



# iTman Discovery

## О системе

Версия: 5.5

Москва

06.12.2024



## Оглавление

<a href="#">1. Обзор возможностей.....</a>	<a href="#">3</a>
<a href="#">2. Глоссарий.....</a>	<a href="#">4</a>
<a href="#">3. Схема работы и компоненты .....</a>	<a href="#">7</a>



## 1. Обзор возможностей

«iTman Discovery» – система для управления ИТ-инфраструктурой (рабочие места, серверы и т.д.) и контроля информационной безопасности. Наше решение помогает обслуживать устройства и проводит инвентаризацию программного обеспечения, железа, пользователей, устройств в одном окне.

Ключевые возможности платформы:

- Сбор данных и обнаружение устройств
  - Автоматический поиск и обнаружение устройств в режиме реального времени
  - Сбор инвентаризационной информации WMI, SSH, SNMP
  - Сбор данных с внешних источников AD, VMWare, SCCM, Samba, FreeIPA
  - Нормализация данных
  - Предоставление данных в реальном времени
  - Аналитические отчеты и графические показатели
  - Настраиваемая модель данных
  - Динамическая модель данных
- Управление ИТ-активами
  - Сохранение и идентификация ИТ-активов
  - Карточки учета ИТ-активов
  - Контроль изменений конфигураций
  - Обогащение данных с ИИ
  - Аналитика исторических данных
  - Графические показатели и аналитические отчеты
- Управление конфигурациями
  - Удаленное развертывание ПО/пакетов
  - Передача данных с технологией peer-to-peer
  - Управление обновлениями программного обеспечения
  - Удаленное управление конфигурациями
  - Управление политиками
  - Применение скриптов и кода
- Выявление инцидентов
  - Поиск уязвимостей по базе (CVE)



- Вывод данных о сроке эксплуатации ОС и ПО
- Сканирование и отображение открытых портов
- Проверка паролей и учетных записей
- Создание собственных правил для поиска уязвимостей
- Настройка правил соответствия конфигураций

Архитектура системы состоит из компонентов, которые общаются между собой: Reader, Server, DataManager, Writer, Interact, Data Base, Agent.

## 2. Глоссарий

**Агент (Discovery Agent)** - программный компонент системы «iTman Discovery», который выполняет сбор данных в рамках задач инвентаризации. Может быть двух видов:

- **Обычный агент (DiscoveryAgentLightNative)** - может только собирать и передавать данные интеракту или другому агенту-шлюзу.
- **Агент-шлюз (DiscoveryAgentNative)** - это агент, который возможностей обычного агента может получать данные от других агентов. Использование агентов-шлюзов позволяет настроить работу агентов в цепочке.

**Активы** - объекты инвентаризации (устройства, ПО, пользователи), которые были добавлены в систему в ходе инвентаризации или вручную.

**Баннер** - всплывающее сообщение с запросом подтверждения, которое отображается пользователю при авторизации в системе. Настраивается в разделе **Администрирование / Общие настройки**.

**Внутренний скрипт** - тип скрипта в сенсоре, который полностью выполняется на уровне агента. Например, к этой группе относятся Файлы, IPMI, LDAP, PortCheck, RestApi, WMI скрипты.

**Идентификация** - этап настроек задачи инвентаризации, определяющий по каким атрибутам система будет идентифицировать объект инвентаризации. На основании этих данных производится сопоставление обнаруженных объектов с теми, которые уже есть в системе. Если сопоставление выявлено - данные объекта обновляются. В ином случае в системе создается новое устройство / ПО / пользователь. Узнайте подробнее о настройке идентификации.

**Инвентаризация** - получение, обработка, хранение, данных об объектах инвентаризации. Автоматическая инвентаризация выполняется агентами с помощью задач. Помимо этого, могут



быть созданы вручную:

- **Устройства** - в разделе **Сбор данных / Все устройства**.
- **Программы** - в разделе **Активы / Все активы / Программное обеспечение**.
- **Пользователи** - в разделе **Активы / Все активы / Пользователи**.

**Интеракт (Discovery Interact)** - программный компонент системы «iTman Discovery», который получает задачи на инвентаризацию от ридера, передает их агентам, получает данные от агентов, обрабатывает их и передает их ридеру.

**Локальный сбор данных** - получение данных агентом с устройства, на котором расположен агент.

**Настраиваемое поле** - поле для заполнения характеристики устройства, которое было создано в системе «iTman Discovery» пользователем в разделе **Администрирование / Поля устройств**. В этом разделе такие поля имеют характеристику "Системное поле" = "Нет". Заполнение таких полей осуществляется в карточках устройств вручную.

**Нормализация** - этап настроек задачи инвентаризации, определяющий какие данные нужно собирать с устройства, с помощью каких сенсоров это нужно делать и какие параметры сенсора содержат те или иные характеристики устройства.

**Объект инвентаризации / Объект сбора данных** - устройство / ПО / пользователь, данные о котором собираются в рамках выполнения инвентаризации.

**Отображаемое имя** - название, которое используется в интерфейсе системы. Обычно настраивается при заполнении каких-либо справочников в системе, например, в разделе **Администрирование**. Ограничений по допустимым символам нет.

**Парольная политика** - требования к паролям пользователей от учетных записей в системе «iTman Discovery». Может задаваться: глобально (для всех пользователей) - в разделе **Администрирование / Общие настройки**. Для группы пользователей - в разделе **Администрирование / Группы пользователей**.

**Пользователь** - в зависимости от места использования:

- **Пользователь системы** - учетная запись пользователя в системе «iTman Discovery», используется для доступа к веб-интерфейсу системы. Управляется в разделе **Администрирование / Пользователи**.

- **Пользователь для инвентаризации** - учетная запись пользователя в вашей системе, из-под которого будет выполнена задача инвентаризации. Данные этих учетных записей управляются в разделе Администрирование / Учетные данные. А далее заполняются в задачах на инвентаризацию. Например, в задаче MS SQL требуется выбрать пользователя, от лица которого будет выполняться запросы к БД.
- **Пользователь устройства** - учетная запись пользователя, под которой он работает на каком-либо устройстве на вашей стороне. Информация об этом собирается при проведении инвентаризации и далее доступна для просмотра в карточке устройства в разделах: **Сбор данных / Все устройства, Активы / Все активы > Устройства, Активы / Все активы > Пользователи.**

**Райтер (Writer)** - программный компонент системы «iTman Discovery», который обеспечивает работу с системными задачами, обработку данных и т.п. Устанавливается и настраивается вместе с сервером.

**Ридер (Reader)** - программный компонент системы «iTman Discovery», который обеспечивает работу задачами инвентаризации, авторизацию в веб-интерфейсе системы, обработку данных при работе с ними через веб-интерфейс. Устанавливается и настраивается вместе с сервером. Имеет отдельные конфигурационные файлы (свои настройки и настройки логов).

**Сенсор** - скрипт, который выполняет сбор данных при инвентаризации. Настраивается в разделе **Сбор данных / Сенсоры** и далее выбирается в задаче на инвентаризацию на этапе **Нормализация.**

**Сервер (Discovery Server)** - программный компонент системы «iTman Discovery», который в том числе осуществляет работу с аккаунтами, отвечает за персонализацию веб-интерфейса системы, хранит ваш лицензионный ключ.

**Сетевой сбор (безагентский сбор)** - сбор данных агентом об устройствах, расположенных в определенном диапазоне сети. Агент должен быть установлен на устройстве, которое также входит в эту сеть. Для сетевого сбора данных не требуется, чтобы агенты были установлены на каждом из устройств, с которого нужно собрать данные.

**Системное имя** - имя какого-либо элемента системы (например, в справочнике), которое используется в качестве идентификатора при интеграции с другими системами (например, при взаимодействии через API). Может содержать только буквы латинского алфавита (A-Z, a-z), цифры (0-9) и специальные символы (точка, дефис, подчеркивание).

**Системное поле** - поле для заполнения характеристики устройства, которое было предустановлено в системе в разделе **Администрирование / Поля устройств**. В этом разделе такие поля имеют характеристику "Системное поле" = "Да". Заполнение таких полей осуществляется автоматически при проведении инвентаризации.

**Статус устройства** - текущий статус устройства. Список статусов вы можете настроить в справочнике **Администрирование / Статусы устройств**. Далее этот статус присваивается устройству: вручную в карточке устройства в разделах **Сбор данных / Все устройства**, или через раздел **Активы / Все активы**. Автоматически, в разделе **Активы / Настройки активов** с помощью задачи **Выставление статусов устройств**.

**Трекинг** - тип задачи инвентаризации, в рамках которой производится отслеживание времени использования ПО пользователем.

**Цепочка агентов** - тип взаимодействия агентов системы «iTman Discovery», при котором некоторые агенты могут передавать данные не напрямую интеракту, а агенту-шлюзу

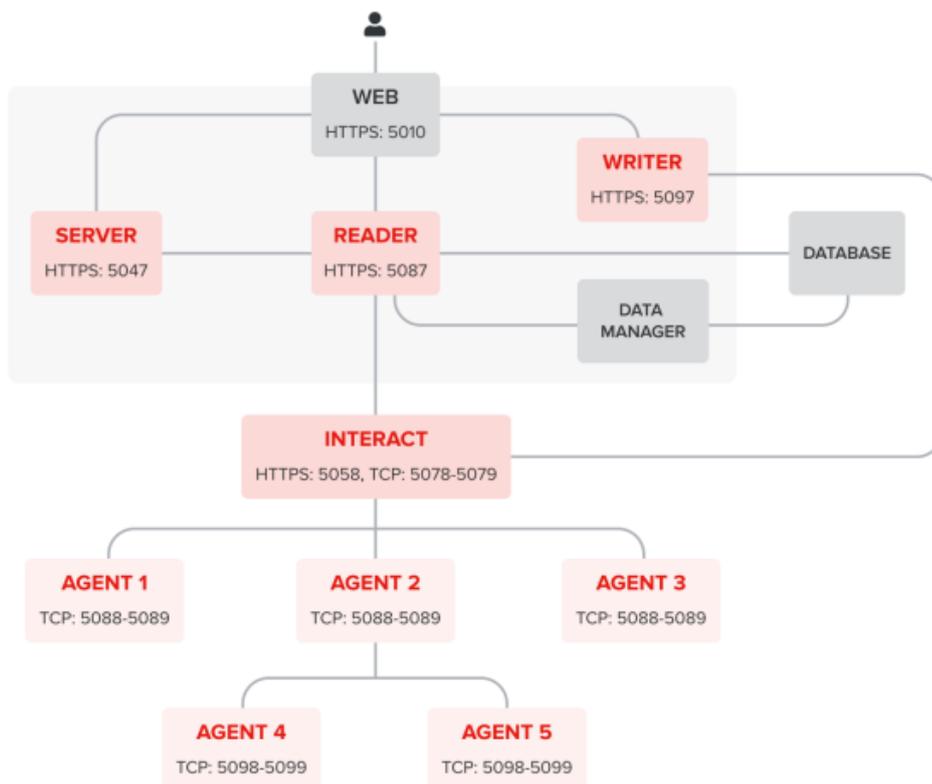
**IP размещение** - название расположения устройства, которое будет отображаться в разделе **Сбор данных / Все устройства**, при соответствии IP-адреса. Позволяет сделать IP адреса "читаемыми", т.е. наглядными для восприятия. Соответствие названий и IP адресов настраивается в разделе **Администрирование / IP размещение**.

### 3. Схема работы и компоненты

Архитектура системы состоит из нескольких компонентов, которые могут быть установлены на разные компьютеры.

Основной процесс работы выглядит следующим образом:

- Вы через веб-интерфейс создаете задачи, например, на проведение инвентаризации.
- Эти задачи через интеракт поступают к агентам, приложениям, которые устанавливаются на компьютеры системы.
- Агенты выполняют сбор данных и возвращают их интеракту.
- Данные агрегируются в системе.
- Вы через веб-интерфейс получаете доступ к результатам выполнения задач и отчетам.



Основные задачи компонентов системы выглядят следующим образом:

#### **Server** (https: 5047)

- Работа с аккаунтами и группами аккаунтов
- Авторизация
- Персонализация системы
- Ключ лицензии

#### **Writer** (https: 5097)

- Работа с системными задачами
- Обработка данных
- Отправка команд на удаление обработанных данных
- Получение служебной информации

#### **Reader** (https: 5087)

- Работа с задачами инвентаризации
- Авторизация
- Обработка данных при редактировании с Web



## Data Manager

- Обработка и анализ данных по задачам инвентаризации

## Interact (https: 5058, tcp: 5078-5079)

- Получение данных от агентов
- Получение служебной информации
- Обработка данных
- Отправка команд на удаление отработанных данных

## Агенты (tcp: 5088-5089)

- Получение задач на инвентаризацию
- Сбор данных с компьютера, на котором установлен агент
- Передача данных интеракту или агенту-шлюзу

Варианты организации работы агентов:

- **Прямое взаимодействие** - агенты передают данные интеракту напрямую.
- **Цепочка агентов** - агенты передают данные другим агентам, которые в свою очередь передают данные интеракту.

Цепочки агентов используются, например, если интеракт и агенты находятся в разных локальных сетях и не имеют доступа во внешнюю сеть.

Такое возможно, если в вашей компании несколько офисов, и в каждом из них только один компьютер имеет доступ во внешнюю сеть.

В таком случае:

- На компьютер, имеющий доступ к внешней сети, устанавливается агент, который выполняет роль шлюза.
- Все агенты внутри локальной сети отправляют данные на агент-шлюз.
- Далее агент-шлюз передает данные или интеракту или (как показано на схеме ниже) другому агенту-шлюзу, который в свою очередь уже передает их интеракту.

ВНЕШНЯЯ СЕТЬ

