RedCheck

СРЕДСТВО АНАЛИЗА ЗАЩИЩЕННОСТИ

Руководство администратора

АЛМЮ.501410.RC02-01.PA

Версия документа 2.8.0.ru

ALTEX SOFT

Содержание

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).

Что нового в RedCheck Nix 2.8.0 для администратора

- Добавлена поддержка Windows аутентификации по протоколу Kerberos
- Улучшена служба очистки
- Улучшена настройка синхронизации контента безопасности
- Добавлена поддержка собственных схем и табличных пространств базы данных

Данное Руководство состоит из следующих разделов:

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

RedCheck NIX на данный момент имеет несколько ограничений:

- отсутствует возможность выполнения задания Аудит уязвимостей образов Docker.

Отсутствующий функционал находится в разработке и появится в следующих версиях.

Содержание

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.

RedCheck внесен в государственный реестр системы сертификации средств защиты информации по требованиям безопасности информации и имеет сертификат соответствия № 3172 от 23.06.2014.

RedCheck внесен в Единый реестр российских программ для электронных вычислительных машин и баз данных, номер в реестре – 765

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 3172

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
23 июня 2014 г.

Выдан: 23 июня 2014 г.
Действителен до: 23 июня 2020 г.
Срок действия продлён до: 23 июня 2025 г.

Настоящий сертификат удостоверяет, что **средство анализа защищенности RedCheck**, разработанное и производимое АО «АЛТЭКС-СОФТ», является средством контроля (анализа) защищенности информации, не содержащей сведений, составляющих государственную тайну, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018) - по 4 уровню доверия и технических условиях ТУ АЛМЮ.501410.RC02-01 при выполнении указаний по эксплуатации, приведенных в формуляре АЛМЮ.501410. RC02-01.30.

Сертификат выдан на основании технического заключения от 10.03.2014, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО «ЦБИ» (аттестат аккредитации от 11.04.2016 № СЗИ RU.0001.01БИ00.Б004), экспертного заключения от 19.05.2014, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002), технических заключений от 25.05.2017, 13.09.2018 и 30.09.2020, оформленных по результатам испытаний испытательной лабораторией ООО «ЦБИ», и экспертного заключения от 17.11.2020, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России».

Заявитель: АО «АЛТЭКС-СОФТ»
Адрес: 141067, Московская обл., г. Королев, мкр-н Болшево, ул. Маяковского, д. 10А, пом. VII
Телефон: (495) 543-3101

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

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://ovaldbru.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).

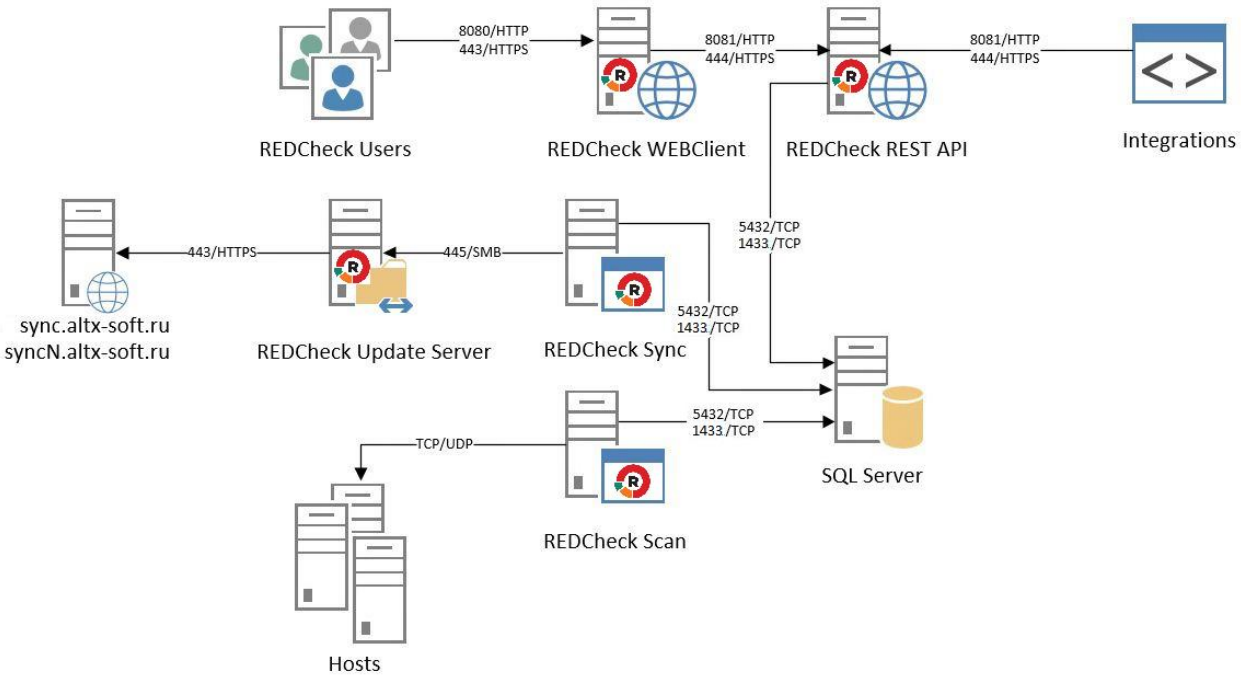
Кроме контента, разработанного компанией АЛТЭКС-СОФТ, его содержание синхронизировано с экспертными ресурсами, такими как БДУ ФСТЭК России, НКЦКИ, бюллетени производителей и ряд других международных экспертных справочников. Периодичность публикации новых определений составляет 2-3 дня в соответствии 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 «АЛТЭКС-СОФТ» в рамках единой платформы, способных функционировать на выделенных серверах и в соответствии с используемой лицензией. Поддерживается установка всех основных компонентов на один сервер при сканировании малых сетей. Пример распределенного расположения компонентов приведен 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.



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

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 стандартизованного формата SCAP позволяет пользователям загружать сторонние конфигурации, или использовать собственные.

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 СУБД

Функция Аудит СУБД в RedCheck предназначена для проверки соответствия 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 агентов 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).

> 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.

1.5 Ролевая модель RedCheck

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	▪ Обладает всеми возможностями в рамкам работы с консолью управления RedCheck
Администратор ИБ	▪ 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; ▪ Управление пользователями для работы с RedCheck

	▪ Запуск синхронизации контента безопасности и импортирование OVAL-сигнатур; ▪ Просмотр журнала событий и справки о программе;
Системный администратор	▪ 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; ▪ Просмотр журнала событий и справки о программе;
Пользователь ИБ	▪ 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	+	+	+	+
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	+	+	+	+

** – на данный момент Аудит уязвимостей образов Docker не реализован в версии 2.8.0. Для сканирования необходимо установить Windows версию службы сканирования.*

Информация о версии и установленных службах программы, а также об ограничениях использующейся 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 СА3 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 «АЛТЭКС-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

- XP[1] / XP Embedded / Vista / 7 / 8/ 8.1 / 10 / 11
- Server 2003[2] / 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 / 2019[3] / 2022

Linux

- AlmaLinux 8.x / 9.x
- Amazon Linux 2 / AMI / 2023
- 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
- 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
- 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
- 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 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

Сетевое оборудование

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

Виртуализация

- 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[4]
- VMware vCenter Server 5.1 / 5.5 / 6.0 / 6.5 / 6.7 / 7
- VMware NSX

СУБД

- IBM Db2
- Jatoba
- 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
- PostgreSQL 8 / 9 / 10 / 11 / 12 / 13 / 14 / 15 / 16
- Pangolin
- SAP HANA

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

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

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

[3]*Для Windows Server 2019 не применим функционал PatchManagment;*

[4]*Для VMware ESXi 7, отсутствует возможность проведения задания "Аудит конфигураций";*

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
Аудит уязвимостей	NA	AL	AL	AL	AL
Аудит обновлений	NA	NA	NA	NA	NA
Аудит конфигураций	AL	AL	AL	AL	AL
Инвентаризация	NA	AL	AL	AL	AL
Фиксация	NA	NA	NA	NA	NA
Аудит в режиме Пентест	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

> 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:

VHDD ≈ Vcp NT

где VHDD – необходимый объем HDD, ГБ; Vcp – средний объем результатов сканирования одного хоста,
Vcp ≈ 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*100*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);
  - Debian 11;
  - РЕД ОС 7.3;
  - SberLinux 8.8 / 8.9;
- СУБД:
  - PostgreSQL версия 12.5 – 16;
  - Postgres Pro версия 14 / 15;
- Браузер на основе ядра Chromium;
- Командная оболочка Bash.

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

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 электронных почтовых сообщений, e-mail	25/TCP	SMTP/Отправка почтовых уведомлений о результатах работы службы
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-soft.ru)	443/TCP	HTTPS/Доступ к сервису синхронизации производителя (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

Содержание

Установка СУБД

Лог терминала находится в файле **~/.bash_history**. В случае возникновения ошибки создайте файл, содержащий лог, и обратитесь в службу [технической поддержки](#).

Bash (оболочка Unix)

```
sudo cat ~/.bash_history >>
/home/имя_пользователя/Загрузки/log.file
```

Установка СУБД PostgreSQL с репозитория Astra Linux

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

Шаг 2. Войдите под root пользователем;

Bash (оболочка Unix)

```
sudo su -
```

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

Шаг 3. 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 репозиториев в файл рекомендуем использовать текстовый редактор **nano**.

Шаг 1. Откройте файл с помощью команды (sudo);

Bash (оболочка Unix)

```
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 4. Обновите пакеты;

Bash (оболочка Unix)

```
apt -y update
```

Шаг 5. Установите PostgreSQL;

Bash (оболочка Unix)

```
apt -y install postgresql
```

Настройка PostgreSQL

Шаг 6. Добавьте службу **postgresql** в автозапуск;

Bash (оболочка Unix)

```
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 7. Создайте пользователя для администрирования СУБД;

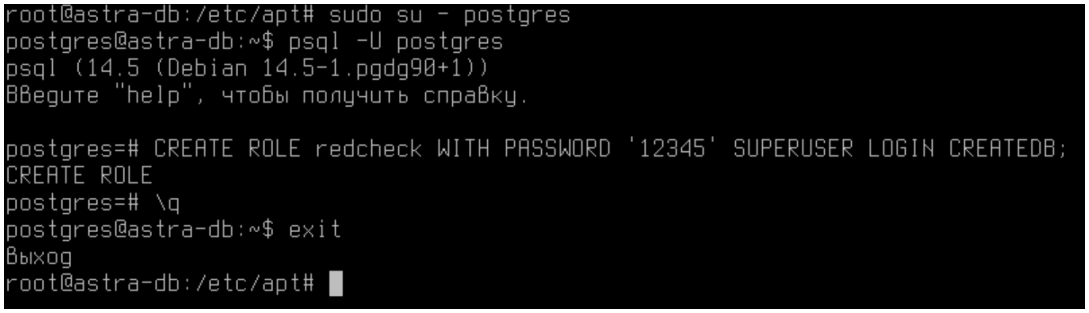
PostgreSQL по умолчанию создает супер-пользователя **postgres**.

Bash (оболочка Unix)

```
sudo su postgres


psql -U postgres


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



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

Шаг 8. Завершите сессию командой **exit**

Шаг 9. Откройте доступ по сети для серверов, на которых планируется установка REST-компонента и служб сканирования и синхронизации RedCheck;

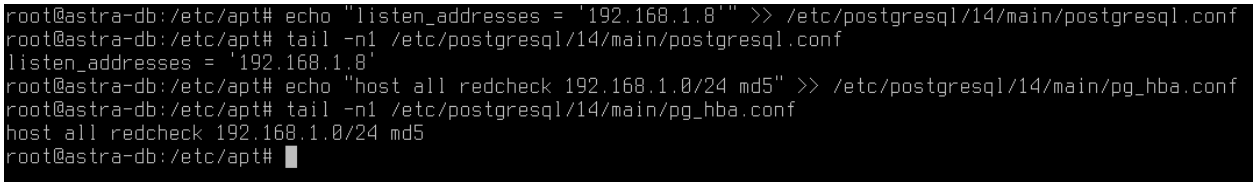
Bash (оболочка Unix)

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

echo host all имя_пользователя_СУБД имя_сети/маска md5 >>
/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;



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

Шаг 10. Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
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)

```
apt install ufw
```

Bash (оболочка Unix)

```
ufw allow 5432/tcp
```

Инсталляция RedCheck

> Все команды в инструкции выполняются под root-пользователем. При необходимости используйте повышение прав (sudo).

> Для обновления RedCheck – 4.8 Обновление RedCheck Nix

Установка компонентов

> Для перемещения по каталогам используйте команду **cd**. Например, чтобы перейти в каталог /mnt, напишите **cd /mnt**
> Чтобы автоматически дополнить название каталога или файла, используйте **Tab**

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

Код

```
apt-cdrom add
```

Шаг 2. Переместите скачанный архив redcheck-repo-2.8.0.9628.tar.gz в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в /mnt;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-repo-2.8.0.9628.tar.gz
/mnt/
```

Шаг 3. Перейдите в каталог и разархивируйте дистрибутив;

Bash (оболочка Unix)

```
cd /mnt
```

Bash (оболочка Unix)

```
tar -xf redcheck-repo-2.8.0.9628.tar.gz
```

Шаг 4. Добавьте GPG-ключ, который находится в только что разархивированном каталоге;

Bash (оболочка Unix)

```
apt-key add redcheck-repo/PUBLIC-GPG-KEY-redcheck
```

Шаг 5. Создайте файл **redcheck.list** и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/apt/sources.list.d/redcheck.list
echo "deb file:/mnt/redcheck-repo/ 1.7_x86-64 non-free dotnet" >
/etc/apt/sources.list.d/redcheck.list
```

Шаг 6. Обновите пакеты;

Bash (оболочка Unix)

```
apt -y update
```

Шаг 7. Установите компоненты RedCheck;

Bash (оболочка Unix)

```
apt -y install redcheck-dotnet-runtime redcheck-aspnetcore-runtime
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-
service redcheck-cleanup-service
```

Конфигурация RedCheck

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

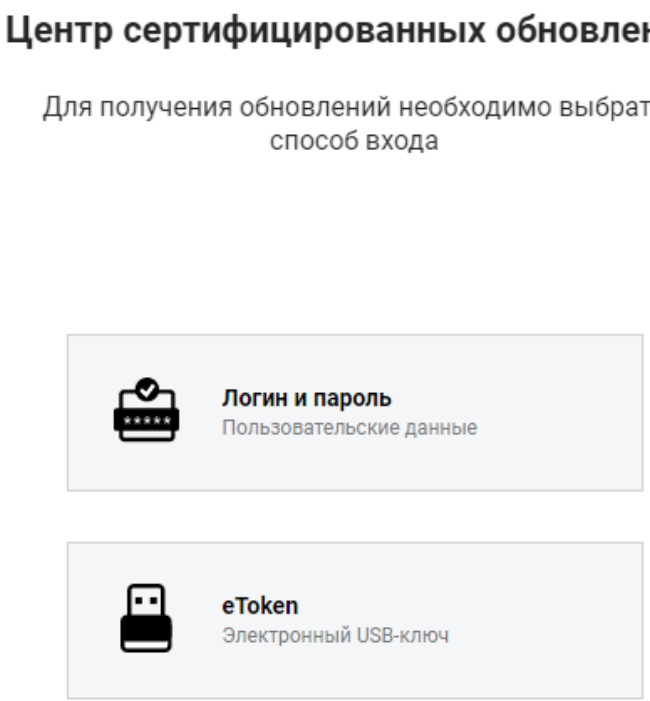
Шаг 1. Сгенерируйте код активации командой:

Bash (оболочка Unix)

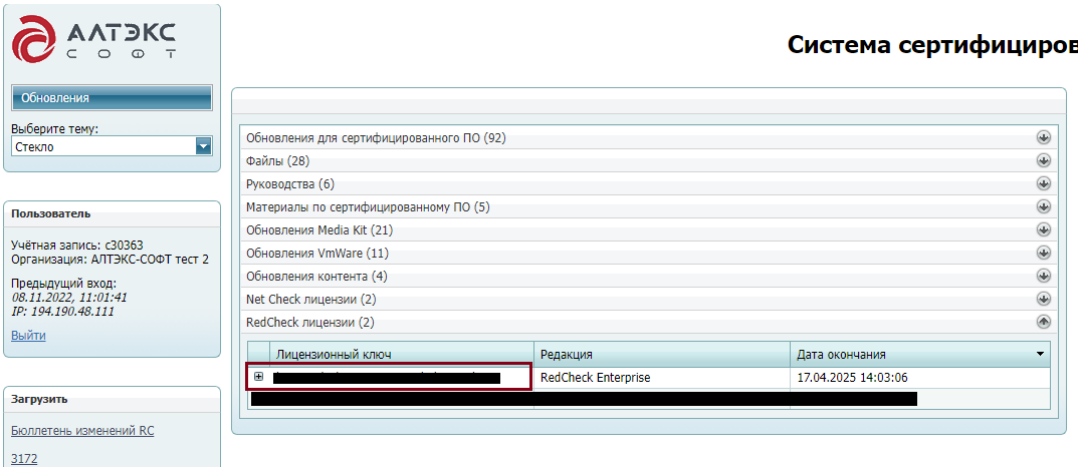
```
redcheck-bootstrap get-code
```

Шаг 2. Авторизуйтесь в Центре сертифицированных обновлений с помощью логина и пароля;

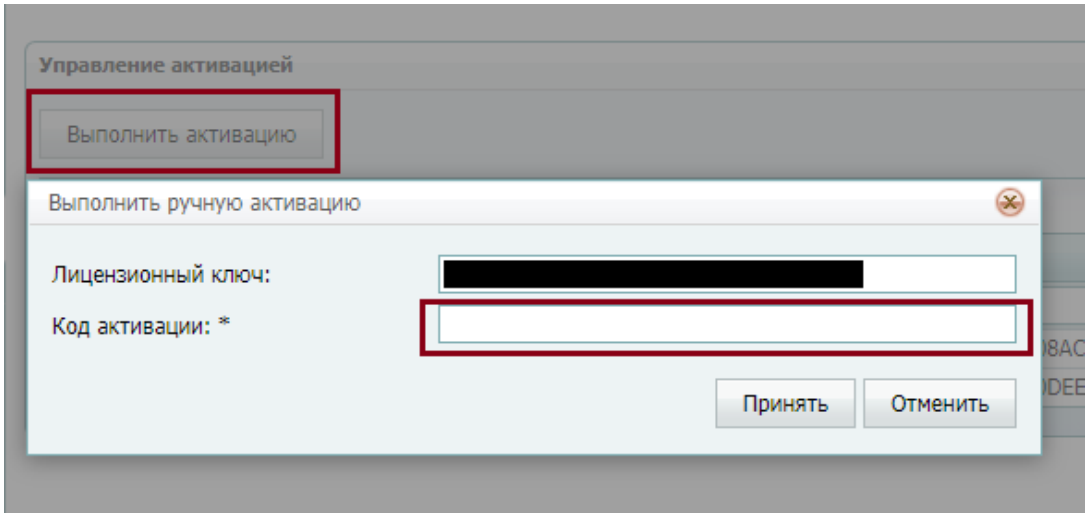
Логин/пароль поставляется всем коммерческим клиентам в разделе 15, «Особые отметки» (начиная с 18.05.2022).



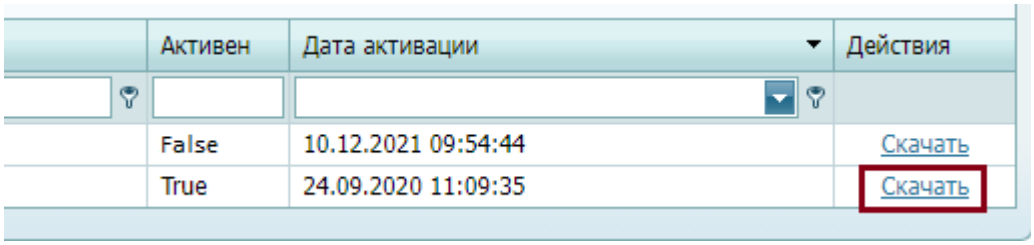
Шаг 3. Раскройте **RedCheck лицензии** → выберите интересующий Вас номер лицензионного ключа;



Нажмите **Выполнить активацию** → введите ранее скопированный код активации → **Принять**;



Шаг 4. Нажмите **Скачать**;



Шаг 5. Сохраните файл **license.xml**;

Шаг 6. Настройте компоненты RedCheck;

Перед повторной конфигурацией **рекомендуем** сделать резервную копию базы данных.

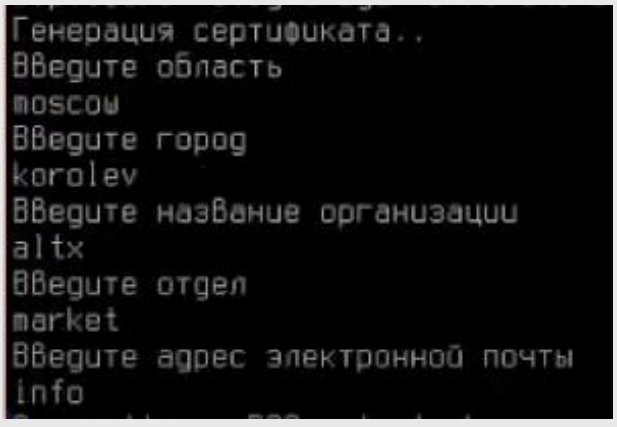
Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=all
```

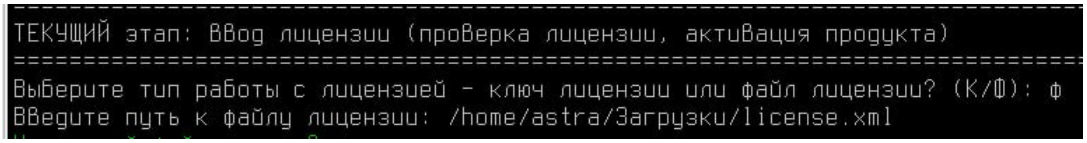
Будет запущен процесс конфигурации компонентов, который потребует ввода данных для доступа к СУБД, лицензионного ключа и других параметров для корректной работы Системы. Данной командой будут сконфигурированы все основные компоненты RedCheck на одном сервере.

Если вы используете собственную схему и табличное пространство, то табличное пространство должно быть создано заранее. По умолчанию используется схема public.

На этапе генерации сертификата для протокола HTTPS необходимо ввести названия: **области (страны), города, организации, отдела, электронной почты**.



Шаг 7. Если хост не подключен к сети Интернет, выберите способ активации файлом и укажите путь к файлу **license.xml**. Если подключен, укажите ключ лицензии:



Шаг 8. Если установлен пакет redcheck-cleanup-service, будет предложено настроить службу очистки БД. В процессе настройки нужно указать URL redcheck-api в формате http://ip:port, а также учетные данные пользователя с ролью RedCheck_Admins.

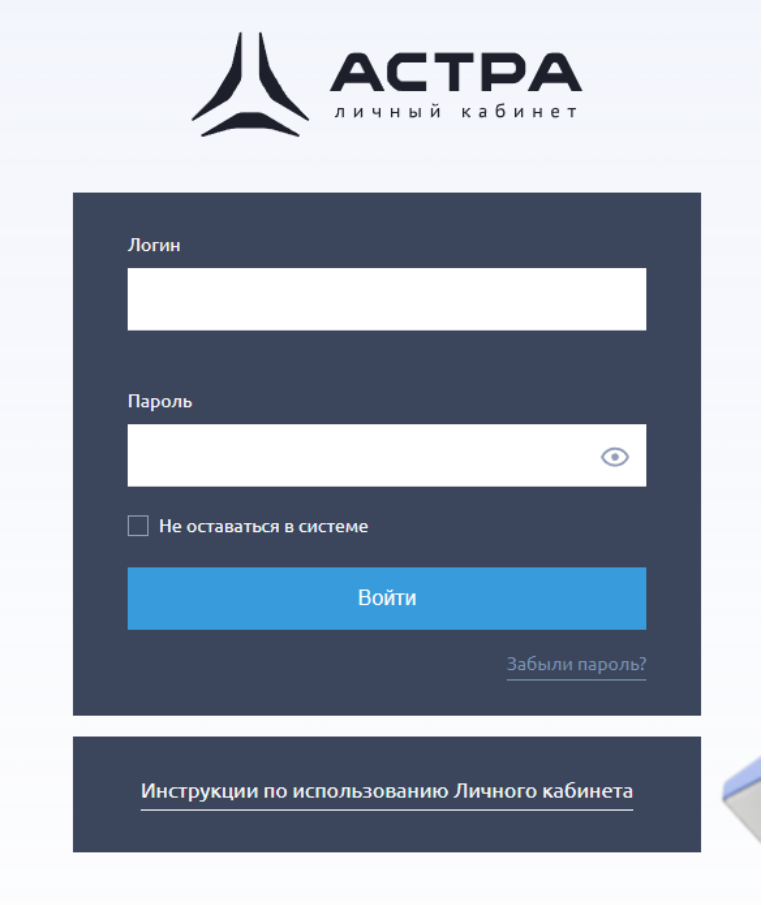
> Логи инсталлятора располагаются в **/var/opt/redcheck-common/log/configuration.log**

При необходимости можете продолжить конфигурацию RedCheck и настроить:

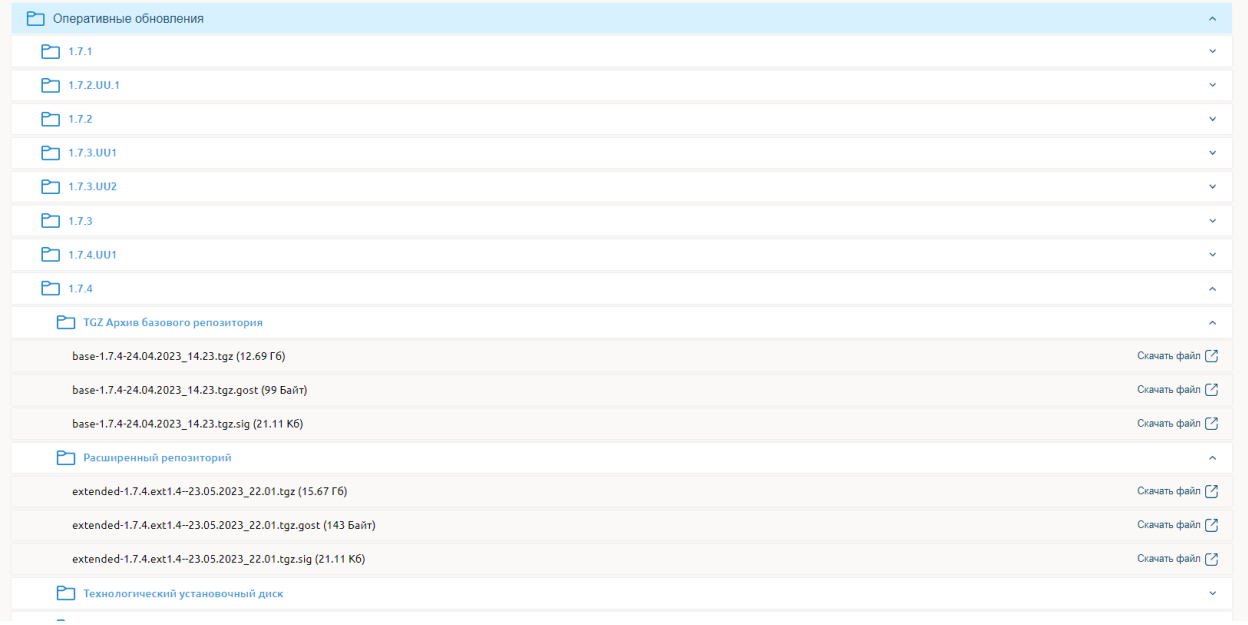
- Сканирование с помощью WinRM
- Доменную аутентификацию в RedCheck (Kerberos)

Подключение репозиториев Astra Linux без доступа к сети Интернет

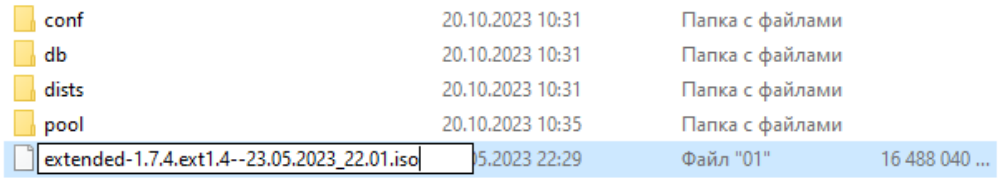
Шаг 1. Войдите в личный кабинет Astra Linux, используя логин (e-mail) и пароль:



Шаг 2. Перейдите в раздел **Лицензии и сертификаты** → выберите необходимую лицензию → перейдите подраздел **Обновления** → раскройте список **Оперативные обновления** → **1.7.6** → скачайте .iso файл из **Расширенного репозитория;**



Шаг 3. Разархивируйте скачанный файл с расширением .tar → переименуйте файл, добавив в конце расширение .iso → разархивируйте .iso файл и переместите получившийся каталог на хост;



> Репозиторий обязательно должен состоять из каталогов **dists** и **pool**

Шаг 4. Переместите каталог в директорию, отличную от пользовательского каталога. В инструкции репозиторий перемещается в /mnt;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/astra-extended /mnt/
```

> В инструкции репозиторий имеет имя **astra-extended**

Шаг 5. Добавьте репозиторий в файл **/etc/apt/sources.list**:

Bash (оболочка Unix)

```
deb file:/mnt/astra-extended/ 1.7_x86-64 astra-ce main contrib non-free
```

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

Шаг 1. Откройте файл с помощью команды (sudo);

Bash (оболочка Unix)

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

Шаг 2. Переместите курсор в конец документа с помощью стрелки вниз. Для перехода на новую строку используйте клавишу **Enter**;

Шаг 3. Скопируйте репозитории и вставьте их с помощью комбинации **Ctrl + U**;

Шаг 4. Сохраните файл с помощью комбинации **Ctrl + O**; Для выхода используйте **Ctrl + X**;

3.2 РЕД ОС

Содержание

Установка СУБД

Лог терминала находится в файле **~/.bash_history**. В случае возникновения ошибки создайте файл, содержащий лог, и обратитесь в службу [технической поддержки](#).

Bash (оболочка Unix)

```
sudo cat ~/.bash_history >>
/home/имя_пользователя/Загрузки/log.file
```

Содержание

Установка СУБД PostgreSQL с репозитория РЕД ОС

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

Шаг 2. Войдите под root пользователем с помощью команды **su**;

Шаг 3. Установите PostgreSQL следующей командой;

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

Bash (оболочка Unix)

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

Шаг 4. Произведите инициализацию базы данных postgresql;

Bash (оболочка Unix)

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

Шаг 5. Запустите службу postgresql и добавьте ее в автозагрузку;

```
Bash (оболочка Unix)
systemctl enable postgresql-15 --now
```

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

Настройка СУБД

Шаг 6. Создайте пользователя для администрирования СУБД;

> PostgreSQL по умолчанию создает супер-пользователя **postgres**.

```
Bash (оболочка Unix)
sudo su postgres

psql -U postgres

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

> 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 серверного-компонента и служб сканирования и синхронизации RedCheck;

```
Bash (оболочка Unix)
```

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

echo host all имя_пользователя_СУБД имя_сети/маска md5 >>
/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 9. Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
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

> Все команды в инструкции выполняются под root-пользователем.

> Для обновления RedCheck – 4.8 Обновление RedCheck Nix

Установка компонентов

> Для перемещения по каталогам используйте команду **cd**. Например, чтобы перейти в каталог /mnt, напишите **cd /mnt**
> Чтобы автоматически дополнить название каталога или файла, используйте **Tab**

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

Шаг 2. Войдите под root пользователем с помощью команды **su**;

Шаг 3. Смонтируйте установочный диск и создайте файл cd.repo:

Код

```
touch /etc/yum.repos.d/cd.repo

[cd]
name=CD
baseurl=file:///run/media/user/redos-DVD-x86_64-MUROM-7.3
gpgcheck=0
enabled=1
```

Шаг 4. Переместите скачанный архив redcheck-redos-repo-2.8.0.9629.tar.gz в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в /mnt;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-redos-repo-
2.8.0.9629.tar.gz /mnt/
```

Шаг 5. Перейдите в каталог и разархивируйте дистрибутив;

Bash (оболочка Unix)

```
cd /mnt


tar -xf redcheck-redos-repo-2.8.0.9629.tar.gz
```

Шаг 6. Создайте файл redcheck.repo и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck.repo

echo -e "[redcheck-repo]
name=RedCheck 2.8.0
baseurl=file:/mnt/redcheck-redos-repo/redcheck-base
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-redos-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck.repo
```

Шаг 7. Создайте файл redcheck-dotnet.repo и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck-dotnet.repo

echo -e "[redcheck-dotnet-repo]
name=ALTX .NET 6.0.35
baseurl=file:/mnt/redcheck-redos-repo/redcheck-dotnet
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-redos-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck-dotnet.repo
```

Шаг 8. Обновите пакеты;

Bash (оболочка Unix)

```
dnf check-update
```

Шаг 9. Установите компоненты RedCheck;

Bash (оболочка Unix)

```
dnf -y install redcheck-dotnet-runtime redcheck-aspnetcore-runtime
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-
service redcheck-cleanup-service
```

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

Конфигурация RedCheck

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

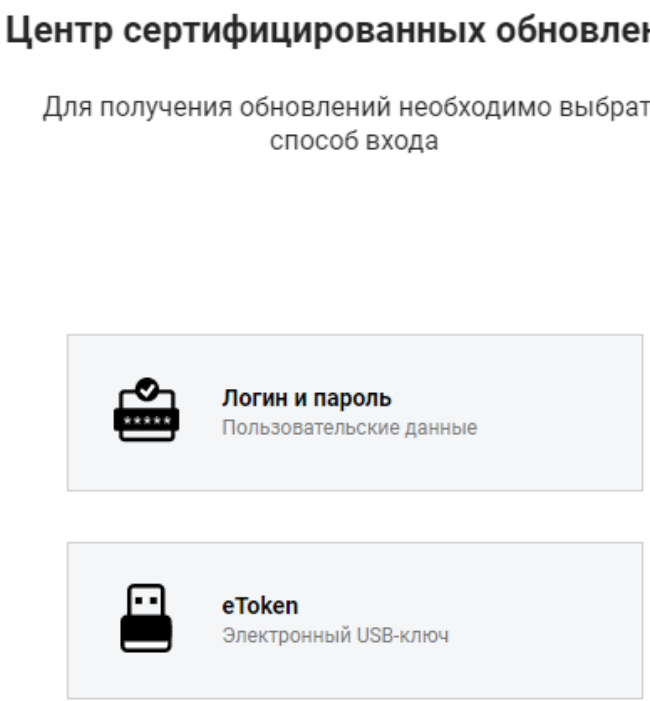
Шаг 1. Сгенерируйте код активации командой:

Bash (оболочка Unix)

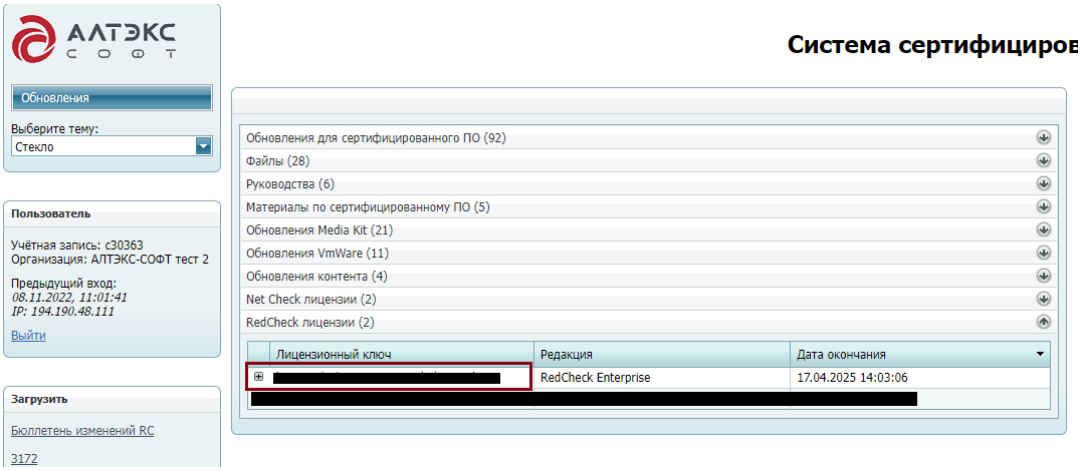
```
redcheck-bootstrap get-code
```

Шаг 2. Авторизуйтесь в Центре сертифицированных обновлений с помощью логина и пароля;

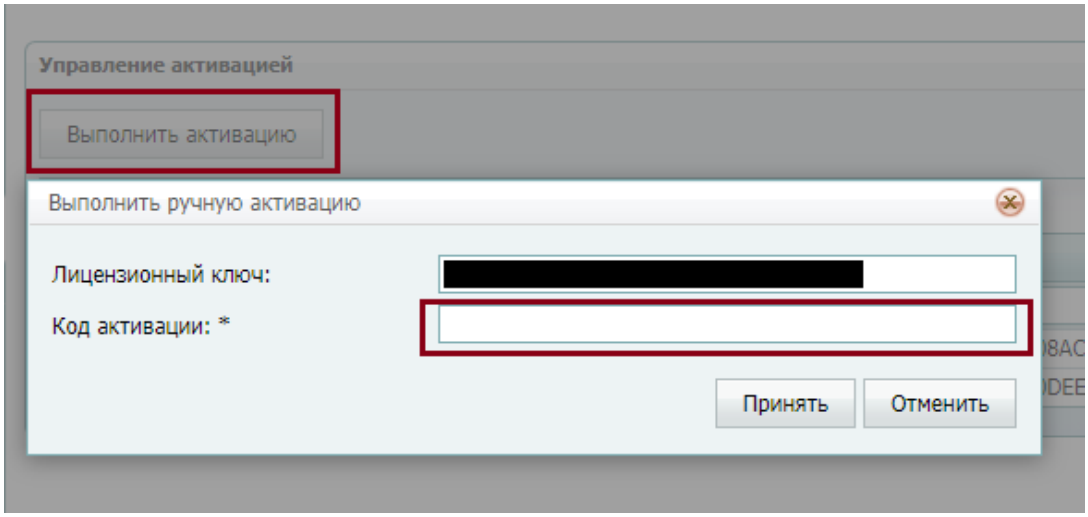
> Логин/пароль поставляется всем коммерческим клиентам в разделе 15, «Особые отметки» (начиная с 18.05.2022).



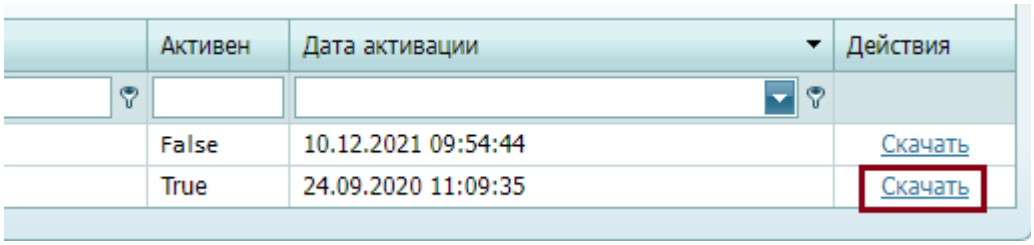
Шаг 3. Раскройте **RedCheck лицензии** → выберите интересующий Вас номер лицензионного ключа;



Нажмите **Выполнить активацию** → введите ранее скопированный код активации → **Принять**;



Шаг 4. Нажмите **Скачать**;



Шаг 5. Сохраните файл license.xml;

Шаг 6. Настройте компоненты RedCheck;

Перед повторной конфигурацией **рекомендуем** сделать резервную копию базы данных.

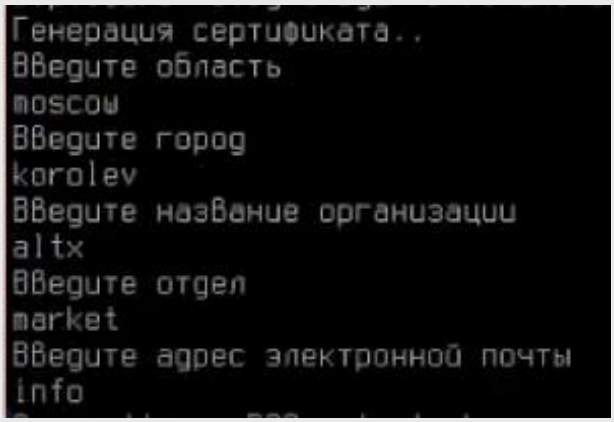
Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=all
```

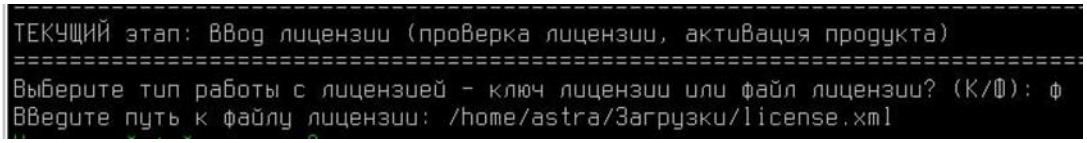
Будет запущен процесс конфигурации компонентов, который потребует ввода данных для доступа к СУБД, лицензионного ключа и других параметров для корректной работы Системы. Данной командой будут сконфигурированы все основные компоненты RedCheck на одном сервере.

Если вы используете собственную схему и табличное пространство, то табличное пространство должно быть создано заранее. По умолчанию используется схема public.

На этапе генерации сертификата для протокола HTTPS необходимо ввести названия: **области (страны), города, организации, отдела, электронной почты**.



Шаг 7. Если хост не подключен к сети Интернет, выберите способ активации файлом и укажите путь к файлу **license.xml**. Если подключен, укажите ключ лицензии:



Для установки firewall используйте команду:

Bash (оболочка Unix)

```
dnf -y install firewalld
```

Запустите firewall:

Bash (оболочка Unix)

```
systemctl start firewalld
```

Добавьте исключения для портов, на которых работают компоненты RedCheck:

Bash (оболочка Unix)

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

firewall-cmd --reload
```

Шаг 8. Если установлен пакет redcheck-cleanup-service, будет предложено настроить службу очистки БД. В процессе настройки нужно указать URL redcheck-api в формате http://ip:port, а также учетные данные пользователя с ролью RedCheck_Admins.

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

При необходимости можете продолжить конфигурацию RedCheck и настроить:

- Сканирование с помощью WinRM

- Доменную аутентификацию в RedCheck (Kerberos)

3.3 SberLinux

Содержание

Установка СУБД

Лог терминала находится в файле **~/.bash_history**. В случае возникновения ошибки создайте файл, содержащий лог, и обратитесь в службу технической поддержки.

Bash (оболочка Unix)

```
sudo cat ~/.bash_history >> /home/имя_пользователя/Загрузки/log.file
```

Содержание

Установка СУБД PostgreSQL с официального репозитория

Шаг 1. Войдите под root пользователем с помощью команды **su**;

Шаг 2. Установите PostgreSQL с помощью следующих команд;

Устанавливать можно любую версию postgresql, имеющуюся в репозитории, согласно требованиям к программному обеспечению.

Bash (оболочка Unix)

```
dnf install -y
https://download.postgresql.org/pub/repos/yum/reporpms/EL-8-
x86_64/pgdg-redhat-repo-latest.noarch.rpm

dnf -qy module disable postgresql

dnf install -y postgresql16-server
```

Шаг 3. Произведите инициализацию базы данных postgresql;

Bash (оболочка Unix)

```
/usr/pgsql-16/bin/postgresql-16-setup initdb
```

Шаг 4. Добавьте службу postgresql в автозагрузку и запустите ее;

Bash (оболочка Unix)

```
systemctl enable postgresql-16

systemctl start postgresql-16
```

Для проверки статуса службы используйте команду **systemctl status postgresql-16**

Шаг 5. Установите расширение pgcrypto;

Bash (оболочка Unix)

```
dnf install postgresql16-contrib

sudo -u postgres psql -U postgres

CREATE EXTENSION pgcrypto;
```

В случае нехватки какого-либо другого расширения используйте команду **CREATE EXTENSION extension_name;**

Настройка СУБД

Шаг 6. Создайте пользователя для администрирования СУБД;

PostgreSQL по умолчанию создает супер-пользователя **postgres**.

Bash (оболочка Unix)

```
sudo su postgres
```

```
psql -U postgres

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

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 серверного-компонента и служб сканирования и синхронизации RedCheck;

Bash (оболочка Unix)

```
echo "listen_addresses = 'ip_СУБД'" >>
/var/lib/pgsql/16/data/postgresql.conf

echo host all имя_пользователя_СУБД имя_сети/маска md5 >>
/var/lib/pgsql/16/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 9. Перезапустите PostgreSQL.

Bash (оболочка Unix)

```
systemctl restart postgresql-16
```

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

Все команды в инструкции выполняются под root-пользователем.

Для обновления RedCheck – 4.8 Обновление RedCheck Nix

Установка компонентов

Для перемещения по каталогам используйте команду **cd**. Например, чтобы перейти в каталог /mnt, напишите **cd /mnt**
Чтобы автоматически дополнить название каталога или файла, используйте **Tab**

Шаг 1. Откройте терминал и войдите под root пользователем с помощью команды **sudo su**;

Для инсталляции пакетов RedCheck необходимо подключить Base и AppStream репозитории.

Шаг 2. Переместите скачанный архив redcheck-sber-repo-2.8.0.9630.tar.gz в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в /mnt;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-sber-repo-2.8.0.9630.tar.gz
/mnt/
```

Шаг 3. Перейдите в директорию и разархивируйте дистрибутив;

Bash (оболочка Unix)

```
cd /mnt

tar -xf redcheck-sber-repo-2.8.0.9630.tar.gz
```

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

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck.repo

echo -e "[redcheck-repo]
name=RedCheck 2.8.0
baseurl=file:/mnt/redcheck-sber-repo/redcheck-base
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-sber-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck.repo
```

Шаг 5. Создайте файл redcheck-dotnet.repo и добавьте в него запись репозитория;

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck-dotnet.repo

echo -e "[redcheck-dotnet-repo]
name=ALTX .NET 6.0.35
baseurl=file:/mnt/redcheck-sber-repo/redcheck-dotnet
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-sber-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck-dotnet.repo
```

Шаг 6. Обновите пакеты;

Bash (оболочка Unix)

```
dnf check-update
```

Шаг 7. Установите компоненты RedCheck;

Bash (оболочка Unix)

```
dnf -y install redcheck-dotnet-runtime redcheck-aspnetcore-runtime
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-
service redcheck-cleanup-service
```

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

Конфигурация RedCheck

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

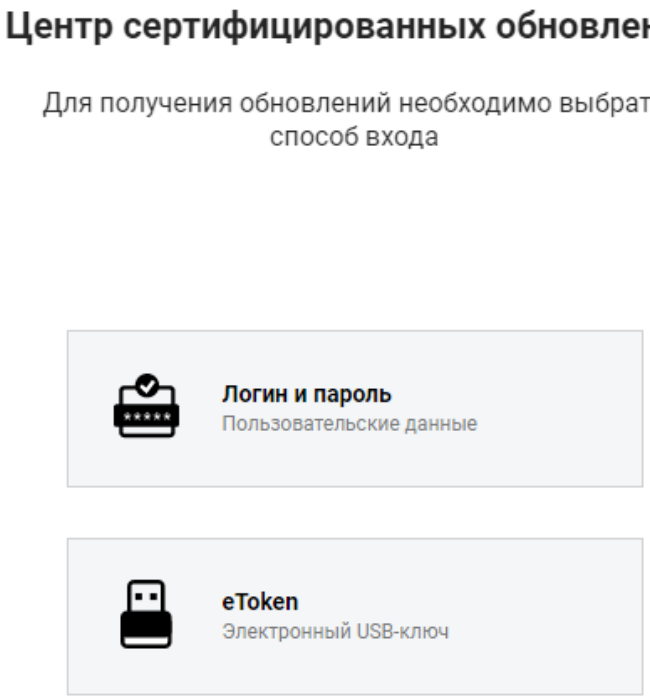
Шаг 1. Сгенерируйте код активации командой:

Bash (оболочка Unix)

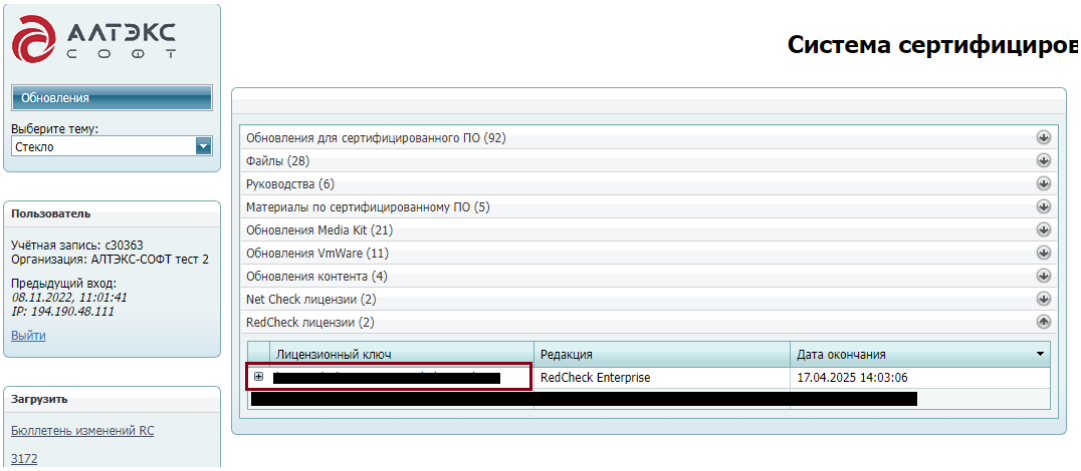
```
redcheck-bootstrap get-code
```

Шаг 2. Авторизуйтесь в Центре сертифицированных обновлений с помощью логина и пароля;

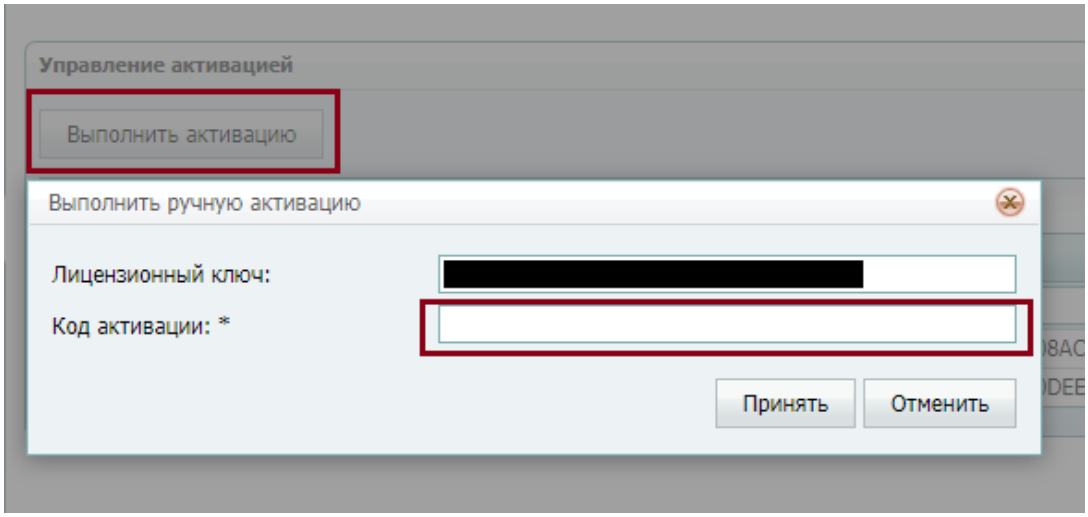
> Логин/пароль поставляется всем коммерческим клиентам в разделе 15, «Особые отметки» (начиная с 18.05.2022).



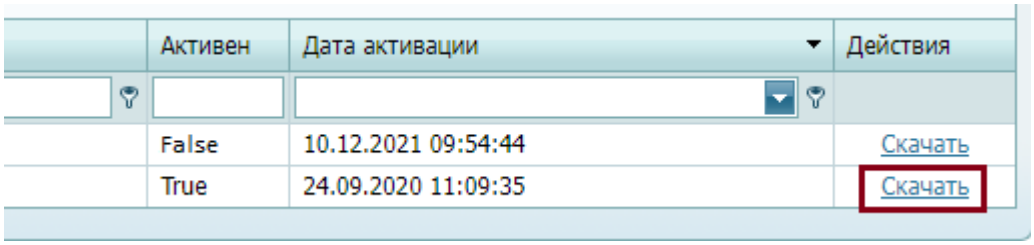
Шаг 3. Раскройте **RedCheck лицензии** → выберите интересующий Вас номер лицензионного ключа;



Нажмите **Выполнить активацию** → введите ранее скопированный код активации → **Принять**;



Шаг 4. Нажмите **Скачать**;



Шаг 5. Сохраните файл license.xml;

Шаг 6. Настройте компоненты RedCheck;

Перед повторной конфигурацией **рекомендуем** сделать резервную копию базы данных.

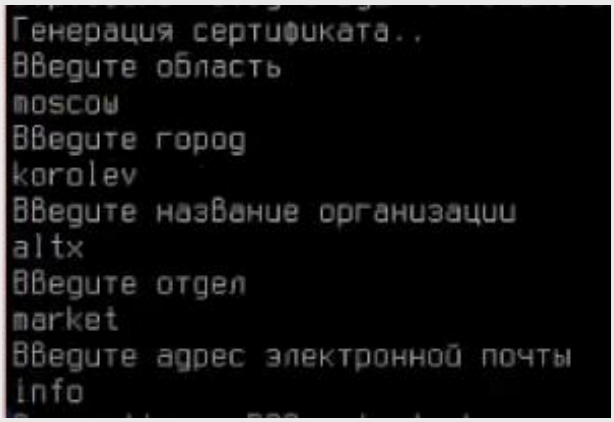
Bash (оболочка Unix)

```
redcheck-bootstrap configure -c=all
```

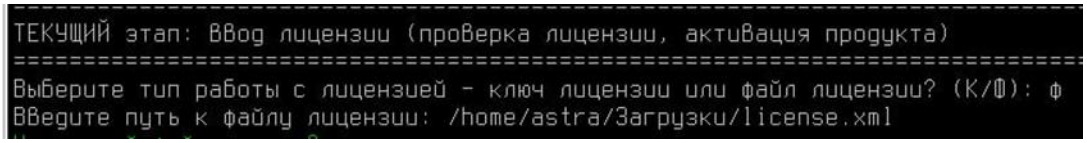
Будет запущен процесс конфигурации компонентов, который потребует ввода данных для доступа к СУБД, лицензионного ключа и других параметров для корректной работы Системы. Данной командой будут сконфигурированы все основные компоненты RedCheck на одном сервере.

Если вы используете собственную схему и табличное пространство, то табличное пространство должно быть создано заранее. По умолчанию используется схема public.

На этапе генерации сертификата для протокола HTTPS необходимо ввести названия: **области (страны), города, организации, отдела, электронной почты**.



Шаг 7. Если хост не подключен к сети Интернет, выберите способ активации файлом и укажите путь к файлу **license.xml**. Если подключен, укажите ключ лицензии:



Для установки firewall используйте команду:

Bash (оболочка Unix)

```
dnf -y install firewalld
```

Запустите firewall:

Bash (оболочка Unix)

```
systemctl start firewalld
```

Добавьте исключения для портов, на которых работают компоненты RedCheck:

Bash (оболочка Unix)

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

firewall-cmd --reload
```

Шаг 8. Если установлен пакет redcheck-cleanup-service, будет предложено настроить службу очистки БД. В процессе настройки нужно указать URL redcheck-api в формате http://ip:port, а также учетные данные пользователя с ролью RedCheck_Admins.

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

При необходимости можете продолжить конфигурацию RedCheck и настроить:

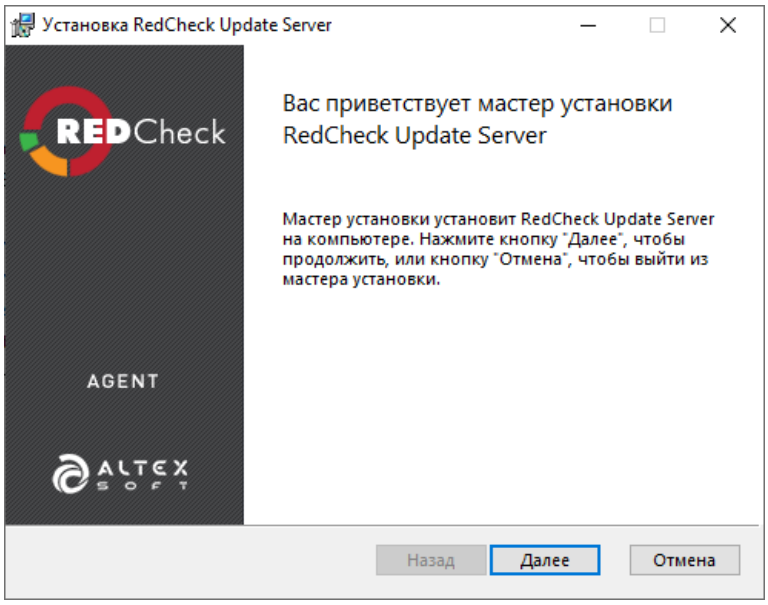
- Сканирование с помощью WinRM

- Доменную аутентификацию в RedCheck (Kerberos)

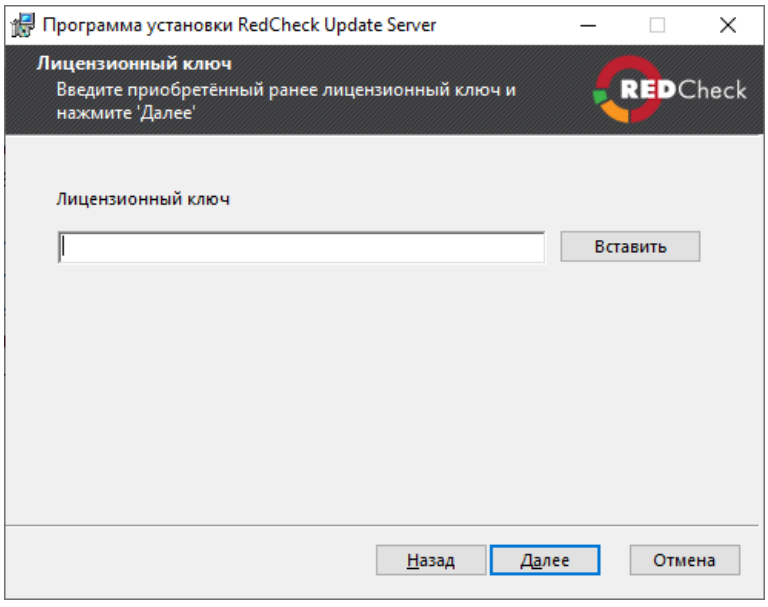
3.4 Установка RedCheck Update Server (Windows)

> Компонент не является обязательным и лицензируется отдельно. Установка RedCheck Update Server производится в DMZ-сегменте сети для обновления контента безопасности без доступа к сети Интернет со стороны службы синхронизации (RedCheck Sync).

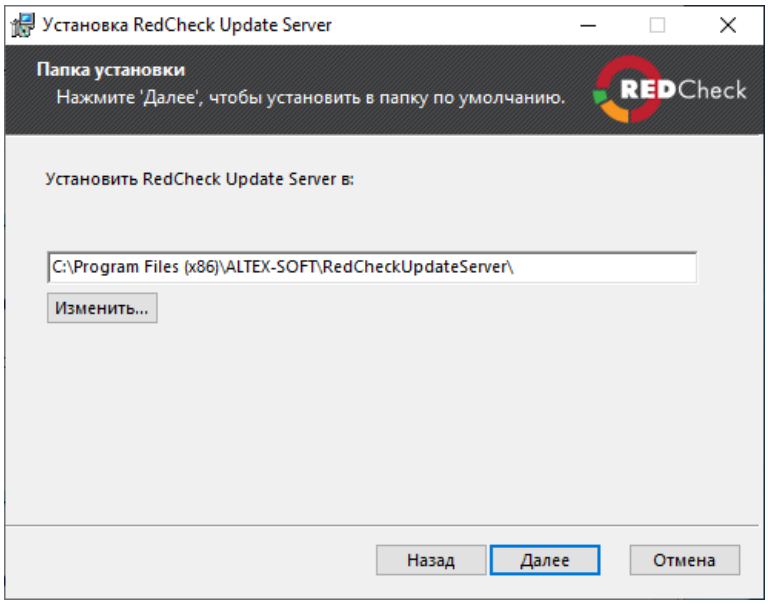
Шаг 1. Запустите инсталляционный пакет **RedCheckUpdateServer.msi**;



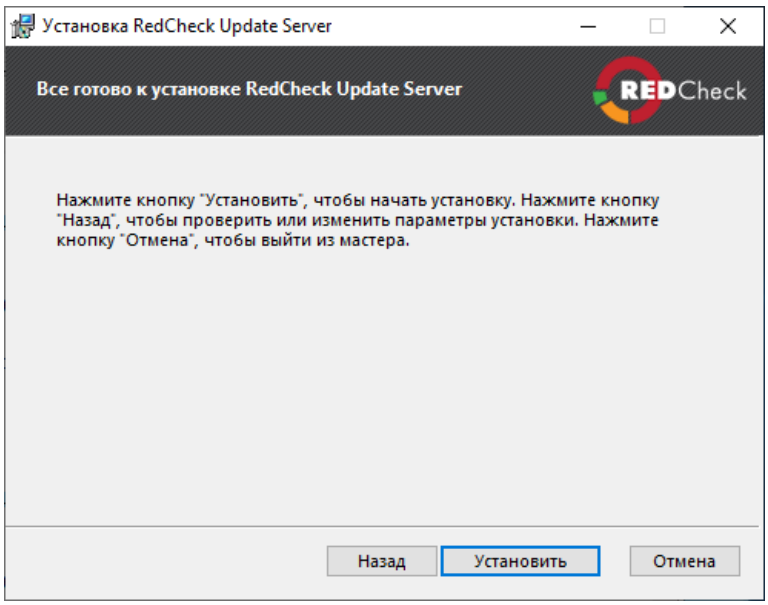
Шаг 2. Введите лицензионный ключ → **Далее**;



Шаг 3. Укажите директорию для установки;



Шаг 4. Нажмите **Установить**.



После установки необходимо произвести настройку (4.3.3 Синхронизация через RedCheck Update Server).

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

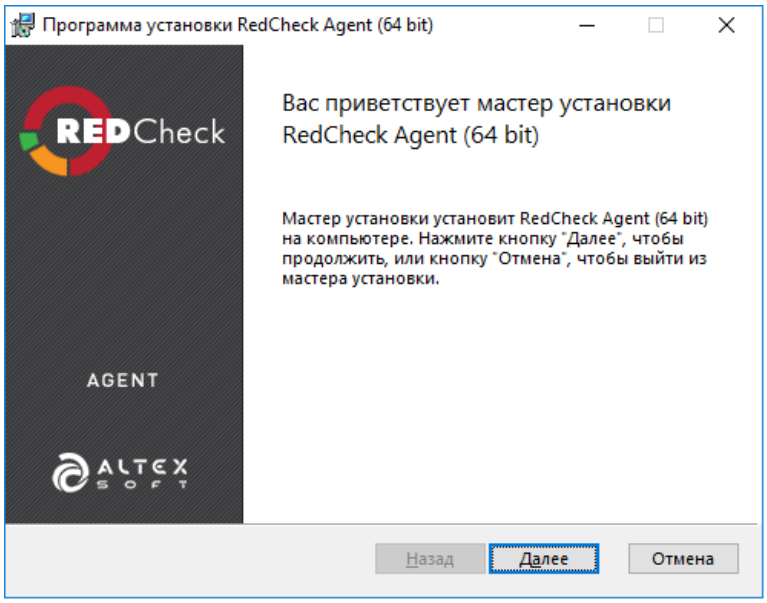
> Агент сканирования входит в состав дистрибутива RedCheck 2.6.9

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

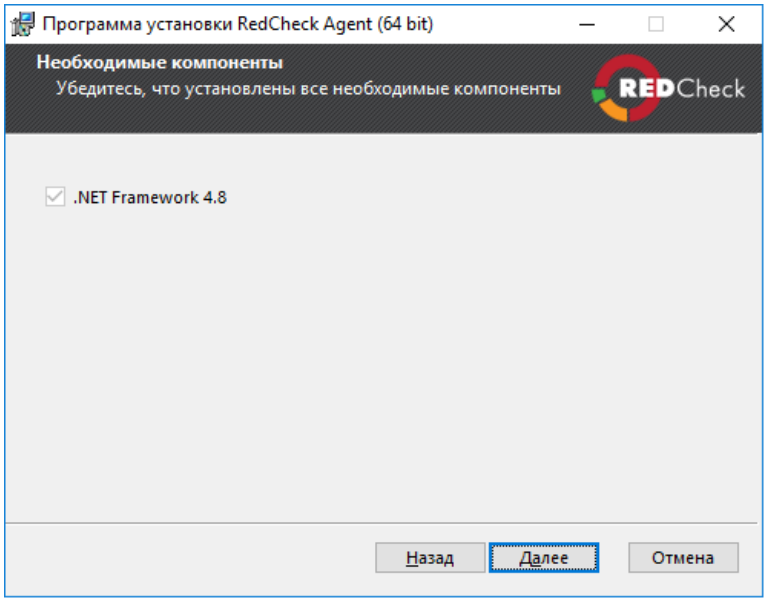
- Microsoft .NET Framework 4.8 (4.3.2 Установка Microsoft .NET Framework).

> Возможна автоматическая установка через командную строку (4.6.3 Агент RedCheck)

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

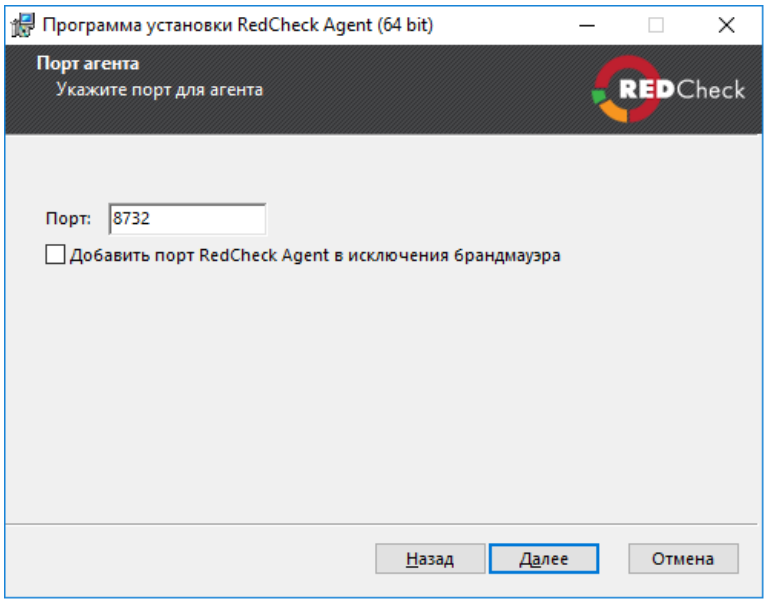


Шаг 2. Инсталлятор проверит наличие всех необходимых компонентов → **Далее**;

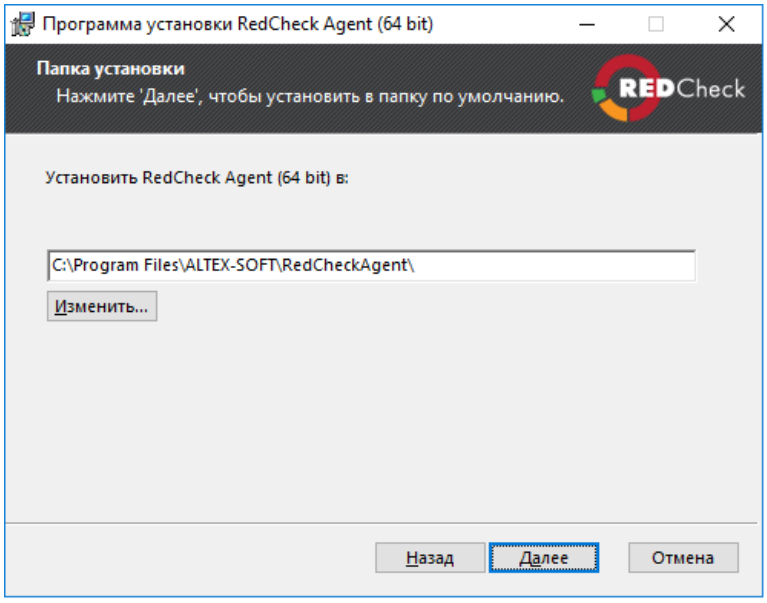


Шаг 3. Задайте порт агента (по умолчанию 8732) и отметьте поле **Добавить порт… в исключение брандмауэра** → **Далее**;

Изменить порт можно после установки (4.11 Изменение порта для Агента сканирования).

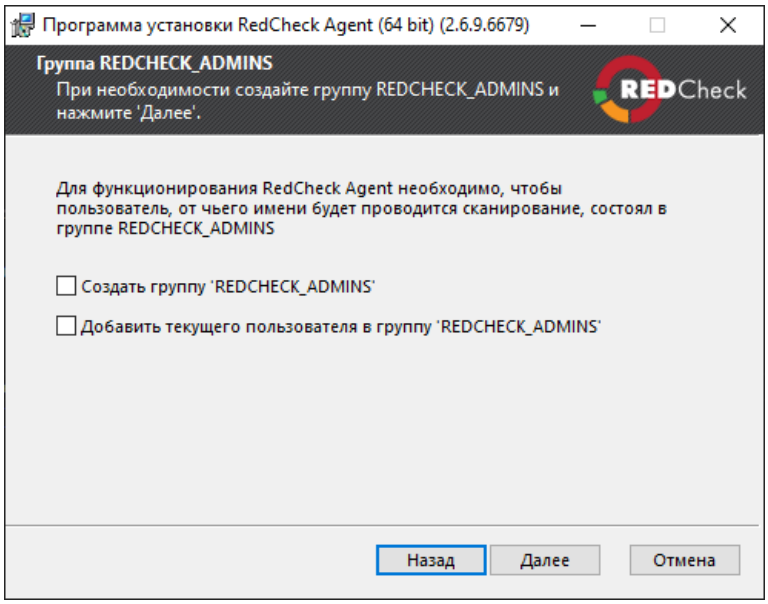


Шаг 4. Укажите директорию для установки агента → **Далее**;



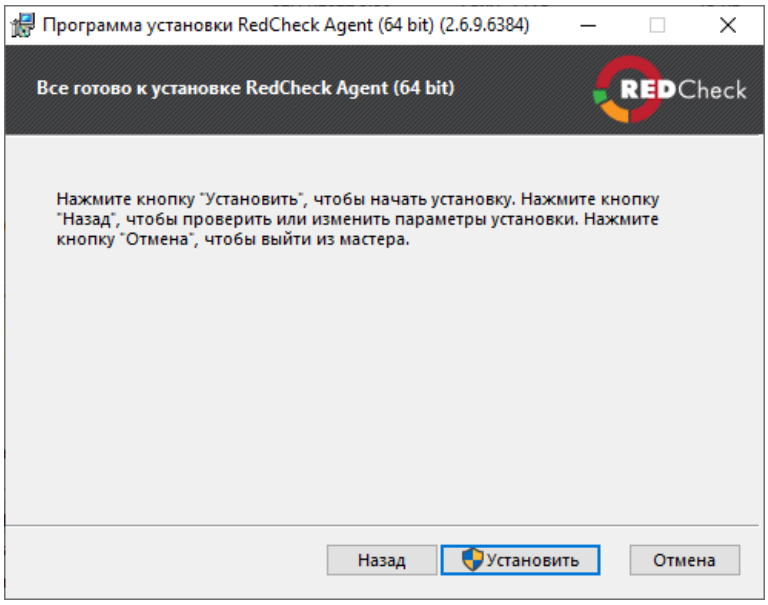
Шаг 5. По необходимости отметьте создание локальной группы безопасности REDCHECK_ADMINS и добавление в нее пользователя, из-под которого производится установка агента → **Далее**;

> 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.

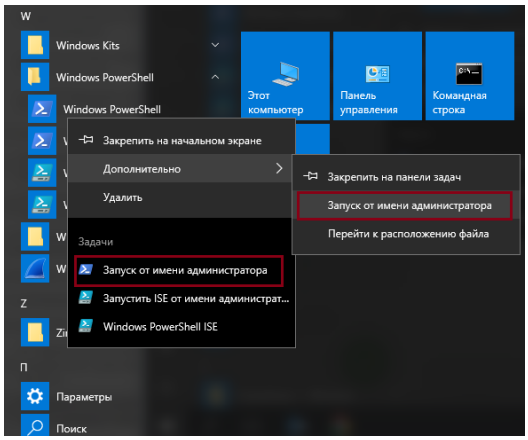
Шаг 6. Нажмите **Установить**;



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:

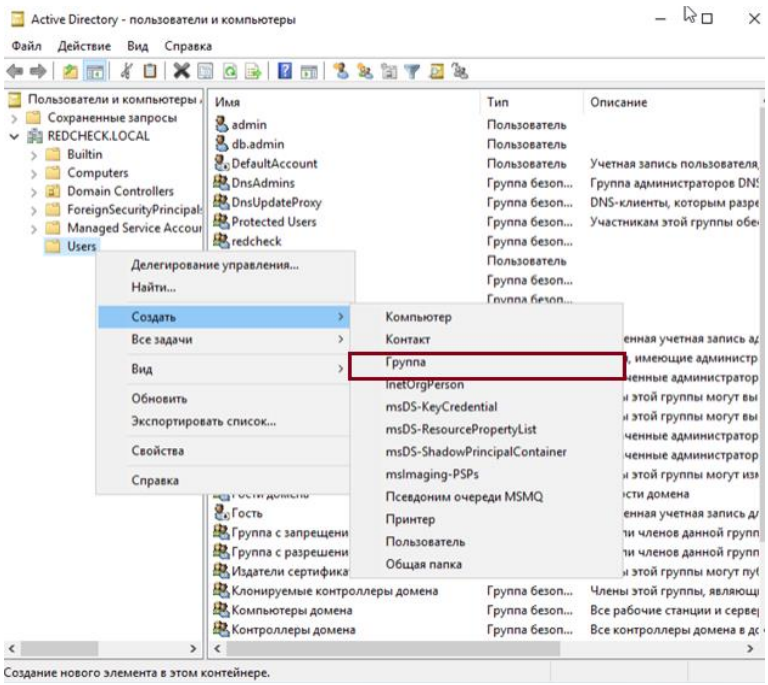
- Создание и настройка группы безопасности
- Создание и настройка сетевой папки
- Настройка групповой политики

> 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.

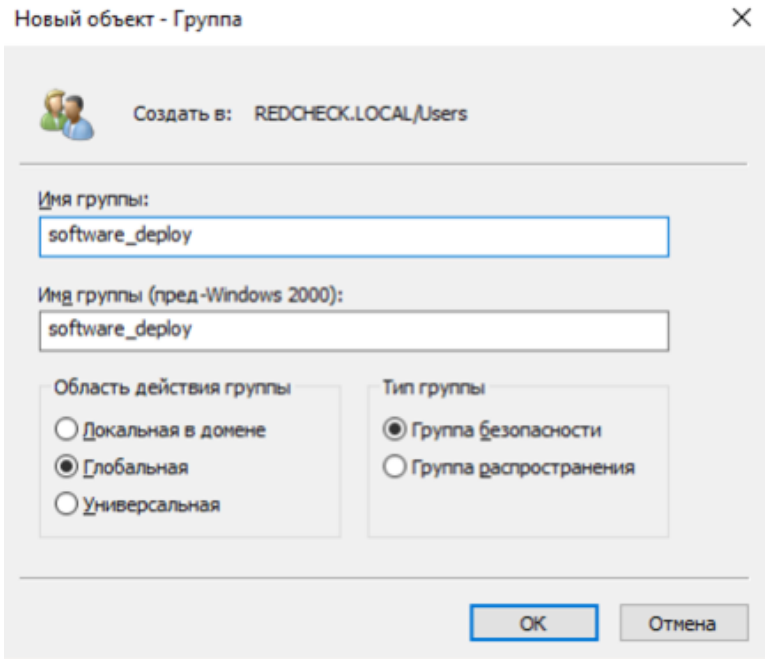
Создание и настройка группы безопасности

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

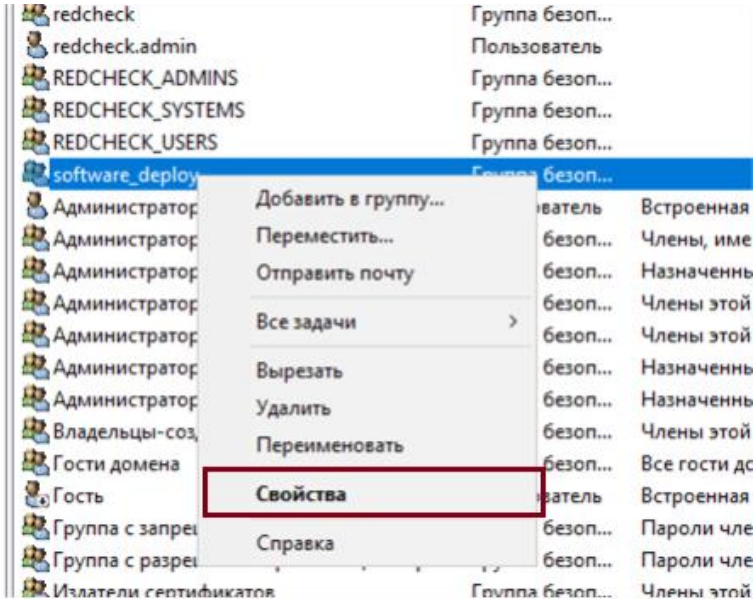
Шаг 2. ПКМ по **Users** → **Создать** → **Группа**;



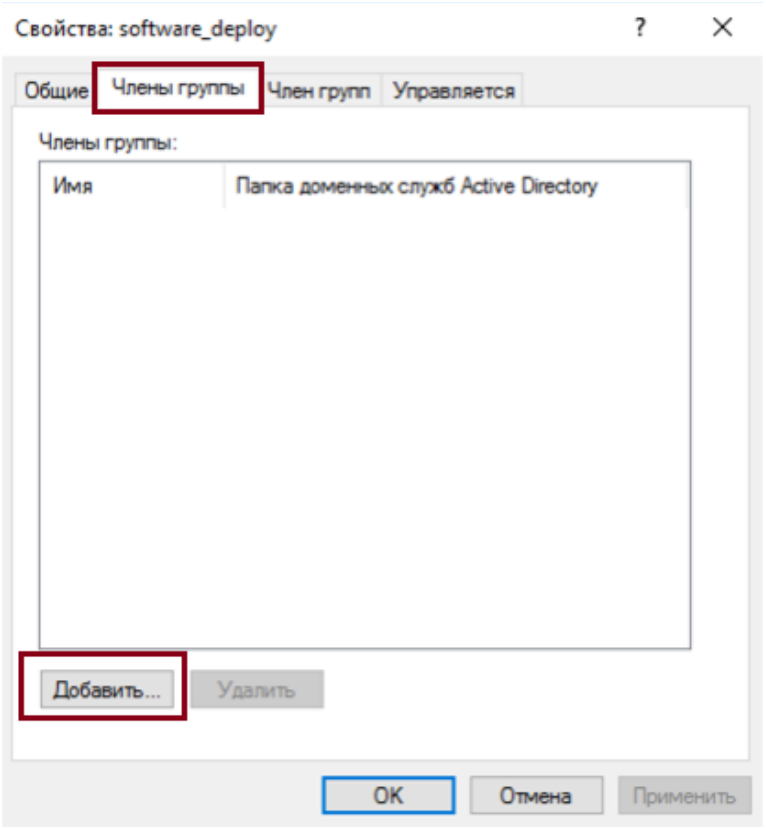
Шаг 3. В поле **Имя группы** укажите название группы (в примере **software_deploy**). Область действия группы **Глобальная**; тип группы **Группа безопасности** → **ОК**.



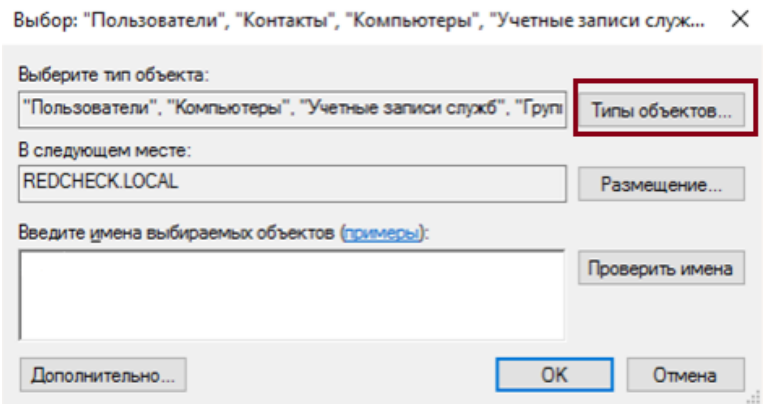
Шаг 4. ПКМ по **software_deploy** → **Свойства**;



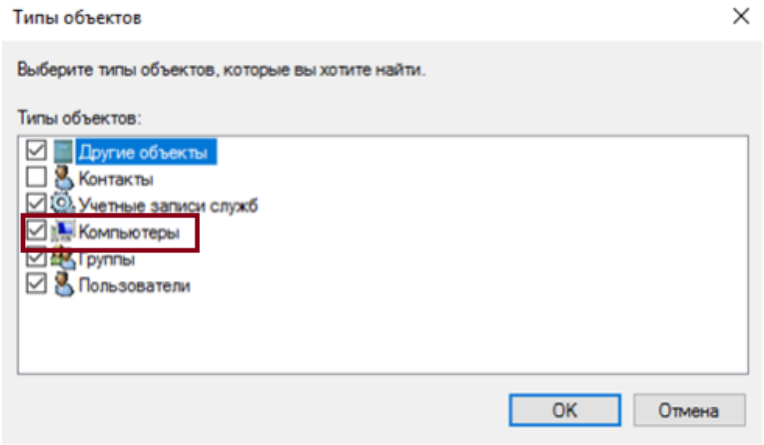
Шаг 5. Выберите **Члены группы** → **Добавить**;



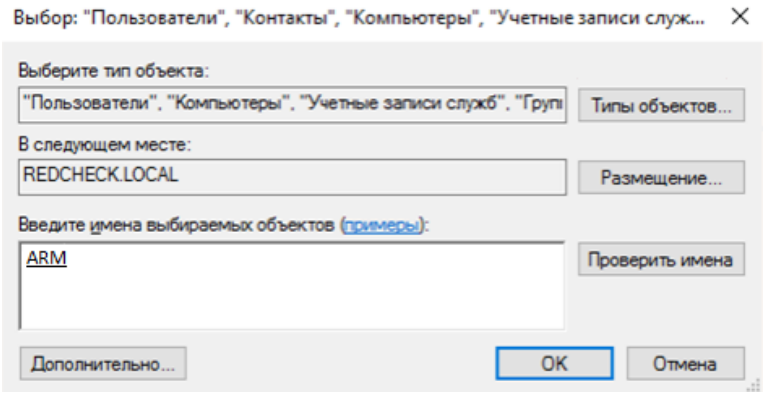
Шаг 6. Нажмите **Типы объектов**



Отметьте **Компьютеры**;

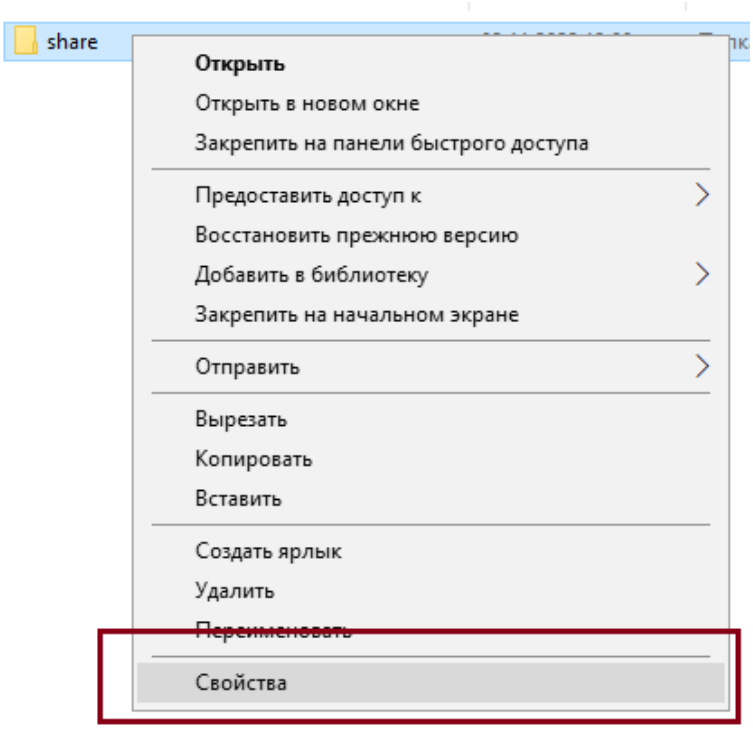


Шаг 7. Укажите имя компьютера, на котором планируется установка агента → **Проверить имена** → **OK**.

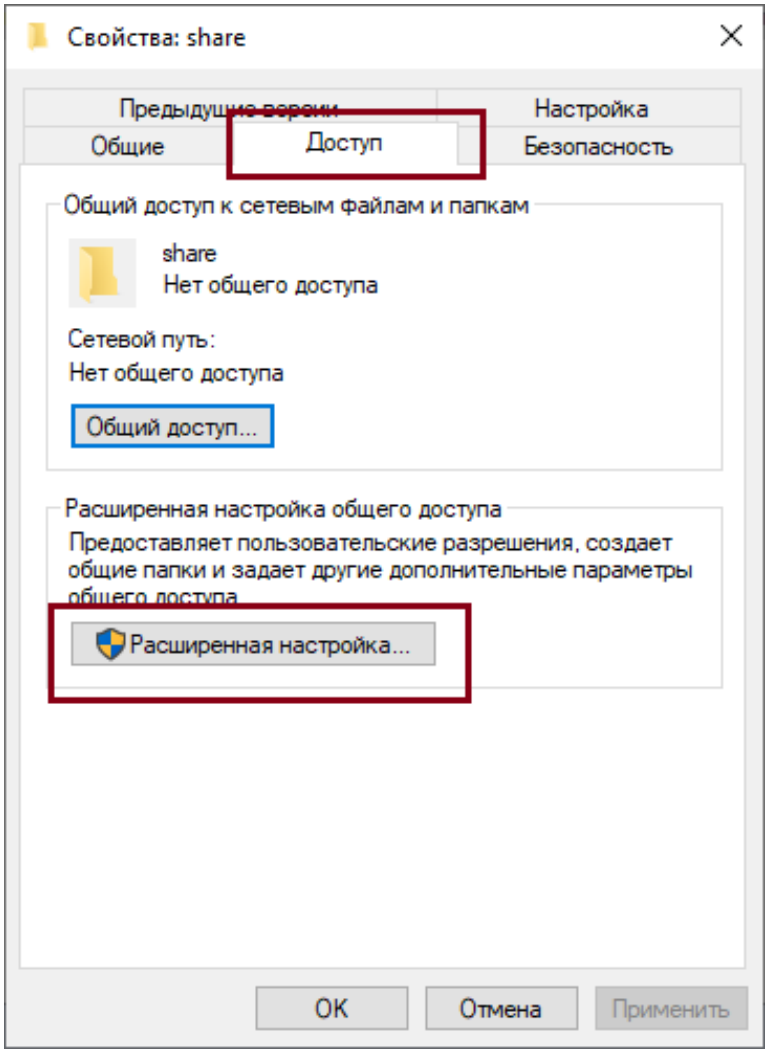


Создание и настройка сетевой папки

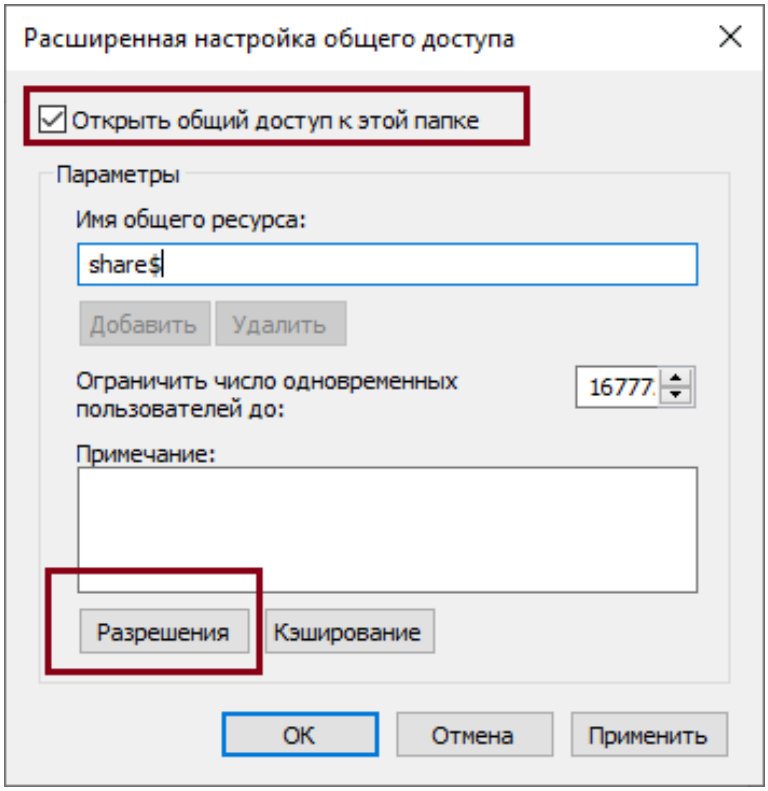
Шаг 8. Создайте директорию с произвольным названием (например, C:\share) → ПКМ по созданной директории → **Свойства**;



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

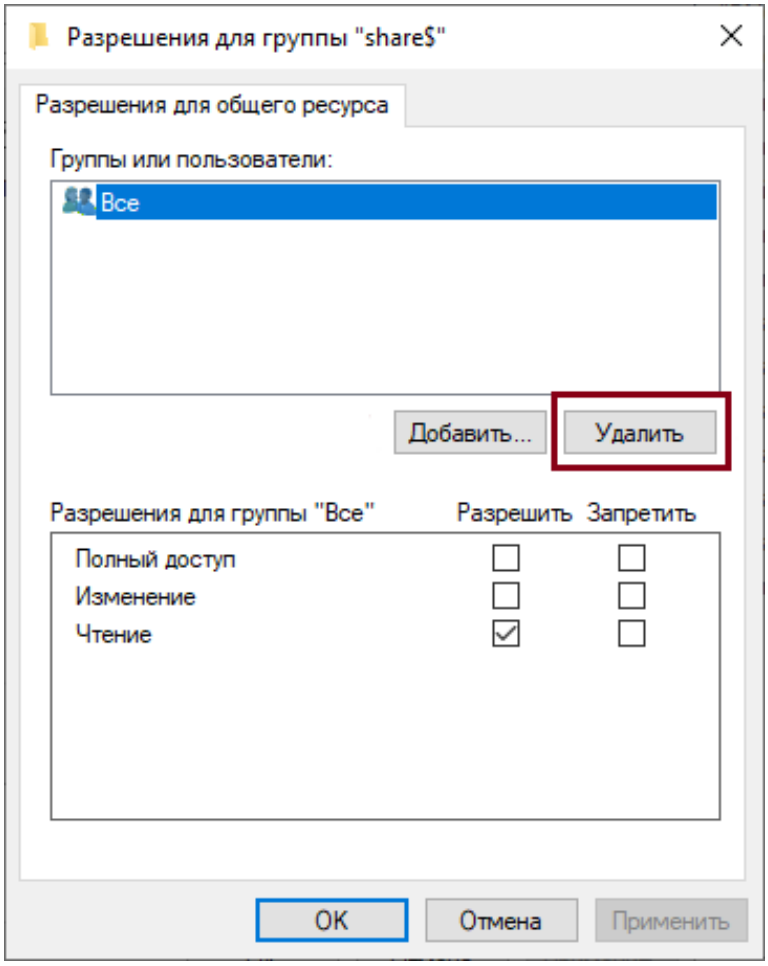


Шаг 10. Отметьте **Открыть общий доступ** → **Разрешения**;

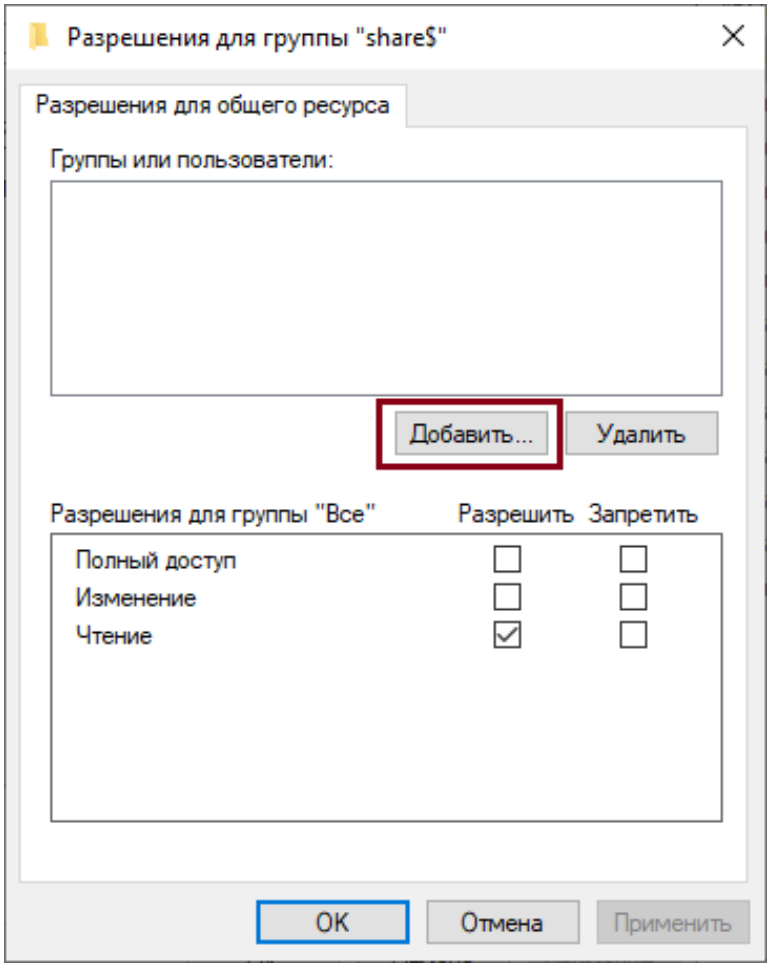


Символ **$** на конце имени папки позволяет скрыть её из сетевого окружения пользователей.

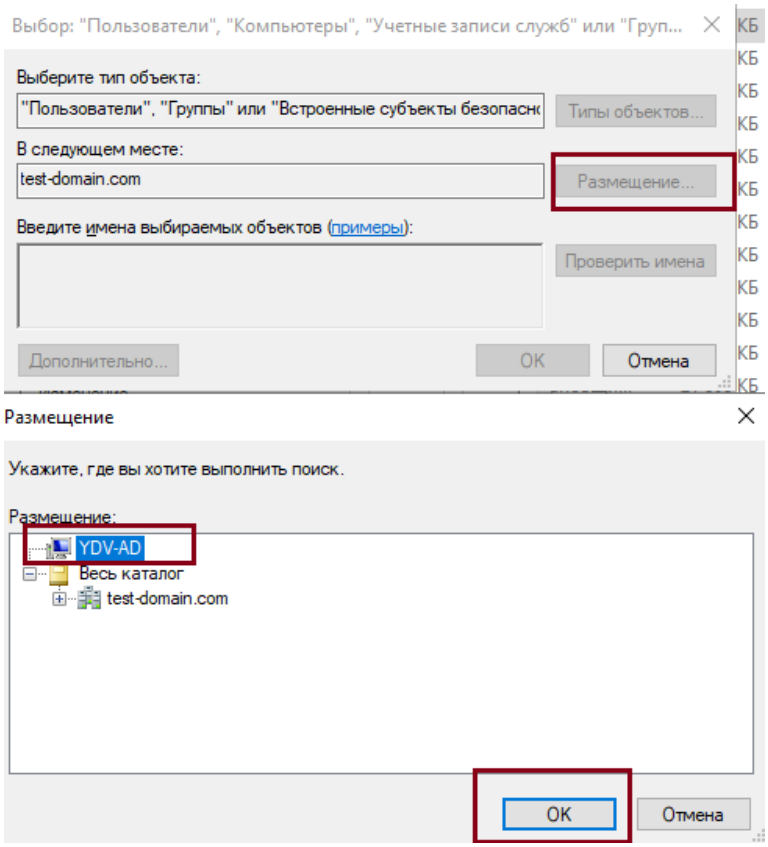
Шаг 11. Удалите группу **Все**;



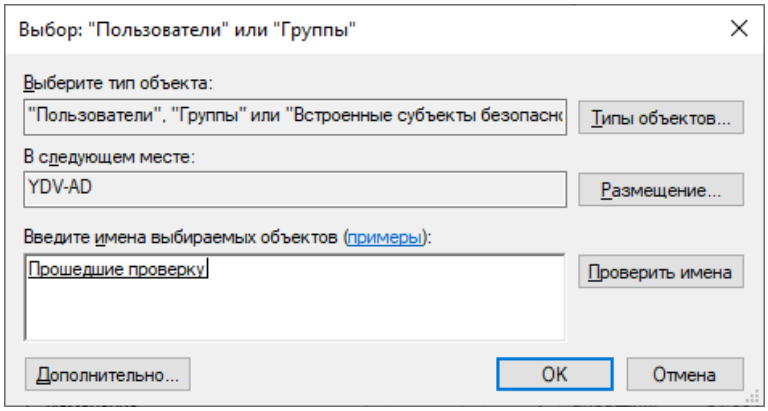
Нажмите **Добавить**;



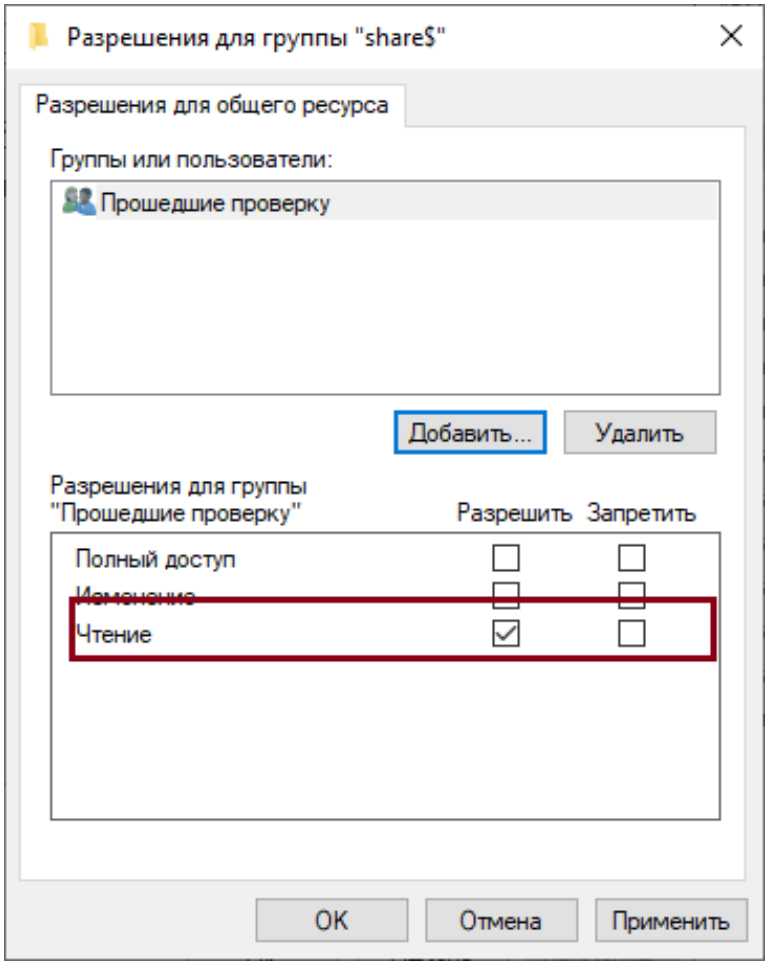
Шаг 12. Нажмите **Размещение** → выберите локальный компьютер → **OK**;



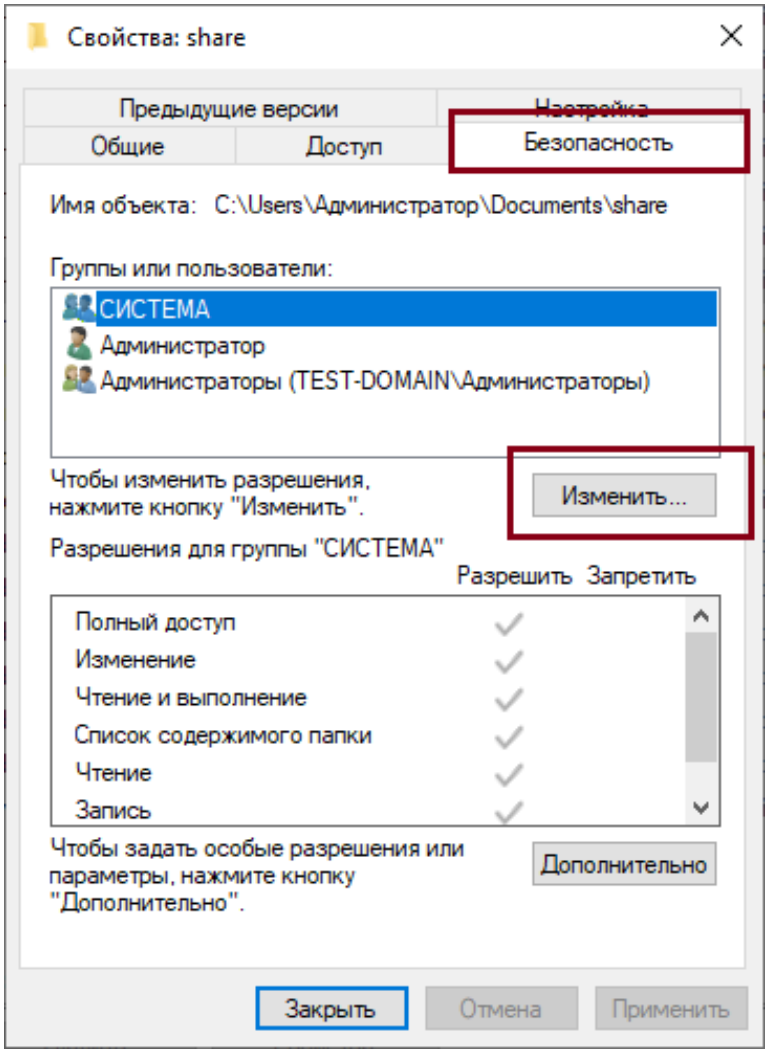
Шаг 13. Введите имя **Прошедшие проверку → Проверить имена → ОК**;



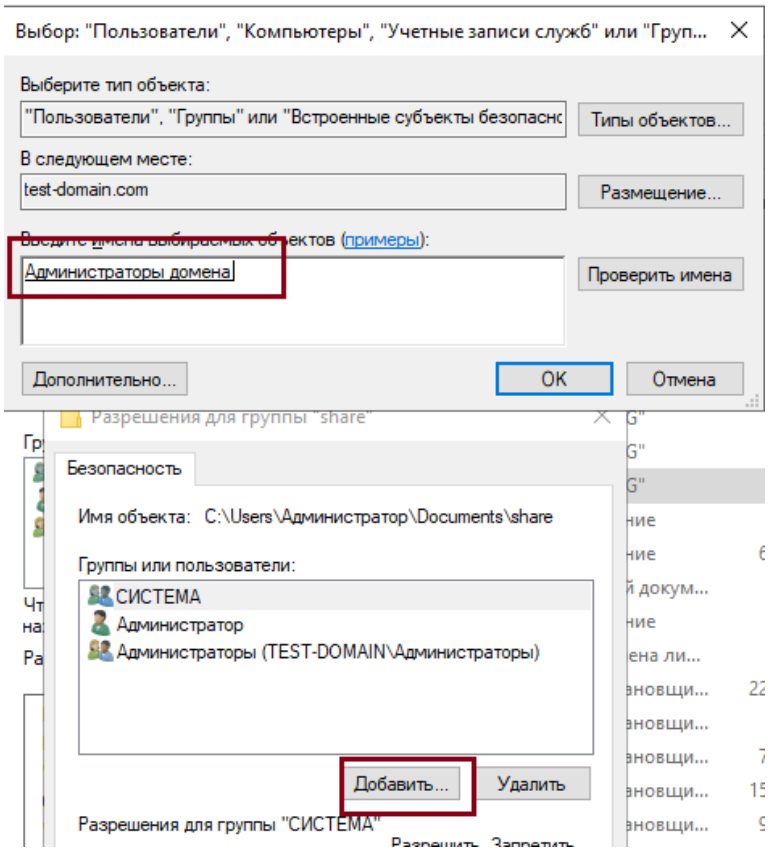
Предоставьте разрешение на **Чтение**;



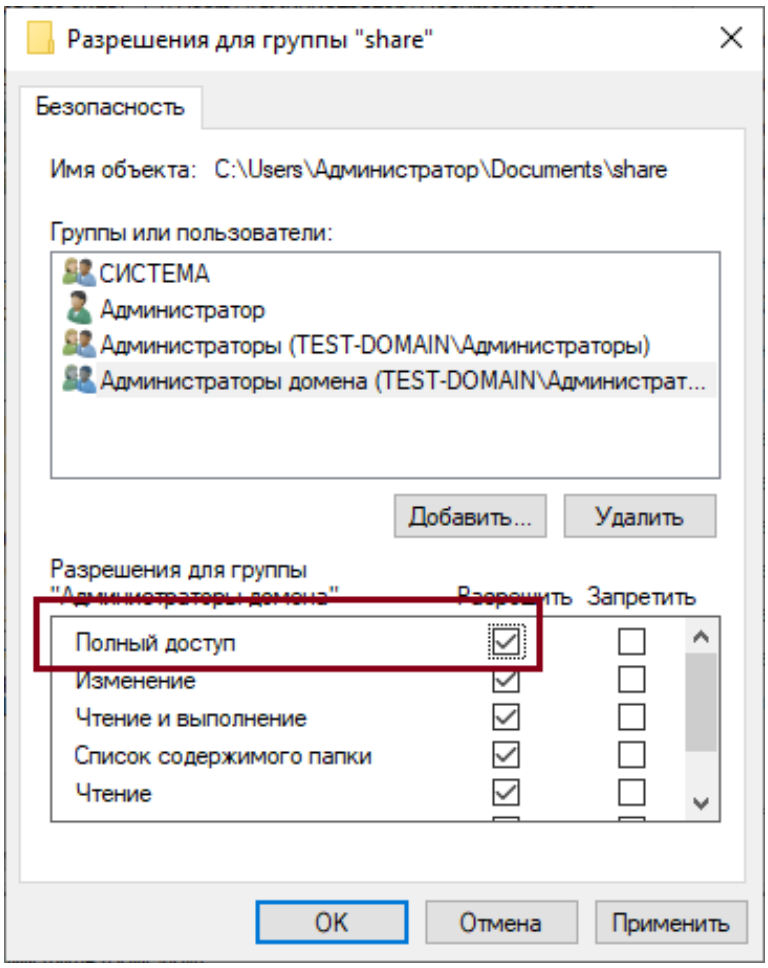
Шаг 14. В свойствах директории перейдите в **Безопасность** → **Изменить**;



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



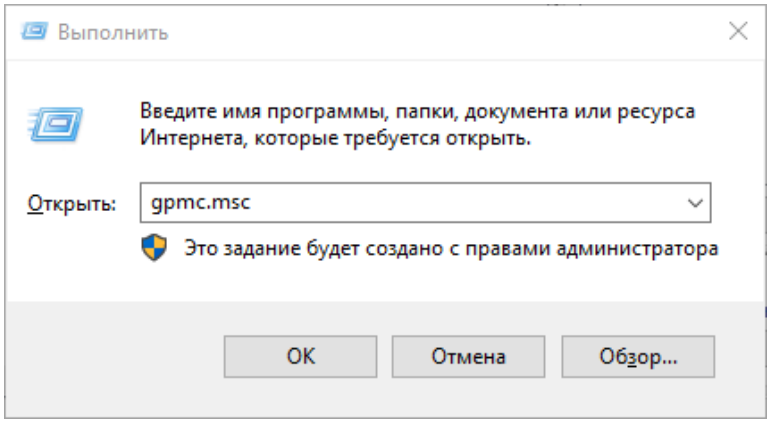
Шаг 16. Для **Администраторы домена** отметьте **Полный доступ** → **OK**;



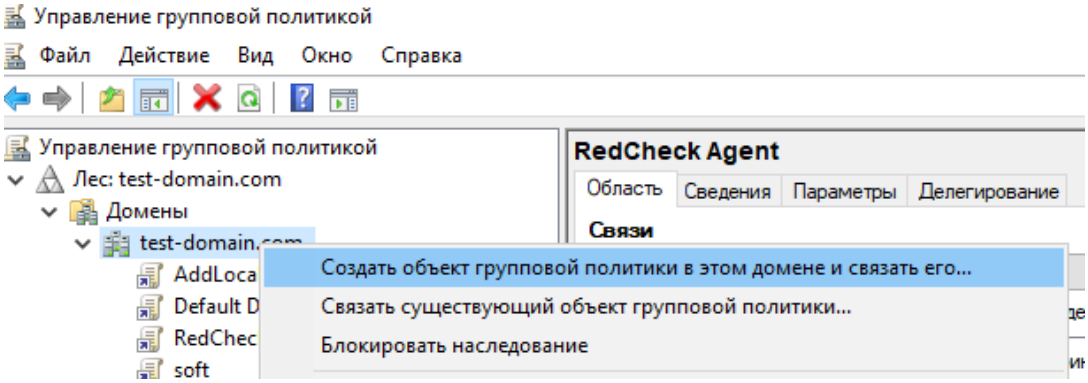
Шаг 17. Скопируйте в созданную директорию установочный файл Агента.

Настройка групповой политики

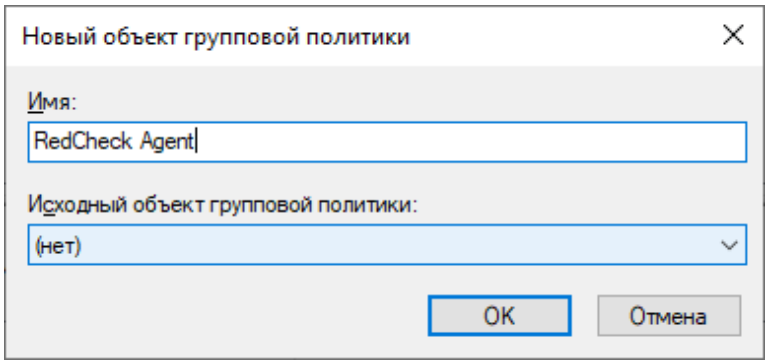
Шаг 18. Нажмите **Win + R** → введите **gpmc.msc**;



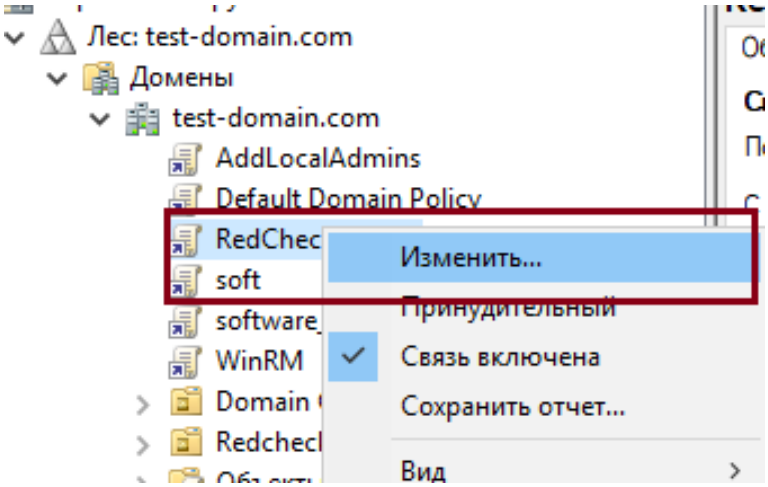
Шаг 19. Раскройте **Домены** → ПКМ по домену → **Создать объект групповой политики в этом домене...**;



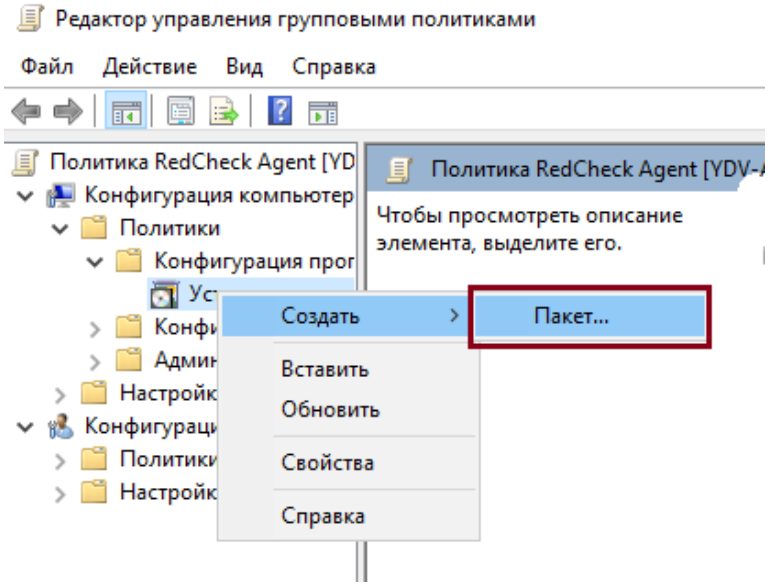
Введите имя для групповой политики → **ОК**;



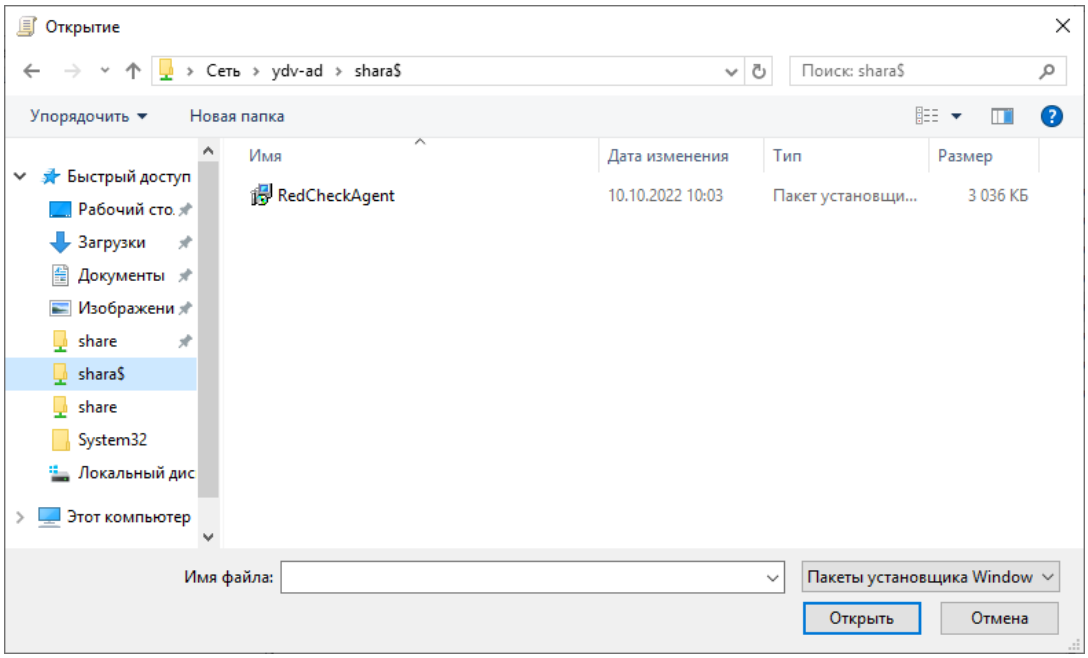
Шаг 20. ПКМ по созданной политике → **Изменить**;



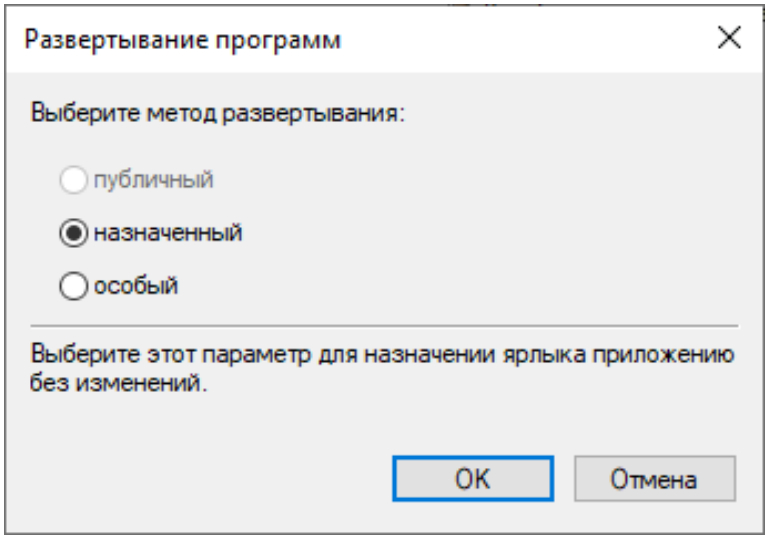
Шаг 21. Раскройте **Конфигурация компьютера** → **Политики** → **Конфигурация программ** → ПКМ по **Установка программ** → **Создать** → **Пакет**;



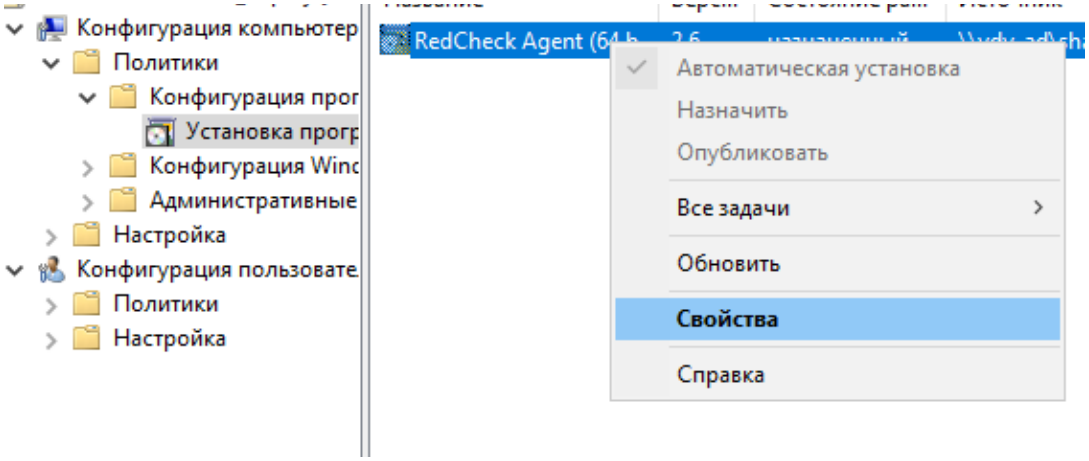
Шаг 22. Введите в адресной строке путь к сетевой папке: **\\<имя_компьютера>\<имя_папки>$** → выберите установочный файл Агента;



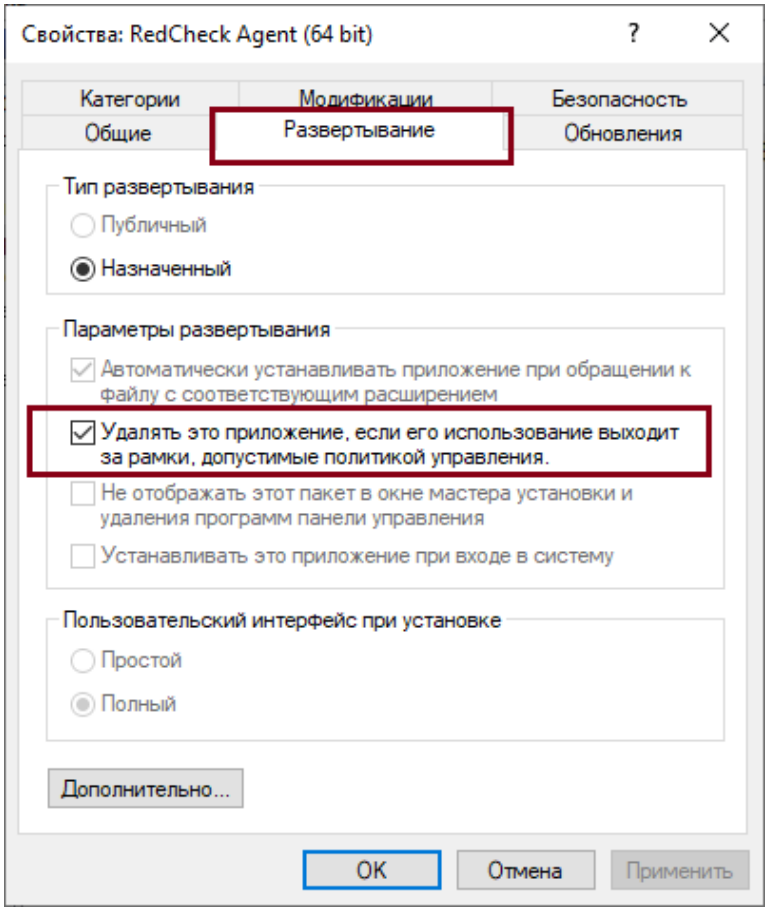
Метод развертывания – **назначенный**;



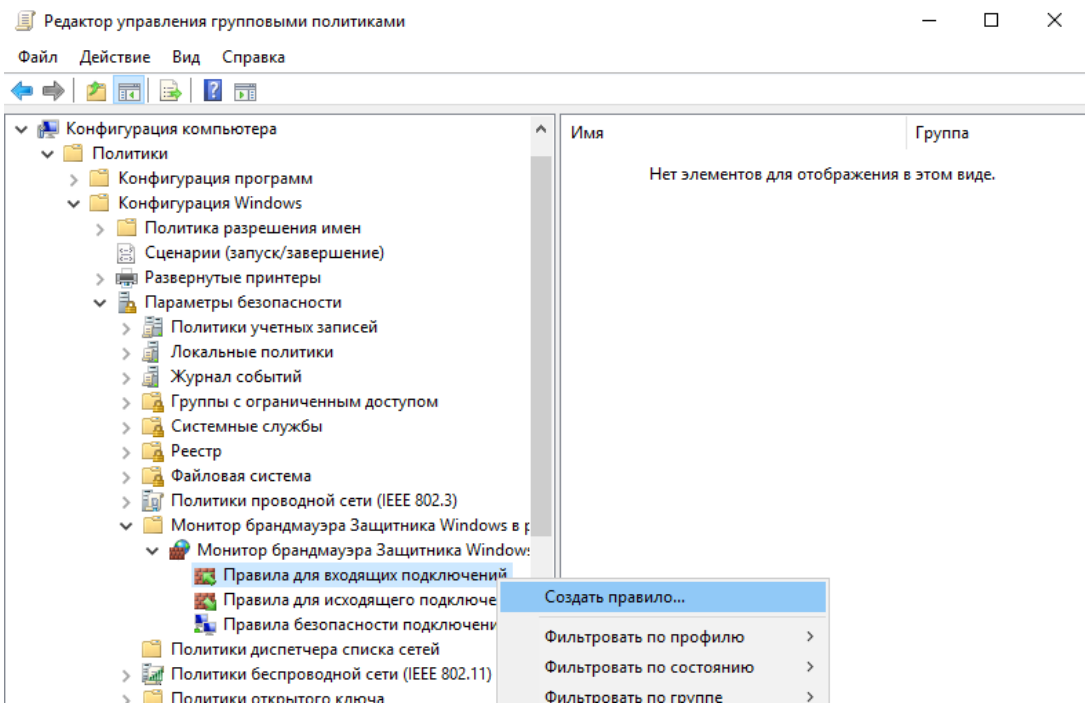
Шаг 23. ПКМ по появившемуся установочному файлу → **Свойства**;



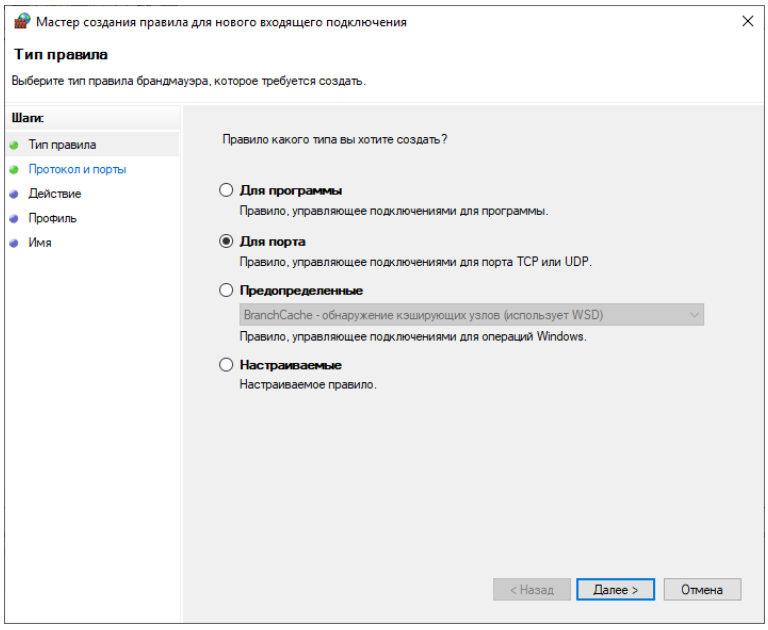
Шаг 24. В **Развертывание** отметьте **Удалять это приложение, если его использование...** → **ОК**;



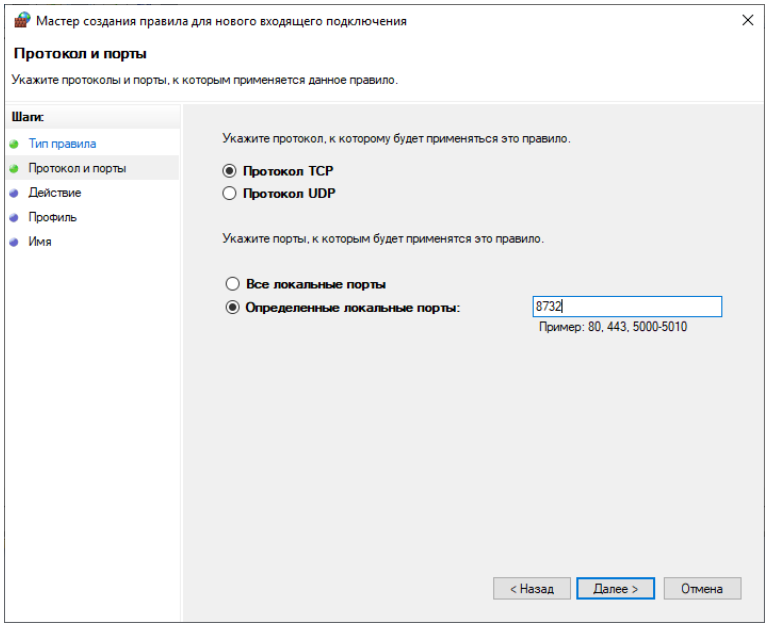
Шаг 25. Перейдите в **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Монитор брандмауэра Защитника Windows...** → ПКМ по **Правила для входящих подключений** → **Создать правило...**;



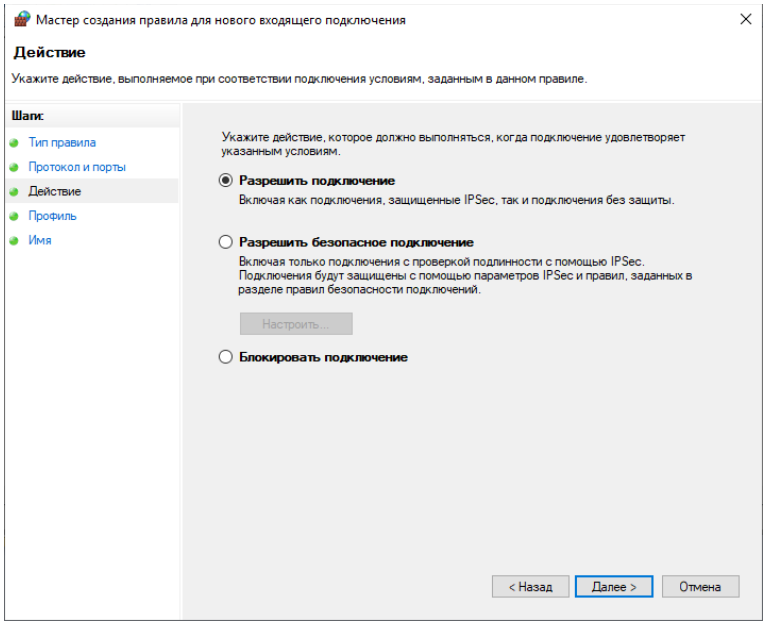
Шаг 26. Укажите тип правила **Для порта** → **Далее**;



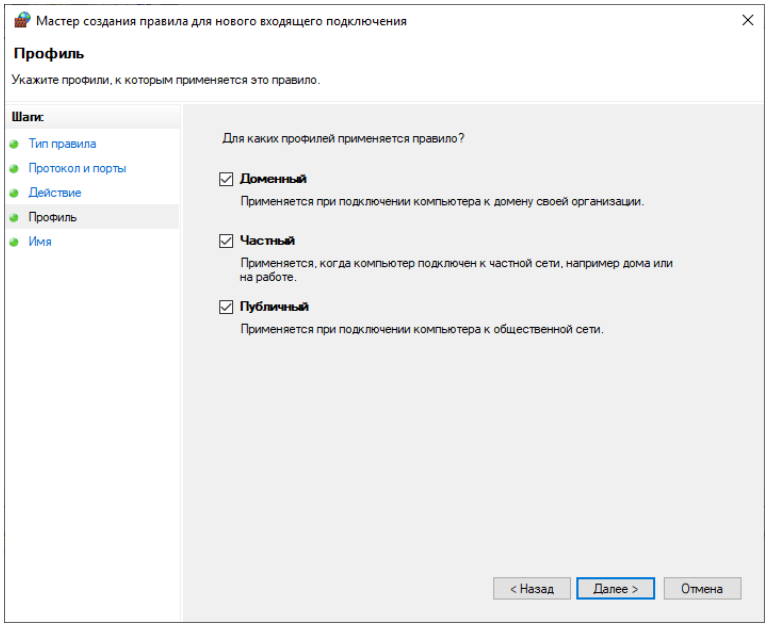
Отметьте **ПротоколTCP** → укажите порт Агента (по умолчанию **8732)** → **Далее**;



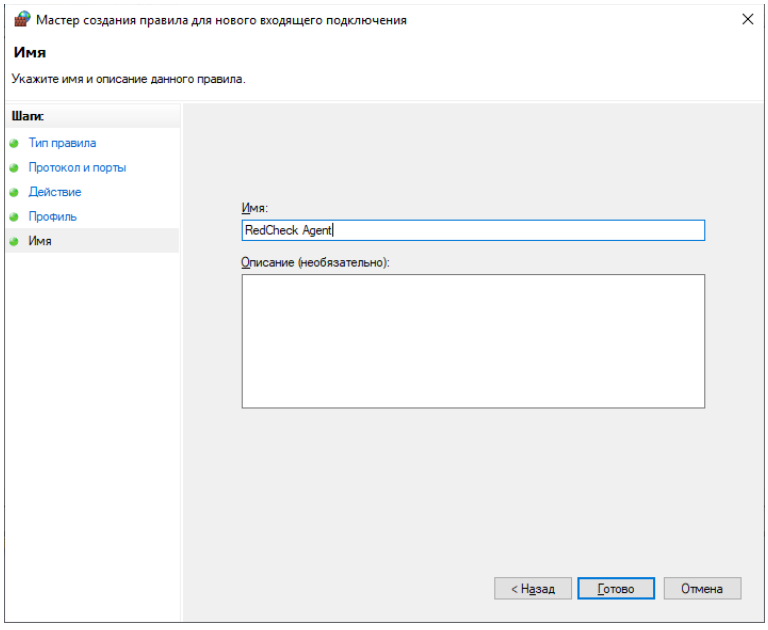
Выберите **Разрешить подключение** → **Далее**;



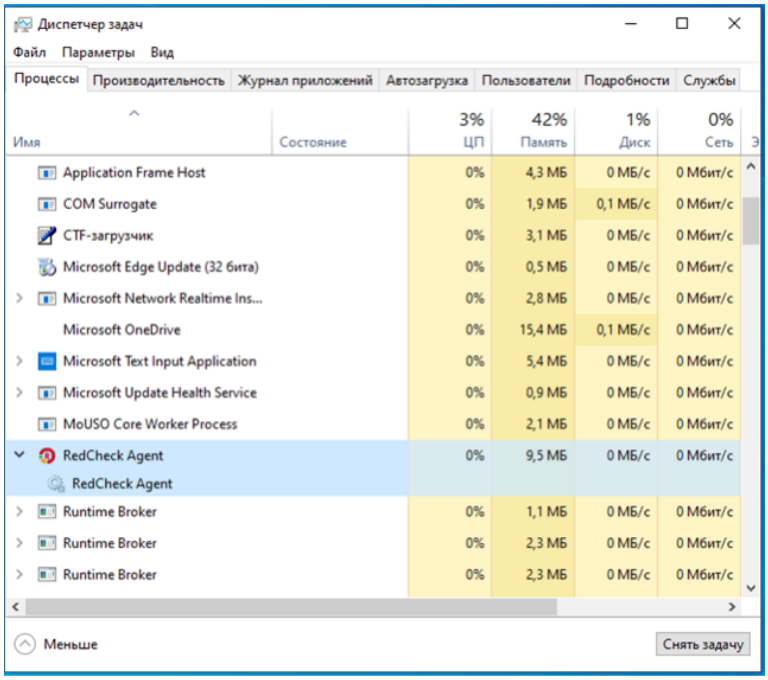
Выберите профили для применения правила (рекомендуется оставить по умолчанию) → **Далее**;



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**.



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 компонентов

Под раздельной установкой компонентов подразумевается инсталляция одного из компонентов отдельно от остальных. Это может быть необходимо, например, при установке дополнительной службы сканирования.

Перед инсталляцией необходимо добавить репозиторий RedCheck в пакетный менеджер:

- Astra Linux: шаги с 1 по 6 (Инсталляция RedCheck)
- РЕД ОС: шаги с 1 по 8 (Инсталляция RedCheck)
- SberLinux: шаги с 1 по 6 (Инсталляция RedCheck)

Для инсталляции компонента установите нужные пакеты. Например, если необходимо установить службу сканирования, то пакетами для инсталляции будут **redcheck-scan-service** и **redcheck-dotnet-runtime**

Bash (оболочка Unix)

```
sudo apt install redcheck-dotnet-runtime redcheck-scan-service
```

После проведите конфигурацию компонента:

Bash (оболочка Unix)

```
sudo redcheck-bootstrap configure -c=all
```

Инсталлятор предложит сконфигурировать только установленные в системе пакеты.

4 Сопровождение Системы

Содержание

4.1 Настройка ролевой модели

Для корректного распределения прав доступа ознакомьтесь с перечнем возможностей каждой из ролей (1.4 Ролевая модель RedCheck).

Создание пользователя

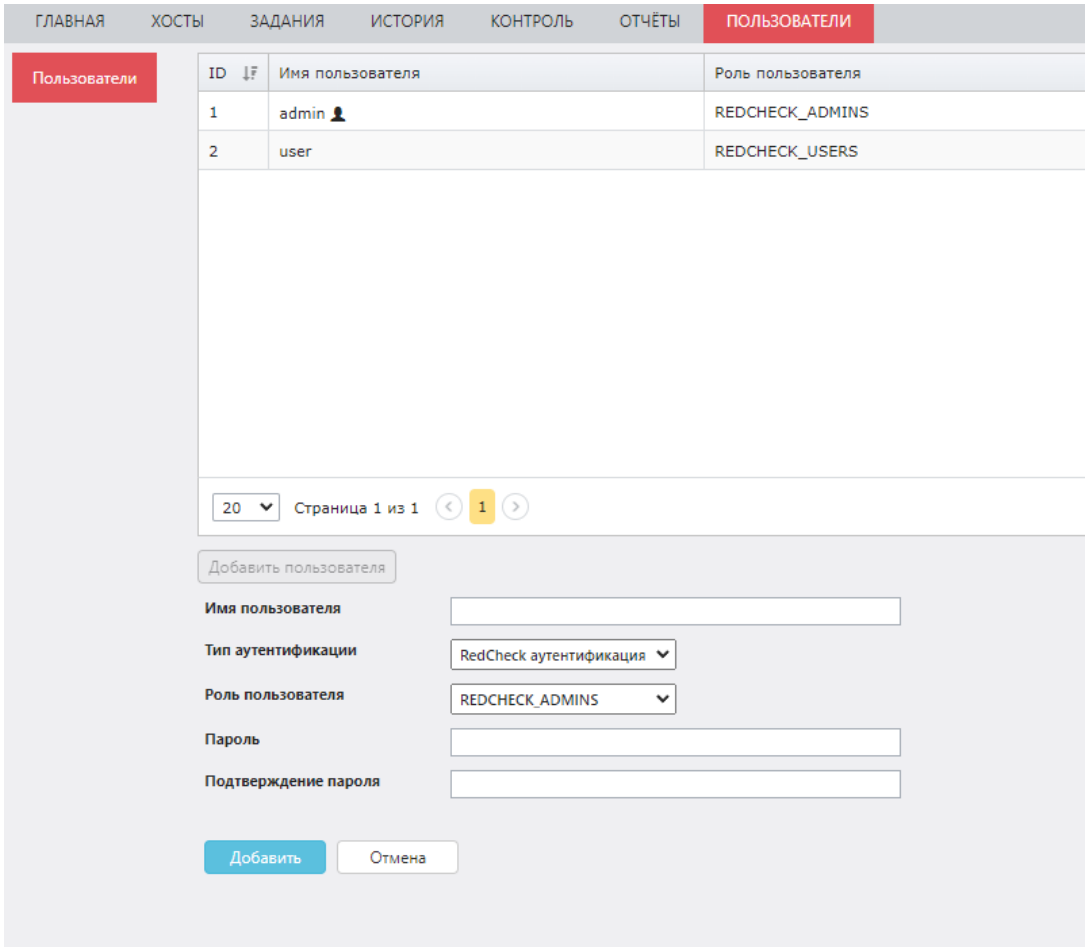
Добавить пользователя может только пользователь с ролью Admins.

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

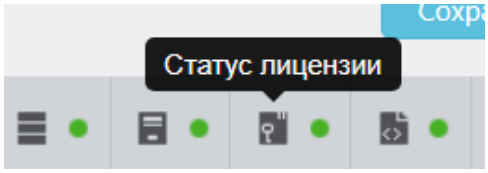


Редактирование: нажмите ⚙ → **Редактировать**.

Удаление: нажмите ⚙ → **Удалить**;

4.2 Активация лицензии

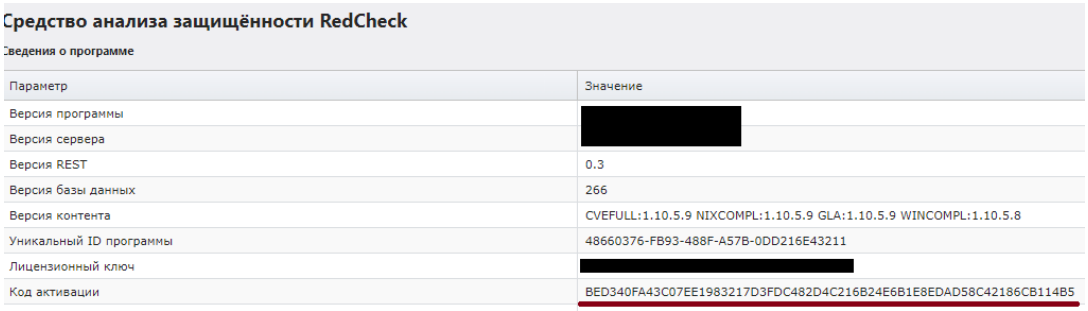
Статус лицензии отображается на статусной панели:



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

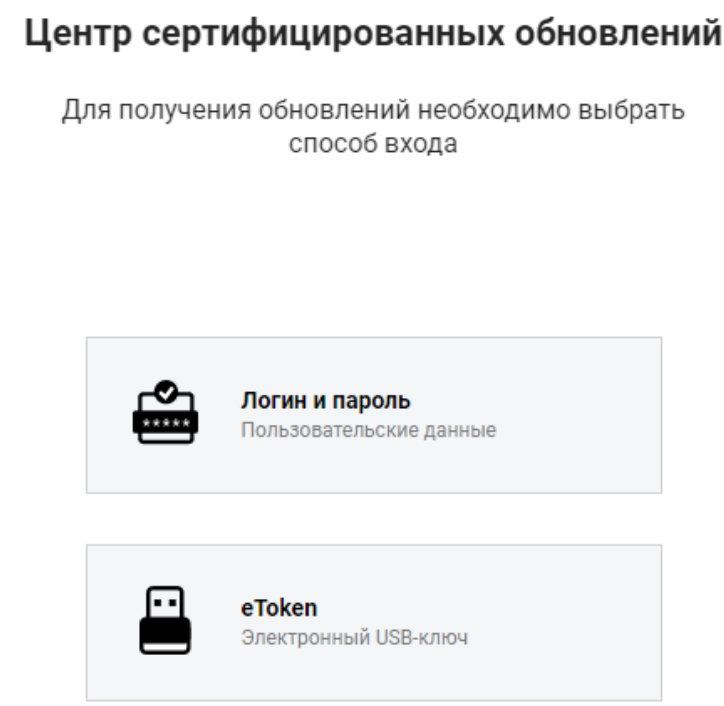
Сведения о программе

Параметр	Значение
Версия программы	[redacted]
Версия сервера	
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	BED340FA43C07EE1983217D3FDC482D4C216B24E6B1E8EDAD58C42186CB114B5

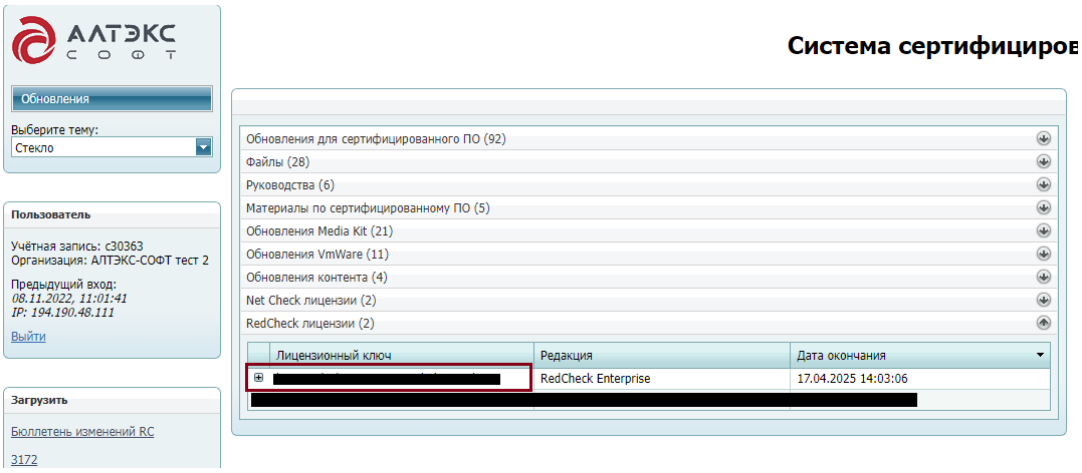
> Код активации также можно получить во время установки (Конфигурация RedCheck).

Шаг 2. Авторизуйтесь в Центре сертифицированных обновлений с помощью логина и пароля;

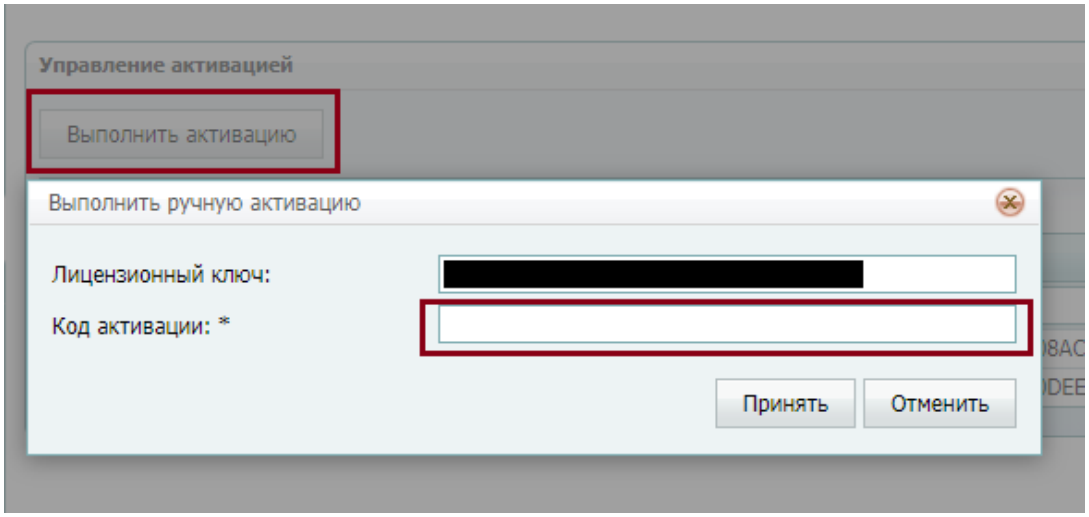
> Логин/пароль поставляется всем коммерческим клиентам в разделе 15, «Особые отметки» (начиная с 18.05.2022).



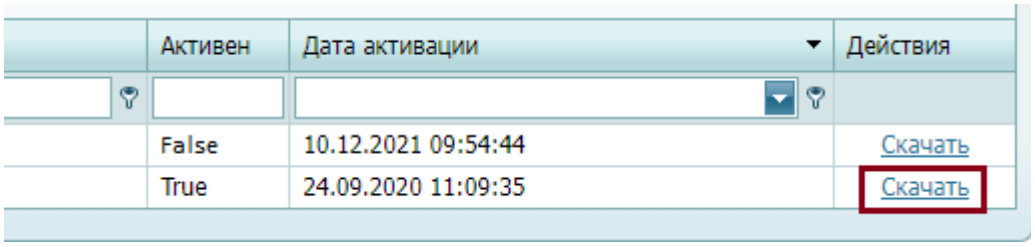
Шаг 3. Раскройте **RedCheck лицензии** → выберите интересующий Вас номер ключа RedCheck;



Нажмите **Выполнить активацию** → введите ранее скопированный код активации → **Принять**;



Шаг 4. Нажмите **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:

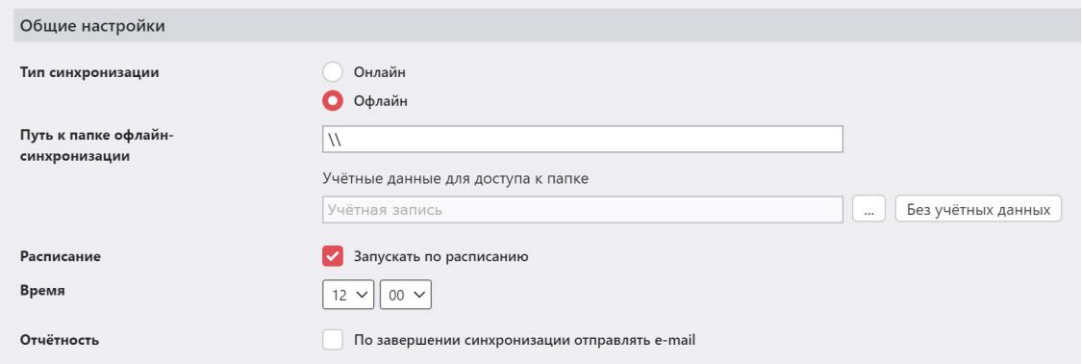
Bash (оболочка Unix)

```
sudo chown redcheck:redcheck /var/opt/redcheck-sync-service/data/license.xml
```

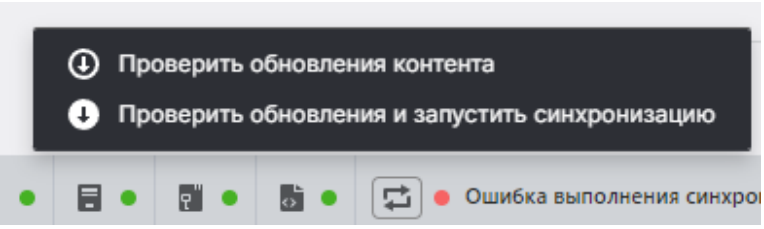
Директория может находиться в произвольном месте в инфраструктуре сети и должна быть доступна для чтения хостом, на котором установлена служба синхронизации. В случае сетевой папки указывается учетная запись RedCheck, пользователь которой имеет разрешение на чтение.

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;



Шаг 7. 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.

4.3 Обновление контента информационной безопасности

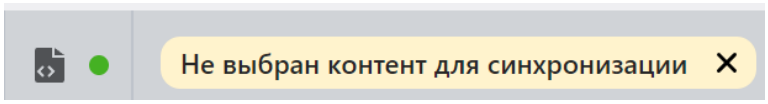
Перед началом работы в RedCheck необходимо обновить контент ИБ. Загрузка обновлений осуществляется посредством синхронизации с внешним сервером обновлений АО «АЛТЭКС-СОФТ».

Содержание

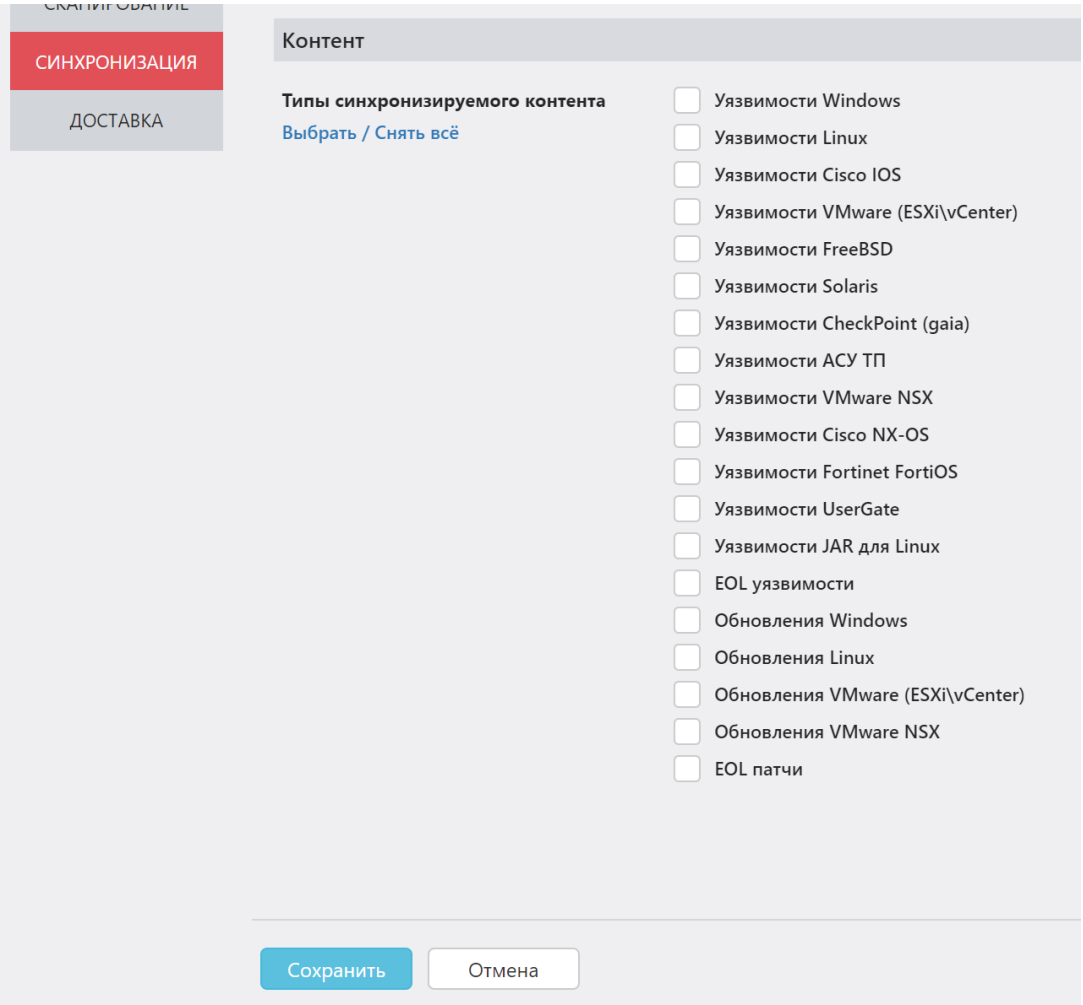
4.3.1 Синхронизация через сеть Интернет

Данный способ является предпочтительным и осуществляется по умолчанию.

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

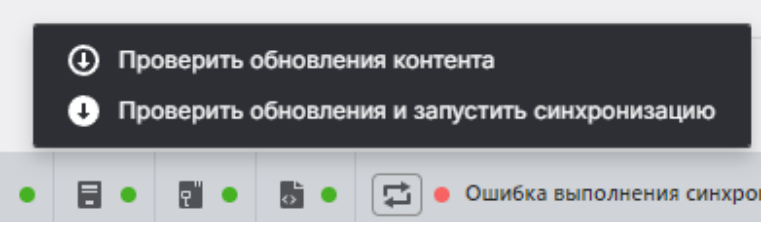


Шаг 1. После установки RedCheck необходимо выбрать контент, который будет синхронизироваться. Для этого нажмите **Инструменты** → **Настройки** → **Синхронизация**;

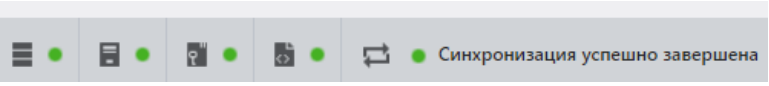


Выберите нужный контент и нажмите **Сохранить**;

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.

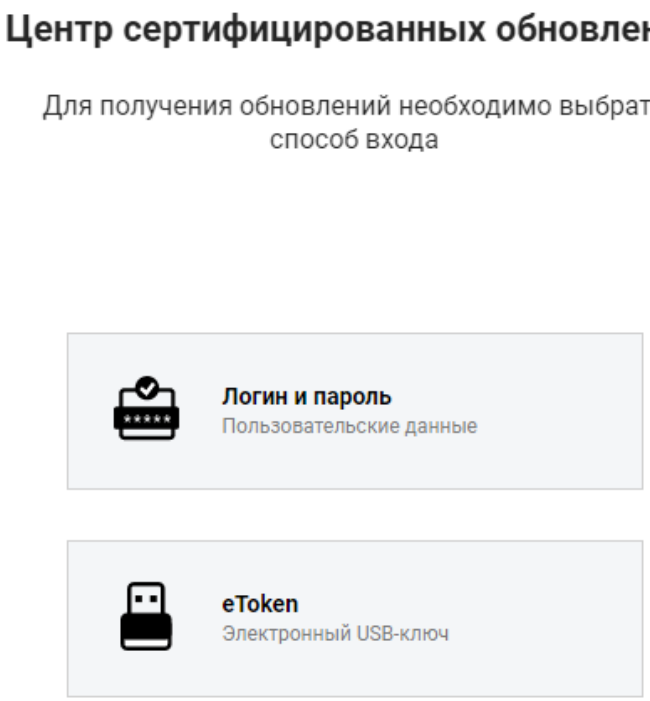


4.3.2 Офлайн-синхронизация

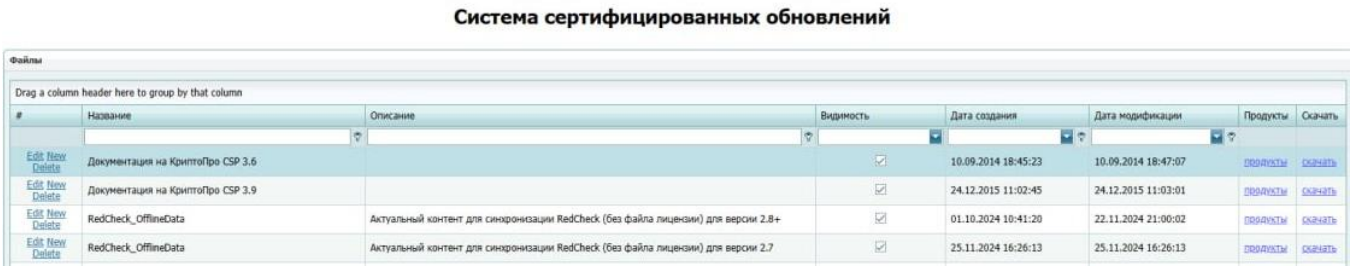
В случае отсутствия доступа к сети Интернет обновление контента ИБ осуществляется посредством архива с необходимым контентом.

Шаг 1. Авторизуйтесь в Центре сертифицированных обновлений с помощью логина и пароля;

> Логин/пароль поставляется всем коммерческим клиентам в разделе 15, «Особые отметки» (начиная с 18.05.2022).



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

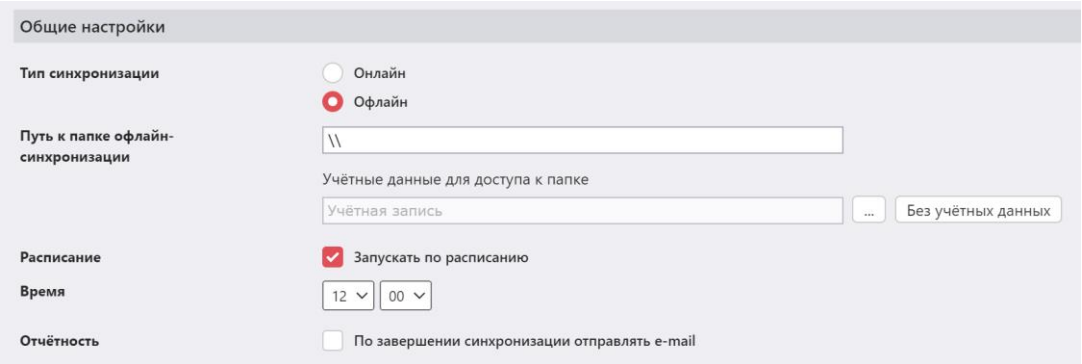


Шаг 3. Распакуйте архив в директорию для офлайн-синхронизации (по-умолчанию **/var/opt/redcheck-sync-service/data**);

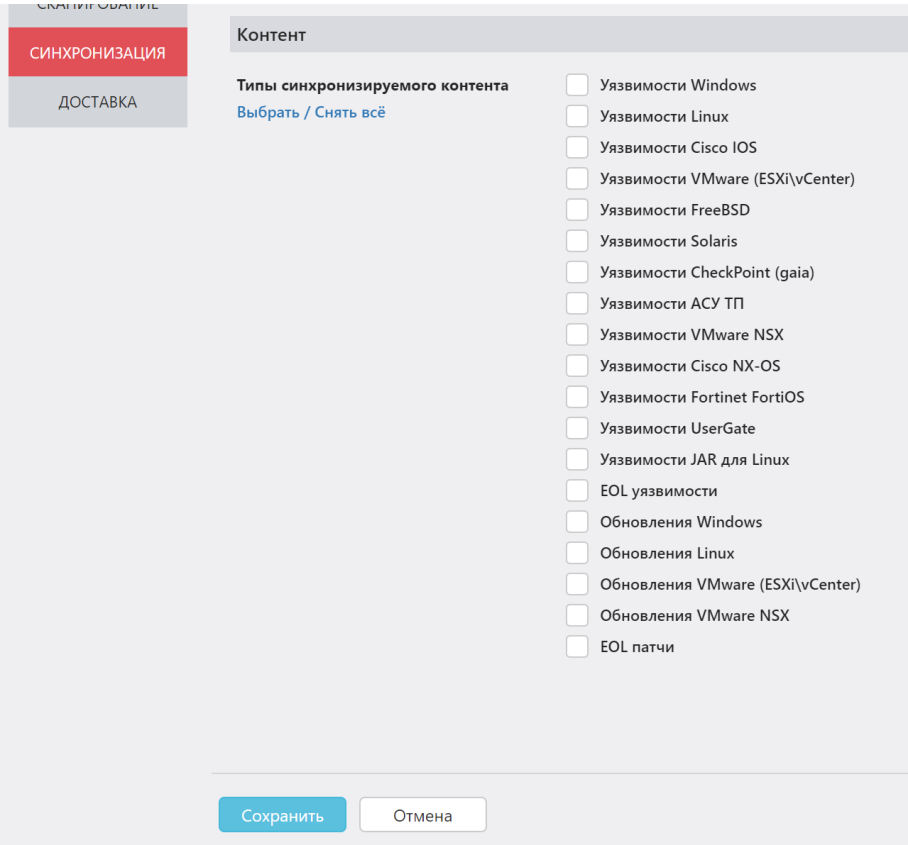
> Директория может находиться в произвольном месте в инфраструктуре сети и должна быть доступна для чтения хостом, на котором установлена служба синхронизации. В случае сетевой папки указывается учетная запись RedCheck, пользователь которой имеет разрешение на чтение.

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;

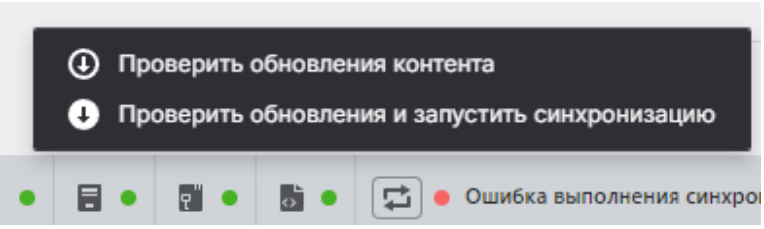


Тут же можно выбрать нужный контент для синхронизации;



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.

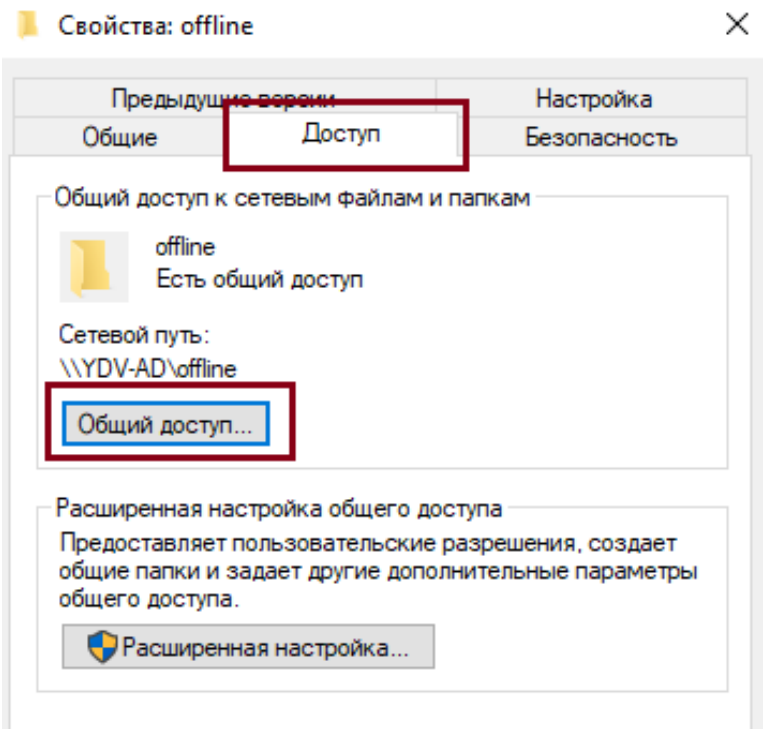
Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.

4.3.3 Синхронизация через RedCheck Update Server

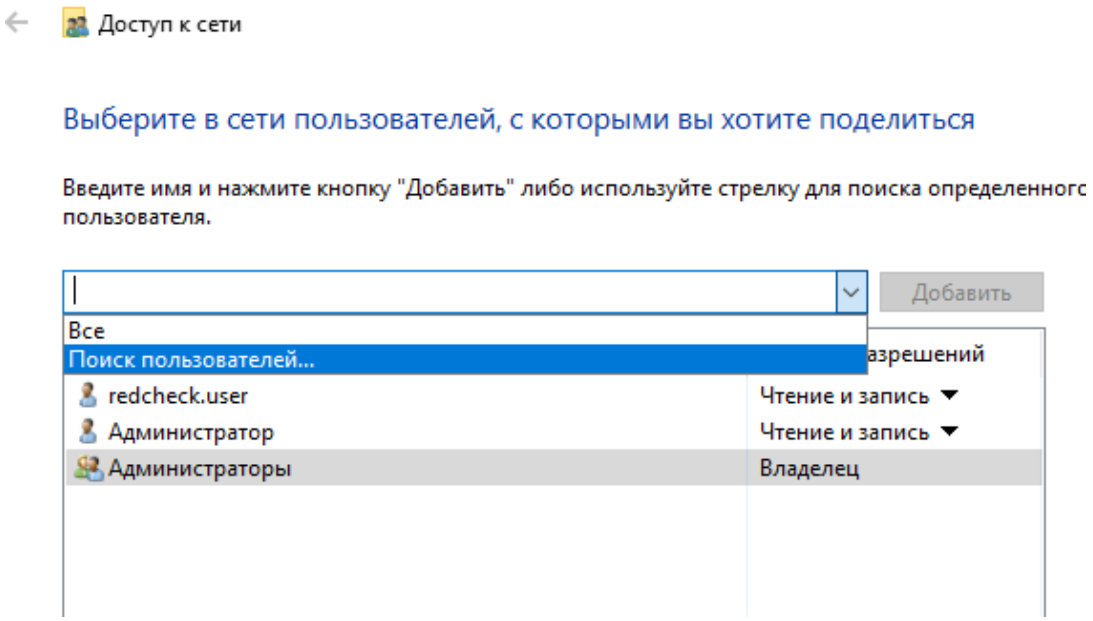
> Более подробная инструкция по работе с компонентов находится в отдельном Руководстве.

Шаг 1. Создайте на хосте с установленным RedCheck Update Server в DMZ-сегменте директорию с произвольным названием и местоположением. В данной инструкции создается директория **offline** (C:\offline);

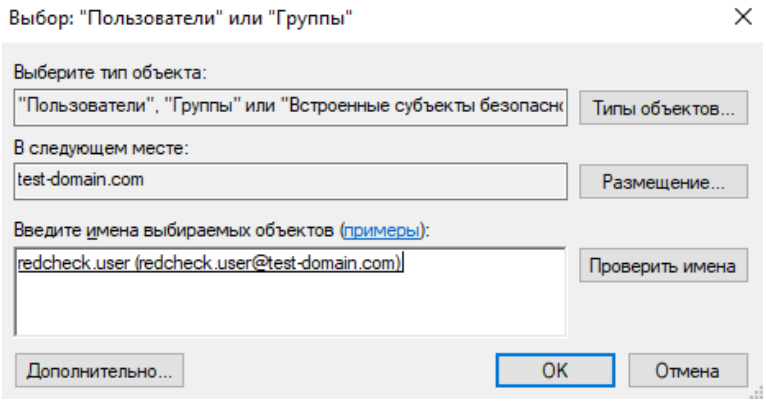
Шаг 2. ПКМ по созданной директории→ **Свойства** → **Доступ** → **Общий доступ**;



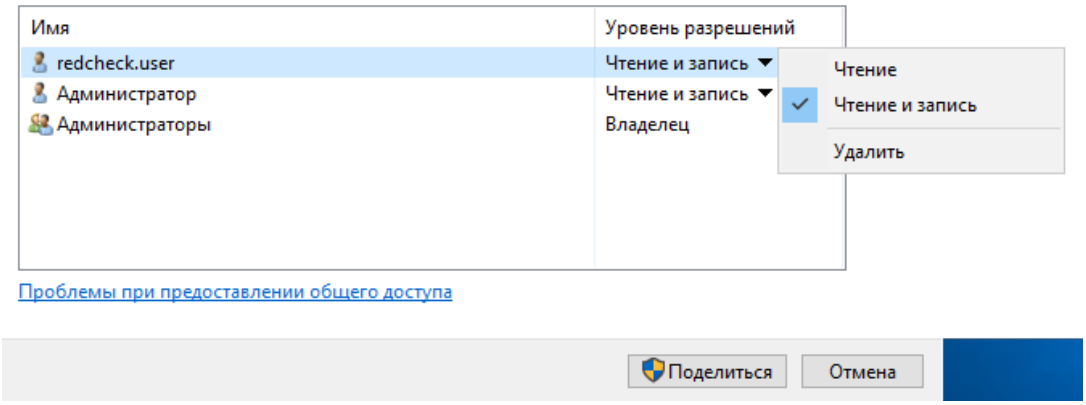
Раскройте список → **Поиск пользователей**;



Укажите имя пользователя, который будет иметь доступ к созданной директории с контентом → **OK**;



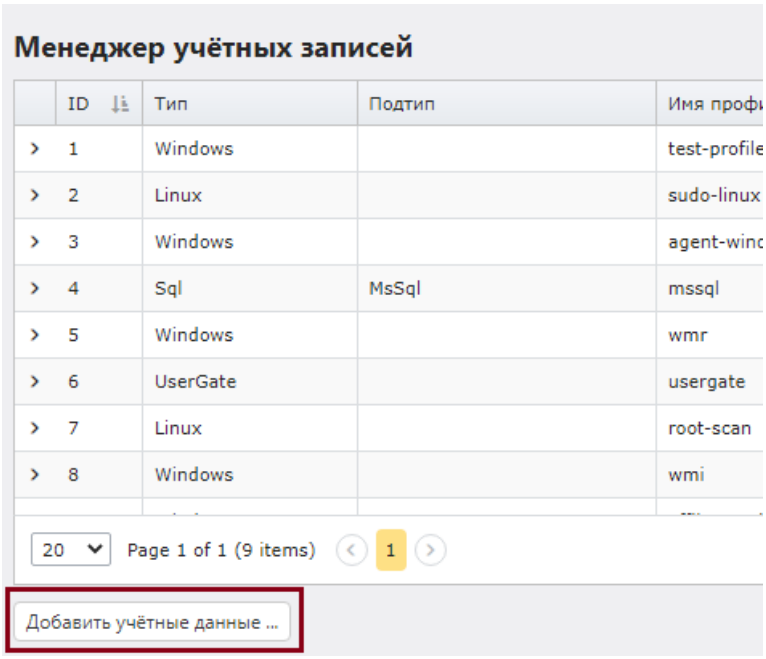
Предоставьте разрешения на **Чтение и запись** → **Поделиться;**



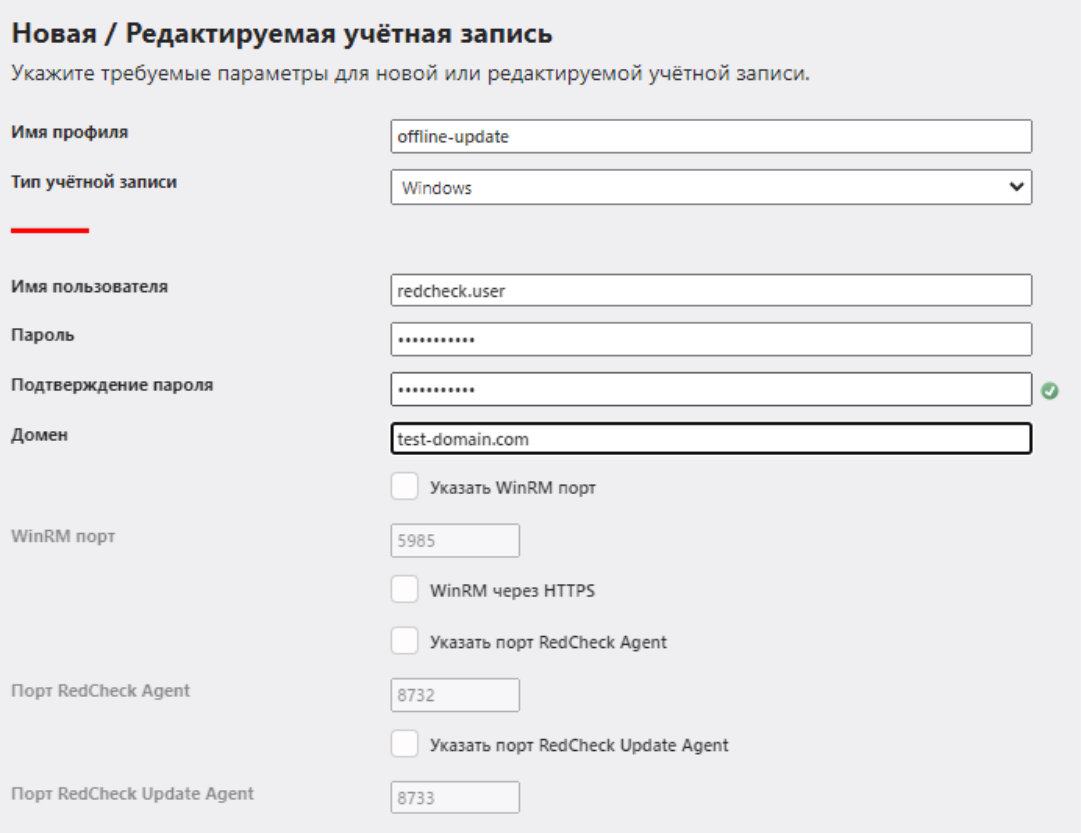
Шаг 3. Откройте консоль управления RedCheck → на панели навигации выберите **Инструменты** → **Менеджер учетных записей**;

> Для изменения настроек RedCheck авторизуйтесь под УЗ с ролью **REDCHECK_SYSTEMS** или **REDCHECK_ADMINS**

Нажмите **Добавить учетные данные;**

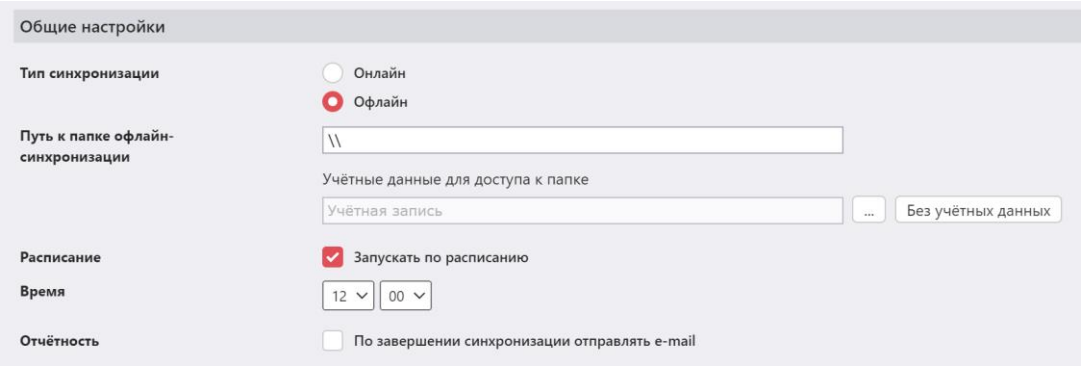


Выберите **Тип учетной записи** – **Windows.** Укажите учетные данные пользователя, у которого есть доступ к сетевой папке → **Сохранить**;

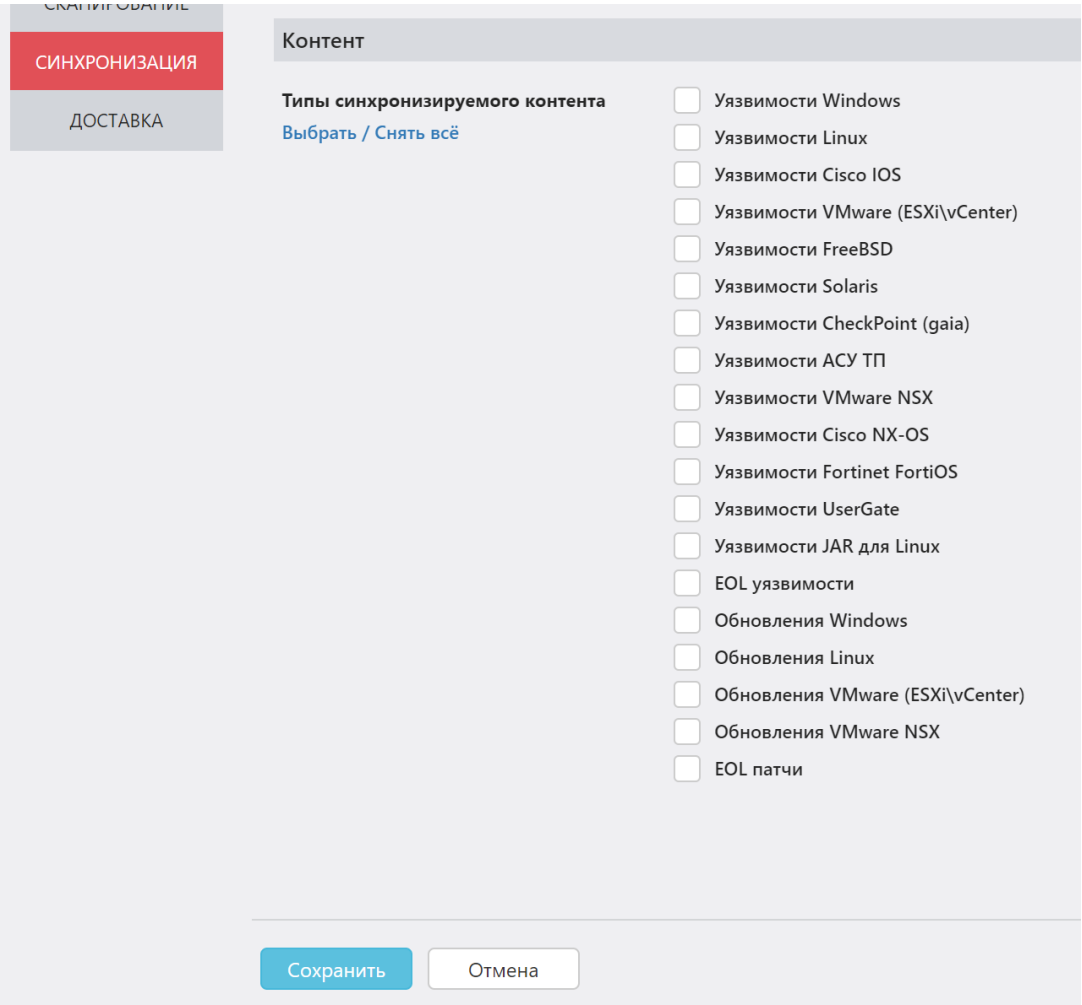


Шаг 4. На панели навигации выберите **Инструменты** → **Настройки** → **Синхронизация**:

- Выберите **Офлайн** и отметьте **Запускать по расписанию**, указав по необходимости время;
- Укажите путь к сетевой папке
- Выберите ранее созданную учетную запись;

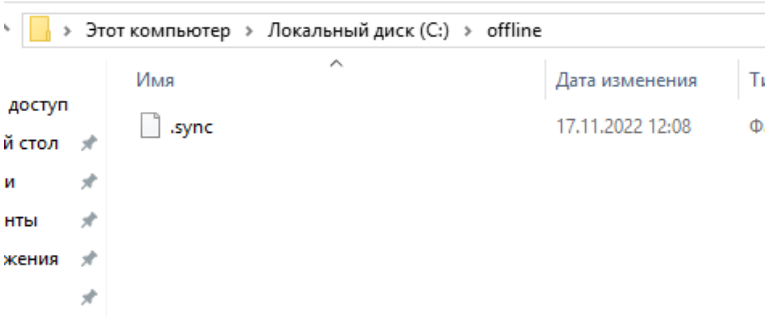


Тут же можно выбрать нужный контент для синхронизации;

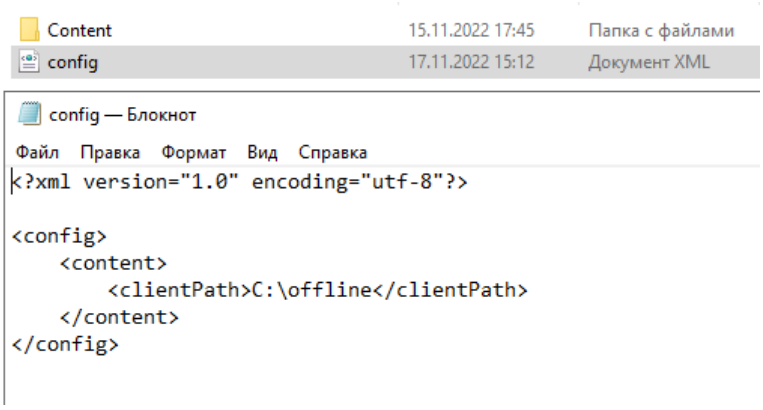


Шаг 5. Нажмите **Сохранить** для внесения изменений;

После сохранения и проверки доступа в сетевой папке в ней появится файл **.sync**;



Шаг 6. Перейдите в директорию C:\ProgramData\ALTEX-SOFT\RedCheckUpdateServer → отредактируйте файл **config.xml**, добавив строку **<clientPath>адрес_директории_для_синхронизации</clientPath>**

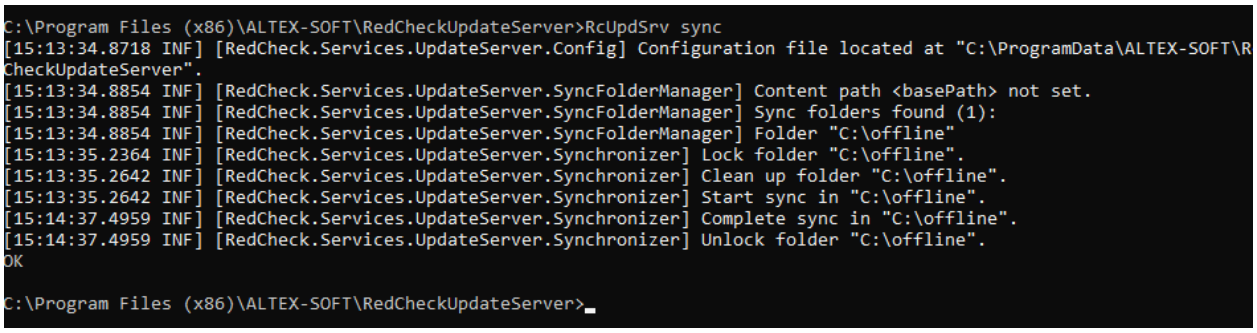


Шаг 7. Перейдите в директорию с установленным RedCheckUpdateServer (по умолчанию C:\ProgramFiles (x86)\ALTEX-SOFT\RedCheckUpdateServer) → введите в поле для адреса **cmd** → выполните команду:

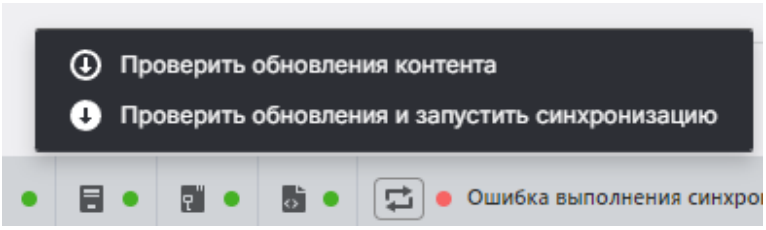
Код

```
RcUpdSrv sync
```

Начнется скачивание недостающего контента ИБ;



Шаг 8. Откройте консоль управления RedCheck → нажмите на статусной панели кнопку синхронизации → **Проверить обновления и запустить синхронизацию**;



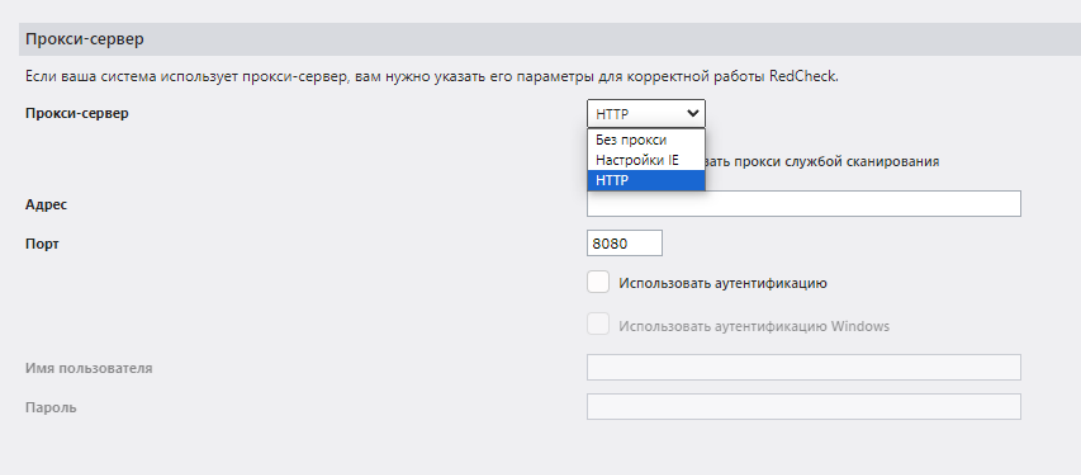
Статус синхронизации отображается на статусной панели. Для создания новых заданий необходимо дождаться завершения процесса.

4.3.4 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**.

4.4 Настройка учетных записей для сканирования

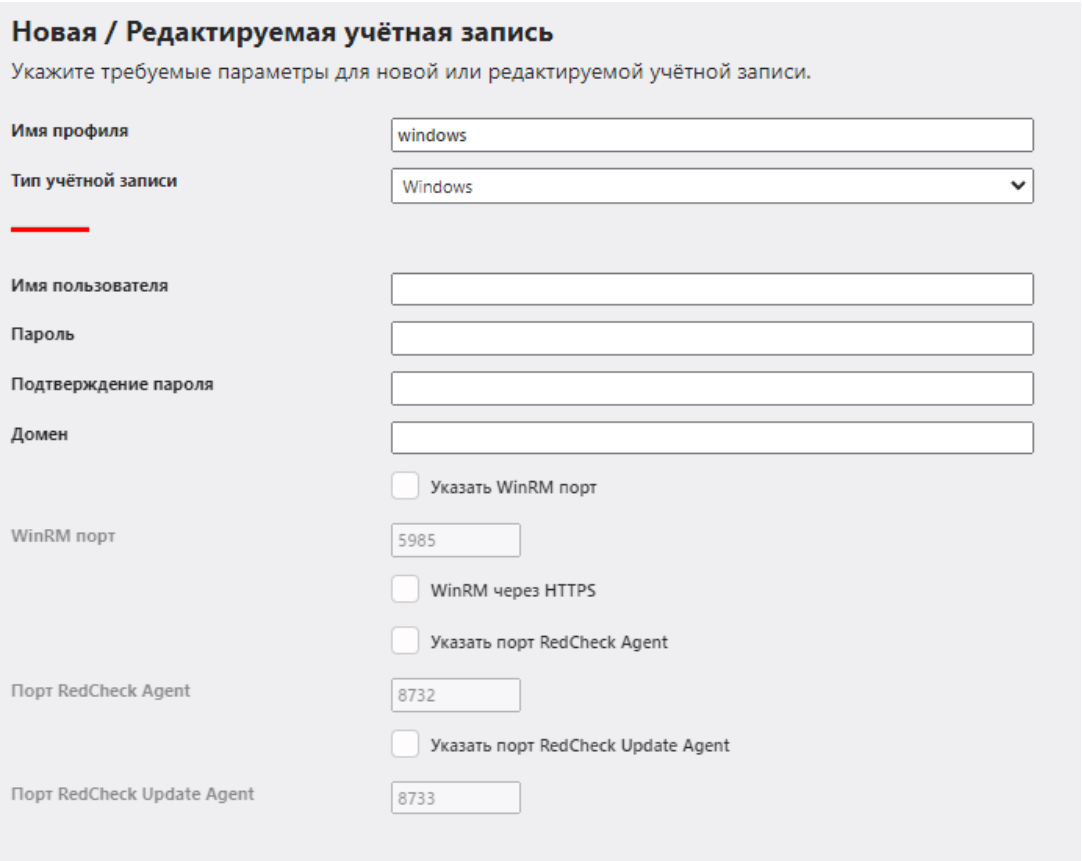
Рекомендуется:

- 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

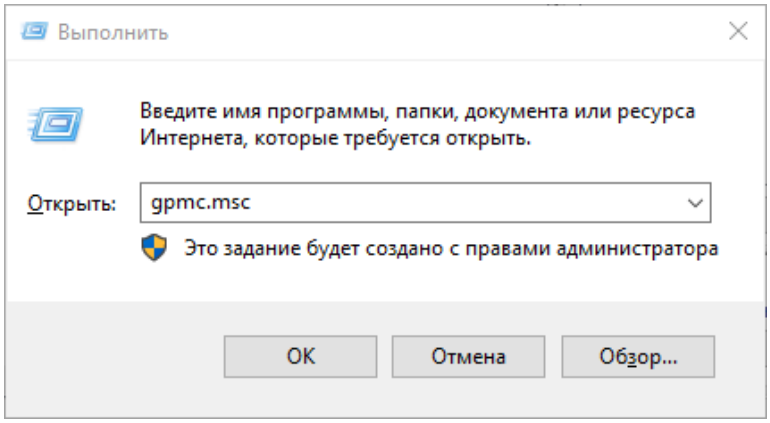
В RedCheck для сканирования удаленного хоста требуется создать учётную запись, **Тип учетной записи** – **Windows**.



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.

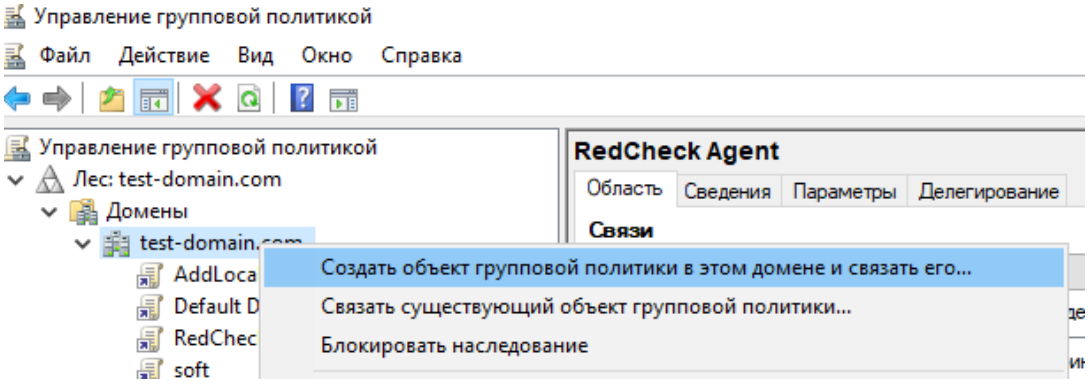
Создание групповой политики

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

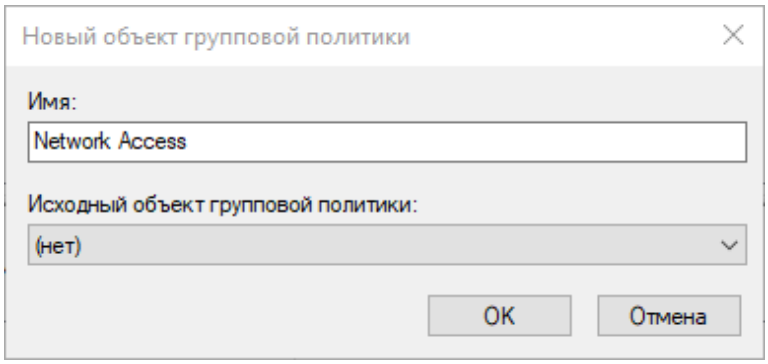


При локальной настройке нажмите **Win + R** → введите **gpedit.msc**;

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

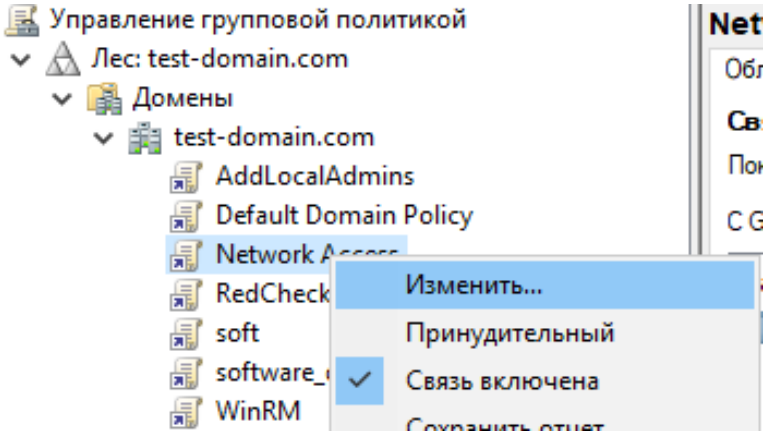


Введите название новой групповой политики;

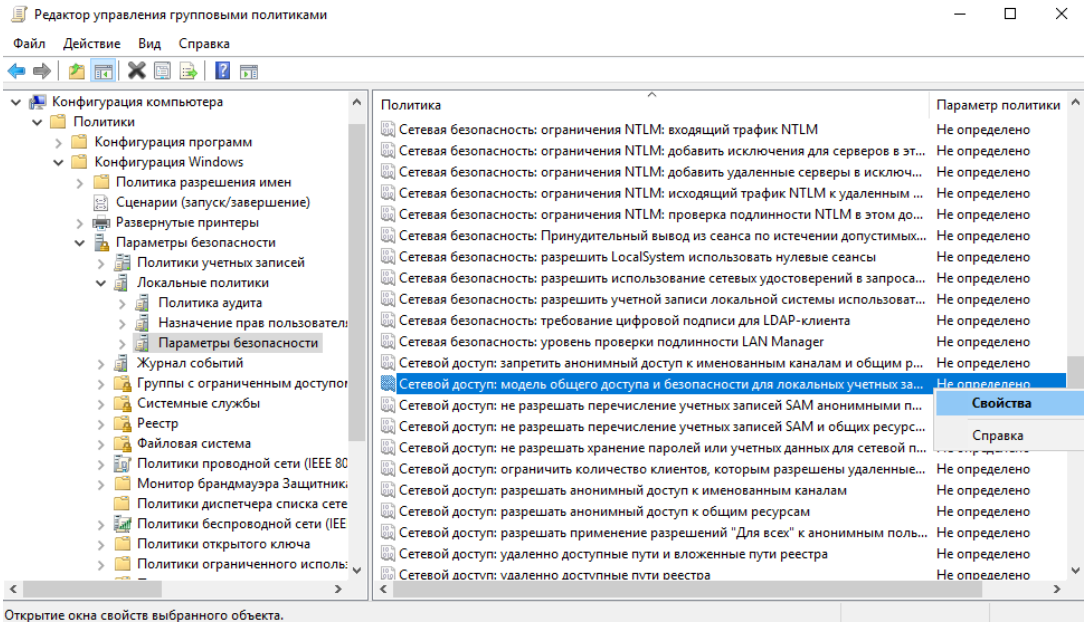


Настройка сетевого доступа

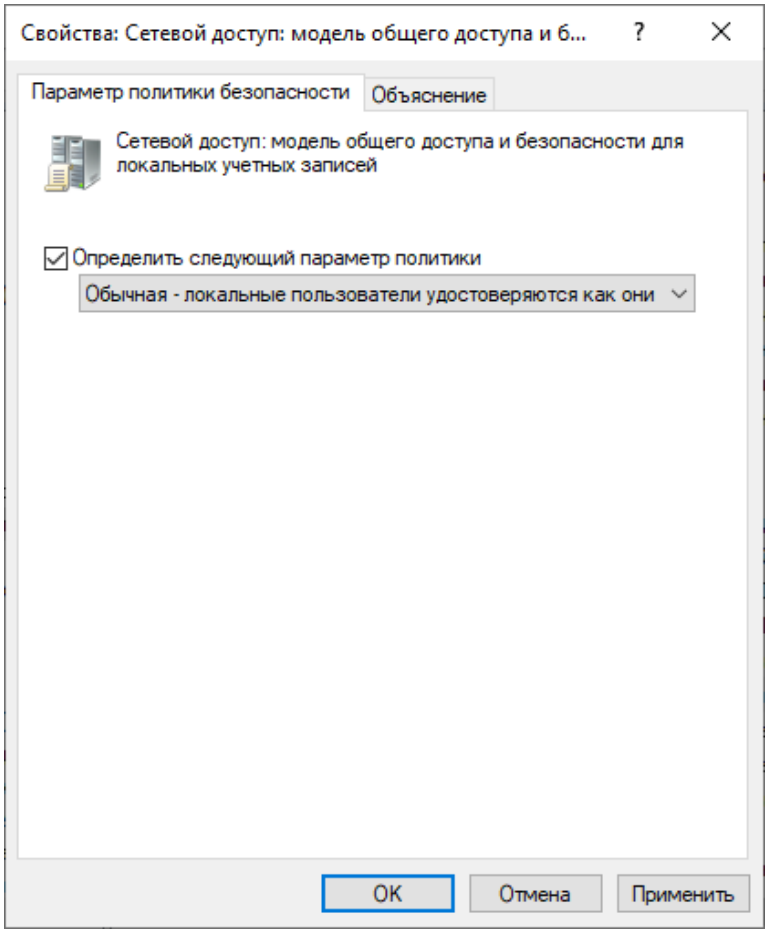
Шаг 3. ПКМ по созданной групповой политике → **Изменить**;



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...**

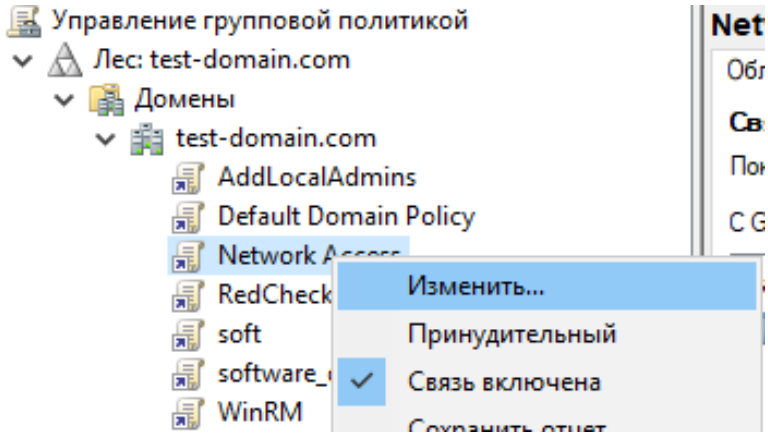


Настройка контроля учетных записей пользователей

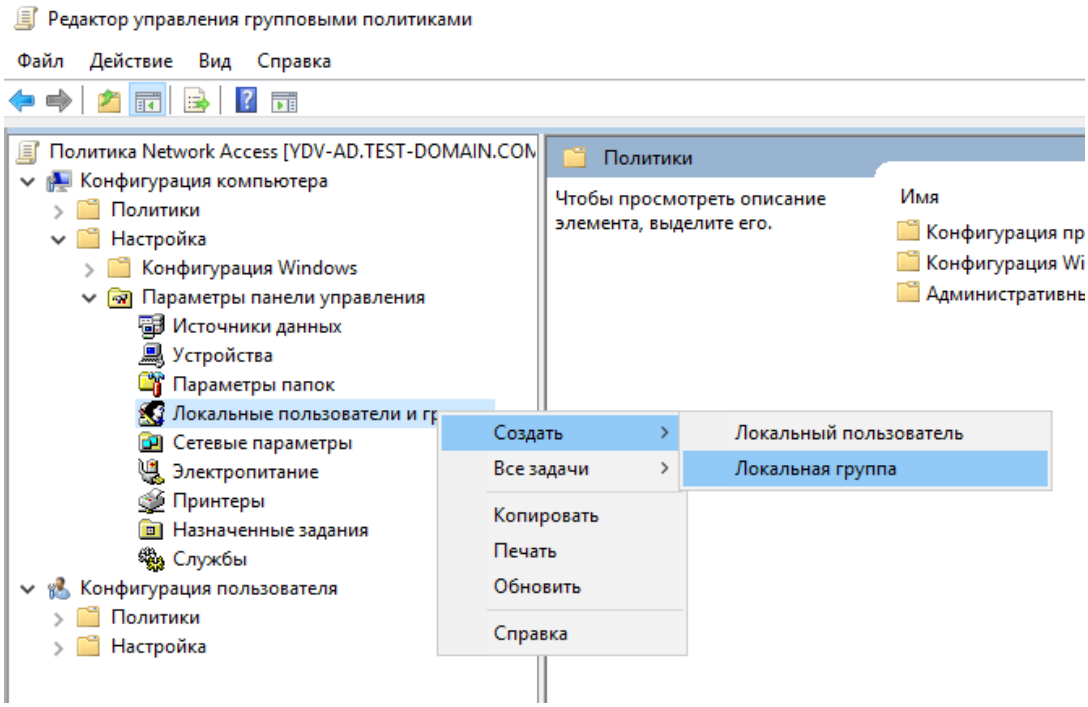
Рекомендуется использовать доменную УЗ для отключения функции UAC.

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

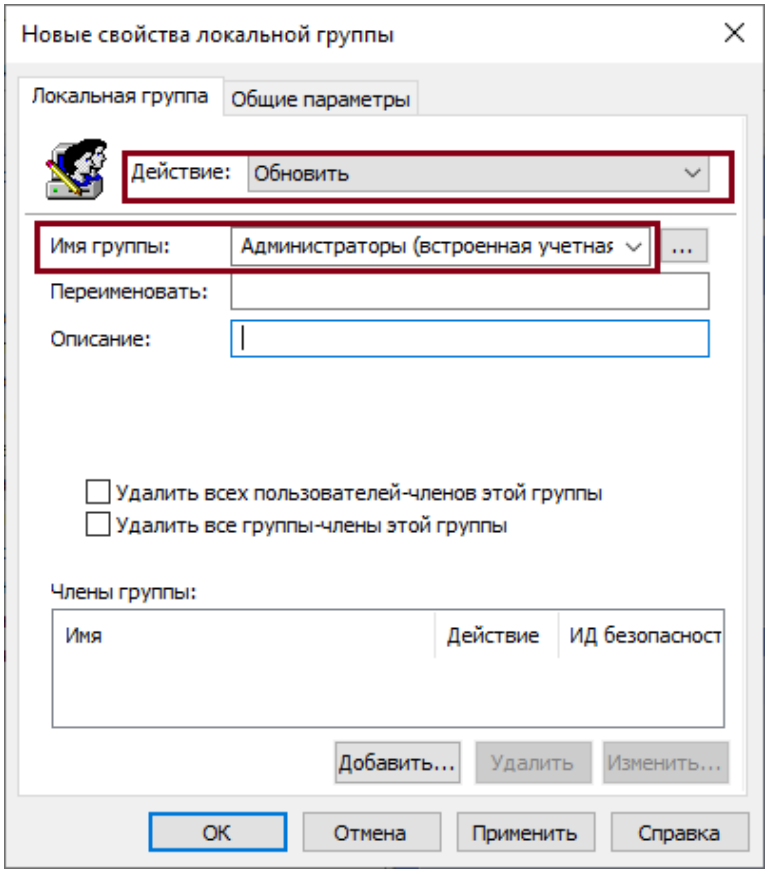
Шаг 2. ПКМ по необходимой групповой политике → **Изменить**;



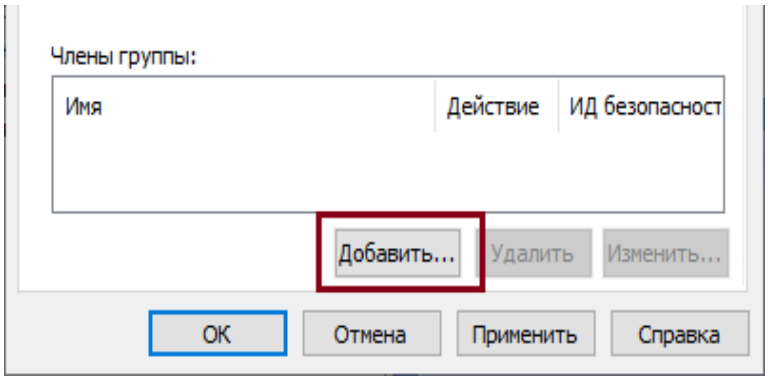
Шаг 3. Добавьте пользователя в группу локальных администраторов сканируемого хоста: **Конфигурация компьютера** → **Настройки** → **Параметры панели управления** → ПКМ по **Локальные пользователи и группы** → **Создать** → **Локальная группа**;



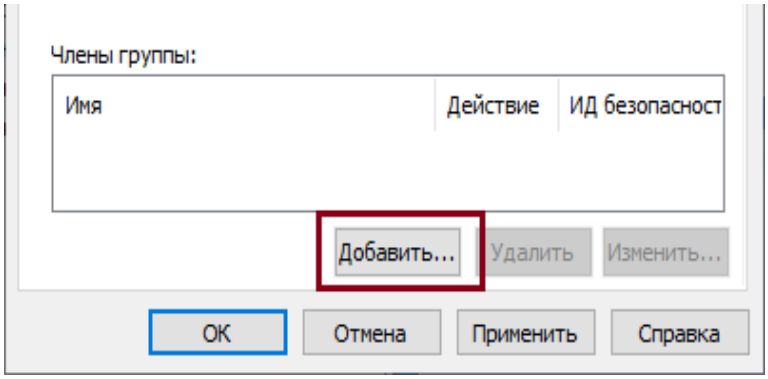
Шаг 4. В **Действие** выберите **Обновить**, в **Имя группы** – **Администраторы (встроенная учетная запись)**;



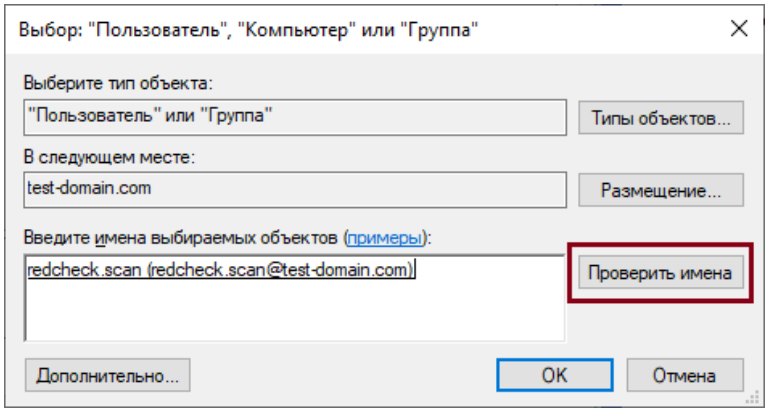
Нажмите **Добавить**;



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 правом удаленного подключения к хосту;
- Пользователь с правами **Вход в качестве службы**, **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 транспорта WinRM на стороне службы сканирования (Astra Linux)

Шаг 1. Для настройки на хосте должны быть установлены пакеты **gcc python3-dev libkrb5-dev**

Bash (оболочка Unix)

```
sudo apt install gcc python3-dev libkrb5-dev
```

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-0.8.1-Astra1.7.tar.gz
```

Шаг 3. Установите python-пакеты:

Bash (оболочка Unix)

```
sudo python3 /var/opt/redcheck-scan-service/pypsrp/pypsrp-0.8.1-
Astra1.7/pip-24.0-py3-none-any.whl/pip install --no-index -f
/var/opt/redcheck-scan-service/pypsrp/pypsrp-0.8.1-Astra1.7 setuptools
wheel Cython

sudo python3 /var/opt/redcheck-scan-service/pypsrp/pypsrp-0.8.1-
Astra1.7/pip-24.0-py3-none-any.whl/pip install --no-index -f
/var/opt/redcheck-scan-service/pypsrp/pypsrp-0.8.1-Astra1.7
pypsrp[kerberos]
```

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/lib/x86_64-linux-gnu/libpython3.7m.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 транспорта WinRM на стороне службы сканирования (Debian)

Шаг 1. Для настройки на хосте должны быть установлены пакеты **gcc python3-dev libkrb5-dev**

```
Bash (оболочка Unix)
sudo apt install gcc python3-dev libkrb5-dev
```

Шаг 2. Установите пакетный менеджер pip;

```
Bash (оболочка Unix)
sudo apt install python3-pip
```

Шаг 3. Установите python-пакеты:

```
Bash (оболочка Unix)
pip3 install setuptools wheel Cython
pip3 install pypsrp[kerberos]
```

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/lib/x86_64-linux-gnu/libpython3.9.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 транспорта WinRM на стороне службы сканирования (РЕД ОС)

Шаг 1. Установите python-пакеты:

Bash (оболочка Unix)

```
sudo python3 /var/opt/redcheck-scan-service/pypsrp/pip-24.2-py3-none-any.whl/pip install --no-index -f /var/opt/redcheck-scan-service/pypsrp setuptools wheel Cython

sudo python3 /var/opt/redcheck-scan-service/pypsrp/pip-24.2-py3-none-any.whl/pip install --no-index -f /var/opt/redcheck-scan-service/pypsrp pypsrp[kerberos]
```

Шаг 2. 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**

Шаг 3. 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 транспорта WinRM на стороне службы сканирования (SberLinux)

Шаг 1. Установите необходимые зависимости:

Bash (оболочка Unix)

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

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.

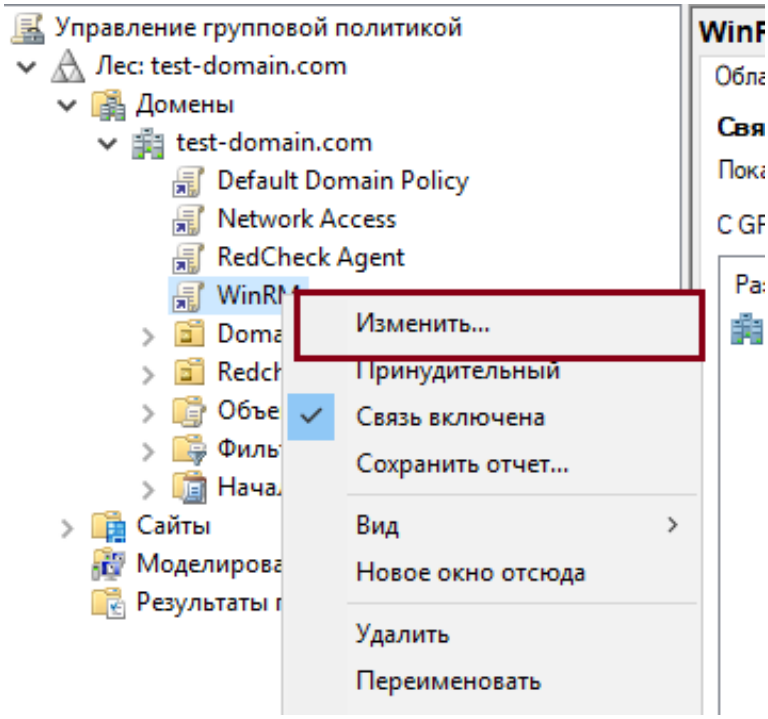
> В случае возникновения проблем с подключением рекомендуется следовать руководству.

Настройка WinRM через групповые политики

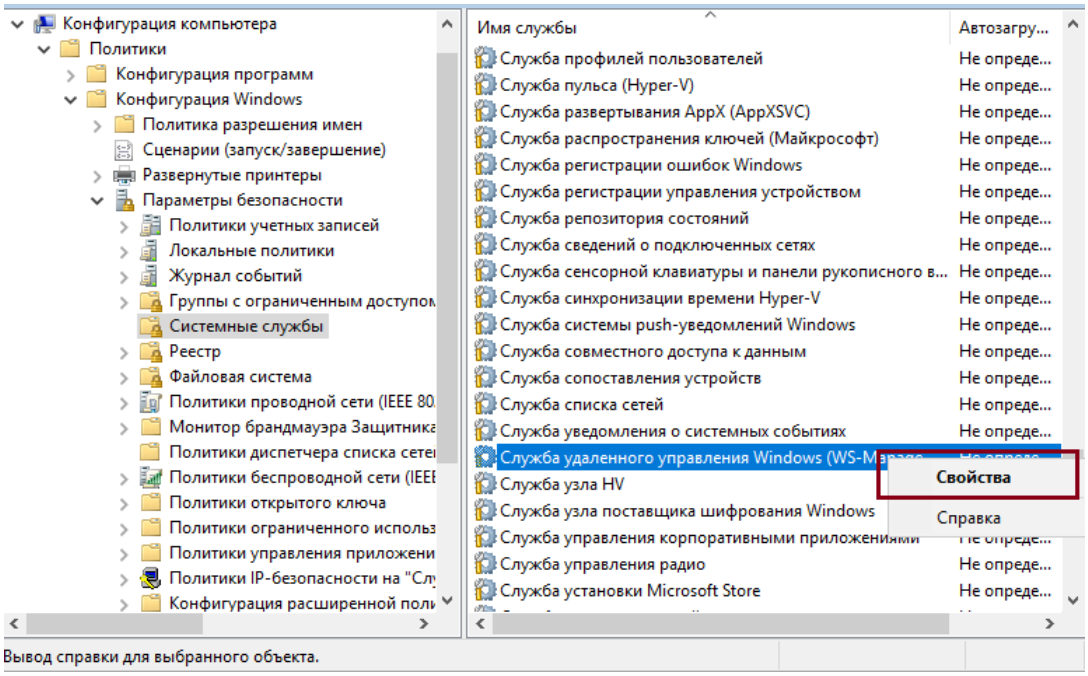
> Для сканирования транспортом WinRM на конечных хостах должен быть установлен .NET Framework 4.0 и выше

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

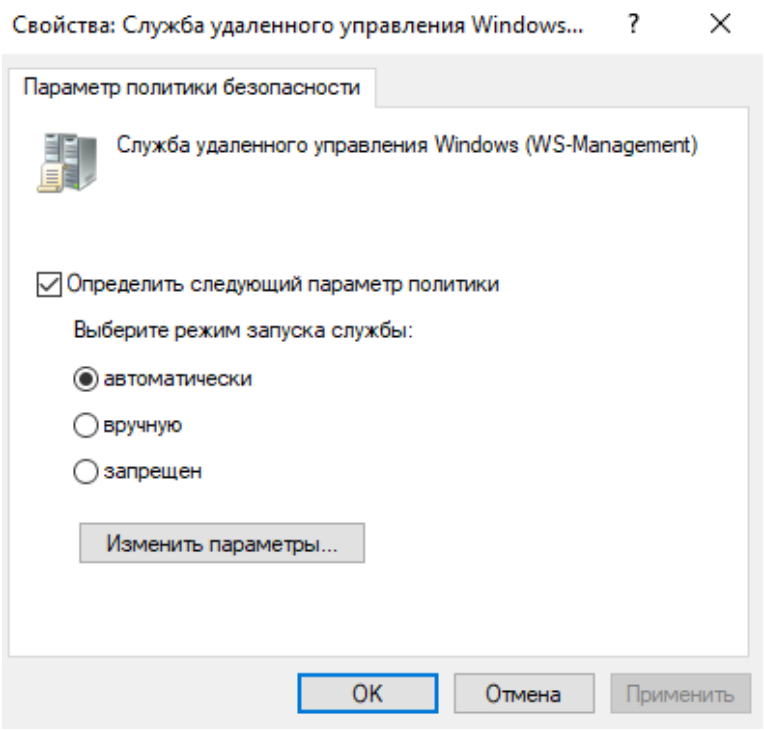
Шаг 1. ПКМ по групповой политике → **Изменить**;



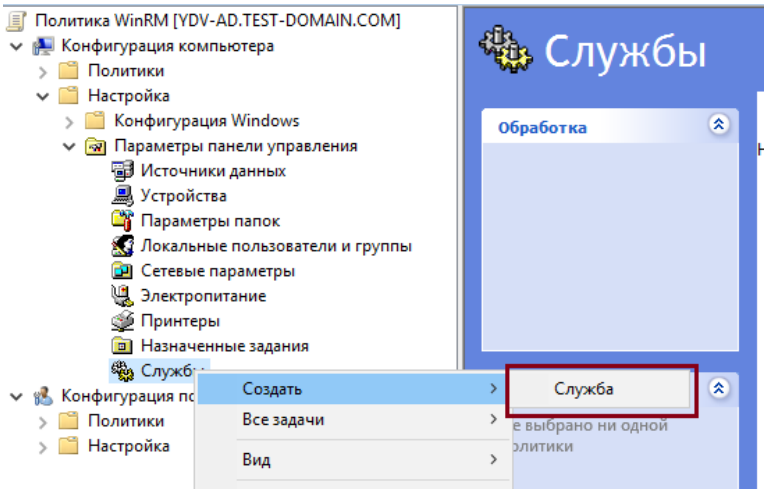
Шаг 2. Перейдите в **Конфигурация компьютера → Политики → Конфигурация Windows → Параметры безопасности → Системные службы** → ПКМ по **Служба удаленного управления Windows (WS-Management) → Свойства**;



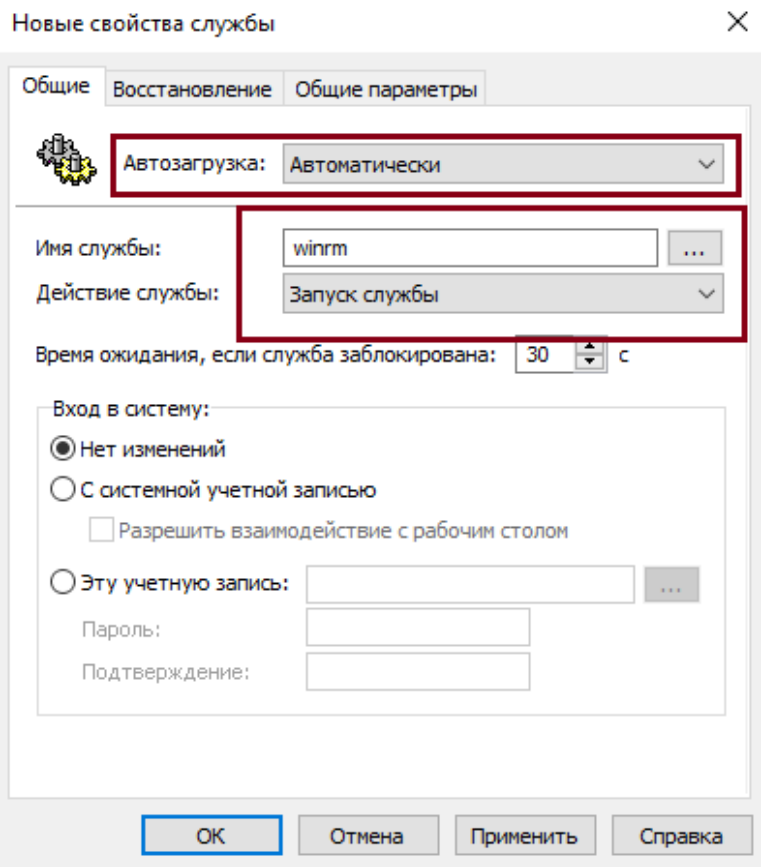
Отметьте **Определить следующий параметр политики**, режим запуска службы – **автоматически → ОК**;



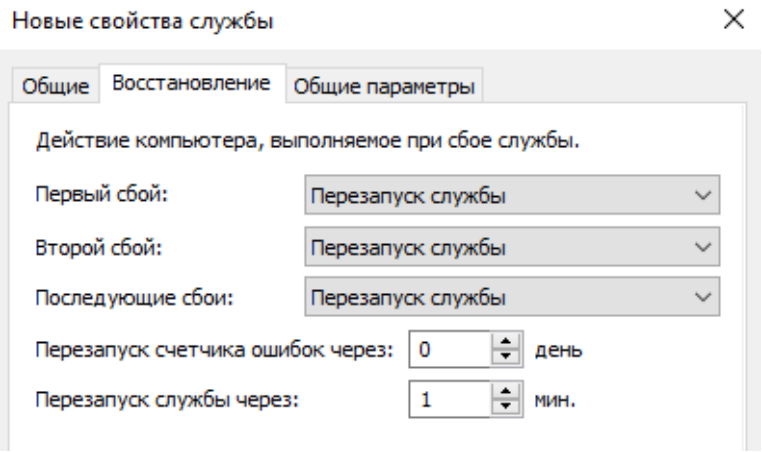
Шаг 3. Перейдите в **Конфигурация компьютера** → **Настройка** → **Параметры панели управления** →ПКМ по **Службы** → **Создать** → **Служба**;



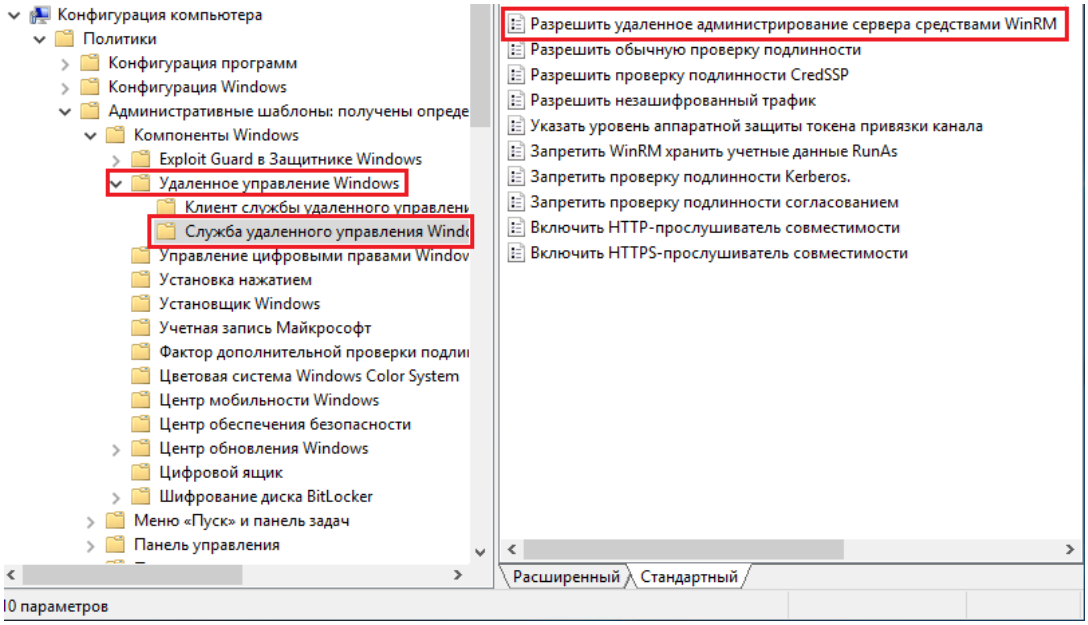
Шаг 4. Имя службы – **winrm**. В **Действия** выберите **Запуск службы;**



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

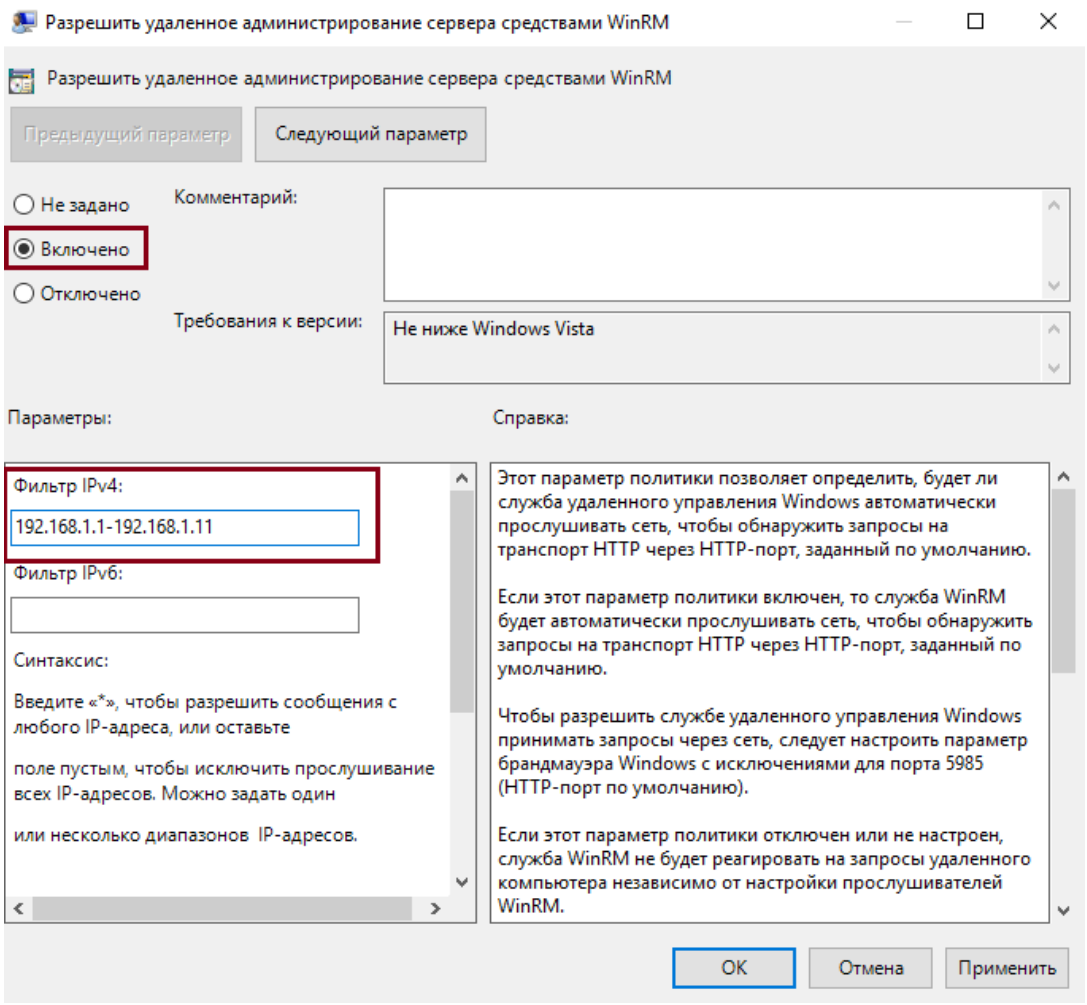


Шаг 5. Перейдите в **Конфигурация компьютера → Политики → Административные шаблоны… → Компоненты Windows → Удаленное управление Windows → Служба удаленного управления Windows** → откройте **Разрешить удаленное администрирование сервера…**;

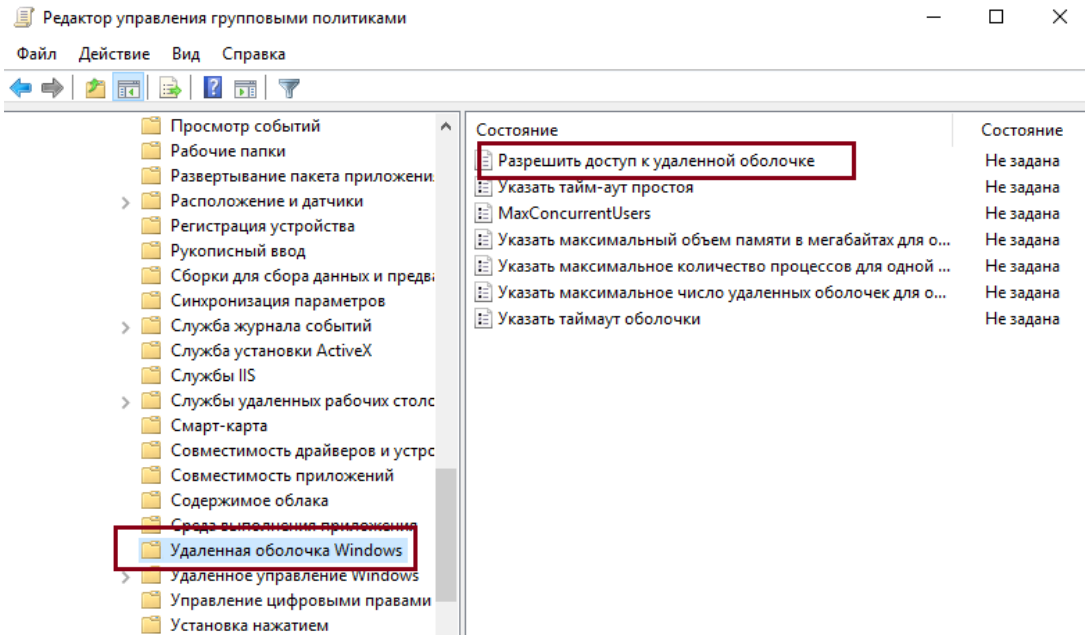


Укажите **Включено** → укажите в **Фильтр IPv4** IP-адреса:

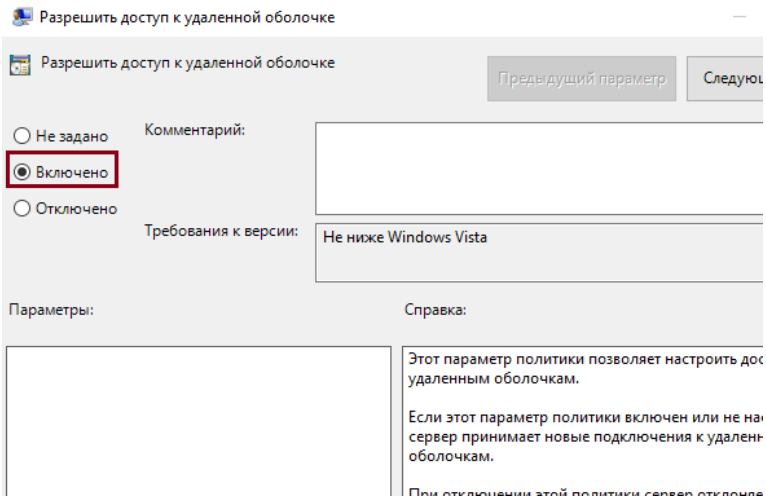
- **Для групповой политики для хоста службы сканирования:** ip-адрес хоста службы сканирования;
- **Для групповой политики для сканирумых узлов:** диапазон ip-адресов.



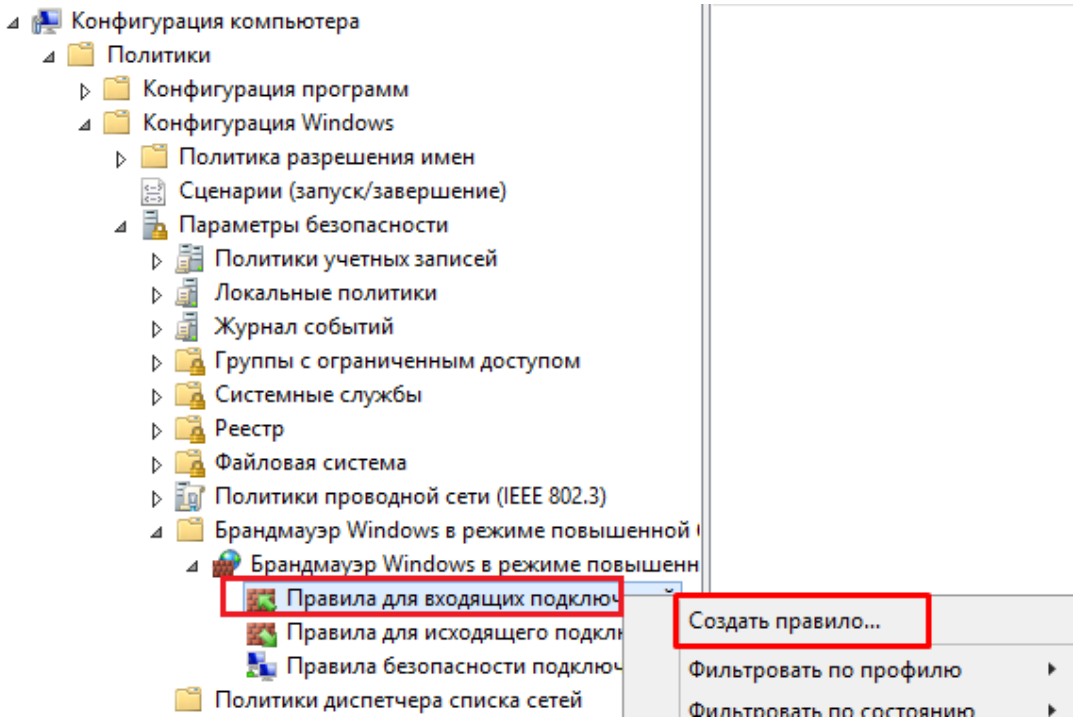
Шаг 6. Перейдите в **Компоненты Windows → Удаленная оболочка Windows** → откройте **Разрешить доступ к удаленной оболочке**;



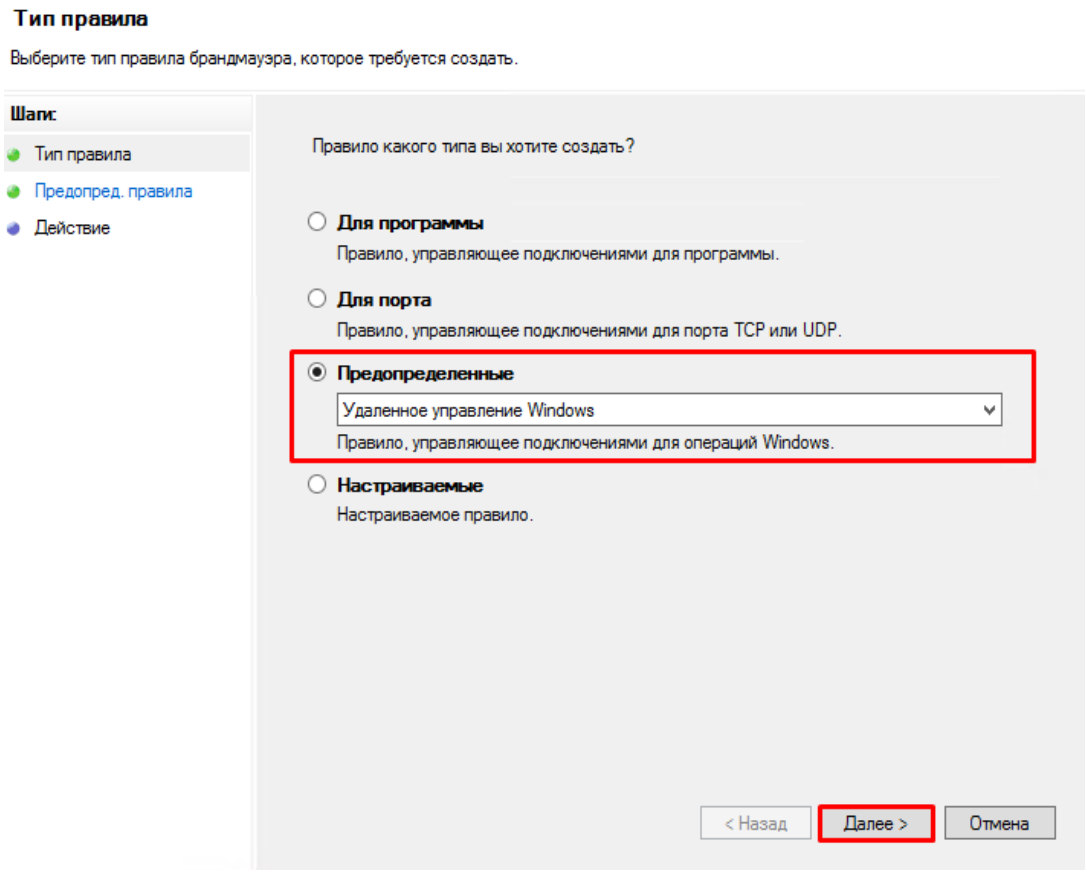
Укажите **Включено**;



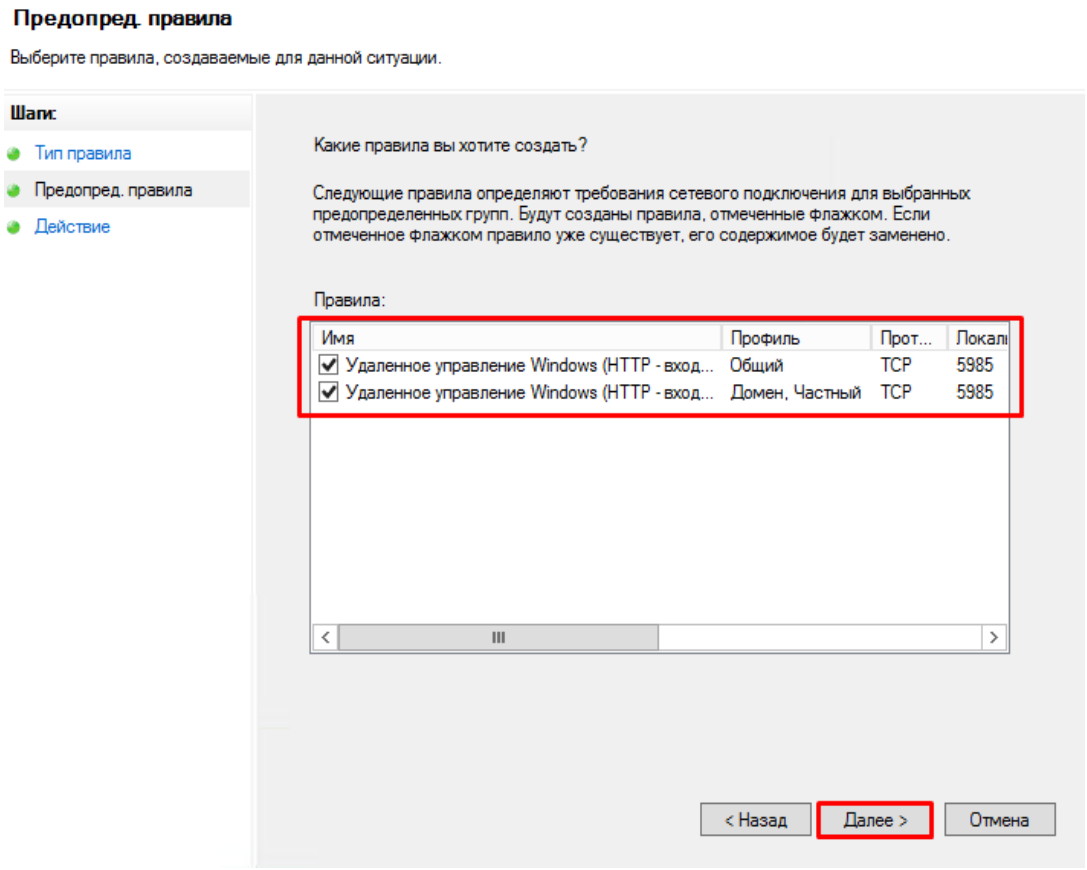
Шаг 7. Перейдите в **Конфигурация компьютера** → **Политики** → **Конфигурация Windows** → **Параметры безопасности** → **Монитор брандмауэра Защитника Windows** → ПКМ по **Правила для входящих подключений** → **Создать правило**;



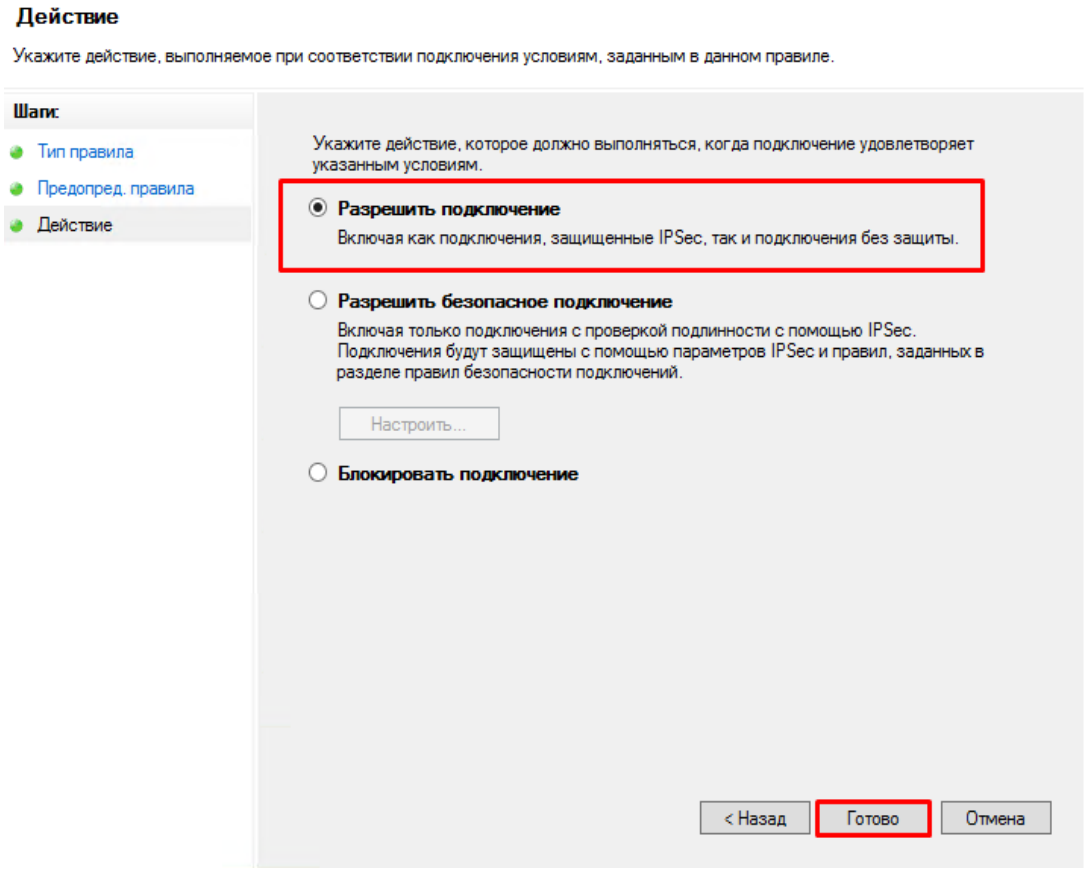
Шаг 8. Отметьте **Предопределенные** → выберите **Удаленное управление Windows** → **Далее**;



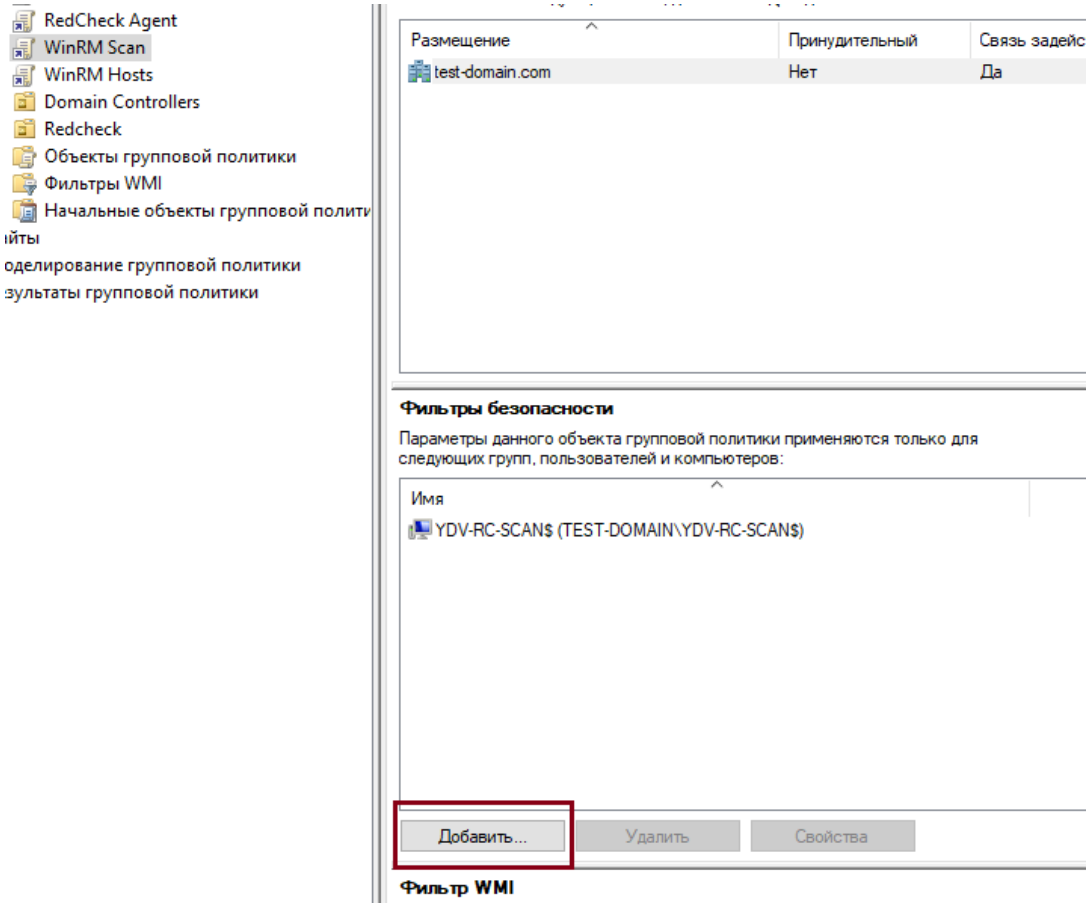
Отметьте два правила **Удаленное управление Windows…** → **Далее**;



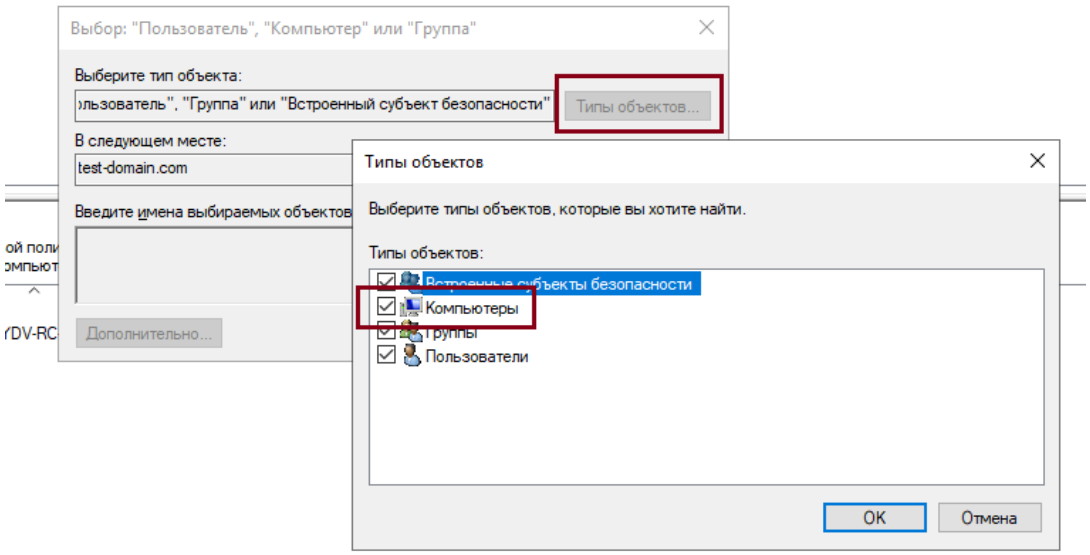
Укажите **Разрешить подключение** → **Готово**;



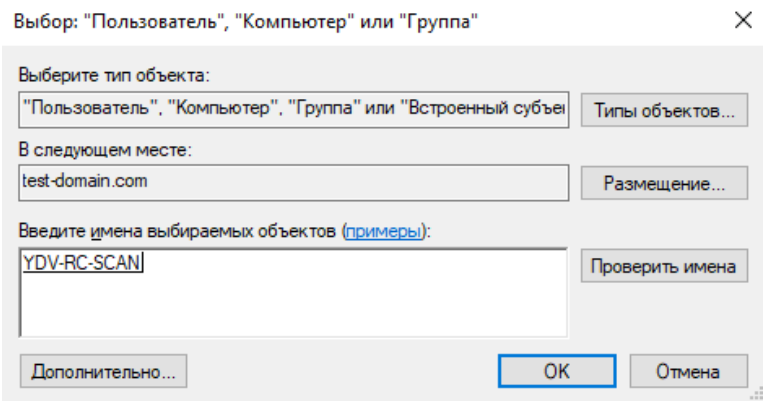
Шаг 9. Укажите каждой групповой политике хосты, для которых эти политики будут применяться. Для хоста службы сканирования удалите группу **Прошедшие проверку** → **Добавить**;



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 субъе
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;

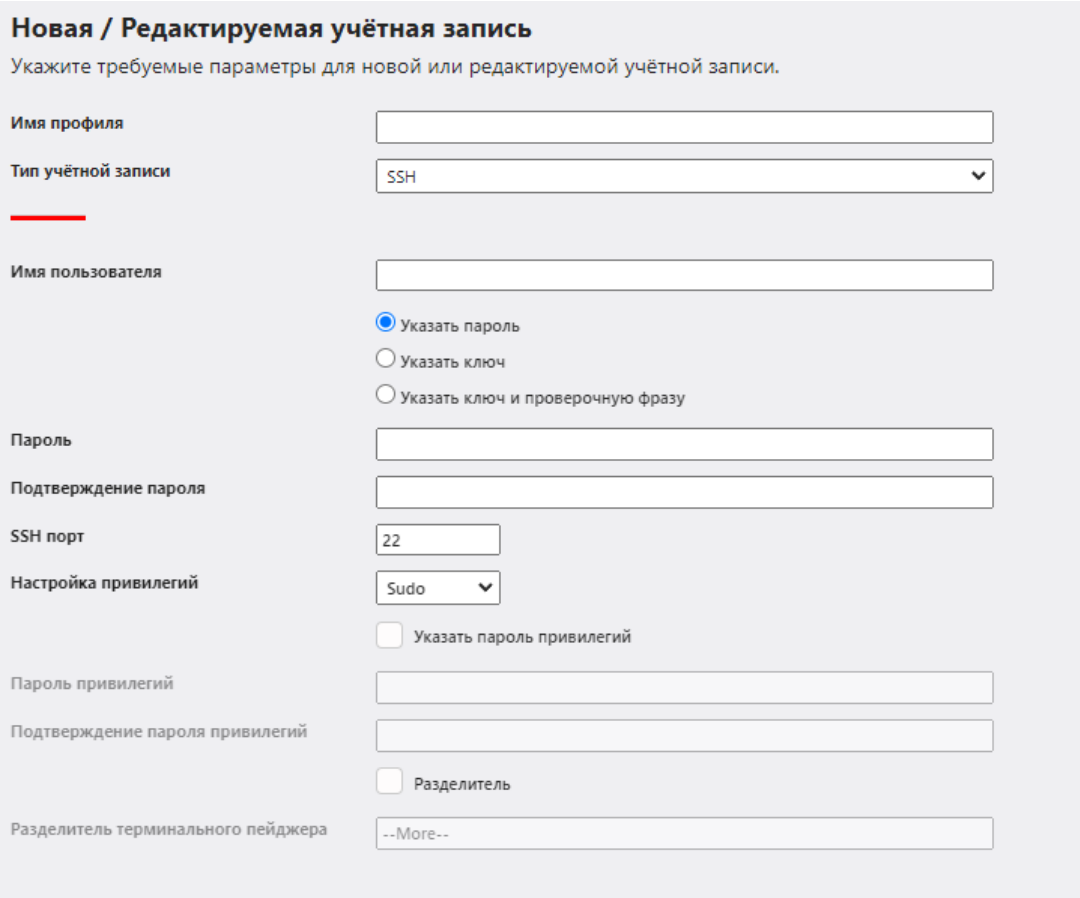
Раздел **[domain_realm]** предоставляет преобразование доменного имени или имени хоста в имя области Kerberos.

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 Unix-систем (SSH)

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**.



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
```

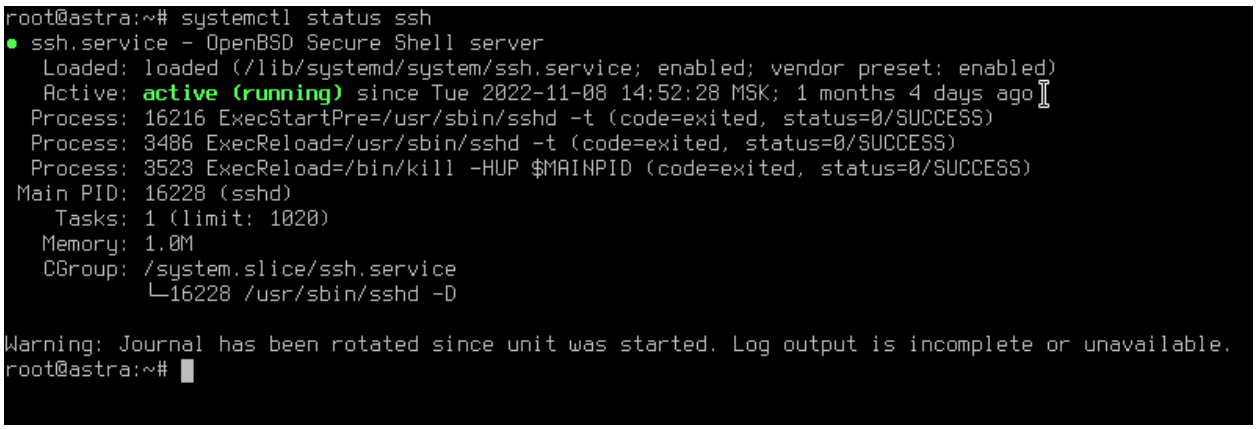
Шаг 2. Запустите сервис:

```
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**).



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

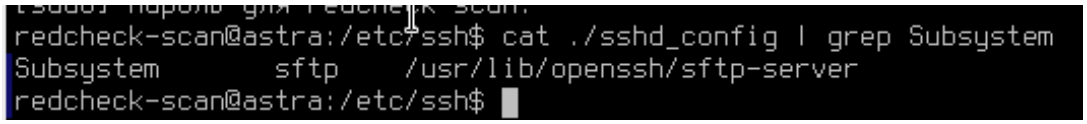
```
Bash (Unix Shell)

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

или

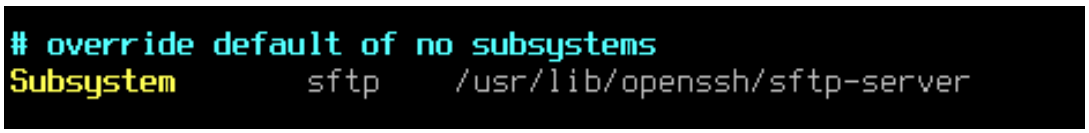
```
Bash (Unix Shell)

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



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

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



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

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
- 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

```
PermitRootLogin yes
```

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

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

или

```
/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, выполнив команду:

```
Bash (Unix Shell)
usermod -aG sudo rc-scan-user
```

Или отредактируйте конфигурацию sudo:

Код

```
echo "rc-scan-user ALL=(root)NOPASSWD:ALL" >> /etc/sudoers
```

При использовании команды **usermod** для учетной записи будет необходимо дополнительно указать пароль для sudo в соответствующем поле в Менеджере учетных записей.
При редактировании конфигурации sudo указывать дополнительные пароли для учетной записи не нужно.

Учетная запись непривилегированного пользователя

> Рекомендуется использовать учетную запись суперпользователя (root) вместо повышения прав с использованием sudo. В противном случае возможны проблемы с производительностью при сканировании.

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
```

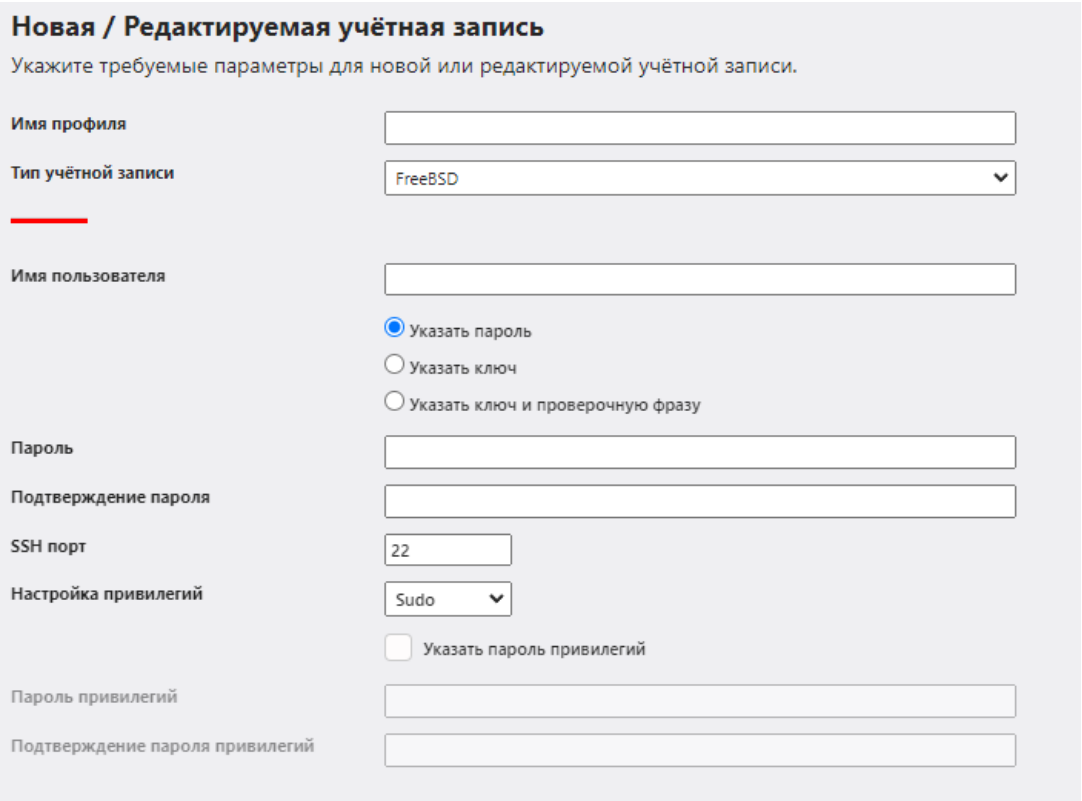
Шаг 2. Задайте пароль для созданной учётной записи пользователя:

Bash (Unix Shell)

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

4.4.3 Сканирование FreeBSD

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



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.

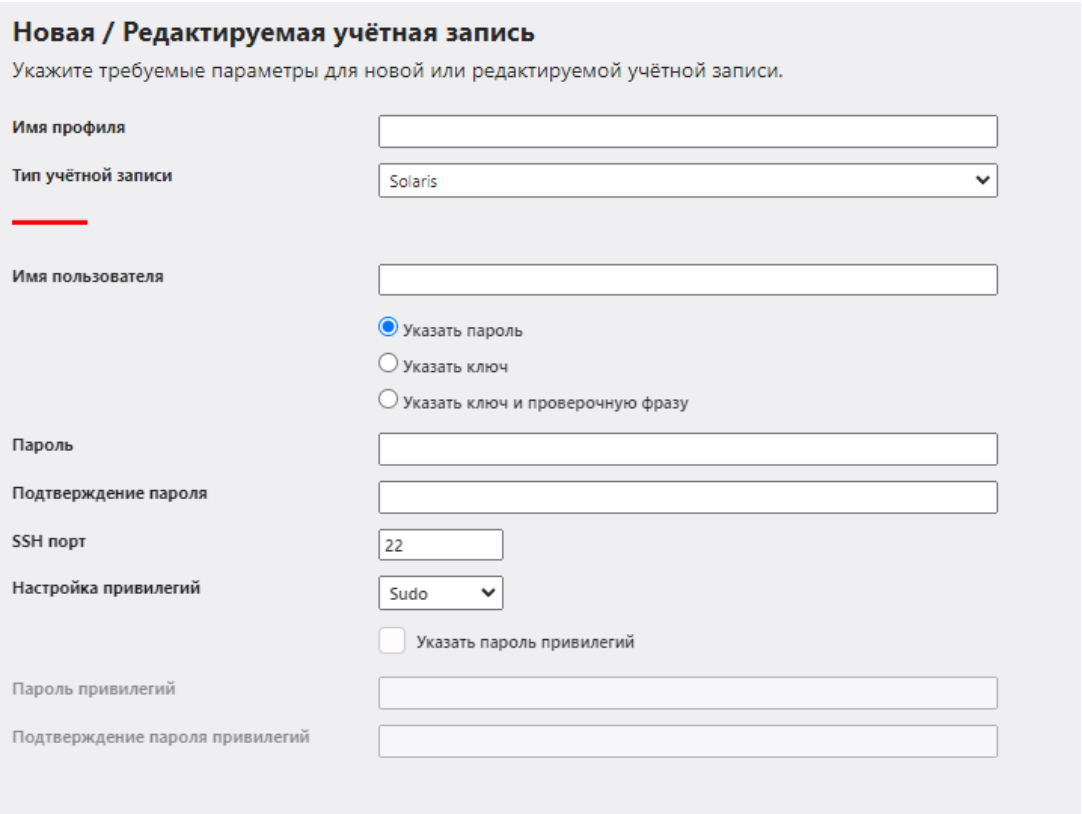
Перечень выполняемых команд в момент сканирования:

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

- basename
- dirname
- which
- ls
- pkg

4.4.4 Сканирование Solaris

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

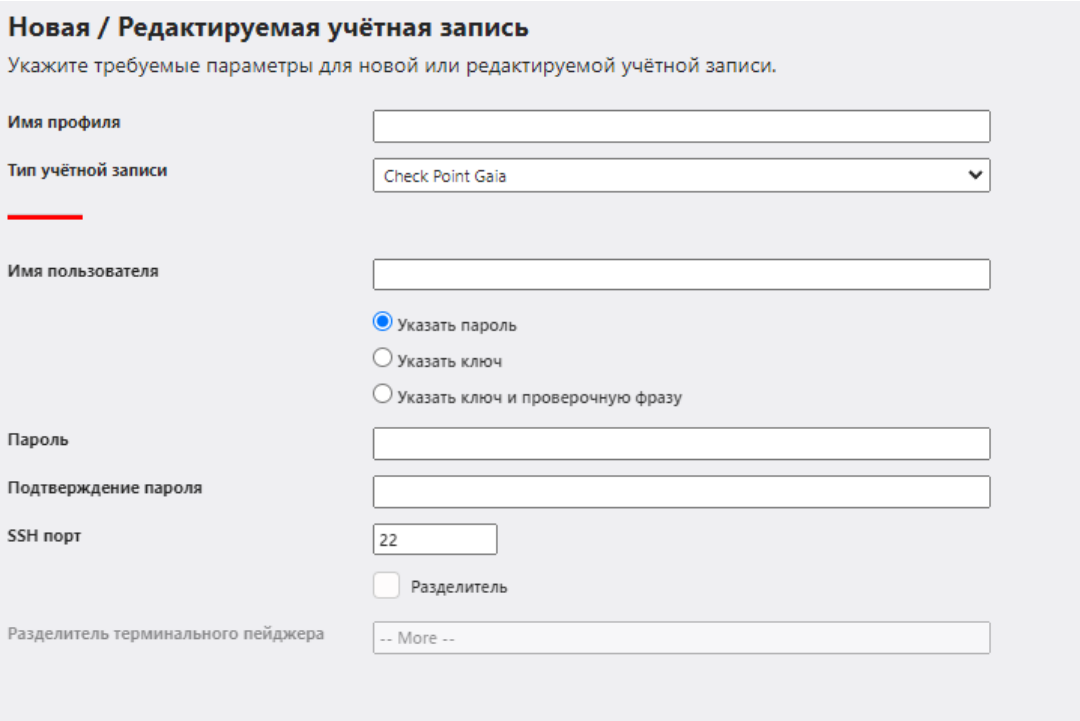


Для сканирования удалённой системы в качестве основного транспорта используется протокол SSH. Убедитесь, что SSH-сервер установлен и настроен, а выбранная учётная запись пользователя имеет возможность подключения к удалённой системе по протоколу SSH. Осуществить проверку подключения можно с помощью любого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

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

4.4.5 Сканирование Check Point

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



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

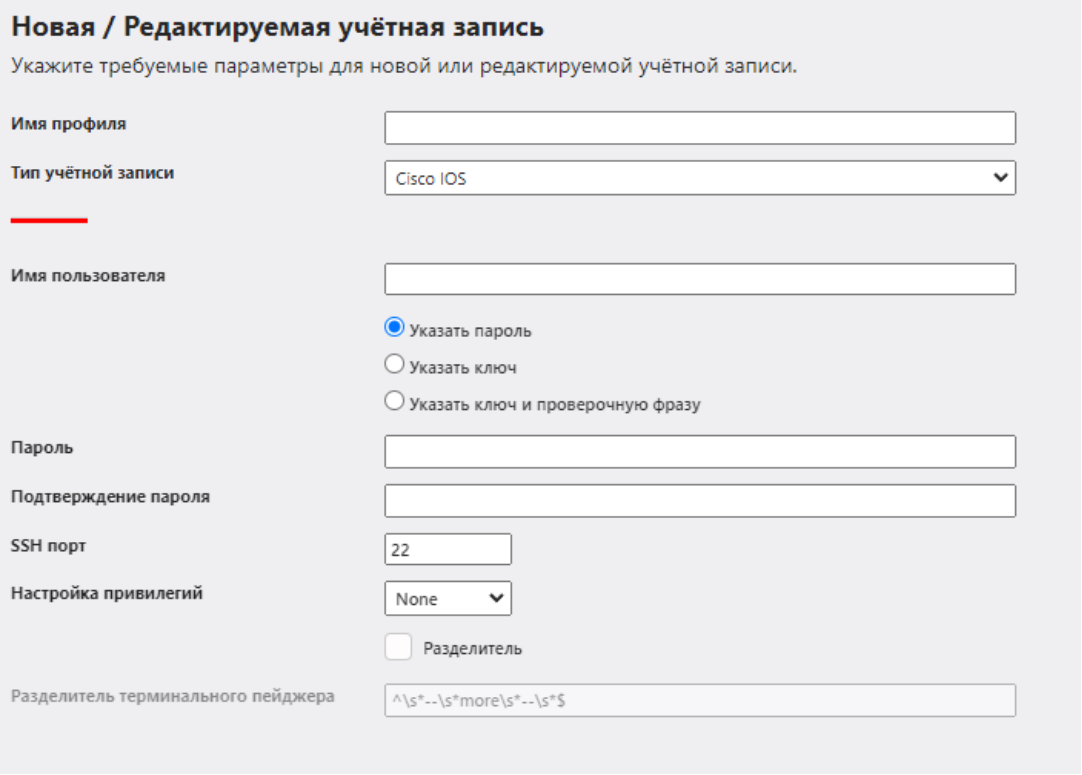
Перечень выполняемых команд в момент сканирования:

- 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**



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:

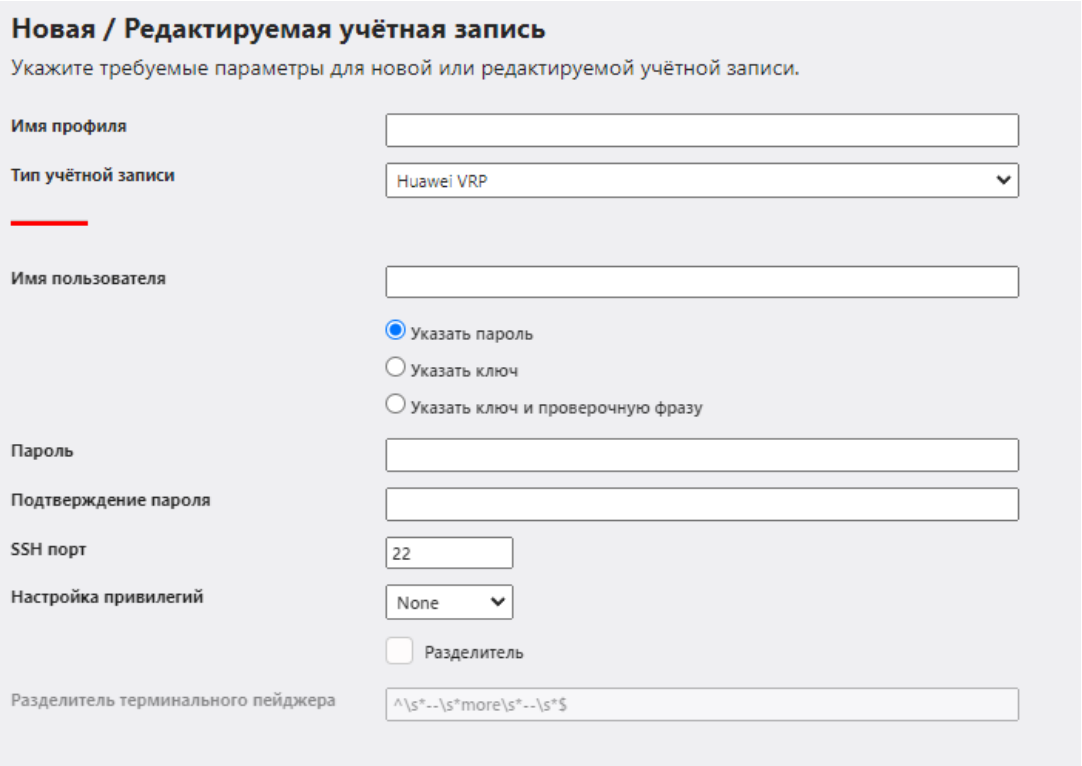
- show file information
- show running-config all
- show logging
- show snmp group
- show startup-config

4.47 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**.



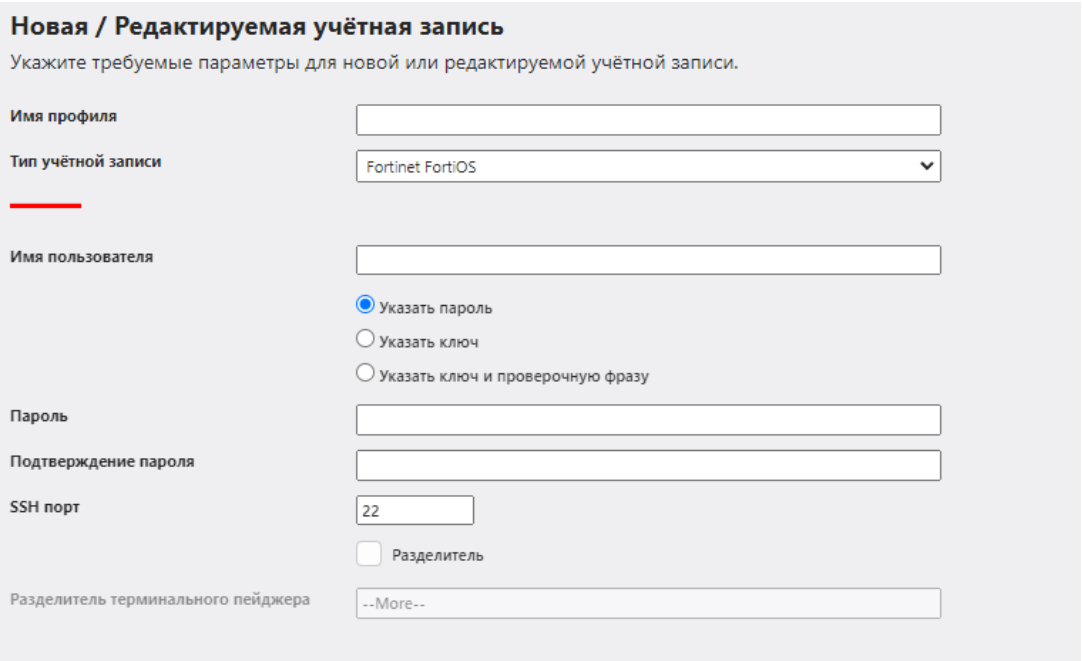
Аналогичные настройки учётных записей производятся и для сетевого оборудования «Булат».

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**.



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:

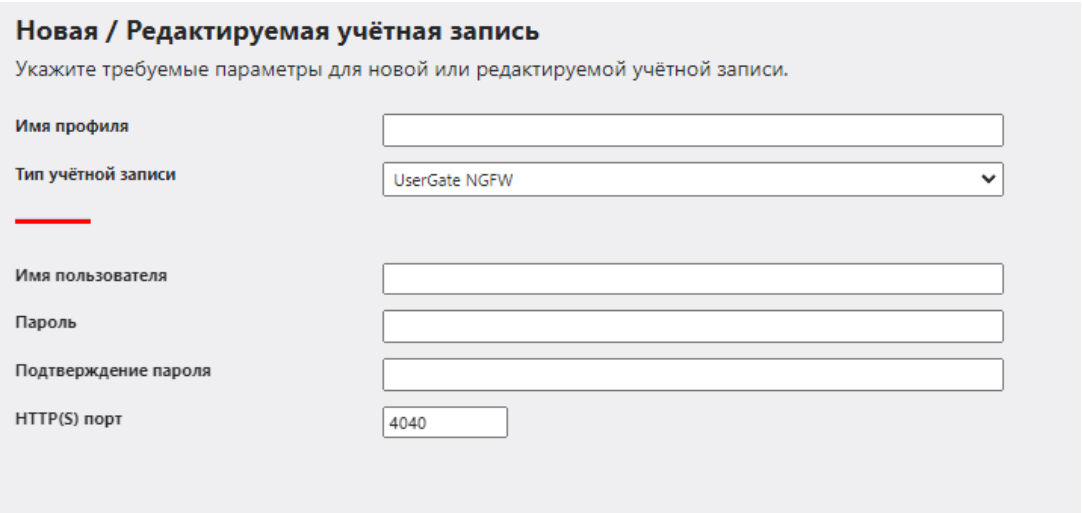
- Разделитель по умолчанию: **"--More-- "**, без пробела внутри, пробел в конце строки;

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**.



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

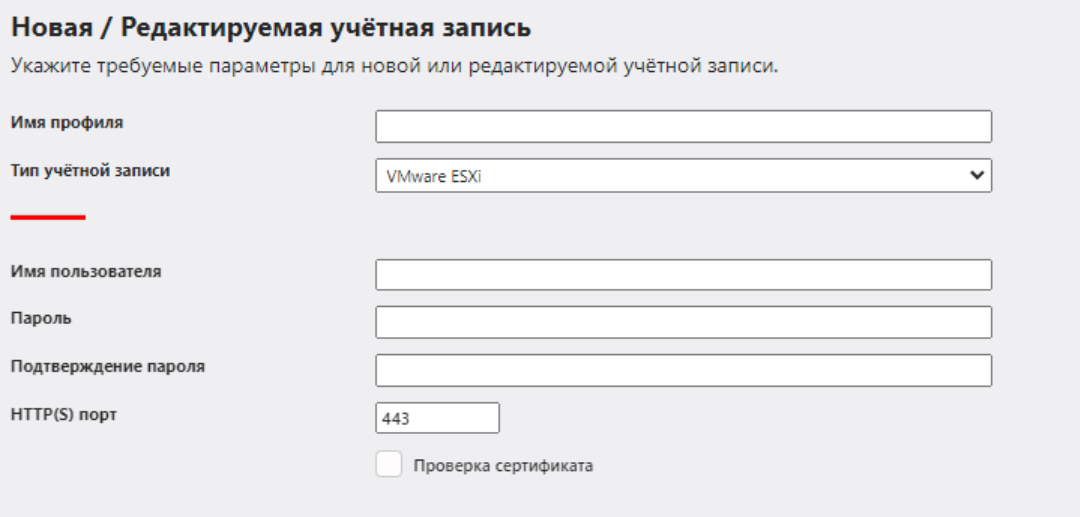
Команда, выполняемая при сканировании VMware ESXi Server:

- VimEsxCLIsoftwareviblist

Содержание

Настройка VMware ESXi Server

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



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 добавленный 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:

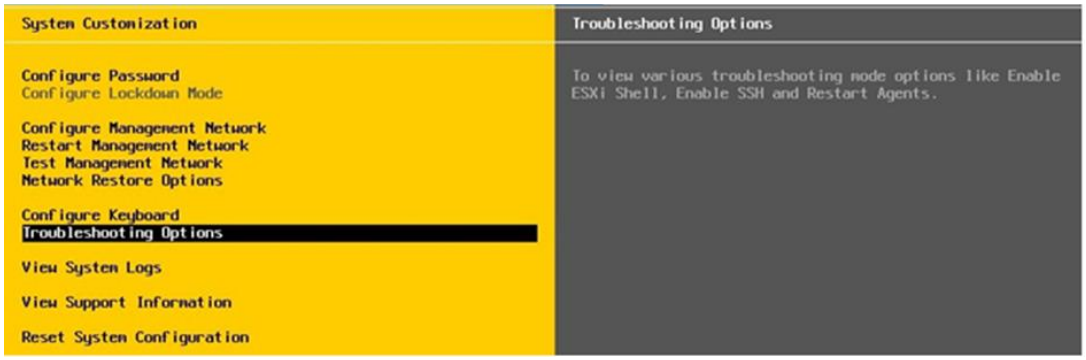
- Включение SSH через DCUI;
- Включение SSH при помощи Web-клиента vSphere.

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**;



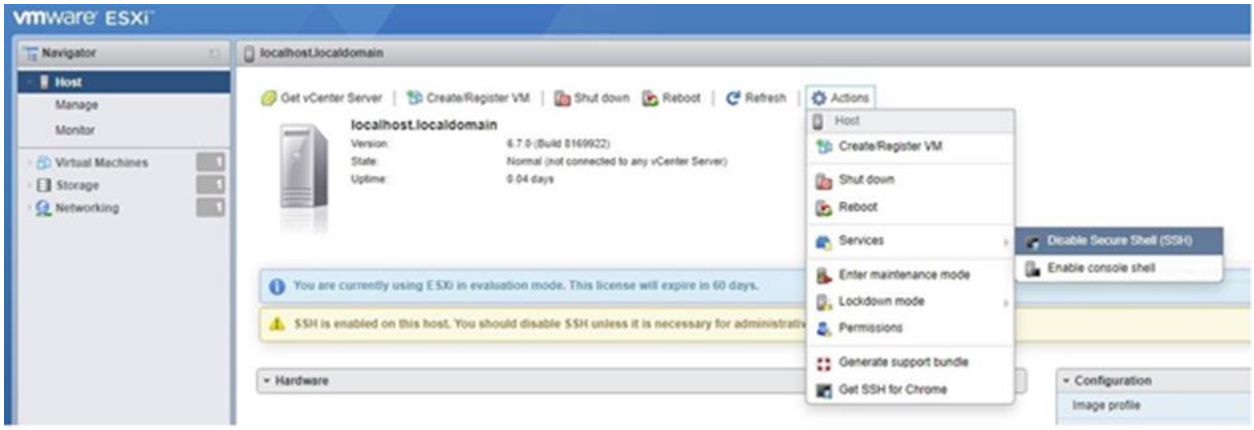
Шаг 3. В **Troubleshooting Mode Options** включите **Enable SSH**;

Для возврата в основное меню нажмите ESC.

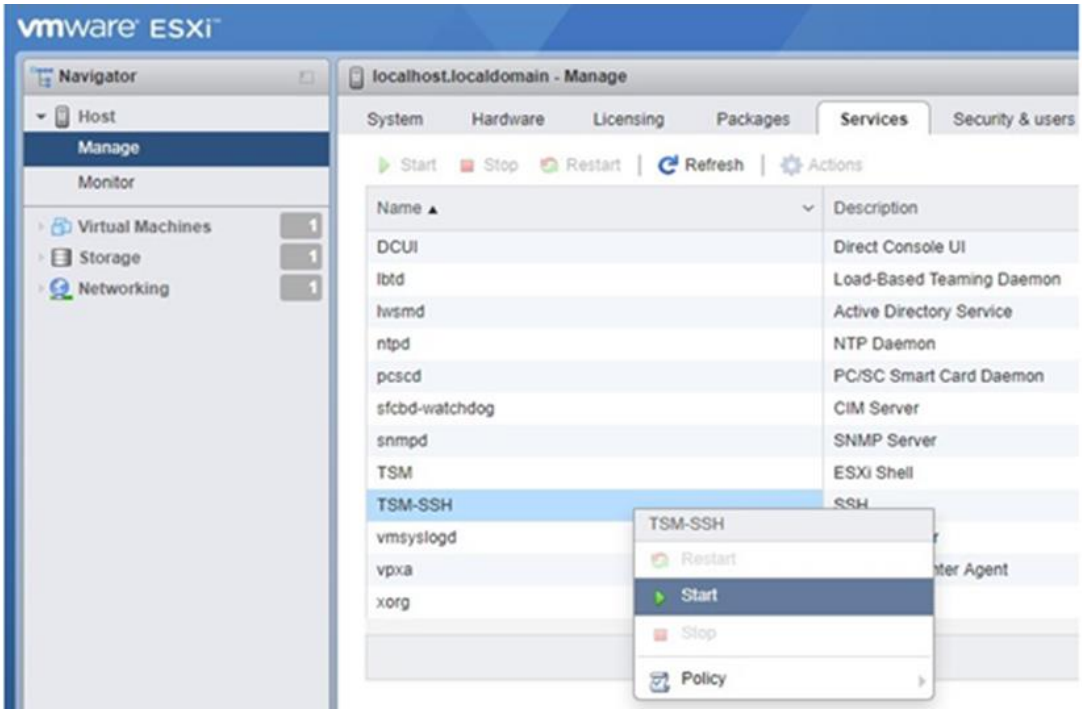
Включение SSH при помощи Web-клиента vSphere

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);**



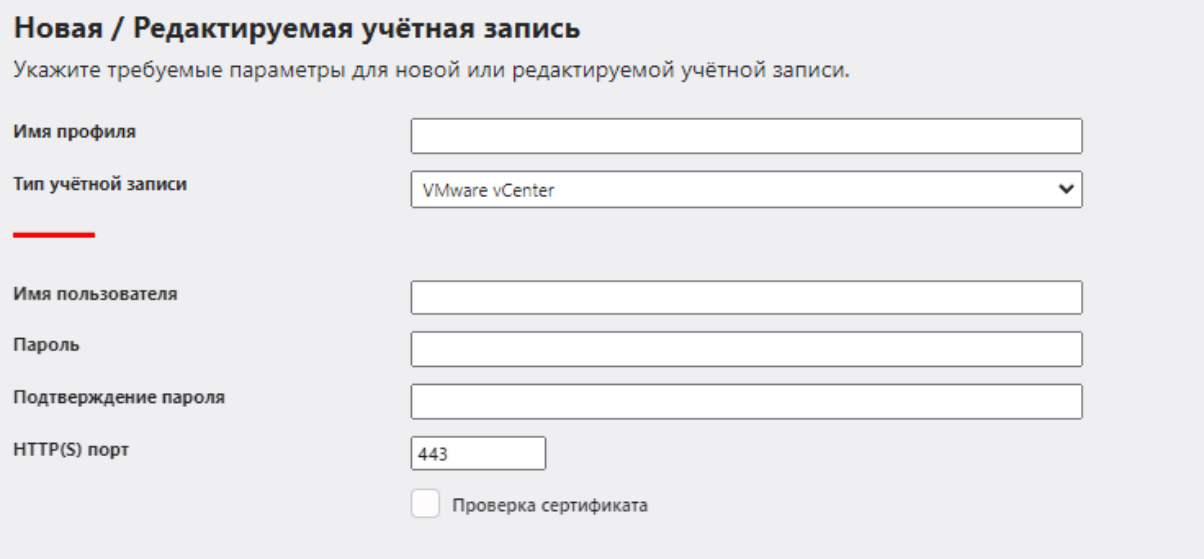
Также активировать SSH можно в разделе **Manage** → **Services** → ПКМ по службе **TSM-SSH** → **Start**



Настройка SSH-туннеля завершена.

Настройка VMware vCenter Server

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



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

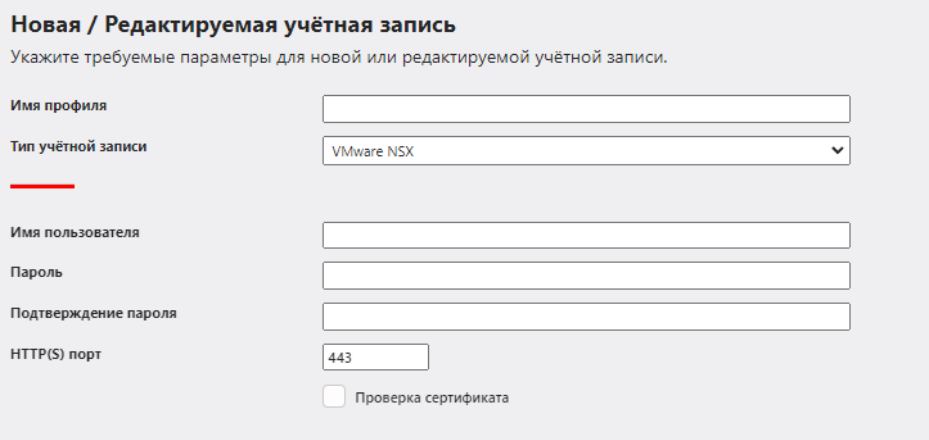
- активированная лицензия на продукт с включенной в нее feature vSphere API;
- наличие учётной записи пользователя VMware vCenter Server;

Для выполнения задания Фиксации необходимо:

- активированная лицензия на продукт с включенной в нее feature vSphere API;
- наличие учетной 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**.



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

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

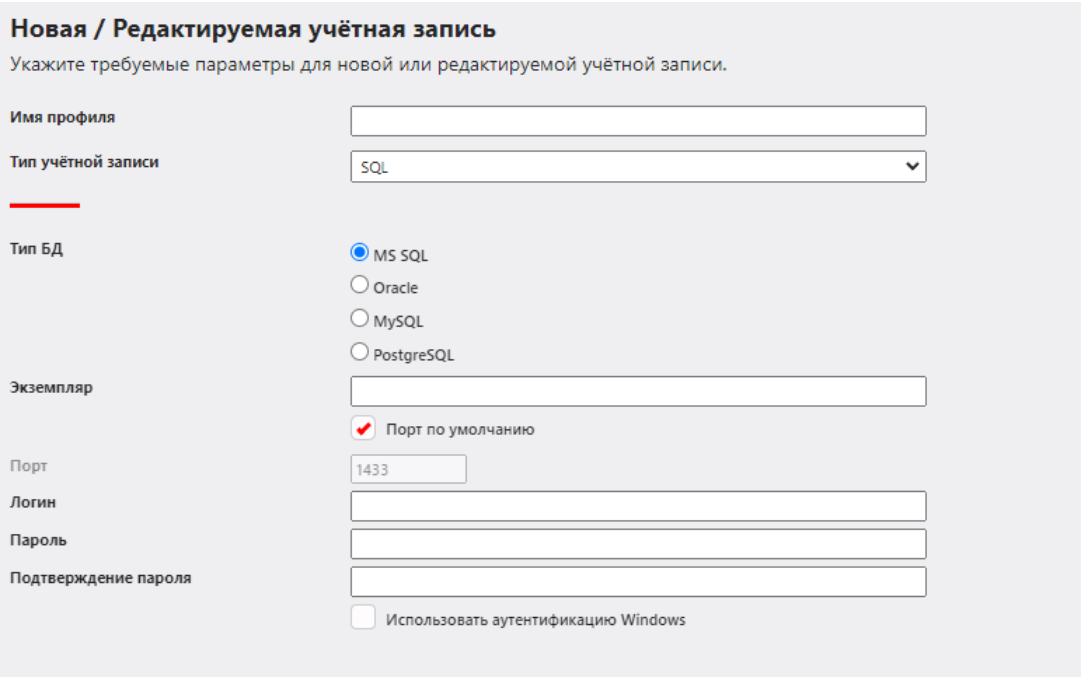
- наличие включенной учётной записи Auditor;
- проверка доступности транспорта внешними средствами (например, Postman);

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**.



Для сканирования СУБД Microsoft SQL Server в экземпляре СУБД может использовать 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**.

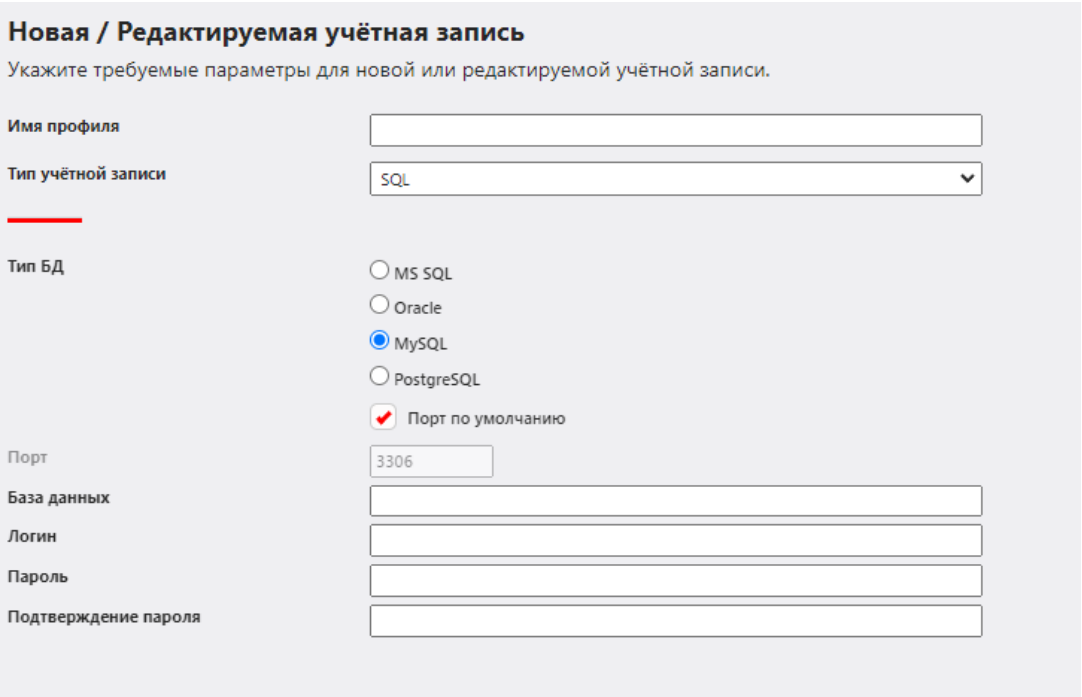
> Поддержка TLS 1.2 начинается с версии SQL Server 2016.
>
> Для сканирования Microsoft SQL Server ниже 2016 необходимо изменить версию протокола в /etc/ssl/openssl.cnf на стороне службы сканирования:

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**.



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)

2. **Права на чтение объектов файловой системы:**

Windows

- C:\ProgramData\MySQL\MySQL Server x.x\
- C:\Program Files\MySQL\MySQL Server x.x\

Linux

- /etc/mysql
- /etc/passwd
- /etc/group
- /home/
- /proc/
- /var/lib/mysql/
- /var/log/mysql/

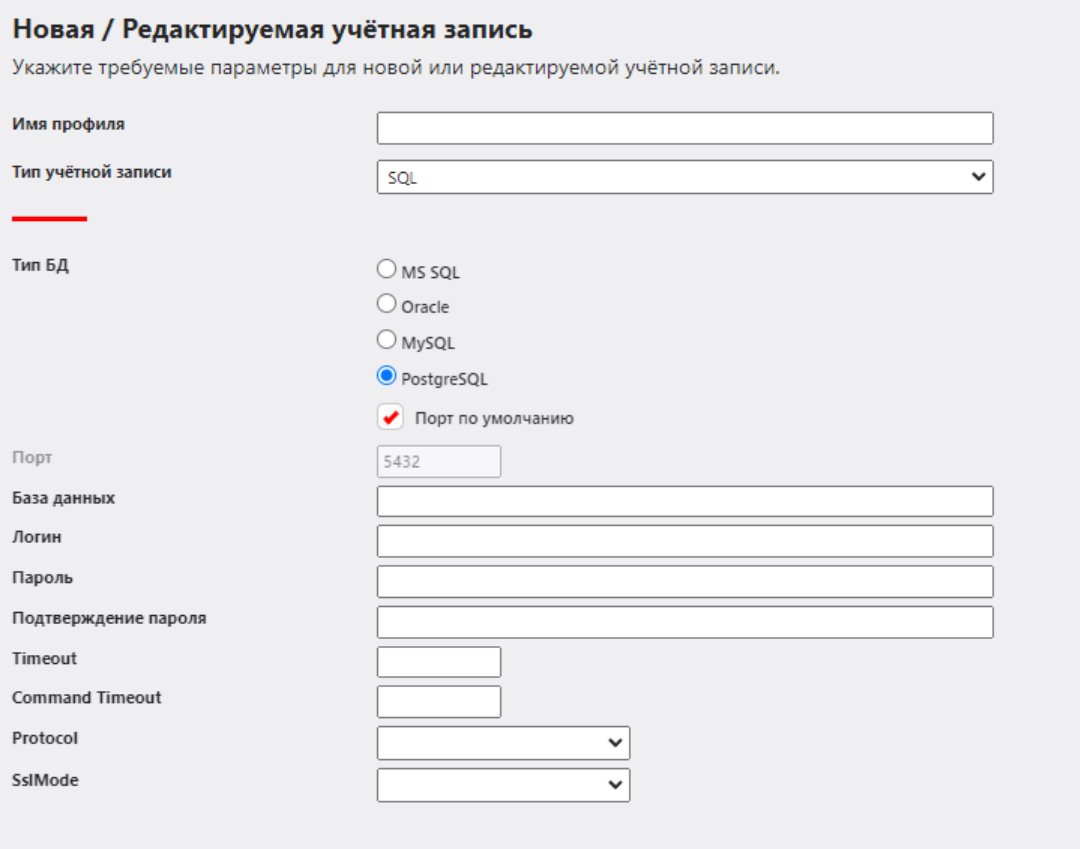
3. **Права на выполнение:**

Linux

- /usr/sbin/mysqld

4.4.13 Сканирование PostgreSQL

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



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
```

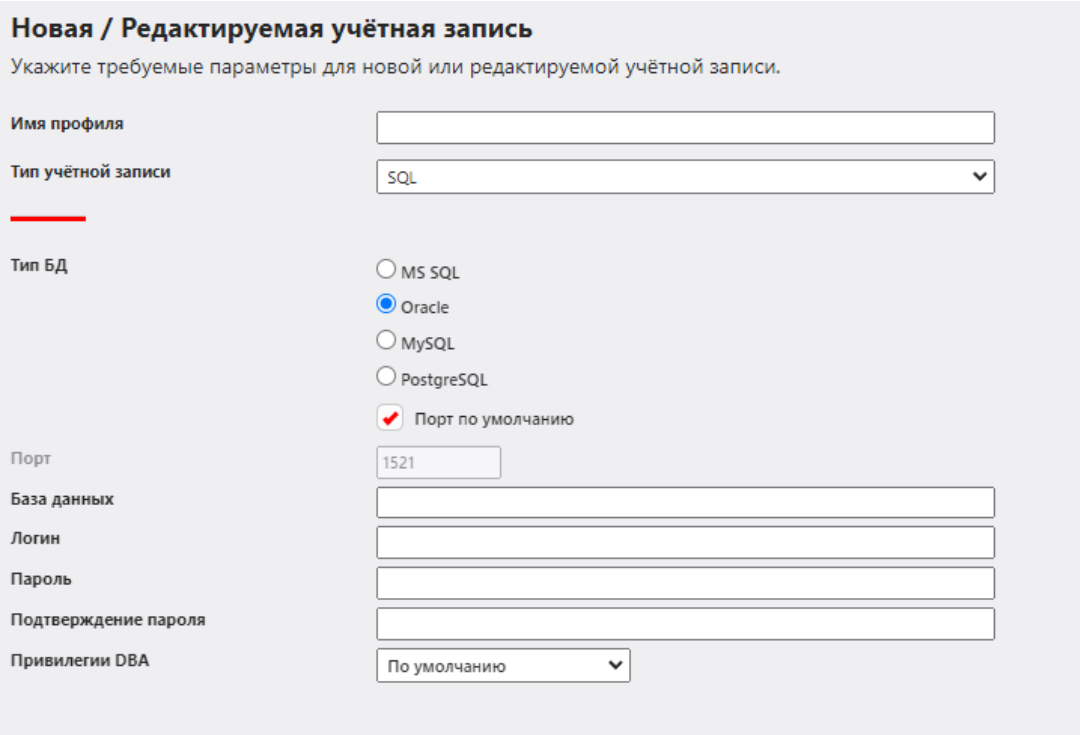
Для BaseAlt

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**.



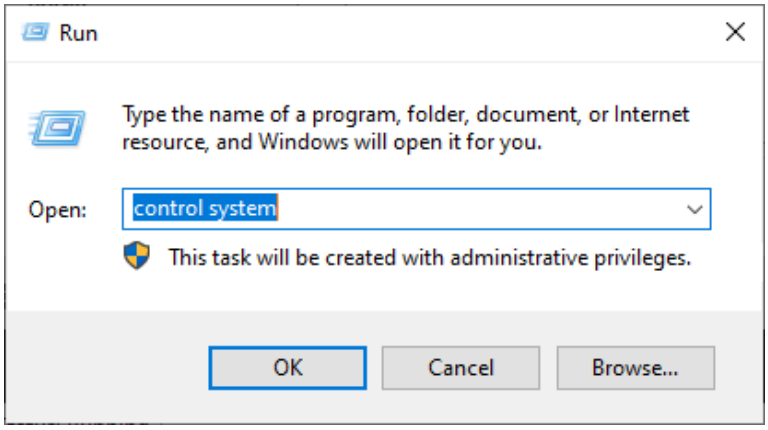
В экземпляре СУБД должен использоваться смешанный тип аутентификации (проверка подлинности Oracle).

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

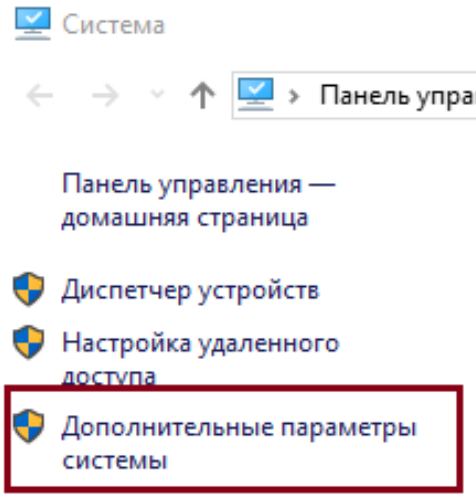
Добавление переменной среды ORACLE_HOME

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

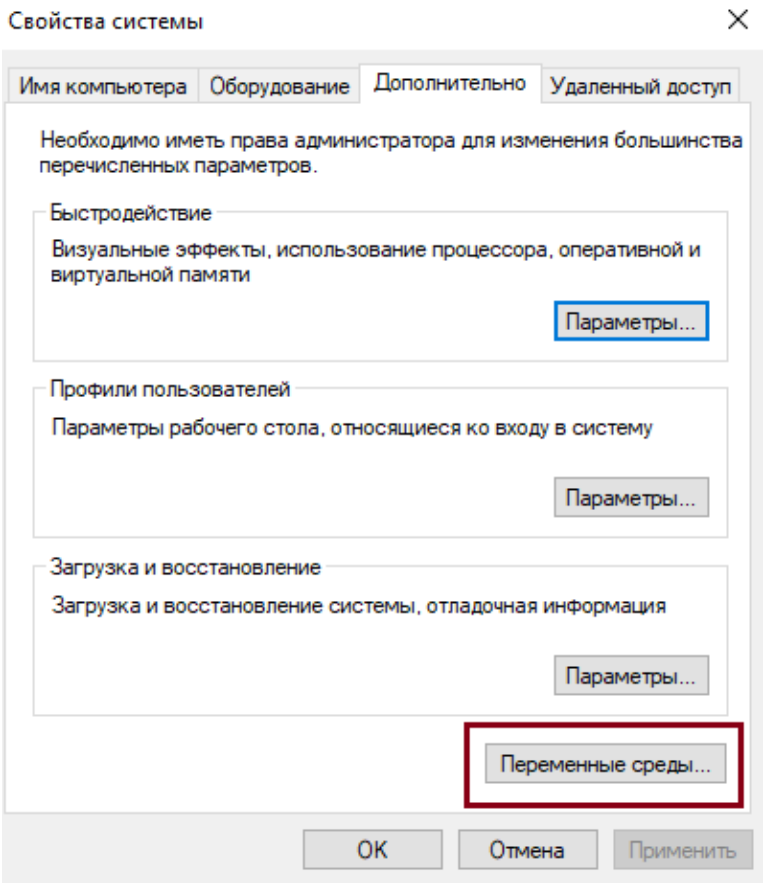
Шаг 1. Нажмите **Win + R** и введите **control system**;



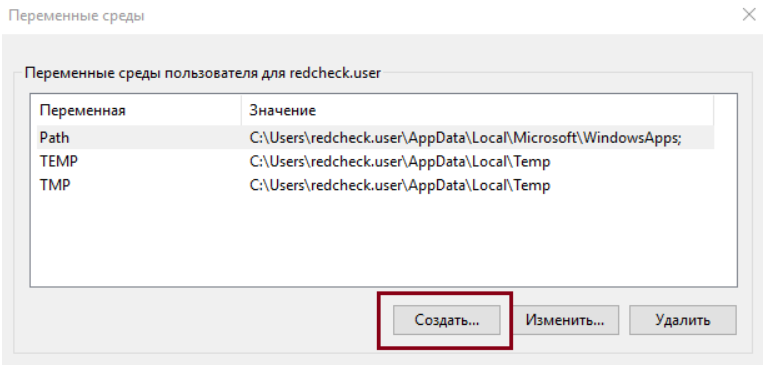
Шаг 2. Перейдите в **Дополнительные параметры системы**;



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

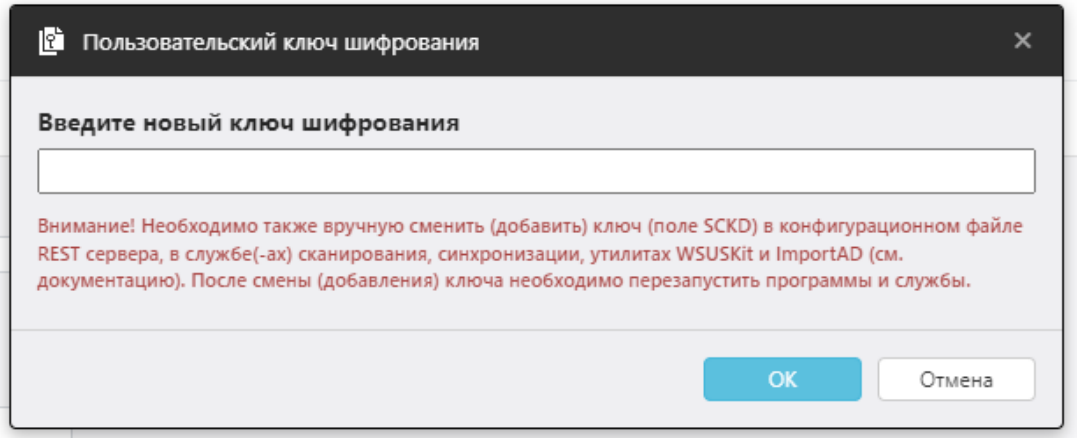
```
GRANT CONNECT TO <USER NAME>;
GRANT SELECT ON DBA_USERS TO <USER NAME>;
GRANT SELECT ON DBA_USERS_WITH_DEFPWD TO <USER NAME>;
GRANT SELECT ON DBA_TAB_PRIVS TO <USER NAME>;
GRANT SELECT ON DBA_PROFILES TO <USER NAME>;
GRANT SELECT ON DBA_TS_QUOTAS TO <USER NAME>;
GRANT SELECT ON DBA_ROLE_PRIVS TO <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.

4.5 Смена ключа шифрования

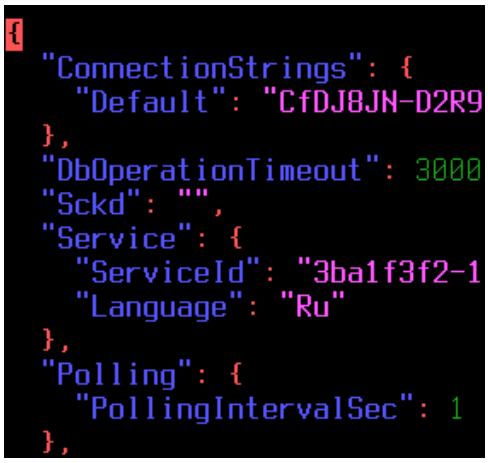
Шаг 1. Откройте консоль управления RedCheck, авторизовавших под учетной записью с ролью RedCheck_Admins → **Справка** → **Сменить ключ шифрования**;

Шаг 2. Введите новый ключ шифрования → **OK**;



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**



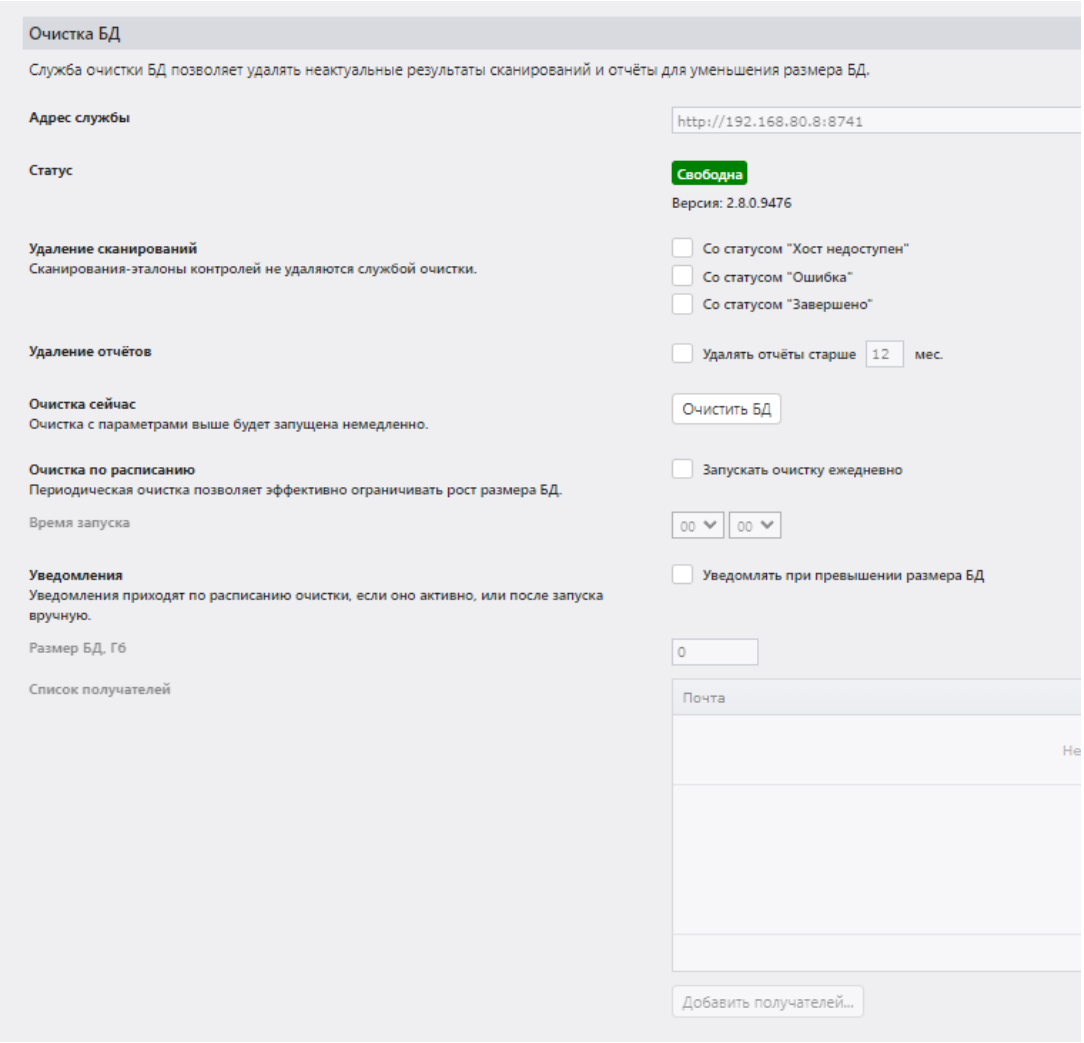
Шаг 5. На хосте с установленной службой синхронизации необходимо открыть файл **/var/opt/redcheck-sync-service/conf/appsettings.json** и заменить старый ключ на новый для параметра **Sckd**

4.6 Обслуживание БД

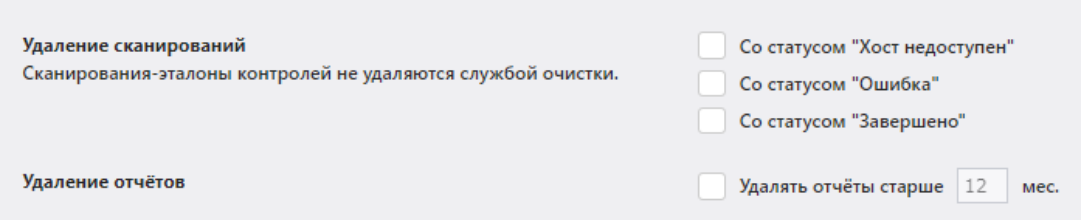
Шаг 1. Откройте консоль управления RedCheck → на панели навигации выберите **Инструменты** → **Настройки**;

> 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;

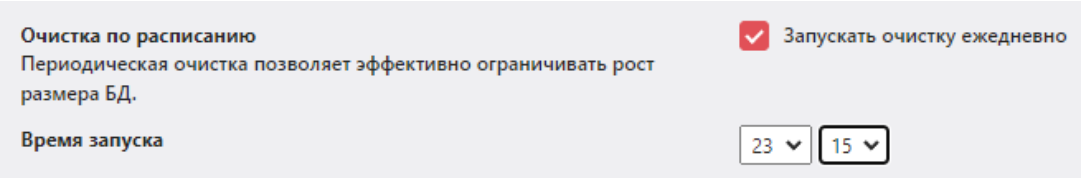


Шаг 3. Выберите какие сканирования и отчеты необходимо удалить;

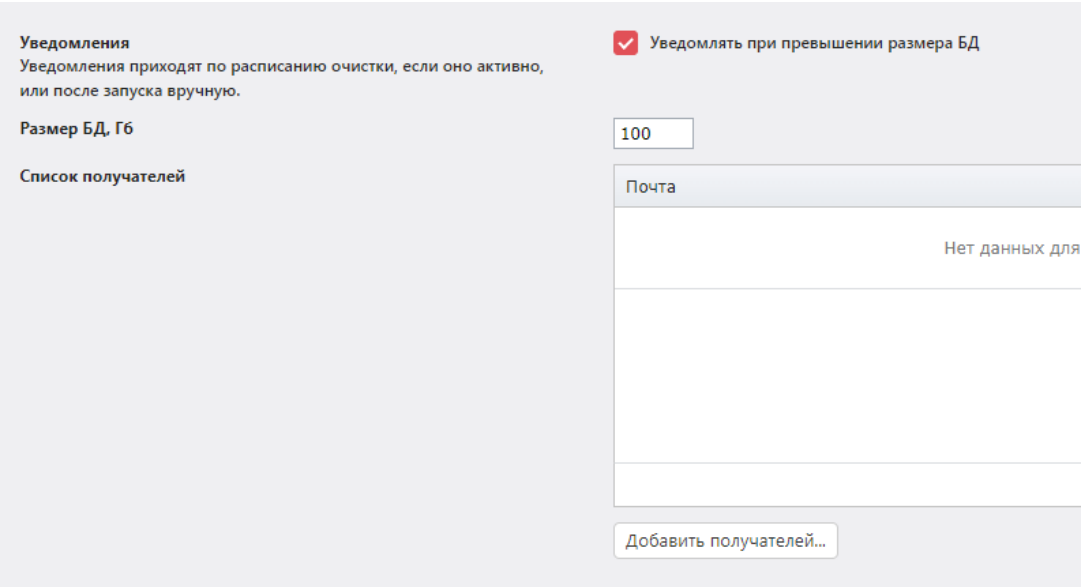


Нажмите **Очистить БД**, чтобы назначить службе задачу;

Шаг 4. Для автоматической очистки БД отметьте **Запускать очистку ежедневно** → выберите время запуска службы очистки;



Шаг 5. При необходимости включите оповещение о превышении БД указанного размера, отметив **Уведомлять при превышении размера БД** и указав почтовые адреса получателей.



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

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.

Для обновления RedCheck необходимо выполнить следующие шаги:

Шаг 1. Скачайте обновленный архив, переместите скачанный архив *.tar.gz в директорию, отличную от пользовательского каталога. В инструкции архив перемещается в /mnt;

Bash (оболочка Unix)

```
mv /home/имя_пользователя/Загрузки/redcheck-repo-2.8.0.tar.gz /mnt/
```

Шаг 2. Перейдите в каталог, удалите текущий репозиторий и разархивируйте свежий дистрибутив;

Bash (оболочка Unix)

```
cd /mnt
rm -R redcheck-repo
tar -xf redcheck-repo-2.7.0.tar.gz
```

Шаг 3. Добавьте информацию в пакетный менеджер о новых .NET пакетах, если ранее это не выполнялось;

Astra Linux:

Для обновления нужен base-репозиторий Astra Linux 1.7.6

Bash (оболочка Unix)

```
echo "deb https://dl.astralinux.ru/astra/frozen/1.7_x86-
64/1.7.6/repository-base 1.7_x86-64 main contrib non-free" >
/etc/apt/sources.list
```

Bash (оболочка Unix)

```
echo "deb file:/mnt/redcheck-repo/ 1.7_x86-64 non-free dotnet" >
/etc/apt/sources.list.d/redcheck.list
```

РЕД ОС:

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck-dotnet.repo

echo -e "[redcheck-dotnet-repo]
name=ALTX .NET 6.0.35
baseurl=file:/mnt/redcheck-redos-repo/redcheck-dotnet
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-redos-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck-dotnet.repo
```

SberLinux:

Bash (оболочка Unix)

```
touch /etc/yum.repos.d/redcheck-dotnet.repo

echo -e "[redcheck-dotnet-repo]
name=ALTX .NET 6.0.35
baseurl=file:/mnt/redcheck-sber-repo/redcheck-dotnet
enabled=1
gpgcheck=0
gpgkey=file:/mnt/redcheck-sber-repo/redcheck-base/PUBLIC-GPG-KEY-
redcheck" > /etc/yum.repos.d/redcheck-dotnet.repo
```

Шаг 4. Обновите пакеты;

Astra Linux:

Bash (оболочка Unix)

```
apt-key add /mnt/redcheck-repo/PUBLIC-GPG-KEY-redcheck

apt -y update
```

РЕД ОС / SberLinux:

Код

```
dnf makecache
```

Шаг 5. Обновите компоненты RedCheck;

Astra Linux:

Bash (оболочка Unix)

```
apt -y install redcheck-dotnet-runtime redcheck-aspnetcore-runtime
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-
service altxmap redcheck-cleanup-service
```

РЕД ОС / SberLinux:

Bash (оболочка Unix)

```
dnf -y upgrade redcheck-dotnet-runtime redcheck-aspnetcore-runtime
redcheck-api redcheck-client redcheck-scan-service redcheck-sync-
service altxmap redcheck-cleanup-service
```

На этапе обновления пакетов введите Y или I для обновления конфигурации:

```
Настраивается пакет redcheck-api (2.7.0~alpha484+build278) …

Файл настройки «/var/opt/redcheck-api/conf/appsettings.json»
 ==> Изменён с момента установки (вами или сценарием).
 ==> Автор пакета предоставил обновлённую версию.
  Что нужно сделать? Есть следующие варианты:
   Y или I : установить версию, предлагаемую сопровождающим пакета
   N или O : оставить установленную на данный момент версию
      D    : показать различия между версиями
      Z    : запустить оболочку командной строки для проверки ситуации
 По умолчанию сохраняется текущая версия файла настройки.
*** appsettings.json (Y/I/N/O/D/Z) [по умолчанию N] ?
Ход выполнения:  [ 79%] [#################################.....]
```

Шаг 6. Заново проведите конфигурацию компонентов RedCheck.

Перед повторной конфигурацией **рекомендуем** сделать резервную копию базы данных.

Bash (оболочка Unix)

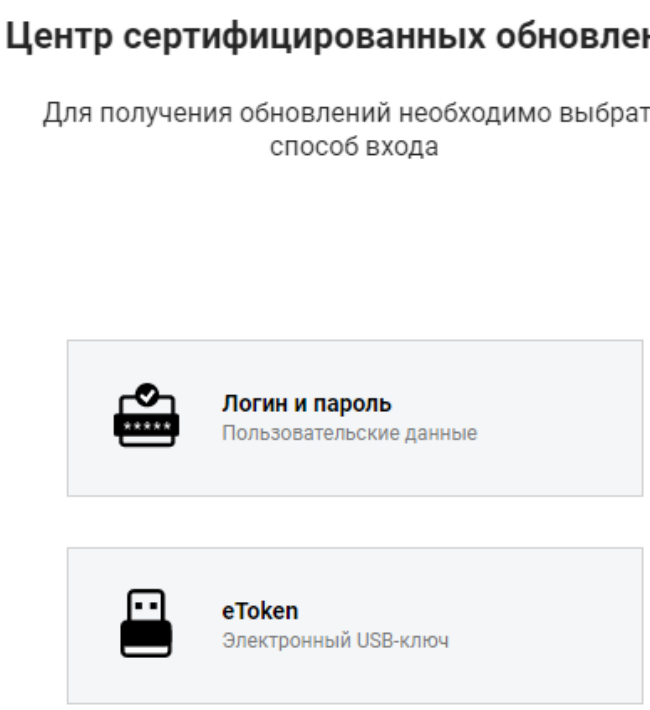
```
redcheck-bootstrap configure -c=all
```

В повторной конфигурации нуждается Web-консоль и служба сканирования / служба синхронизации. Этап с **настройкой подключения к БД** можно пропустить.

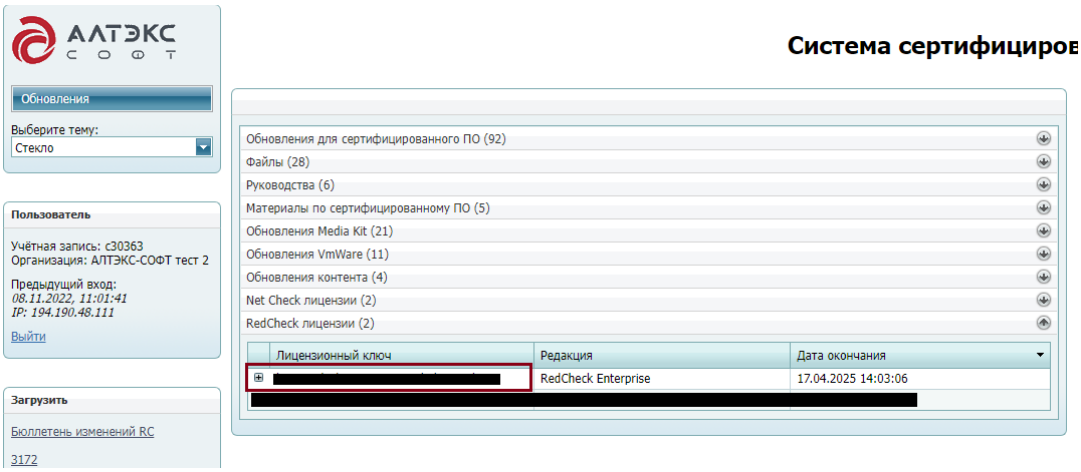
4.9 Сброс привязки лицензии

Шаг 1. Авторизуйтесь в Центре сертифицированных обновлений с помощью логина и пароля;

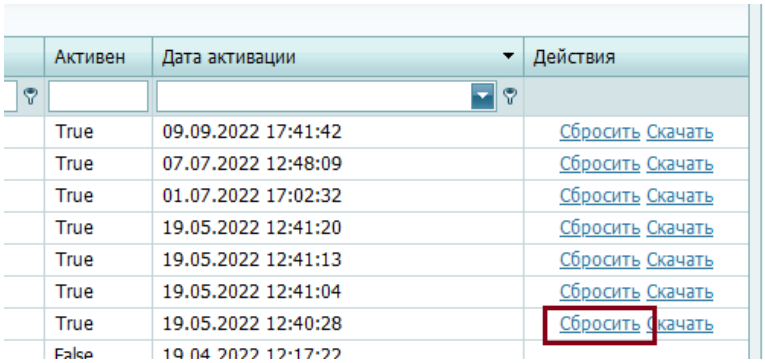
> Логин/пароль поставляется всем коммерческим клиентам в разделе 15, «Особые отметки» (начиная с 18.05.2022).



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



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

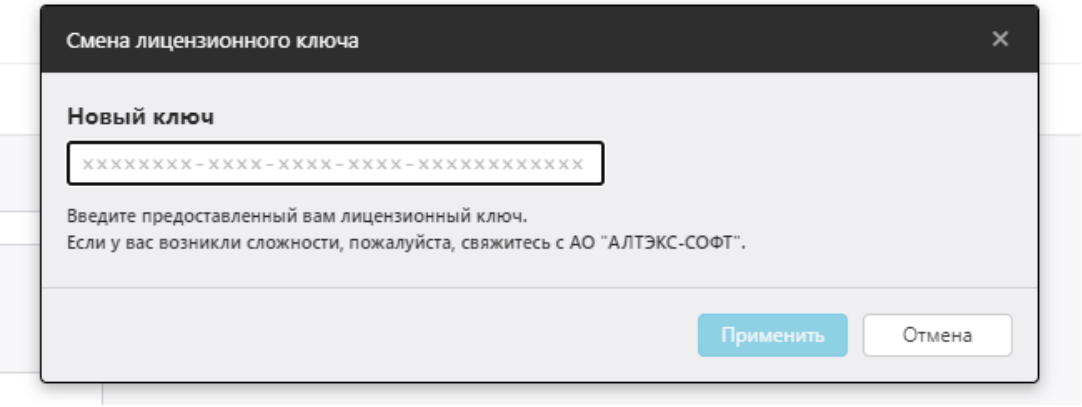


Шаг 4. Нажмите **ОК**.

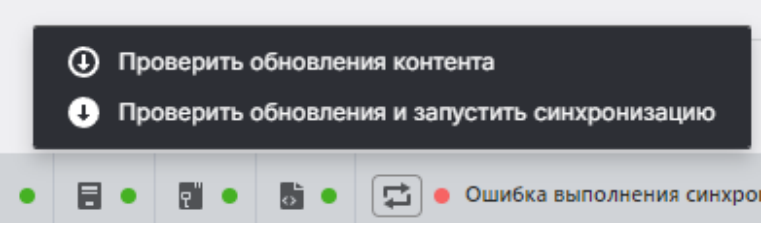
4.10 Смена лицензионного ключа

Шаг 1. Откройте консоль управления RedCheck, авторизовавших под учетной записью с ролью RedCheck_Admins → **Справка** → **Сменить лицензионный ключ**;

Шаг 2. Введите новый лицензионный ключ → **ОК**;



Шаг 3. Выполните синхронизацию (4.3 Обновление контента информационной безопасности).



> Для офлайн-синхронизации необходимо получить License.xml файл (4.2 Активация лицензии)

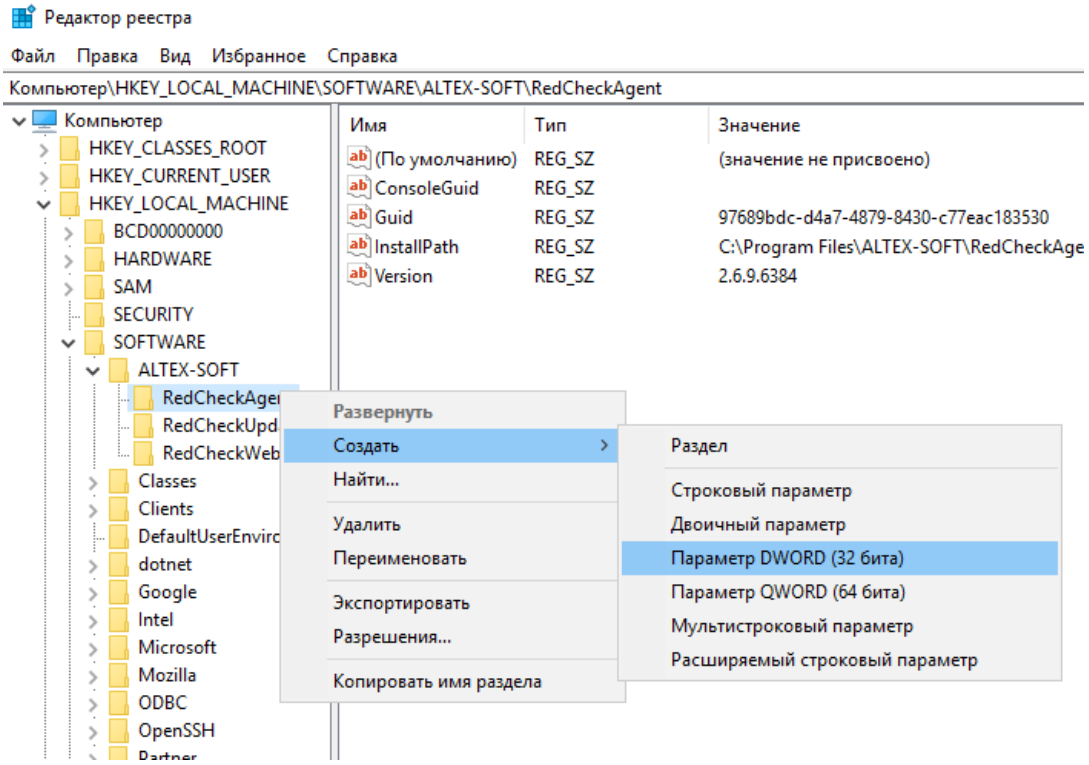
> Смена ключа и его активация осуществляется после завершения синхронизации контента.

4.11 Изменение порта для Агента сканирования

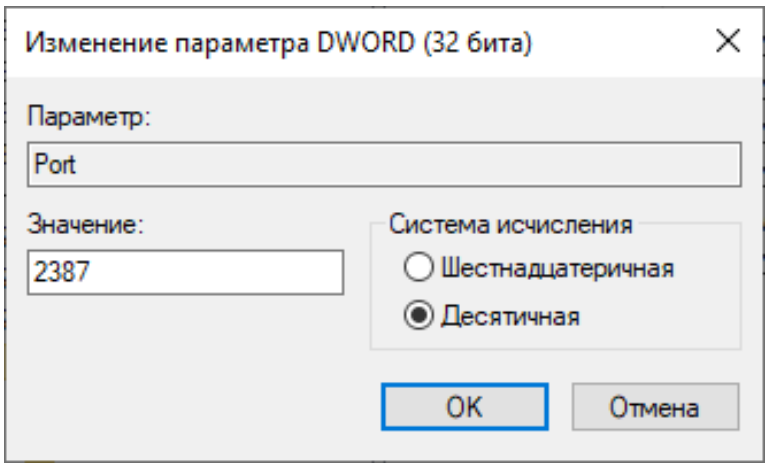
Стандартный порт Агента **TCP/IP 8732**.

Шаг 1. Зайдите в реестр хоста с установленным агентом и создайте новый параметр **DWORD** с именем **Port**;

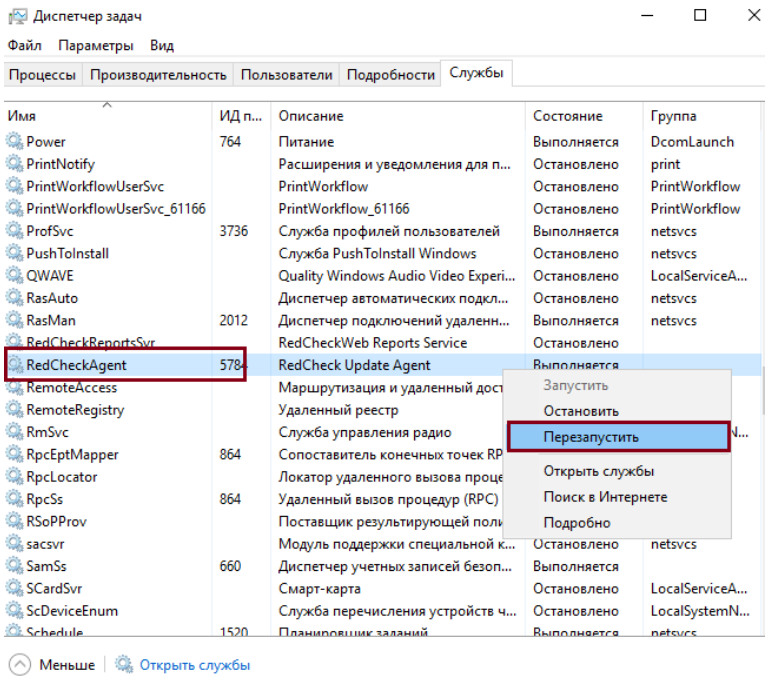
> Для x-86 разрядных систем: **HKEY_LOCAL_MACHINE\ SOFTWARE\ Wow6432Node\ ALTEX-SOFT\ RedCheckAgent\ Port (DWORD)**
> Для x-64 разрядных систем: **HKEY_LOCAL_MACHINE\ SOFTWARE\ ALTEX-SOFT\ RedCheckAgent\ Port (DWORD) D)**



Присвойте ему необходимое значение → **OK**;



Шаг 2. Нажмите **Ctrl + Alt + Delete** → **Диспетчер задач**. Перейдите в **Службы** → ПКМ по **RedCheckAgent** → **Перезапустить**;

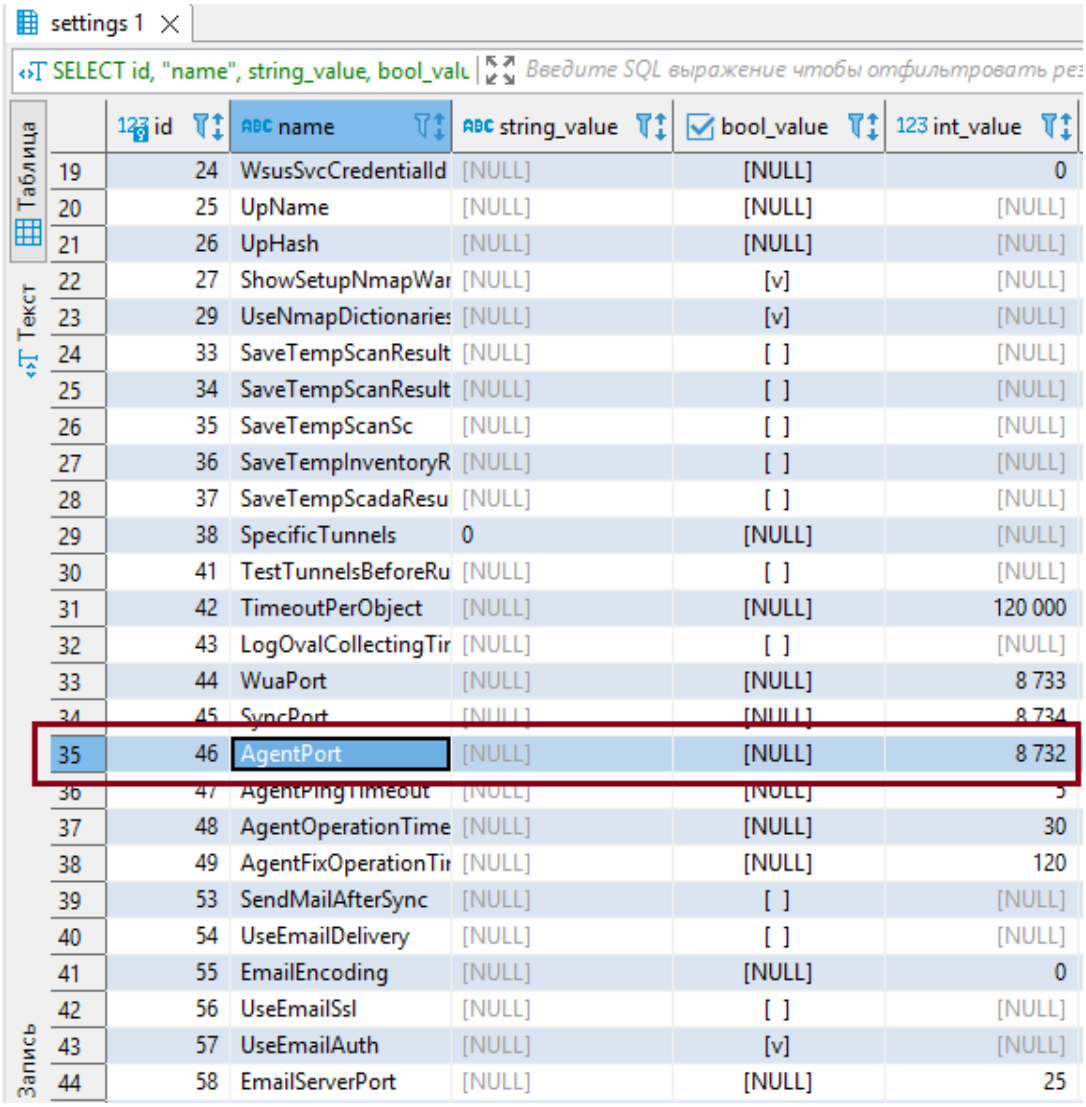


Для сканирования сегмента сети, в которой для Агента установлен альтернативный порт, используется учетная запись RedCheck с указанием переопределенного порта по умолчанию.

Изменение порта по умолчанию

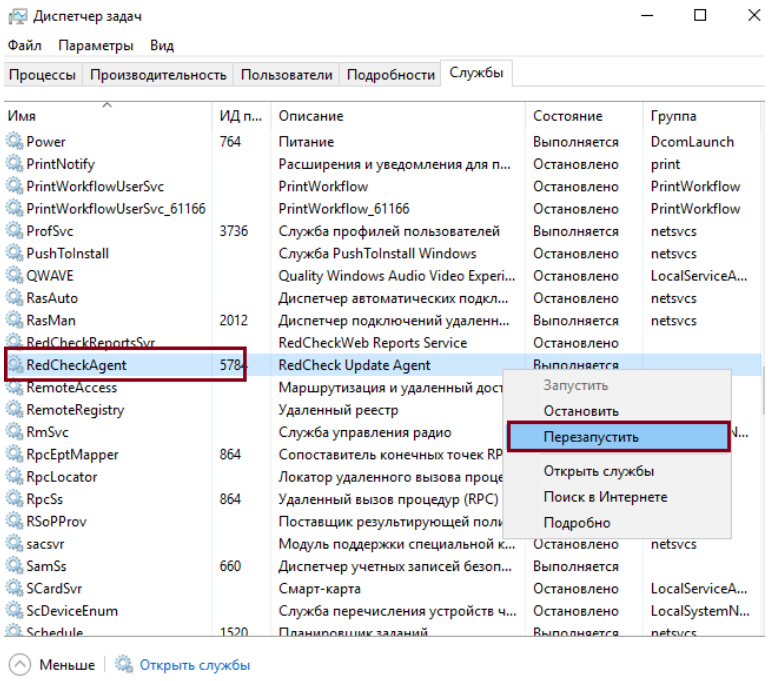
Порт по умолчанию используется для сканирования в тех случаях, когда не указано альтернативное значение в УЗ RedCheck.

Шаг 1. В БД RedCheck найдите таблицу **settings** → в столбце **name** найдите поле **AgentPort** и внесите новое значение порта;



	id	name	string_value	bool_value	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
RedCheckReportsSvc RedCheckWeb Reports Service Остановлено
RedCheckAgent 5784 RedCheck Update Agent Выполняется
RemoteAccess Маршрутизация и удаленный дост
RemoteRegistry Удаленный реестр
RmSvc Служба управления радио
RpcEptMapper 864 Сопоставитель конечных точек RP
RpcLocator Локатор удаленного вызова проце
RpcSs 864 Удаленный вызов процедур (RPC)
RSoPProv Поставщик результирующей поли
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
Запустить
Остановить
Перезапустить
Открыть службы
Поиск в Интернете
Подробно
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.

Обычные логи располагаются в каталогах /var/opt

- /redcheck-api/log – серверный компонент;
- /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.

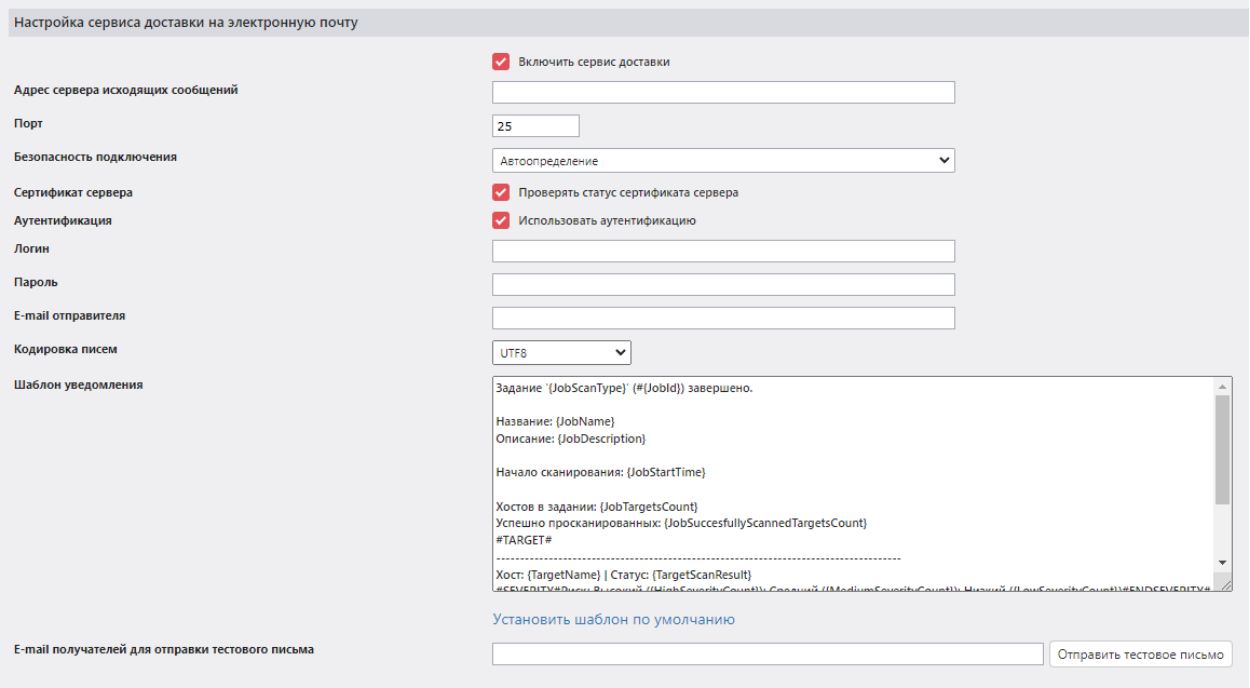
4.13 Настройка сервиса доставки отчетов

Возможна доставка отчетов через комплексы однонаправленной передачи данных InfoDiode из защищаемого сегмента в иные сетевые сегменты.

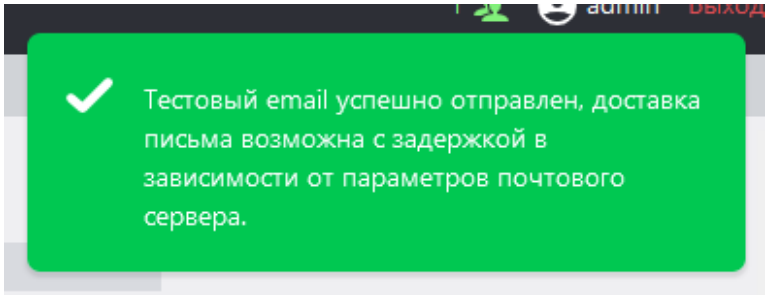
- Информационная справка
- Сайт производителя

Инструкция по настройке предоставляется производителем по запросу или в составе эксплуатационной документации.

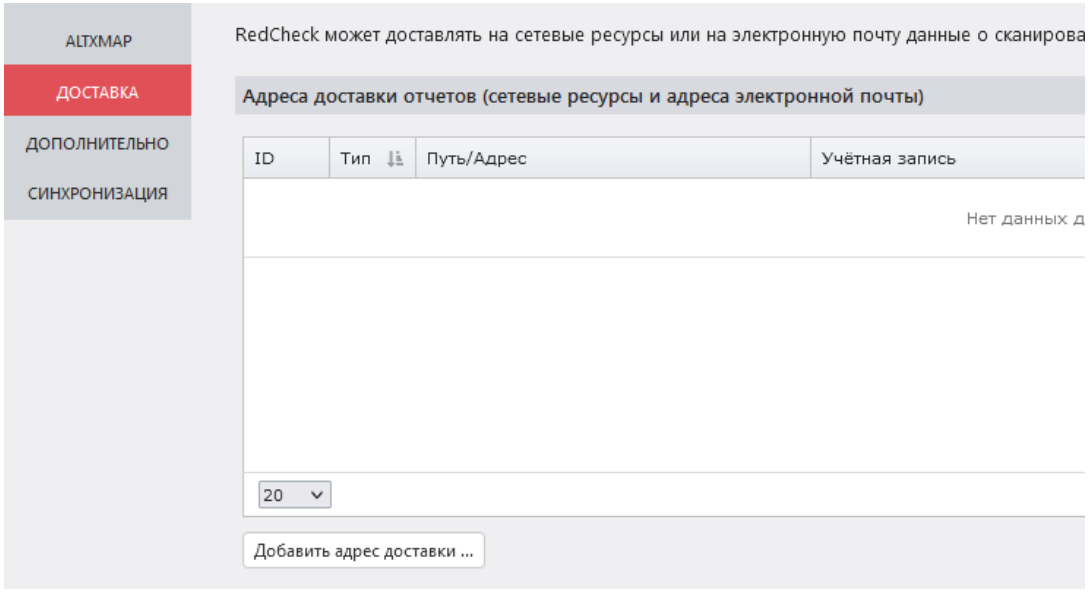
Шаг 1. Откройте консоль управления RedCheck, авторизовавших под учетной записью с ролью RedCheck_Admins / RedCheck_Systems → **Инструменты** → **Настройки** → перейдите в **Доставка** → в разделе **Настройка сервиса доставки на электронную почту** отметьте **Включить сервис доставки**;



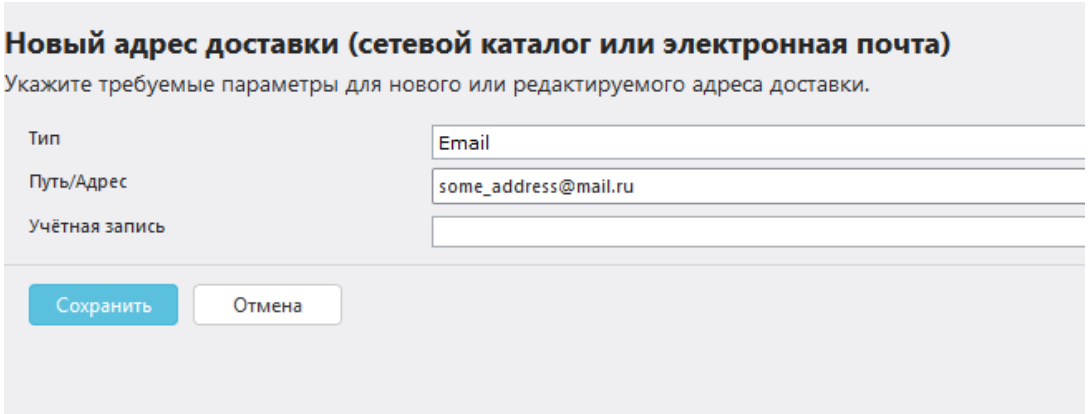
Шаг 2. Укажите необходимые данные для отправки писем → нажмите **Отправить тестовое письмо** для проверки;



Шаг 3. Чтобы добавить email, нажмите **Добавить адрес доставки**;



Шаг 4. Укажите **Тип** адреса доставки **Email** и адрес почты в поле **Путь/Адрес**→ **Сохранить**;



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
Дополнительные компоненты (Windows-компоненты)	

Сервер обновлений: C:\Program Files (x86)\ALTEX-SOFT\RedCheckUpdateServer	\RcUpdSrv.exe
Агент сканирования: C:\Program Files\ALTEX-SOFT\RedCheckAgent C:\Program Files (x86)\ALTEX-SOFT\RedCheckAgent	\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

```
Bash (оболочка Unix)
sudo apt -y install realmd krb5-user sssd-tools sssd libnss-sss libpam-sss adcli
```

РЕД ОС

```
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

sudo reboot
```

Шаг 4. Настройте сеть для доступа к DNS-серверу, который используется контроллером домена;

Astra Linux

Bash (оболочка Unix)

```
sudo nano /etc/resolv.conf

search domain.local
nameserver ip_dns_server
```

- search domain.local – укажите имя домена;
- nameserver ip_dns_server – укажите IP-адрес DNS-сервера;

РЕД ОС

Создайте файл ifcfg-[идентификатор интерфейса];

Bash (оболочка Unix)

```
sudo touch /etc/sysconfig/network-scripts/ifcfg-eth0

PEERDNS=no
DNS1=IP_address

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

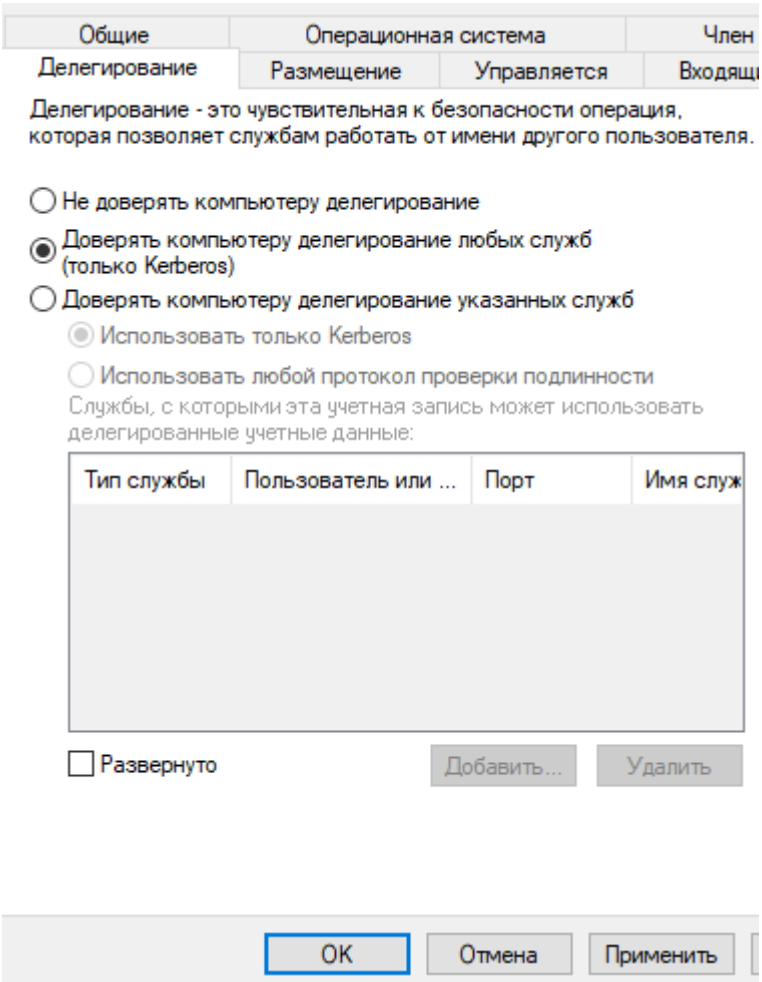
Bash (оболочка Unix)

```
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)** → **OK**;



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

[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

klist
```

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

read_kt /etc/krb5.keytab

list -k -e
```

Получим примерно следующий вывод:

Bash (оболочка Unix)

```
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
--------
   1    2 ASTRA$@DOMAIN.LOCAL (arcfour-hmac)
(0x28b528ce88fba1e27fdcc3ff4cea627a)
   2    2 ASTRA$@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)
(0x28b528ce88fba1e27fdcc3ff4cea627a)
   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)
(0x28b528ce88fba1e27fdcc3ff4cea627a)
   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)
(0x28b528ce88fba1e27fdcc3ff4cea627a)
  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)  (0x28b528ce88fba1e27fdcc3ff4cea627a)
  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 1 -e aes256-cts-hmac-sha1-96

write_kt /etc/astra.HTTP.keytab

sudo chown root.redcheck /etc/astra.HTTP.keytab

sudo chmod g+r /etc/astra.HTTP.keytab
```

При необходимости можно просмотреть содержимое astra.HTTP.keytab

Bash (оболочка Unix)

```
sudo ktutil

read_kt /etc/astra.HTTP.keytab

list -k -e
```

Создание Keytab файла на контроллере домена (Способ 2)

Шаг 1. Выполните следующие команды в PowerShell:

Bash (оболочка Unix)

```
setspn -S HTTP/astra.domain.local ASTRA

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:

Bash (оболочка Unix)

```
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-api, в директорию /etc/:

Bash (оболочка Unix)

```
sudo chown root.redcheck /etc/astra.HTTP.keytab

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

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

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 configure -c=all

sudo nano /var/opt/redcheck-client/conf/redcheck-web.dll.config
```

```
  GNU nano 3.2                                  /var/opt/redcheck-clien

<?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>
```

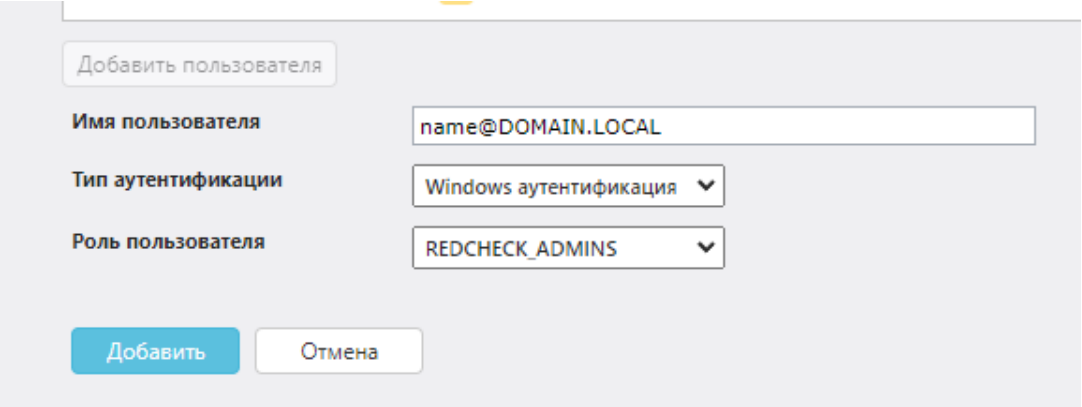
Перезапустите redcheck-client;

Bash (оболочка Unix)

```
sudo systemctl restart redcheck-client
```

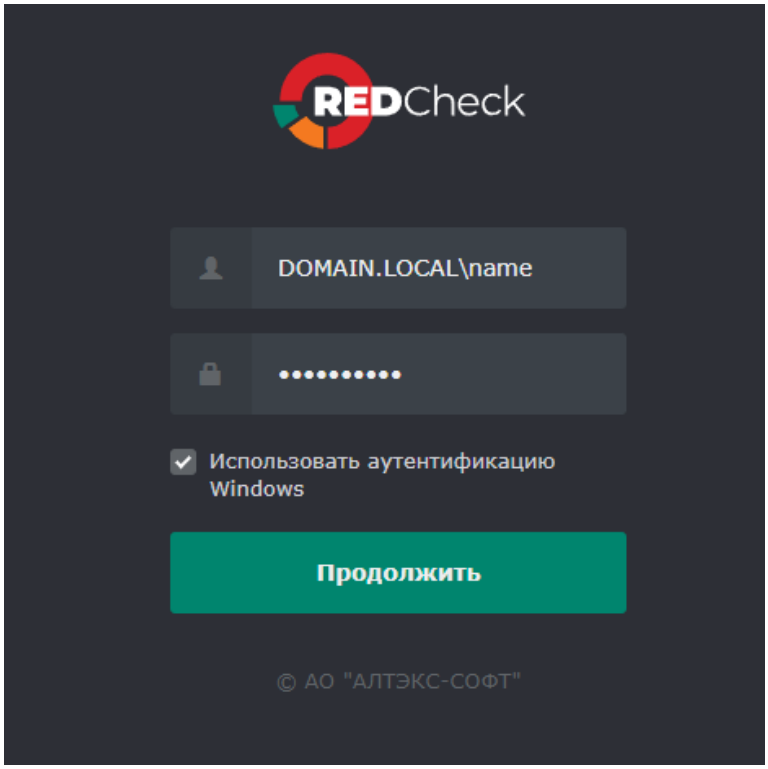
Шаг 13. Создайте пользователя для авторизации в RedCheck (4.1 Настройка ролевой модели):

- Тип аутентификации – Windows аутентификация
- Имя пользователя – name@DOMAIN.LOCAL



Для авторизации:

- Указывайте имя пользователя в формате **DOMAIN.LOCAL\name** или **name@DOMAIN.LOCAL**
- Отметьте **Использовать аутентификацию Windows**


REDCheck
DOMAIN.LOCAL\name
••••••••••
Использовать аутентификацию Windows
Продолжить
© АО "АЛТЭКС-СОФТ"

4.16 Дополнительные настройки для сканирования

Откройте консоль управления → **Инструменты** → **Настройки** → **Сканирование**;

Параллельность сканирования

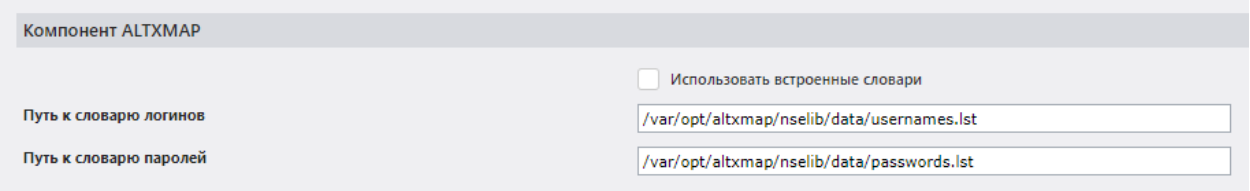
- Число параллельных заданий [1-5] – сколько заданий может выполняться одновременно. При увеличении значения увеличивается нагрузка на ЦП;
- Число параллельных сканирований в задании – сколько хостов будут сканироваться одновременно в рамках одного задания. Не рекомендуется указывать значение, превышающее 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.

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



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 «АЛТЭКС-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 OVALdb	БД определений проблем безопасности
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