могут привести к ошибкам;
- Error – сообщения об ошибках;
- Fatal – критические ошибки.

Рекомендуется использовать уровень Info для отслеживания событий безопасности.

4.13 Настройка сервиса доставки отчетов

Возможна доставка отчетов через комплексы однонаправленной передачи данных InfoDiode из защищаемого сегмента в иные сетевые сегменты.

- [Информационная справка](#)
- [Сайт производителя](#)

Инструкция по настройке предоставляется производителем по запросу или в составе эксплуатационной документации.

Шаг 1. Откройте консоль управления RedCheck, авторизовавшись под учетной записью с ролью RedCheck_Admins / RedCheck_Systems
→ **Инструменты** → **Настройки** → перейдите в **Доставка** → в разделе **Настройка сервиса доставки на электронную почту** отметьте **Включить сервис доставки**;

Настройка сервиса доставки на электронную почту

Включить сервис доставки

Адрес сервера исходящих сообщений

Порт: 25

Безопасность подключения: Автоопределение

Сертификат сервера

Аутентификация

Логин

Пароль

E-mail отправителя

Кодировка писем: UTF8

Шаблон уведомления

Задание: {JobScanType} ({JobId}) завершено.
Название: {JobName}
Описание: {JobDescription}
Начало сканирования: {JobStartTime}
Хостов в задании: {JobTargetsCount}
Успешно просканированных: {JobSuccessfullyScannedTargetsCount}
#TARGET#

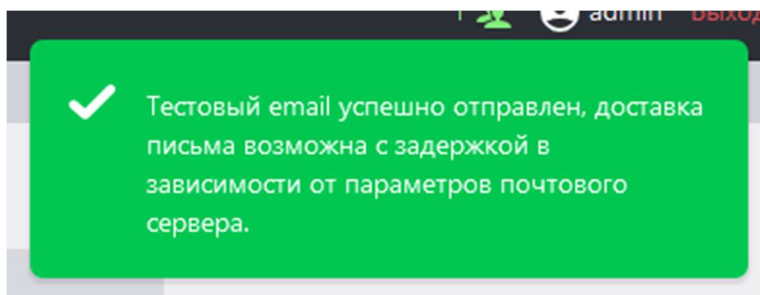
Хост: {TargetName} | Статус: {TargetScanResult}
#SECURITY# {JobSecurityCount} | Средний: {MediumSecurityCount} | Низкий: {LowSecurityCount} #ENDSECURITY#

Установить шаблон по умолчанию

E-mail получателей для отправки тестового письма

Отправить тестовое письмо

Шаг 2. Укажите необходимые данные для отправки писем → нажмите **Отправить тестовое письмо** для проверки;



Шаг 3. Чтобы добавить email, нажмите **Добавить адрес доставки**;

The screenshot shows the "ДОСТАВКА" (Delivery) section of the RedCheck interface. On the left is a sidebar with menu items: "АЛТХМАР", "ДОСТАВКА" (highlighted in red), "ДОПОЛНИТЕЛЬНО", and "СИНХРОНИЗАЦИЯ". The main content area has a header "RedCheck может доставлять на сетевые ресурсы или на электронную почту данные о сканирова" and a sub-header "Адреса доставки отчетов (сетевые ресурсы и адреса электронной почты)". Below this is a table with columns: "ID", "Тип" (with a dropdown arrow), "Путь/Адрес", and "Учётная запись". The table is currently empty, with the text "Нет данных д" at the bottom right. At the bottom of the table area, there is a dropdown menu showing "20" and a button labeled "Добавить адрес доставки ...".

Шаг 4. Укажите **Тип** адреса доставки **Email** и адрес почты в поле **Путь/Адрес** → **Сохранить**;

The screenshot shows the "Новый адрес доставки (сетевой каталог или электронная почта)" form. The title is "Новый адрес доставки (сетевой каталог или электронная почта)". Below the title is the instruction: "Укажите требуемые параметры для нового или редактируемого адреса доставки." The form has three input fields: "Тип" (Type) with the value "Email", "Путь/Адрес" (Path/Address) with the value "some_address@mail.ru", and "Учётная запись" (Account name) which is empty. At the bottom of the form are two buttons: "Сохранить" (Save) and "Отмена" (Cancel).

Для отправки отчетов на почту после завершения задания необходимо создать [шаблон отчетов](#).

4.14 Исключения для средств защиты (САЗ, СЗИ)

Не рекомендуется устанавливать RedCheck на один сервер с другими средствами защиты в противном случае, могут быть внесены изменения в библиотеки среды функционирования, что нарушит работу RedCheck.

Общий перечень директорий и исполняемых файлов, подлежащих добавлению в списки исключений средств защиты, используемых в сети предприятия:

Список директорий установки	Исполняемый файл
Основные компоненты RedCheck	
Серверный компонент (RestAPI): /opt/redcheck-api	/redcheck-api /reports-export/redcheck-reports-export-service
Консоль управления: /opt/redcheck-client	/redcheck-web
Служба сканирования: /opt/redcheck-scan-service /opt/altxmap	/redcheck-scan-service /nmap /nping
Служба синхронизации: /opt/redcheck-sync-service	/redcheck-sync-service
Сервер обновлений:	/redcheck-update-server

/opt/redcheck-update-server	
Дополнительные компоненты (Windows-компоненты)	
<p>Сервер обновлений:</p> <p>C:\Program Files (x86)\ALTEX-SOFT\RedCheckUpdateServer</p>	\RcUpdSrv.exe
<p>Агент сканирования:</p> <p>C:\Program Files\ALTEX-SOFT\RedCheckAgent</p> <p>C:\Program Files (x86)\ALTEX-SOFT\RedCheckAgent</p>	\RedCheckAgent.exe

4.15 Настройка Windows-аутентификации (Kerberos)

RedCheck позволяет использовать доменные учетные записи для аутентификации в веб-консоли. Для корректной настройки необходимо выполнить следующие шаги:

Шаг 1. Установите необходимые пакеты;

Astra Linux / Debian

Bash (оболочка Unix)

```
sudo apt -y install realmd krb5-user sssd-tools sssd libnss-sss  
libpam-sss adcli
```

РЕД ОС / SberLinux

Bash (оболочка Unix)

```
sudo dnf -y install realmd krb5-workstation
```

Шаг 2. Выполните настройку времени;

Bash (оболочка Unix)

```
sudo timedatectl set-timezone Europe/Moscow
```

Шаг 3. Измените имя хоста, добавив к нему домен;

Bash (оболочка Unix)

```
sudo hostnamectl set-hostname name.domain.local
```

Bash (оболочка Unix)

```
sudo reboot
```

Шаг 4. Настройте сеть для доступа к DNS-серверу, который используется контроллером домена;

Astra Linux / Debian

Bash (оболочка Unix)

```
sudo nano /etc/resolv.conf
```

Свойства (файлы .properties)

```
search domain.local  
nameserver ip_dns_server
```

- search domain.local – укажите имя домена;
- nameserver ip_dns_server – укажите IP-адрес DNS-сервера;

РЕД ОС / SberLinux

Создайте файл ifcfg-[идентификатор интерфейса];

Bash (оболочка Unix)

```
sudo touch /etc/sysconfig/network-scripts/ifcfg-eth0
```

Bash (оболочка Unix)

```
PEERDNS=no  
DNS1=IP_address
```

Bash (оболочка Unix)

```
sudo systemctl restart NetworkManager
```

Шаг 5. Создайте директорию /etc/krb5.conf.d, если ее не существует;

Bash (оболочка Unix)

```
sudo mkdir /etc/krb5.conf.d
```

Шаг 6. Подключитесь к домену:

Указывайте имя домена заглавными буквами

Bash (оболочка Unix)

```
sudo realm join domain.local -U 'Admin@DOMAIN.LOCAL' -v
```

```
* Added the entries to the keytab: host/astra.k
* Added the entries to the keytab: RestrictedKr
* Added the entries to the keytab: RestrictedKr
* /usr/sbin/update-rc.d sssd enable
* Successfully enrolled machine in realm
root@astra:/home/redcheck-admin# _
```

После успешного выполнения команды в AD должна появиться запись компьютера.

Шаг 7. На контроллере домена в оснастке **Active Directory - пользователи и компьютеры** откройте свойства только что добавленного компьютера → **Делегирование** → выберите **Доверять компьютеру делегирование любых служб (только Kerberos)** → **ОК**;

Общие	Операционная система		Член
Делегирование	Размещение	Управляется	Входящи

Делегирование - это чувствительная к безопасности операция, которая позволяет службам работать от имени другого пользователя.

Не доверять компьютеру делегирование
 Доверять компьютеру делегирование любых служб (только Kerberos)
 Доверять компьютеру делегирование указанных служб

Использовать только Kerberos
 Использовать любой протокол проверки подлинности

Службы, с которыми эта учетная запись может использовать делегированные учетные данные:

Тип службы	Пользователь или ...	Порт	Имя служ

Развернуто
 Добавить...
Удалить

Шаг 8. Отредактируйте /etc/krb5.conf, указав DNS-имя KDC и контроллера домена:

Перед внесением изменений создайте резервную копию данного файла, скопировав его в пользовательскую директорию

Bash (оболочка Unix)

```
sudo nano /etc/krb5.conf
```

Bash (оболочка Unix)

```
[libdefaults]
    default_realm = DOMAIN.LOCAL

[realms]
    DOMAIN.LOCAL = {
        kdc = NAME.DOMAIN.LOCAL
        admin_server = NAME.DOMAIN.LOCAL
```

```
}
```

Секцию [domain_realm] оставьте пустой.

Шаг 9. Протестируйте выдачу kerberos-билета, используя имя доменного пользователя;

```
Bash (оболочка Unix)
```

```
kinit UserName@DOMAIN.LOCAL
```

```
Bash (оболочка Unix)
```

```
klist
```

```
Valid starting      Expires            Service principal
15.11.2024 10:36:50 15.11.2024 20:36:50 krbtgt/KERBEROS-AD.RU@KERBEROS-AD.RU
        renew until 22.11.2024 10:36:46
root@astra:/home/redcheck-admin#
```

```
Bash (оболочка Unix)
```

```
kdestroy
```

Далее необходимо создать Keytab файл одним из способов.

Создание Keytab файла на Linux (Способ 1)

Шаг 1. Создайте keytab-файл на машине с Linux. Для этого потребуется утилита ktutil:

```
Bash (оболочка Unix)
```

```
sudo ktutil
```

```
Bash (оболочка Unix)
```

```
read_kt /etc/krb5.keytab
```

Bash (оболочка Unix)

```
list -k -e
```

Получим примерно следующий вывод:

Bash (оболочка Unix)

```
slot KVNO Principal
-----
-----
 1      2 ASTRA$@DOMAIN.LOCAL (arcfour-hmac)
(0x28b528ce88fbale27fdcc3ff4cea627a)
 2      2 ASTRA$@DOMAIN.LOCAL (aes128-cts-hmac-sha1-96)
(0x540d98e5691950af3a480dbf1f1c7ac1)
 3      2 ASTRA$@DOMAIN.LOCAL (aes256-cts-hmac-sha1-96)
(0xe834b161f1cd1b18aa019f5acac6459accb58b36072c80d48755a0517a7c154f)
 4      2 host/ASTRA@DOMAIN.LOCAL (arcfour-hmac)
(0x28b528ce88fbale27fdcc3ff4cea627a)
 5      2 host/ASTRA@DOMAIN.LOCAL (aes128-cts-hmac-sha1-96)
(0x540d98e5691950af3a480dbf1f1c7ac1)
 6      2 host/ASTRA@DOMAIN.LOCAL (aes256-cts-hmac-sha1-96)
(0xe834b161f1cd1b18aa019f5acac6459accb58b36072c80d48755a0517a7c154f)
 7      2 host/astra.kerberos-ad.ru@DOMAIN.LOCAL (arcfour-hmac)
(0x28b528ce88fbale27fdcc3ff4cea627a)
 8      2 host/astra.kerberos-ad.ru@DOMAIN.LOCAL (aes128-cts-hmac-
sha1-96) (0x540d98e5691950af3a480dbf1f1c7ac1)
 9      2 host/astra.kerberos-ad.ru@DOMAIN.LOCAL (aes256-cts-hmac-
sha1-96)
(0xe834b161f1cd1b18aa019f5acac6459accb58b36072c80d48755a0517a7c154f)
10      2 RestrictedKrbHost/ASTRA@DOMAIN.LOCAL (arcfour-hmac)
(0x28b528ce88fbale27fdcc3ff4cea627a)
11      2 RestrictedKrbHost/ASTRA@DOMAIN.LOCAL (aes128-cts-hmac-sha1-
96) (0x540d98e5691950af3a480dbf1f1c7ac1)
12      2 RestrictedKrbHost/ASTRA@DOMAIN.LOCAL (aes256-cts-hmac-sha1-
96)
(0xe834b161f1cd1b18aa019f5acac6459accb58b36072c80d48755a0517a7c154f)
13      2 RestrictedKrbHost/astra.kerberos-ad.ru@DOMAIN.LOCAL
(arcfour-hmac) (0x28b528ce88fbale27fdcc3ff4cea627a)
14      2 RestrictedKrbHost/astra.kerberos-ad.ru@DOMAIN.LOCAL
(aes128-cts-hmac-sha1-96) (0x540d98e5691950af3a480dbf1f1c7ac1)
15      2 RestrictedKrbHost/astra.kerberos-ad.ru@DOMAIN.LOCAL
(aes256-cts-hmac-sha1-96)
(0xe834b161f1cd1b18aa019f5acac6459accb58b36072c80d48755a0517a7c154f)
```

Для создания дополнительного keytab-файла можно использовать ключ для AES256-SHA1 типа шифрования.

Bash (оболочка Unix)

```
3      2 ASTRA$@DOMAIN.LOCAL (aes256-cts-hmac-sha1-96)
(0xe834b161f1cd1b18aa019f5acac6459accb58b36072c80d48755a0517a7c154f)
```

Скопируйте значение ключа без **0x** из любой строки с выбранным типом шифрования (e834b161f1cd1b18aa019f5acac6459accb58b36072c80d48755a0517a7c154f)

Шаг 2. Выполните команды, не выходя из ktutil:

Bash (оболочка Unix)

```
add_entry -key -p HTTP/astra.domain.local@DOMAIN.LOCAL -k
значение_из_столбца_KVNO -e тип_шифрования
```

После чего укажите значение ключа без **0x**

Bash (оболочка Unix)

```
write_kt /etc/astra.HTTP.keytab
```

Bash (оболочка Unix)

```
sudo chown root:redcheck /etc/astra.HTTP.keytab
```

Bash (оболочка Unix)

```
sudo chmod g+r /etc/astra.HTTP.keytab
```

При необходимости можно посмотреть содержимое astra.HTTP.keytab

Bash (оболочка Unix)

```
sudo ktutil
```

Bash (оболочка Unix)

```
read_kt /etc/astra.HTTP.keytab
```

Bash (оболочка Unix)

```
list -k -e
```

Создание Keytab файла на контроллере домена (Способ 2)

Шаг 1. Выполните следующие команды в PowerShell:

Код

```
setspn -S HTTP/astra.domain.local ASTRA
```

Код

```
setspn -S HTTP/astra@DOMAIN.LOCAL ASTRA
```

astra.domain.local ASTRA – имя_компьютера.домен

ИМЯ_КОМПЬЮТЕРА_В_ДОМЕНЕ

astra@DOMAIN.LOCAL ASTRA –

имя_компьютера@ДОМЕН ИМЯ_КОМПЬЮТЕРА_В_ДОМЕНЕ

Шаг 2. Создайте keytab файл:

Код

```
ktpass -princ HTTP/astra.domain.local@DOMAIN.LOCAL -pass password -  
mapuser DOMAIN.LOCAL\ASTRA$ -pType KRB5_NT_PRINCIPAL -out  
c:\astra.HTTP.keytab -crypto AES256-SHA1
```

Шаг 3. Переместите этот файл на сервер, где установлен redcheck-арі, в директорию /etc/:

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/astra.HTTP.keytab /etc/
```

Шаг 4. Изменить права доступа для файла:

Bash (оболочка Unix)

```
sudo chown root:redcheck /etc/astra.HTTP.keytab
```

Bash (оболочка Unix)

```
sudo chmod g+r /etc/astra.HTTP.keytab
```

Продолжение настройки

Шаг 10. Добавьте переменную окружения в сервис redcheck-api:

Bash (оболочка Unix)

```
sudo nano /usr/lib/systemd/system/redcheck-api.service
```

Bash (оболочка Unix)

```
Environment=KRB5_KTNAME=/etc/astra.HTTP.keytab
```

```
[Service]
WorkingDirectory=/opt/redcheck-api
ExecStart=/opt/redcheck-api/redcheck-api
Restart=always
# Restart service after 10 seconds if the dotnet se
RestartSec=10
KillSignal=SIGINT
Environment=ASPNETCORE_ENVIRONMENT=Production
Environment=ASPNETCORE_URLS=http://localhost:5011
Environment=KRB5_KTNAME=~/.astra.HTTP.keytab
TimeoutStopSec=30
```

Шаг 11. Перезапустите redcheck-api:

Bash (оболочка Unix)

```
sudo systemctl daemon-reload
```

Bash (оболочка Unix)

```
sudo systemctl restart redcheck-api
```

Шаг 12. Переконфигурируйте redcheck на использование HTTPS-протокола и DNS-имени. Убедитесь, что в конфигурационном файле для redcheck-client в параметре RestUrl указано DNS-имя, например astra.domain.local.

Bash (оболочка Unix)

```
sudo redcheck-bootstrap
```

Bash (оболочка Unix)

```
sudo nano /var/opt/redcheck-client/conf/redcheck-web.dll.config
```

```
GNU nano 3.2 /var/opt/redcheck-client
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <appSettings>
    <add key="RestUrl" value="astra.domain.local" />
    <add key="RestPort" value="445" />
    <add key="RestApiVersion" value="0.3" />
    <add key="RestProtocol" value="https" />
    <add key="RestExtendedConnectionTimeout" value="100" />
    <add key="SessionTimeout" value="151" />
    <add key="CleanupServiceUrl" value="" />
  </appSettings>
</configuration>
```

Перезапустите redcheck-client;

Bash (оболочка Unix)

```
sudo systemctl restart redcheck-client
```

Шаг 13. Создайте пользователя для авторизации в RedCheck ([4.1 Настройка ролевой модели](#)):

- Тип аутентификации – Windows аутентификация
- Имя пользователя – name@DOMAIN.LOCAL

Добавить пользователя

Имя пользователя

Тип аутентификации

Роль пользователя

Для авторизации:

- Указывайте имя пользователя в формате **DOMAIN.LOCAL\name** или **name@DOMAIN.LOCAL**
- Отметьте **Использовать аутентификацию Windows**

REDCheck

Использовать аутентификацию Windows

© АО "АЛТЭКС-СОФТ"

4.16 Дополнительные настройки для сканирования

Откройте консоль управления → **Инструменты** → **Настройки** → **Сканирование**;

Параллельность сканирования

- Число параллельных заданий [1-5] – сколько заданий может выполняться одновременно. При увеличении значения увеличивается нагрузка на ЦП;
- Число параллельных сканирований в задании – сколько хостов будут сканироваться одновременно в рамках одного задания. Не рекомендуется указывать значение, превышающее количество логических ядер на хосте с установленной службой сканирования;
- Использовать кэш контента для ускорения сканирования – перед выполнением задания RedCheck единожды выгрузит нужный контент безопасности и сохранит его в базе данных. Это позволяет значительно ускорить сканирование;
- Хранить кэш в файловой системе – аналогично **Использовать кэш контента для ускорения сканирования**, но контент безопасности будет сохранен не в базе данных, а в файловой системе на хосте с установленной службой сканирования.

Настройки сканирования

Число параллельных заданий [1-5]

Число параллельных сканирований в задании

Использовать кэш контента для ускорения сканирования

Хранить кэш в файловой системе

Пути приложения

Рабочая папка службы сканирования – информация о директории, где находятся конфигурационные файлы службы сканирования.

Компонент ALTXmap

Если необходимо использовать собственные словари для Подбора паролей (опция в задании Аудит в режиме «Пентест»), снимите отметку с **Использовать встроенные словари** и укажите пути к файлам с расширением .lst

Компонент ALTXMAP	
	<input type="checkbox"/> Использовать встроенные словари
Путь к словарю логинов	<input type="text" value="/var/opt/altxmap/nselib/data/usernames.lst"/>
Путь к словарю паролей	<input type="text" value="/var/opt/altxmap/nselib/data/passwords.lst"/>

Системные настройки сканирования

- Таймаут проверки по умолчанию - максимальное время, которое сканер ждёт выполнения одной SCAP-проверки (контроль, правило, тест);
- Таймаут SSH сессии, мс. - максимальное время ожидания установления SSH-соединения с узлом;
- Таймаут ожидания данных после достижения таймаута SSH сессии, мс. - дополнительное «окно ожидания» данных после основного таймаута SSH. Используется для корректного закрытия сессии и получения запоздавших ответов;
- Задержка отправки keep-alive пакета, мс. - время ожидания перед первой отправкой keep-alive пакета в SSH-сессии. Нужно, чтобы сессия не закрывалась по таймауту на сетевых устройствах;
- Интервал отправки keep-alive пакета, мс. - периодичность отправки keep-alive пакетов в активной SSH-сессии. Поддерживает соединение «живым» при долгих проверках;
- Таймаут shell команды, мс. - максимальное время выполнения одной команды в shell. Если команда не завершилась — она прерывается;
- Таумаут shell ответа, мс. - максимальное время ожидания полного вывода команды. Актуально для команд с большим объёмом вывода (например, **display current-configuration**);
- Продолжительность ожидания порции данных shell ответа, мс. - интервал ожидания следующей части вывода команды. Используется для определения, что вывод завершён;

- Кодировка shell - кодировка, в которой сканер интерпретирует вывод команд. Важно для корректного разбора текста на сетевых устройствах;
- Количество колонок окна виртуального терминала - ширина виртуального терминала (TTY). Большое значение снижает перенос строк и упрощает парсинг вывода команд.

Системные настройки сканирования

Настройки по рекомендации техподдержки вендора

Настройки SCAP сканирования

Таймаут проверки по умолчанию

Настройки протокола SSH

Таймаут SSH сессии, мс

Таймаут ожидания данных после достижения таймаута SSH сессии, мс

Задержка отправки keep-alive пакета, мс

Интервал отправки keep-alive пакета, мс

Таймаут shell команды, мс

Таймаут shell ответа, мс

Продолжительность ожидания порции данных shell ответа, мс

Кодировка shell

Количество колонок окна виртуального терминала

4.17 Удаление RedCheck

Для удаления RedCheck выполните следующие команды:

Astra Linux / Debian

Удаление компонентов RedCheck:

Bash (оболочка Unix)

```
sudo apt remove redcheck-api redcheck-client redcheck-scan-service  
redcheck-sync-service redcheck-cleanup-service
```

Удаление всех библиотек ОС, которые необходимы для функционирования RedCheck:

Bash (оболочка Unix)

```
sudo apt autoremove
```

Удаление конфигурационных файлов:

Bash (оболочка Unix)

```
sudo apt purge altxmap redcheck-common redcheck-api redcheck-client  
redcheck-scan-service redcheck-sync-service redcheck-cleanup-service
```

РЕД ОС / SberLinux

Удаление компонентов RedCheck:

Bash (оболочка Unix)

```
sudo dnf remove redcheck-api redcheck-client redcheck-scan-service  
redcheck-sync-service redcheck-cleanup-service
```

Удаление всех библиотек ОС, которые необходимы для функционирования RedCheck:

Bash (оболочка Unix)

```
sudo dnf autoremove
```

Конфигурационные файлы удаляются автоматически.

5 Термины и сокращения

Термин	Определение
Администратор	Должностное лицо организации, участвующее в функционировании Системы и имеющее полные права ко всем функциям Системы
Гипервизор	ПО, которое дает базовому оборудованию хостов возможность автономного запуска и управления виртуальными машинами (имеющими права гостевых) изолированно от аппаратной части
Интернет	Информационно-телекоммуникационная сеть Интернет
Пользователь	Лицо, участвующее в функционировании Системы или использующее результаты её функционирования
Руководство	Руководство администратора
Хост	Любое устройство, которое подвергается сканированию Системой
Сокращение	Расшифровка
АО «АЛТЭК-СОФТ»	Организация-разработчик Системы
АСУ ТП	Автоматизированная система управления технологическими процессами
БД	База данных
ИБ	Информационная безопасность
ИС	Информационная система
ОС	Операционная система
ПО	Программное обеспечение
Репозиторий	БД определений проблем безопасности

OVALdb	
СЗИ	Средства защиты информации
Система	Программное средство анализа защищенности RedCheck
СУБД	Система управления базами данных
УЗ	Учётная запись
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
CPE	Common Platform Enumeration – перечисление общих платформ. Структурированная схема именования систем, ПО и пакетов информационных технологий. Включает в себя формальный формат имени, метод проверки имен в системе и формат описания для привязки текста и тестов к имени
CSV	Импорт хостов из CSV-файла
CVSS	Common Vulnerability Scoring System – общая оценка уязвимостей. Открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы, обычно с целью принять ее приоритет
DMZ	DeMilitarized Zone – демилитаризованная зона, ДМЗ. Сегмент сети, содержащий и предоставляющий организации общедоступные сервисы, а также отделяющих их от остальных участков локальной сети, что позволяет обеспечить внутреннему информационному пространству дополнительную защиту от внешних атак
DNS	Domain Name System – система доменных имен. Технология, которая отвечает за хранение и обработку информации о доменных адресах. Инструмент используется для преобразования доменных имен в IP-адреса в момент отправки пользователем запроса на сервер
FQDN	Full Qualified Domain Name – полностью определенное имя домена. Доменное имя, однозначно определяющее узел в сети

	Интернет. Включает в себя имена всех родительских доменов
HTML	HyperText Markup Language – язык разметки гипертекста. Стандартизированный язык разметки Web-страниц
IP	Internet Protocol – «Интернет-протокол». Набор правил, регулирующих формат данных, отправляемых через интернет или локальную сеть
IP-адрес	Уникальный адрес, идентифицирующее устройство в интернете или локальной сети
Kubernetes	Портативная расширяемая платформа с открытым исходным кодом для управления контейнеризованными рабочими нагрузками и сервисами
PDF	Portable Document Format – межплатформенный открытый формат электронных документов
SCAP	Security Content Automation Protocol – протокол автоматизации управления данными безопасности. Набор открытых стандартов, определяющих технические спецификации для представления и обмена данными безопасности
SSH	Secure Shell – «безопасная оболочка». Сетевой протокол для удаленного управления операционной системой с помощью командной строки и передачи данных в зашифрованном виде
TCP	Transmission Control Protocol/Internet Protocol – протокол передачи данных в сети Интернет
UUID	Universally Unique identifier – универсальный уникальный идентификатор. Уникальный идентификатор, сгенерированный машиной в определенном диапазоне
VMware	Технология виртуализации сервера, созданная для консолидации серверов уровня предприятия, организации их непрерывной работы, а также для разработчиков. Виртуализация требуется для того, чтобы разделить сервер на множество изолированных друг от друга виртуальных выделенных серверов

XML	eXtensible Markup Language – расширяемый язык разметки
-----	--