Документация с информацией, необходимой для эксплуатации экземпляра программного обеспечения для управления, мониторинга и настройки систем учета рабочего времени и контроля доступа, охранных и пожарных систем «Smartec Security Platform», предоставленного для проведения экспертной проверки

Содержание

1. ВВЕДЕНИЕ

ПО "*Smartec Security Platform*" (SSP) предназначено для настройки, управления и мониторинга систем безопасности и контроля доступа. ПО имеет мискросервисную архитектуру и является кроссплатформенным. Взаимодействие пользователя с ПО может осуществляться как с помощью графического интерфейса в веб браузере, так и с помощью интерфейса прикладного программирования. ПО позволяет управлять настройками аппаратных средств систем контроля доступа; осуществлять мониторинг состояния всех систем, аудит перемещения сотрудников и посетителей; оповещать о событиях, в том числе нарушениях доступа, взломах, авариях.

2. ТРЕБОВАНИЯ К ПРОГРАММНОМУ И АППАРАТНОМУ ОБЕСПЕЧЕНИЮ

ПО Smartec Security Platform может использоваться на операционных системах, поддерживающих ПО Docker. Для работы приложения также требуется ПО docker compose версии не ниже 2.20.

Минимальные аппаратные требования для работы серверной части системы приведены в таблице:

Количество сотрудников	Количество устройств	ОЗУ (ГБ)	Процессор (ядра, частота)
100	10	24	Intel Core i5 10 поколения/AMD Ryzen 5, не менее 6 ядер, не менее 3 GHz
5 000	30	32	
10 000	10	32	8C, 2.1 GHz
	100	64	
50 000	10	64	10C, 2.1 GHz
	100	128	
100 000	10	128	16C, 2.4GHz
	100	160	
250 000	100	192	20C, 2.4GHz
	250	256	
500 000	100	256	24C, 2.4GHz
	250	384	
	500	512	
1 000 000	250	768	40C, 2.6 GHz
	500	1024	
	10000	2048	

Для работы веб-приложения на клиентских машинах необходим браузер и не менее 8 ГБ ОЗУ. Список поддерживаемых браузеров и их версий представлен ниже:

Браузер	Версия
Chrome	84+
Edge	84+
Firefox	79+
Opera	70+
Yandex Browser	20.7+
Safari	14+

В корпоративной среде должен быть предусмотрен штат администраторов, которые устанавливают, настраивают ПО, а также обеспечивают техническую поддержку пользователей.

3. СОСТАВ ДИСТРИБУТИВА

Имя	Назначение
ssp-<номер версии>.tar	Архив с образами docker-контейнеров сервисов ПО
docker-compose.cluster.servicemesh.yml	Конфигурационный файл для docker-контейнеров, обеспечивающих связь между элементами системы
docker-compose.common.release.yml	Конфигурационные файлы для docker-контейнеров, обеспечивающие хранение и передачу информации между элементами системы
docker-compose.common.yml	
docker-compose.services.release.yml	Конфигурационные файлы для docker-контейнеров, обеспечивающие функции системы мониторинга и контроля управления доступом
docker-compose.services.yml	
release.env	Файл для первоначальной настройки ПО
Install.sh	Файл для установки ПО
Remove.sh	Файл для удаления ПО
Update.sh	Файл для обновления ПО до новой версии
install	Папка, содержащая вспомогательные скрипты, которые могут быть полезны в процессе эксплуатации ПО

В папке install есть следующие скрипты:

- TakeLogsFromContainers.sh – скрипт для формирования архива с логами сервисов;

- VolumeBackup.sh – скрипт для сохранения volume в архив. Для функционирования может понадобиться подключение к сети Internet для получения базового образа (по умолчанию ubuntu, но можно использовать любой образ, в котором есть утилита tar).

- VolumeRestore.sh – скрипт для восстановления volume из архива. Для функционирования может понадобиться подключение к сети Internet для получения базового образа (по умолчанию ubuntu, но можно использовать любой образ, в котором есть утилита tar).

4. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ ПО

Для установки ПО необходимо распаковать архив с установочными файлами в любую доступную оператору папку.

Настроить учетные и сетевые параметры в release.env в соответствии с конфигурацией системы пользователя. Для доступа к веб-приложению обязательно нужно задать переменную HOST_ADDRESS. Значением этой переменной должен быть задан адрес в сети, по которому будут обращаться другие клиенты.

Запустить скрипт для установки ПО:

- на ОС семейства Windows запустить файл Install.sh
- на ОС семейства Linux сделать скрипты исполняемыми:

chmod +x Install.sh, Update.sh, Remove.sh

а затем запустить установку: ./Install.sh.

Для обновления ПО до актуальной версии необходимо распаковать архив с новой версией в папку, в которой лежат установочные файлы от предыдущей версии, или перенести файлы release.env, combined.release.env, tokens.env, pass.kibana_system (при наличии) из папки, откуда была выполнена предыдущая установка.

Запустить скрипт для обновления ПО:

- на ОС семейства Windows запустить файл Install.sh
- на ОС семейства Linux сделать скрипты исполняемыми:

chmod +x Install.sh, Update.sh, Remove.sh

а затем запустить обновление: ./Update.sh.

В процессе обновления будут остановлены все контейнеры системы, затем запущены новые версии контейнеров, которые при запуске запустят миграции своих баз данных.

Для удаления ПО нужно запустить файл Remove.sh.

5. ОПИСАНИЕ СИСТЕМЫ

Развертывание (установка) системы осуществляется в среде Docker, где создается отдельный проект ssp, а также собственная docker-сеть sspweb в подсети 172.30.0.*.

Кластер SSP работает внутри service mesh на основе HashiCorp Consul и Envoy. Service mesh обеспечивает связь между сервисами, а также TLS шифрование. Кроме того, Consul обеспечивает функционирование Service Discovery внутри кластера.

Название	Внешний порт	Volume	Описание	Комментарий
consul	8500	consul	Отвечает за связь между сервисами и service discovery. На web-интерфейсе на порту 8500 отображается текущее состояние узлов и сервисов кластера. Для логина требуется указать токен (Bootstrap token), который находится в файле tokens.env в папке, откуда производилась установка кластера.	При остановке может нарушаться связь между сервисами. Должен запускаться первым.
postgresdb	5432	elasticsearch	Сервер Postgres, на котором находятся все БД сервисов.	
pgadmin	5051	pgadmin	Web-интерфейс для работы с БД.	Connection должен быть настроен на

				адрес хоста контейнера (если контейнер развернут отдельно от остальных контейнеров кластер) или на внутренний адрес контейнера (172.30.0.105)
rabbitmq	15675	rabbitmq	Брокер сообщений. Отвечает за прием и передачу событий от устройств и между сервисами. На Web-интерфейсе отображается текущая информация об очередях передачи сообщений.	На web-интерфейс используется только по указанию тех. поддержки.
Identity	5054		Сервис для авторизации оператора в системе.	Имеет собственную БД
Gateway	5121		API, через который можно взаимодействовать с системой. Также используется web-интерфейсов SSP.	
Employee			Сервис, отвечающий за работу с основными	Имеет собственную БД

			сущностями системы (сотрудники, объекты, уровни доступа и т.д.).	
Reports			Сервис, отвечающий за формирование отчетов по событиям и уровням доступа.	
Events			Сервис, отвечающий за получение событий из внешних источников (устройства, интеграции).	Имеет собственную БД
Files	5122		Сервис, отвечающий за хранение и доступ к данным большого размера (изображения, файлы).	Имеет собственную БД
Devicerouter			Сервис, отвечающий за маршрутизацию связи с сервисами устройств, в случае, если в системе их несколько.	Имеет собственную БД
Smartecdevice			Сервис, отвечающий за работу с контроллерами Smartec.	Имеет собственную БД
Frontend			Web-интерфейс SSP	

6. ОПИСАНИЕ WEB-ИНТЕРФЕЙСА

При первом входе в веб-приложение (http://localhost:10000) будет предложено создать учетную запись администратора. В последствии можно будет создать дополнительные учетные записи для администрирования системы.

В версии SSP 25.1 доступны следующие разделы интерфейса:

1. Мониторинг.
   В мониторинге пользователь может настроить личные (отображаемые только этому оператору) и общие виды, в которых будут отображаться события, приходящие в реальном времени. События могут быть показаны в ячейках двух типов – «События», где события показаны списком, или «Фотоверификация», где выводится информация о событии и связанном сотруднике.
2. Сотрудники.
   В этом разделе осуществляется управление структурой организации (создание/редактирование/удаление подразделений), должностями, сотрудниками. В карточке сотрудника задаются уровни доступа и назначаются номера карт.
3. Администрирование.
   В этом разделе осуществляется управление операторами и ролями. В версии 25.1 доступны роли, ограничивающие доступ к отдельным вкладкам интерфейса.
4. Системы.
   В этом разделе осуществляется управление устройствами (добавление, удаление, конфигурация, запуск операций) и объектами.
5. Контроль доступа.
   В этом разделе можно настроить уровни доступа и временные зоны.
6. Отчеты.
   В этом разделе можно построить отчеты по событиям и уровням доступа, экспортировать их в pdf/csv файлы.

7. ПОЛУЧЕНИЕ СОБЫТИЙ ЧЕРЕЗ API (SIGNALR) В РЕАЛЬНОМ ВРЕМЕНИ

Для получения событий в реальном времени в Gateway функционирует SignalR Hub. Подключиться можно по адресу http://<HOST_ADDRESS>:5121/signalR/events.

На стороне клиента должен быть реализован метод ReceivedEvent. Ниже представлен пример подключения к хабу и обработки полученных событий на C#:

```
signalRConnection.On< string >( "ReceivedEvent", message =>
        {
                Log.Information( $"{DateTime.Now.ToString( "yyyy-MM-dd HH:mm:ss.fff", CultureInfo.InvariantCulture )}: {message}" );
        } );
try
{
        await signalRConnection.StartAsync( stoppingToken );
        Log.Information( $"Connected with id {signalRConnection.ConnectionId}" );
}
catch ( Exception ex )
{
        Log.Error( ex.ToString() );
}
```