

OOO «СОЛАР СЕКЬЮРИТИ»
Компания группы ПАО «Ростелеком»
Никитский пер.7, cтр.1, г. Москва, Россия,
125009

T +7 (499) 755-07-70
E info@rt-solar.ru
W [rt-solar.ru](http://rt-solar.ru)

Solar Lighthouse.

Руководство системного администратора.

Москва, 2024

Оглавление

[1. Обозначения и сокращения 4](#_Toc183522897)

[2. Термины и определения 5](#_Toc183522898)

[3. Введение 6](#_Toc183522899)

[4. Общие сведения 7](#_Toc183522900)

[4.1 Наименование программы 7](#_Toc183522901)

[4.2 Назначение и область применения программы 7](#_Toc183522902)

[4.3 Основные функции программы 7](#_Toc183522903)

[4.3.1 Настройка модулей и их конфигурации 7](#_Toc183522904)

[4.3.2 Агрегация информации об активах из различных источников 8](#_Toc183522905)

[4.3.3 Поиск активов путем активного сканирования 8](#_Toc183522906)

[5. Условия выполнения программы 8](#_Toc183522907)

[5.1 Требования к составу и параметрам технических средств 8](#_Toc183522908)

[5.1.1 Аппаратное обеспечение для установки (развертывания ПО) 8](#_Toc183522909)

[5.1.2 Аппаратное обеспечение для пользователей 10](#_Toc183522910)

[5.2 Требования к установленному общесистемному и прикладному программному обеспечению 10](#_Toc183522911)

[5.2.1 Программное обеспечение для среды функционирования 10](#_Toc183522912)

[5.2.2 ПО для работы пользователей 10](#_Toc183522913)

[6. Роли пользователей 11](#_Toc183522914)

[7. Архитектура ПО Solar Lighthouse 12](#_Toc183522915)

[8. Варианты развертывания 15](#_Toc183522916)

[Вариант №1 15](#_Toc183522917)

[9. Установка (развертывание программы) 16](#_Toc183522918)

[9.1 Подготовка к установке 17](#_Toc183522919)

[9.2 Установка 17](#_Toc183522920)

[9.4 Удаление программы 18](#_Toc183522921)

[9.5 Проверка работоспособности программы 19](#_Toc183522922)

# 1. Обозначения и сокращения

|  |  |
| --- | --- |
| **Сокращение** | **Расшифровка** |
| АРМ | Автоматизированное рабочее место |
| БД | База данных |
| ОС | Операционная система |
| ПО | Программное обеспечение |
| ПК | Персональный компьютер |
| CD | Continious delivery |
| CI | Continious integration |
| CLI | Command Line Interface |
| JSON | JavaScript Object Notation |
| RAM | Random Access Memory |
| SSD | Solid-State Drive |
| HDD | Hard Disk Drive |
| ОЗУ | Оперативное запоминающее устройство |

# 2. Термины и определения

|  |  |
| --- | --- |
| Термин | Определение |
| Программное обеспечение | Совокупность компьютерных программ (программ для ЭВМ) и программных документов, необходимых для эксплуатации этих программ. |
| Секреты | Идентификационная и аутентификационная информация, которая используется системами и приложениями для аутентификации или в качестве входных данных для сервисов и алгоритмов. |

# 3. Введение

Руководство администратора содержит информацию по администрированию программного обеспечения Solar Lighthouse (далее в тексте также могут быть использованы термины и сокращения: ПО, программа, программное обеспечение, ПО Solar Lighthouse). В руководстве приведено описание действий по администрированию программы, установке (развертыванию), а также проверке работоспособности ПО. Описание действий, доступных для пользователей с другими ролями, приведено в документе "Руководство пользователя".

# 4. Общие сведения

## 4.1 Наименование программы

Наименование ПО – Solar Lighthouse

## 4.2 Назначение и область применения программы

Solar Lighthouse это продукт для управления информационной безопасностью, основная задача которого — помочь пользователям привести свои активы в безопасное состояние, лучше понимать их и выстраивать эффективные процессы для их защиты.

Solar Lighthouse позволит пользователям эффективно интегрироваться с различными источниками информации, проводить активные сканирования инфраструктуры, реализовывать аудит соответствия требованиям и строить процессы по обеспечению безопасности инфраструктуры.

## 4.3 Основные функции программы

### 4.3.1 Настройка модулей и их конфигурации

В интерфейсе реализованы экраны для возможности просмотра/добавления/управления запускаемыми модулями.

Для добавленных модулей есть возможность создать, редактировать и удалить конфигурацию модуля, которая является частным способом настройки модуля.

### 4.3.2 Агрегация информации об активах из различных источников

В продукте предоставлен механизм для запуска модулей, которые могут интегрироваться с различными источниками активов (например хосты) и сохранять их в БД продукта.

В продукте из коробки доступен один модуль для интеграции с Active Directory.

### 4.3.3 Поиск активов путем активного сканирования

В продукте предоставлен механизм для запуска модулей, которые могут проводить активное сканирование инфраструктуры и сохранять найденные активы в БД продукта.

В продукте из коробки доступен один модуль для сканирования с помощью nmap.

# 5. Условия выполнения программы

## 5.1 Требования к составу и параметрам технических средств

### 5.1.1 Аппаратное обеспечение для установки (развертывания ПО)

ПО Solar Lighthouse предназначено для функционирования на аппаратной платформе с архитектурой процессора x86 64-бит.

Требования к аппаратному обеспечению применительно к компонентам программы приведены в Таблице №1.

Таблица . Требования по компонентам

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Компонент** | **Количество** | **Требования** | **Процессор** | **ОЗУ** | **Диск** |
| Core Service  | 1 на инфраструктуру | Желательные | 2 ядра | 4Gb | 100Gb |
| Минимальные | 2 ядра | 4Gb | 100Gb |
| База данных Core Service | 1 на инфраструктуру | Желательные | 2 ядра | 4Gb | 100Gb |
| Минимальные | 2 ядра | 4Gb | 100Gb |
| Asset Manager | 1 на инфраструктуру | Желательные | 4 ядра | 8Gb | 100Gb |
| Минимальные | 2 ядра | 4Gb | 50Gb |
| База данных Asset manager  | 1 на инфраструктуру | Желательные | 8 ядра | 16Gb | 100Gb |
| Минимальные | 4 ядра | 8Gb | 50Gb |
| Reflector | 1 на инфраструктуру | Желательные | 2 ядра | 2Gb | 5Gb |
| Минимальные | 2 ядра | 2Gb | 5Gb |
| KeeperModuleБаза данных KeeperVault | По 1 на инфраструктуру | Желательные | 4 ядра | 8Gb | 150Gb |
| Минимальные | 2 ядра | 4Gb | 75Gb |

### 5.1.2 Аппаратное обеспечение для пользователей

Персональный компьютер (или ноутбук) с параметрами не хуже: центральный процессор (CPU) 1,5 ГГц, оперативная память 4 ГБ (RAM), дисковая подсистема 20 ГБ (HDD или SSD), разрешение монитора 1920х1080px, сетевой адаптер 100 Мбит/с (Network).

## 5.2 Требования к установленному общесистемному и прикладному программному обеспечению

### 5.2.1 Программное обеспечение для среды функционирования

* ПО предназначено для работы в среде (в том числе, обеспечивает безопасность среды) со следующими характеристиками и параметрами: операционная система: ОС на базе Linux, такая как: Ubuntu версии 24.04, версия ядра Linux должна быть не ниже версии 4.18 и не выше версии 6.8.

### 5.2.2 ПО для работы пользователей

Для ПК (или ноутбука) пользователя:

* браузер: Google Chrome версии 130 и выше, Firefox версии 131 и выше.

# 6. Роли пользователей

Для работы в программе предусмотрено несколько типов ролей пользователей с предварительно настроенными правами доступа к функциональности. Перечень ролей и их описание приведены в Таблице №2. Некоторые роли имеют технический характер, созданы для работы системы и не предназначены для работы пользователя в графическом интерфейсе. Информация о системных ролях приведена для справочных целей.

Таблица . Роли пользователей ПО Solar Lighthouse

|  |  |
| --- | --- |
| **Роль в программе** | **Описание роли** |
| Администратор | Эта роль предназначена для администраторов. Данная роль применяется для того, чтобы предоставить пользователю доступ на чтение и запись ко всем ресурсам. |

# 7. Архитектура ПО Solar Lighthouse

**Центральные сервисы** – включают компоненты: Core Service, Core Service Database, Asset Manager, Asset Manager Database, Reflector, Keeper, Keeper Database, Vault, Module.

Core Service – Ключевой компонент, отвечающий за бизнес-логику и предоставления API для web-интерфейса. Содержит функционал по управлению и настройкой модулей.

Core Service Database – база данных, в которой хранится данные для настройки модулей.

Asset Manager – сервис, отвечающий за примитивные операции с активами - вариации CRUD, обогащение, установка связей, простейшие фильтры.

Asset Manager Database – база данных, в которой хранится активы, история изменений, модификации, связи, теги.

Reflector – компонент, упрощающий взаимодействие ключевых сервисов с Keeper`ов в закрытых зонах.

Keeper – оркестратор модулей, занимается деплоем и запуском модулей, также отправляет ассеты в ассет-менеджер.

Keeper Database– база данных, в которой хранится информация о модулях и запусках.

Vault – защищенное хранилище секретов.

Module – контейнер выполняющий определенную функциональность по идентификации или сбору активов.

На Рисунке №1 графически представлена архитектура ПО Solar Lighthouse.

Рисунок . Архитектура ПО Solar Lighthouse

Наименования составных частей (программных компонент) и описание их взаимодействия между собой и с внешними сервисами представлены в Таблице №3.

Таблица . Взаимодействие сервисов между собой

|  |  |  |  |
| --- | --- | --- | --- |
| **Наименование компонента** | **Направление взаимодействия** | **С чем взаимодействует** | **Описание взаимодействия** |
| Core Service | -> | База данных Core Service | Персистентное хранилище данных для Core Service  |
| Core Service | -> | Asset Manager | Core Service запрашивает актуальные данные по активам, а так же инициирует создание новых активов пользователем |
| Core Service | -> | Keeper(Через Reflector) | Core Service осуществляет управление и запуск модулей. |
| Asset Manager | -> | База данных Asset Manager | Персистентное хранилище данных для Asset Manager |
| Keeper | -> | Asset Manager(Через Reflector) | Keeper передает найденные ассеты в Asset Manager |
| Keeper | -> | Vault | Сохраняет и получает секреты |
| Keeper | -> | База данных Keeper | Персистентное хранилище данных для Keeper |
| Keeper | -> | Module | Устанавливает, запускает и получает ассеты от модулей |

# 8. Варианты развертывания

В зависимости от той инфраструктуры, где планируется развернуть программное обеспечение и особенностей проекта, возможны разные варианты развертывания программы. Архитектура решения достаточно гибкая и позволяет использовать различные варианты. В данном разделе представлены типовой вариант развертывания программы (но не все возможные). Описание назначения и взаимодействия составных частей (компонентов программы) приведено разделе "Архитектура программы".

## Вариант №1

Через Docker Compose В файле docker-compose.yml описываются все микросервисы. И продукт, состоящий из нескольких микросервисов, запускается одной командой `***docker-compose up -d***`.

# 9. Установка (развертывание программы)

Комплект поставки содержит набор образов контейнеров с компонентами программы и файл `docker-compose.yml` для установки программы. Образы передаются или в виде набора архивов или при помощи доступа в репозиторий образов. Типовой набор содержит файлы согласно данным в Таблице №4:

Таблица . Файлы для установки (развертывании программы)

|  |  |  |  |
| --- | --- | --- | --- |
| **Файл** | **Образ** | **Что содержит** | **Примечание** |
| docker-compose.yml | - |  | Единая точка запуска |
| web-api-server.tar | web-api-server:<tag> | web-api-server |  |
| web-ui.tar | web-ui:<tag> | web-ui |  |
| asset-manager.tar | asset-manager:<tag> | asset-manager |  |
| keeper.tar | keeper:<tag> | keeper |  |

Дополнительную информацию о компонентах программы и их взаимодействии смотри в разделе "Архитектура" (см. раздел 7).

## 9.1 Подготовка к установке

Для установки требуется ПК (или ноутбук) администратора с операционной системой на базе Linux (Debian, Ubuntu и др.) или Windows (с возможностью запустить терминал и команду `***ssh***`).

## 9.2 Установка

Необходимо загрузить файл docker-compose.yml на сервер, на котором будет происходить установка.

Если Docker образа невозможно скачать из публично доступного репозитория, то их необходимо загрузить на сервер через промежуточные сервера, например в сегменте DMZ.

`docker image load -i keeper.tar` - пример запуска для каждого архива с образом

Для установки программы необходимо последовательно выполнить следующие команды в терминале:

* docker-compose up -d
* docker-compose ps

## 9.4 Удаление программы

Для корректного удаления программы необходимо выполнить команды:

***docker-compose down -v***

## 9.5 Проверка работоспособности программы

По результатам установки выполнить команду:

***docker-compose logs -f***

При наличии ошибок или сбоев в работе рекомендуется обратиться к разработчикам программы.