# Руководство по установке

# Продукта Platform V SOWA

# (Код продукта SWA)

# ОГЛАВЛЕНИЕ

# Руководство по установке

## Системные требования

Для развертывания СПО SOWA существуют следующие минимальные технические требования:

### Системное программное обеспечение

Для установки, настройки, контроля и функционирования продукта Platform V SOWA необходима установка программного обеспечения сторонних правообладателей, перечисленного в данном разделе.

#### Операционная система

| Наименование | Версия | Применение |
|---|---|---|
| Альт 8 СП | 8/9/10 | Рекомендовано |
| Red Hat Enterprise Linux | 8.5.2 и выше | Опционально |
| РЕД ОС | 7.1/7.2 | Опционально |
| AlmaLinux | 8.3 и выше | Опционально |
| CentOS | 7 | Опционально |
| CentOs Stream | 8 | Опционально |

Объем оперативной памяти зависит от количества сервисов, количества профилей и количества одновременных сессий и запросов.

#### Java-машина

| Наименование | Версия | Применение |
|---|---|---|
| OpenJDK | 1.8 и выше | Рекомендовано |
| OracleJDK | 1.8 и выше | Опционально |

#### Средства управления системными службами

| Наименование | Версия | Применение |
|---|---|---|
| systemd | 219 | Рекомендовано |

### Криптографические провайдеры

| Наименование | Версия | Применение |
|---|---|---|
| CryptoPro JCP | jcp-2.0.40035 | Опционально** |

** Требуется только в случае необходимости использования сервиса service_gost_proxy. Также для использования модуля ГОСТ Proxy необходимо наличие лицензий на продукты КриптоПро JCP и КриптоПро JTLS.

### Средства мониторинга

| Наименование | Версия | Применение |
|---|---|---|
| Zabbix | 3.0 и выше | Опционально |

## Аппаратные требования

Для развертывания СПО SOWA требуется следующая минимальная конфигурация аппаратного обеспечения:

- Архитектура процесса: x86-64.
- Количество ядер: 4.
- ОЗУ: 2-24 ГБ.

Параметры точек монтирования для СПО SOWA приведены в таблице:

| Точка монтирования | Значение по умолчанию | Опции подключения |
|---|---|---|
| /usr/ | 6 ГБ | |
| /usr/local/sowa | 1 ГБ | Владелец 0755, root, root, аналогично всем другим системным директориям. |
| /opt | 2 ГБ | Владелец 0755, root, root, аналогично всем другим системным директориям. |
| /sowa | 12 ГБ | |
| /sowalogs | 50 ГБ | Владелец 1774, sowactl:sowactl. |
| /sowarun | 10 ГБ | Владелец 1770, sowactl:sowactl. |
| /tmp | 4 ГБ | |
| /var | 12 ГБ | Swap не менее 4 GB |

## Настройка окружения

При установке и эксплуатации СПО Platform V SOWA на ОС Альт 8 СП обязательным требованиям является использование в качестве подсистемы инициализации и управления службами сервиса systemd, что обеспечивается например путем установки пакета systemd-sysvinit (https://www.altlinux.org/Systemd)

Для осуществления функции репликации событий интеграция с системами управления событиями безопасности и сервисами логирования посредством использования системного сервиса syslog, а также протоколов Kafka, HTTP и Zabbix. Наличие каких-либо компонентов для поддержки данных протоколов кроме указанных в системных требованиях отсутствует.

В Platform V SOWA возможна интеграция с любыми антивирусами с поддержкой протокола ICAP. Процесс настройки антивируса подробно описан в разделе "Настройка антивируса в SOWA" в Руководстве по системному администрированию.

С системой SIEM существует интеграция с помощью системного сервиса rsyslog. Тип и версия системы SIEM не имеет значения. Использование системы SIEM опционально.

В Patform V SOWA возможна работа с любыми системами управления секретами, осуществляющими интеграцию по API, подобному HashiCorp.

## Ролевая модель

Для работы с SOWA доступны несколько ролей, каждой из которых соответствует определенное количество пользователей.

| Группа | Пользователь | Назначение |
|---|---|---|
| sowaspo | sowaspo | Установка и/или обновление СПО при ручных действиях администратора |
| sowaspo | sowaspodpl | Установка и/или обновление СПО автоматизированными системами DevOps |
| sowactl | sowacfg | Установка и/или обновление ППО при ручных действиях администратора |
| sowactl | sowacfgdpl | Установка и/или обновление ППО автоматизированными системами DevOps |
| sowactl | sowactl | Пользователь, из под которого запускаются системные службы |
| sowactl | sowauser | Просмотр и чтение логов |

# Установка

## Установка СПО SOWA

### Подготовительные действия на сервере

Для развертывания СПО SOWA необходимо выполнить следующие шаги:

1. Обновить пакетный менеджер и репозиторий.
    1. Сервер должен иметь активную подписку на RPM-репозитории rhel7 в случае использования ОС RHEL.
    2. Конфигурационный файл должен быть расположен в */etc/yum.repos.d/*. Для просмотра списка подключенных RPM-репозиториев можно воспользоваться командой:

```
yum repolist all
```

3. Рекомендуется удалить неиспользуемые пакеты (например: gdm, firefox):

```
sudo yum remove gdm firefox -y
```

4. Включить репозиторий EPEL7/EPEL8, если он не включен:

```
sudo yum-config-manager --enable EPEL7
```

```
sudo yum-config-manager --enable EPEL8
```

5. Обновить пакетный менеджер:

```
sudo yum update -y
```

2. Настроить области функционирования для СПО SOWA:

**Внимание! Все нижеперечисленные шаги повлияют на возникновение новых записей в списке блочных устройств.**

**Если необходимо подключить дополнительные диски или создать логический том из нестандартных групп или новых дисков, то можно использовать инструкцию по ссылке: https://kifarunix.com/how-to-create-an-lvm-logical-volume/.**

1. Проверить список, выполнив следующую команду:

```
lsblk
```

2. Создать логические тома в группе rootvg:

*Rootvg* - это дефолтная группа для новых виртуальных машин, в которую включены диски, указанные при создании виртуальной машины.

```
sudo lvcreate -L 10G -n lvsowa rootvg sudo lvcreate -L 10G -n lvsowarun rootvg sudo lvcreate -L 20G -n lvsowalogs rootvg sudo lvcreate -L 2G -n lvusrlocalsowa rootvg
```

**В примере указаны тестовые размеры логических томов, и они должны меняться в зависимости от объема памяти внутренних дисков.**

3. Создать файловые системы для новых блочных устройств:

```
sudo mkfs.ext4 /dev/mapper/rootvg-lvsowa sudo
mkfs.ext4 /dev/mapper/rootvg-lvsowarun sudo
mkfs.ext4 /dev/mapper/rootvg-lvsowalogs sudo
mkfs.ext4 /dev/mapper/rootvg-lvusrlocalsowa
```

4. Создать основные разделы (для логов, артефактов, кэша) в корне системы:

```
sudo mkdir /sowa sudo mkdir /sowarun sudo mkdir
/sowalogs sudo mkdir /usr/local/sowa
```

5. Смонтировать файловые системы в созданные разделы:

```
sudo mount /dev/mapper/rootvg-lvsowa /sowa sudo
mount /dev/mapper/rootvg-lvsowarun /sowarun/ sudo
mount /dev/mapper/rootvg-lvsowalogs /sowalogs/
sudo mount /dev/mapper/rootvg-lvusrlocalsowa
/usr/local/sowa/
```

6. Добавить автомонтирование:

```
sudo sh -c "echo '/dev/mapper/rootvg-lvsowa /sowa
ext4 defaults 1 2' >> /etc/fstab" sudo sh -c "echo
'/dev/mapper/rootvg-lvsowarun /sowarun ext4
defaults 1 2' >> /etc/fstab" sudo sh -c "echo
'/dev/mapper/rootvg-lvsowalogs /sowalogs ext4
defaults 1 2' >> /etc/fstab" sudo sh -c "echo
'/dev/mapper/rootvg-lvusrlocalsowa
/usr/local/sowa ext4 defaults 1 2' >> /etc/fstab"
```

3. Настроить группы и пользователей для работы с СПО и ППО SOWA:
   1. Добавить группы:

```
sudo groupadd sowauser sudo groupadd sowactl
```

   2. Добавить пользователей:

```
sudo useradd -g sowactl -m sowactl sudo usermod -
L -e 1 sowactl   sudo useradd -g sowauser -s
/bin/bash sowauser sudo useradd -g sowactl -s
/bin/bash sowaspo sudo useradd -g sowactl -s
/bin/bash sowaspodpl sudo useradd -g sowactl -s
/bin/bash sowacfgdpl sudo useradd -g sowactl -s
/bin/bash sowacfg
```

*sowauser* - пользователь для чтения логов. Принадлежит любой группе, кроме sowactl. Пользователь должен работать в rbash.

Назначение всех пользователей описано в разделе "Ролевая модель".

3. Скачать и установить утилиту **im-sowa**, необходимую для установки дистрибутива СПО. Данная утилита подробно описана в разделе "SOWA Install manager (im-sowa)". В дистрибутиве вместе с утилитой содержится файл im-sowa.sha256, содержащий хеш-сумму, которую необходимо прописать в алиасе sudoers на следующем шаге.
4. Добавить sudo права для пользователей:

```
sudo bash -c "echo 'Cmnd_Alias
SOWASPO_ALLOW_CMD_001 = sha256:<тут укажите хеш из
файла im-sowa.sha256> /usr/bin/im-sowa *' >
/etc/sudoers.d/sowaspo" sudo bash -c "echo
'sowaspo ALL=(root) NOPASSWD :
SOWASPO_ALLOW_CMD_001' >> /etc/sudoers.d/sowaspo"
sudo bash -c "echo 'Cmnd_Alias
SOWASPODPL_ALLOW_CMD_001 = sha256:<тут укажите хеш
из файла im-sowa.sha256> /usr/bin/im-sowa *' >
/etc/sudoers.d/sowaspodpl" sudo bash -c "echo
'sowaspodpl ALL=(root) NOPASSWD :
SOWASPODPL_ALLOW_CMD_001' >>
/etc/sudoers.d/sowaspodpl
```

5. Изменить права пользователей на директории:

```
sudo chown sowaspo:sowactl -R /sowa/ sudo chown
sowactl:sowactl -R /sowarun/ sudo chown
sowactl:sowactl -R /sowalogs/ sudo chown
sowactl:sowactl -R /usr/local/sowa/
```

6. Изменить пароли:

```
sudo passwd sowactl sudo passwd sowaspo sudo passwd sowaspodpl sudo passwd sowacfg sudo passwd sowacfgdpl sudo passwd sowauser
```

## Процесс развертывания дистрибутива

Последующие действия необходимо выполнять под УЗ sowaspo.

1. Скачать и разархивировать 2 части дистрибутива (owned и party) в каталог /sowa.

```
unzip CI********_*NAME*-owned-distrib.zip -d owned-distrib unzip CI********_*NAME*-party-distrib.zip -d party-distrib
```

   Инсталляционные скрипты будут расположены в каталогах *owned-distrib/bin* и *party-distrib/bin*.

2. Перейти в каталог *owned-distrib*.
3. В зависимости от используемой ОС перейти в соответствующий каталог (для ОС Альт – папка altlinux, для rhel based - rhel). Далее будет рассмотрен пример установки для ОС Альт.
4. Для установки нового дистрибутива выполните скрипт *install.sh*:

```
cd owned-distrib/bin/ altlinux sudo im-sowa ./install.sh
```

5. Перейти в каталог *party-distrib*. Для установки нового дистрибутива выполните скрипт *installPartyLibs.sh*:

```
cd party-distrib/bin/altlinux sudo im-sowa ./installPartyLibs.sh
```

В результате выполнения скриптов *install.sh* и *installPartyLibs.sh* RPM-пакеты SOWA и зависимости будут установлены в системные директории.

Логи установки будут расположены в директории */(owned|party)-distrib/bin/(rhel|altlinux)/logs*. Следует убедиться, что в логах отсутствуют ошибки.

## Установка КриптоПРО и JCP для service_gost_proxy

Для использования модуля ГОСТ proxy необходимо выполнить установку плагина gost_proxy и JCP в соответствии с приведенным ниже описанием.

1. Установка gost_proxy плагина.

   Для установки дополнительных модулей КриптоПРО с необходимыми лицензиями необходимо выполнить скрипт установки *installGost.sh*. Пример запуска скрипта ниже:

```
cd owned-distrib/bin/altlinux sudo im-sowa
./installPlugin.sh -i -f "GOST Proxy"
```

Полный список ключей *installPlugin.sh* (должны быть указаны до названия плагина):

| Ключ | Значение ключа |
|---|---|
| -i | Установка плагина и зависимостей. |
| -u | Удаление плагина и зависимостей. |
| -f | Подавляет пользовательский ввод о подтверждении установки. |

Также необходимо установить часть библиотек из party-дистрибутива:

```
cd party-distrib/bin/altlinux sudo im-sowa
./installGostPartyLibs.sh
```

2. Установка JCP

Скачать архив https://www.cryptopro.ru/download?pid=129 .

Выполнить установку со следующими ключами:

1. Команда для быстрой установки, без лицензионных ключей (указывается путь в jdk/jre):

```
printf
'i\n\nyes\nyes\nno\nno\nyes\nno\nyes\nyes\nno'  |
sudo ./setup_console.sh /etc/alternatives/java
```

2. Команда для последовательной установки с лицензионными ключами (указывается путь в jdk/jre):

```
sudo ./setup_console.sh /etc/alternatives/java
```

3. Выбрать вариант install ( i )3Java CryptoGraphic provider - yes.
4. Encryption module - yes.
5. Card Module - no.
6. Card Module - no.
7. Java TLS Provider - yes.
8. Cades module - no.
9. JCP trial - лицензионный ключ JCP или значение "yes", если лицензии нет.

10. Java TLS provider trial - лицензионный ключ JTLS или значение "yes", если лицензии нет.
11. Enable StrengthenedKeyUsageControl - no.

Скопировать jar файл из распакованного архива *\Doc\WebServerIntegration\Tomcat9\JCPTomcatAdapter\target* в каталог */usr/local/sowa/lib/gostLibs*.

3. Настройка JCP

Для серверов без доступа в интернет требуется отключить проверку списков отзыва для сертификатов с помощью следующих команд:

```
sudo java ru.CryptoPro.JCP.Util.SetPrefs -system -
node ru/CryptoPro/ssl -key
Enable_CRL_revocation_ofline_default -value false
sudo java ru.CryptoPro.JCP.Util.SetPrefs -system -
node ru/CryptoPro/ssl -key Enable_revocation_default
-value false
```

Для переопределения ГОСТового хранилища закрытых ключей используется команда:

```
sudo java ru.CryptoPro.JCP.Util.SetPrefs -system -
node ru/CryptoPro/JCP/KeyStore/HDImage -key
HDImageStore_class_default -value /mnt/profiles
```

4. Настройка Java

В файле */etc/alternatives/jre/lib/security/java.security* заменить значения параметров с

```
ssl.KeyManagerFactory.algorithm=GostX509
ssl.TrustManagerFactory.algorithm=GostX509
```

на следующие:

```
ssl.KeyManagerFactory.algorithm=SunX509
ssl.TrustManagerFactory.algorithm=SunX509
```

Для Oracle JDK убрать экспортные ограничения java. Для этого необходимо скачать *local_policy.jar* и *US_export_policy.jar* и установить их в каталог */etc/alternatives/jre/lib/security*, а также в каталог */usr/local/sowa/lib/gostLibs*.

https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/44/6/snjatie-ehksportnykh-ogrnichenijj

## SOWA Install manager (im-sowa)

Требуется предоставить обычному пользователю sudo права на инсталляционные скрипты, выполняющие привилегированные действия. При этом необходимо избежать модификации этих скриптов с целью повышения привилегий. Для решения этой проблемы можно использовать следующие подходы:

- Сделать скрипт нередактируемым для пользователя (chown root. или chattr +i);
- Проверка контрольной суммы с помощью sudo;
- Скрипт-обертка с проверкой контрольной суммы;

Однако, первый подход малореалистичен ввиду того, что пользователь должен иметь возможность самостоятельно и с некоторой периодичностью выкачивать свежий дистрибутив, содержащий актуальные версии инсталляционных скриптов. Оставшиеся два подхода предполагают модификацию прав в sudoers с пересчетом контрольных сумм для каждой новой версии дистрибутива, что тоже затрудняет процесс обновления.

В качестве решения поставленной задачи и избежания описанных выше проблем был реализован подход, базирующийся на внедрении ЭЦП для скриптов, которые необходимо защитить от модификации и при этом сохранить возможность выполнять заданные в них привилегированные действия.

Для этого была разработана утилита **im-sowa**, выступающая в качестве обертки при запуске инсталляционных скриптов, но при этом она не обладает вышеописанными недостатками, так как не содержит в себе контрольных сумм. Для ее использования достаточно выполнить инсталляцию rpm-пакета и однократно прописать в sudoers путь к исполняемому бинарнику с указанием его хеш-суммы. Например, для текущей версии утилиты наполнение sudoers для условного пользователя sowaspo будет выглядеть следующим образом:

```
Cmnd_Alias           SOWASPO_ALLOW_CMD_001           =
sha256:2a2e471de9e393809c844ad24238d5c8497f5ceb99d2d8
ac66d4be876a03e607    /usr/bin/im-sowa    *    sowaspo
ALL=(root) NOPASSWD : SOWASPO_ALLOW_CMD_001
```

Для того чтобы запустить скрипт с помощью этой утилиты, необходимо, чтобы рядом с ним был расположен файл подписи с тем же именем, что и сам скрипт и дополнительным расширением .sig

Например:

```
install.sh install.sh.sig
```

Пример запуска скрипта *install.sh*:

```
sudo im-sowa /path/to/install.sh
```

Утилита **im-sowa** доступна в составе дистрибутива СПО SOWA.

Хеш-сумма, необходимая для заполнения sudoers, содержится в дистрибутиве в файле im-sowa.sha256.

Стоит отметить, что в общем случае обновление утилиты не требуется, чем обусловлено удобство ее применения. Единственный случай, когда это может потребоваться - это компрометация ключа, которым были сформированы ЭЦП инсталляционных скриптов.

## Установка SOWA в режиме отладки

Для установки SOWA в режиме отладки необходимо выполнить следующие шаги:

1. Остановить профиль командой:

```
sowa-config -s profile_name
```

2. Убедиться, что в профиле выставлен уровень debug. За это отвечает параметр *log_level*.

```
... system:   optional:     log_level: debug ...
```

3. Установить отлаженную версию СПО SOWA с помощью команды:

```
./install.sh -g
```

4. Убедиться, что установлены отлаженные версии пакетов с помощью команды:

```
yum list installed \*sowa-nginx-debug\*
```

5. Запустить профиль в режиме отладки с помощью команды:

```
sowa-config -r profile_name --debug --log-type=file
```

Установка SOWA в режиме отладки завершена.

## Установка ППО SOWA

Для развертывания ППО необходимо выполнить следующие шаги:

1. Заполнить файл со средозависимыми параметрами *list_values.yml*, расположенный в корне поставки.
2. Скопировать дистрибутив ППО и средозависимые артефакты (сертификаты) на сервер.
3. Проверить правильность выдачи прав на сервере, где установлено СПО SOWA:

```
sowa-config --check-permissions
```

4. Создать профиль с именем . Названия профилей, которые требуется создать, содержатся в корневых файлах профилей поставки. Обычно они соответствуют названию директории.

```
sowa-config --add-profile <profile>
```

5. После успешного создания профиля, необходимо поместить ресурсы профиля в ресурсный каталог.
   1. Публичную и приватную часть сертификата (public.cer и private.key) необходимо поместить в */sowa/profile_storage/custom/ /* .

      ```
      certificate: serv1/public.cer certificate_key: serv1/private.key
      ```

      В данном случае, расположение будет следующим: */sowa/profile_storage/custom/ /serv1/public.cer* .

   2. Клиентский сертификат client_certificate.pem необходимо также поместить в */sowa/profile_storage/custom/ /* .

      ```
      client_certificate: client_certificate.pem
      ```

   3. Схемы валидации сообщений (json/xsd (wsdl схема относится к валидации по xsd) поместить в */sowa/profile_storage/custom/ /json/* и в */sowa/profile_storage/custom/<profile_name>/xsd* соответственно.
6. После того, как все ресурсы перемещены, необходимо выполнить конфигурирование профиля.

   Конфигурирование с использованием шаблона средозависимых параметров:

   ```
   sowa-config --config path/to/file/<profile>.yml -e path/to/file/list_value.yml
   ```

   Если значения параметров в конфигурационном файле заданы явно:

   ```
   sowa-config --config path/to/file/<profile>.yml
   ```

7. Запуск сконфигурированного профиля осуществляется следующим образом:

   ```
   sowa-config --run <profile>
   ```

8. Проверка статуса всех профилей. Отображение списка профилей с указанием их статуса:

```
sowa-config --show-profiles
```

Значение *configured* созданного профиля *true* и *pid* > 0.

9. Проверка статуса заданного профиля:

```
sowa-config --status <profile>
```

В результате, если профиль запущен успешно, поле Active примет значение *running*. Для проверки подключения необходимо ввести команду:

```
sudo netstat -ntulp | grep <port>
```

где *port* - порт, на котором развернут профиль. Выполнение этой команды покажет, находится ли указанный порт в состоянии *LISTEN*. Если запуск профиля произошел корректно, то можно будет увидеть значения портов, указанных в конфигурационном файле.

Развертывание ППО SOWA завершено.

## Установка sowa-zabbix-agent

Предполагается, что на стенде уже установлено СПО SOWA. Процесс установки СПО описан в разделе "Установка СПО SOWA".

В процессе развертывания дистрибутива, в числе прочего, устанавливаются следующие компоненты: *sowa-nginx* и *sowa-config*.

Установка компонента *sowa-zabbix-agent* осуществляется с помощью скрипта *installZabbix.sh*, расположенного в каталоге *distrib*. Следует убедиться, что скрипты в */sowa/distrib/bin* имеют права на выполнение. В противном случае необходимо добавить данное право. Для выполнения скрипта *bin/installZabbix.sh* необходимо выполнить команду:

```
cd /sowa/distrib/ chmod u+x bin/*.sh sh bin/installZabbix.sh
```

Если, по каким-либо причинам, компоненты не установились, то находясь в каталоге */sowa/distrib/* необходимо выполнить команду:

```
sudo yum install rpm/x86_64/sowa-zabbix-agent-<version>.x86_64.rpm
```

### Запуск zabbix-agent

После установки *sowa-zabbix-agent* запускаем *zabbix-agent*:

```
sudo systemctl start zabbix-agent
```

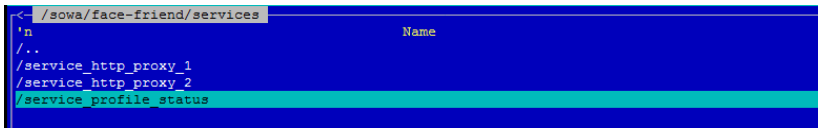
Рестарт zabbix-agent'a необходим в случае, если профиль был создан и запущен ранее:

```
sudo systemctl restart zabbix-agent
```

Проверить, действительно ли запущен *zabbix-agent*, можно с помощью команды:

```
sudo systemctl status zabbix-agent
```

После развертывания ППО SOWA, в каталоге */sowa/ /services/* автоматически создается сервис *service_profile_status*, который используется *zabbix-agent'ом*:




Пример файла конфигурации (service.conf), создаваемого zabbix-agent'ом:

```
server {    listen 55000;        server_name localhost;
location = /status {        allow 127.0.0.1;        deny
all;             vhost_traffic_status_bypass_limit  on;
vhost_traffic_status_bypass_stats                    on;
vhost_traffic_status_display;
vhost_traffic_status_display_format json;     } }
```

Процессы интеграции SOWA с системами Zabbix и SIEM Qradar подробно рассмотрены в соответствующих разделах в Руководстве по системному администрированию.

## Обновление

### Обновление СПО SOWA

Перед началом обновления следует остановить все запущенные профили, используя команду:

```
sowa-config --stopall
```

После обновления СПО рекомендуется переконфигурировать профиль (флаг --config).

Администраторам СПО требуется загрузить новую версию дистрибутива из доверенного источника. Соответственно, чем "свежее" дата, тем новее дистрибутив.

Сравнивать два дистрибутива можно при соблюдении следующих условий: одинаковый тип сборки и одинаковый тип ОС.

**Внимание! Обновление СПО необходимо производить под пользователем *sowaspo* или *sowaspodpl*.**

Для обновления СПО SOWA необходимо выполнить следующие шаги:

1. Разархивировать дистрибутив в каталог */sowa* (разархивированные ранее каталоги с дистрибутивом следует удалить):

```
tar -xvf CI********_*NAME*-distrib.tar.gz
```

2. Необходимо убедиться, что скрипты в */sowa/distrib/bin* имеют права на выполнение, иначе нужно добавить данное право, например с помощью команды:

```
chmod u+x <ПУТЬ_ДО_ФАЙЛА>/<ИМЯ_ФАЙЛА>
```

3. Перейти в каталог *distrib*. Для "чистой" установки необходимо выполнить скрипт *uninstall.sh*, который удалит предыдущий дистрибутив:

```
./bin/uninstall.sh
```

4. Для установки нового дистрибутива необходимо выполнить скрипт *bin/install.sh*:

```
./bin/install.sh
```

5. По завершению установки рекомендуется проверить версию установленного СПО с помощью команды:

```
sowa-version
```

6. Запустить остановленные ранее профили.

```
sowa-config --runall
```

Обновление СПО SOWA завершено.

### Обновление ППО SOWA

Если профиль, для которого требуется обновить конфигурацию, запущен, то нужно произвести остановку профиля.

```
sowa-config --stop <profile_name>
```

Если ресурсы для нового конфигурационного файла менялись, следует скопировать новые ресурсы в ресурсный каталог, в соответствующие подкаталоги.

Изменения будут видны после переконфигурации:

```
sowa-config                                          --config
path_to_new_file_<profile_name>.yml
```

Запуск профиля:

```
sowa-config --run <profile_name>
```

Для проверки того, запущен ли профиль, необходимо ввести команду:

```
sowa-config --status <profile_name>
```

В результате, если профиль запущен успешно, в поле Active будет значение *running*.

Для проверки подключения необходимо ввести команду:

```
sudo netstat -ntulp | grep <port>
```

Команда покажет, находится ли указанный порт в состоянии LISTEN. Если запуск профиля произошел корректно, то можно будет увидеть значения портов, указанных в конфигурационном файле.

Обновление ППО SOWA завершено.

## Удаление

### Удаление СПО SOWA

Для удаления СПО SOWA необходимо выполнить следующие шаги:

1. Остановить профили с помощью команды:

```
sowa-config --stopall
```

2. Перейти в каталог с дистрибутивом (например, */sowa/distrib/*) и выполнить скрипт *uninstall.sh*, который удалит текущую поставку:

```
sudo ./bin/uninstall.sh
```

Удаление СПО SOWA завершено.

### Удаление ППО SOWA

Для удаления ППО SOWA требуется выполнить следующие шаги:

1. Остановить запущенный профиль (профили), который требуется удалить: Остановка одного профиля:

```
sowa-config --stop <profile>
```

Остановка всех, запущенных профилей:

```
sowa-config --stopall
```

2. Удалить профиль (при необходимости действие выполняется для каждого профиля отдельно):

Удаление профиля, с сохранением конфигурационных ресурсов:

```
sowa-config --del-profile <profile>
```

Удаление профиля, без сохранения конфигурационных ресурсов ("чистое удаление"):

```
sowa-config --del-profile <profile> --clean
```

Удаление ППО SOWA завершено.

## Откат

### Откат СПО SOWA

Для отката СПО SOWA на нужную версию необходимо выполнить следующие шаги:

1. Остановить профили с помощью команды:

```
sowa-config --stopall
```

2. Перейти в каталог с дистрибутивом (например, */sowa/distrib/*) и выполнить скрипт *uninstall.sh*, который удалит текущую поставку:

```
sudo ./bin/uninstall.sh
```

3. Выполнить установку требуемой версии СПО (процесс развертывания СПО SOWA подробно описан в разделе "Процесс развертывания дистрибутива" данного руководства).

Откат СПО SOWA на нужную версию завершен.

### Откат ППО SOWA

Для отката ППО SOWA к старой версии требуется выполнить следующие шаги:

1. Выполнить восстановление из backup'а:

```
sowa-config --recovery <profile> config | system | controller
```

2. Выполнить установку требуемой версии (процесс описан в разделе "Установка ППО SOWA").

## Проверка работоспособности

Для проверки работоспособности необходимо убедиться, что скрипт установки *bin/install.sh* отработал без ошибок.

Проверить версию установленного дистрибутива СПО SOWA можно с помощью команды:

```
sowa-version
```

Логи установки будут расположены в директории */sowa/distrib/logs*. Следует убедиться, что в логе *install.log* отсутствуют ошибки.

## Часто встречающиеся проблемы и пути их решения

В данном разделе рассмотрены встречающиеся проблемы при установке СПО и ППО, и способы их устранения.

1. Профиль не конфигурируется (и он выключен) по причине того, что порт занят кем-то другим.

   Способ решения:

   1. Проверить, кем занят порт:

      ```
      netstat -lpt | grep порт
      ```

2. Если этим же профилем, то попытаться отключить автоподключение:

```
systemctl stop sowa-имя профиля
```

3. Остановить процесс, который запущен на этом порту и попытаться сконфигурировать его еще раз.

2. Профиль не останавливается штатными средствами.

Способ решения: Необходимо остановить профиль с помощью ключей конфигуратора:

```
--stop --kill
```

1. Для этого необходимо авторизоваться под учетной записью *sowaroot*. Если на сервере версия шаблона 7.1 и ниже, то через у/з *sowaadm*, скрипт1.sh).
2. Вычислить PID профиля:

```
ps -ef | grep sowa
```

3. Остановить процессы профиля

```
sudo kill -9
```

Далее запустить профиль обычным способом (из-под у/з *sowacfg*).

Пример:

```
$ ps -ef | grep sowa sowactl 3790 1 0 Jan14 ? 00:00:00
sowa: master process /usr/local/sowa/bin/sowa-nginx
-c /sowa/<ВНИМАНИЕ!! здесь должно быть указано имя
профиля,                 который                 нужно
остановить!!>/system/sowa.conf sowactl 3791 3790 0
Jan14 ? 00:14:21 sowa: worker process sowactl 3793
3790 0 Jan14 ? 00:15:25 sowa: worker process sowactl
3794 3790 0 Jan14 ? 00:14:16 sowa: worker process
sowactl 3795 3790 0 Jan14 ? 00:14:54 sowa: worker
process  $ sudo kill -9 3790 3791 3793 3794 3795
```

3. При конфигурировании профиля возникает ошибка **"Cannot find required key 'allowed_methods'"**.

Способ решения: Скорее всего версия СПО не соответствует версии ППО, так как ключ 'allowed_methods' называется теперь 'allowed_queries'.

4. nginx: [warn] **the number of "worker_processes"** is not equal to the number of "worker_cpu_affinity" masks, using last mask for remaining worker processes

   Способ решения: На сервере доступно количество ядер, не соответствующее конфигурации.

   1. В типовых виртуальных машинах дают 4 ядра.
   2. В системах контейнеризации Platform V может быть любое количество ядер. Для контейнеров необходимо указывать 1.

   Следует изменить количество рабочих процессов на auto или 1 в корне профиля:

   ```
   system:   wrk_count: auto
   ```

5. Can't configure profile: Failed to configure profile: File '/sowa/profile_storage/custom/sbc_web_8092/schemes/json/RECOVERY/check-user.request.v1.json' does not exists

   Способ решения:

   Не скопированы схемы валидации из поставки.

   Выполнить копирование схем валидации командой:

   ```
   cp                    -R                    */schemes
   /sowa/profile_storage/custom/*name_profile*
   ```

6. Can't configure profile: Failed to configure profile: Can't link resource: Resource /sowa/profile_storage/custom/sbc_web_8092/sbc_web_sowa_serv_public.crt does not exist

   Способ решения:

   Не хватает сертификатов.

   Скопировать открытую и закрытую части серверного сертификата в корень профиля.

7. Can't configure profile: Failed to configure profile: "Specified port '8091' currently used in system!"

   Способ решения:

   Убедиться, что порт не совпадает с другими профилями в файле list_value.yml, строка - sbc_web_port: 8091

   Поиск порта в конфигах - find /sowa/ -type f -iname *yml -exec grep -Hn \номер_порта\b {} ;

8. Job for sowa-test.service failed because the control process exited with error code. See "systemctl status sowa-test.service" and "journalctl -xe" for details. Сброс Account locked due to xx failed logins (через sh)

   Способ решения:

   Сбросить *Account locked* можно командой */sbin/pam_tally2 -u <имя_пользователя> -r*.

Посмотреть количество Login Failures можно командой */sbin/pam_tally2 -u <имя_пользователя>*.

9. При удалении профиля ошибка: "Permission denied: '/sowarun/BFPSI02/body/2'".

   Способ решения:

   При буферизации (которая происходит при достижении сообщением определенного размера) запросов создаются временные файлы в директории /sowarun/profile_name/body/. Создаются от пользователя *sowactl* с правами 700.

   Бывают случаи, когда данные файлы не успевают очиститься и остаются там после остановки профиля, что и влечет за собой проблему permission denied, т.к. профиль удаляется из-под пользователя *sowacfg*.

   Для решения необходимо выполнить команду:

```
sudo runuser sowactl -s /bin/sh -c 'rm -rf /sowarun/ИМЯ ПРОФИЛЯ/body/*'
```

10. Can't run profile 'имя профиля'. Can't execute command - process return code!=0.

    Способ решения:

    Смотрим подробный статус профиля

```
sowa-config --status <имя_профиля> --full
```

    Пример ошибки:

```
Jan 17 09:57:08 pvle-erib0360 runuser[12850]: nginx: [emerg] PEM_read_bio_X509_AUX("/sowa/erib-rbs/cert/public/service_main_proxy_mypay_main_proxy/_online_mycompany_ru_2020_09_02.pem") failed (SSL: error:0909006C:PEM routines:get_name:no start line:Expecting: TRUSTED CERTIFICATE)
```

    Способ решения:

    Необходимо проверить корректность и целостность сертификата (в данном случае _online_mycompany_ru_2020_09_02.pem). Нужно открыть его текстовым редактором, проверить, что он в формате base64, т.е. имеет вид

```
-----BEGIN CERTIFICATE----- <тело_сертификата>-----END CERTIFICATE-----
```

Если сертификат в .pem, то можно скопировать его себе на "машину", переименовать в .crt и попытаться открыть штатными средствами ОС. Корректный сертификат должен открыться.

```
[sowacfg@tkle-mvp0272 /sowa/profile_storage/custom]$ sowa-config --run SendToAlpha sudo: sorry, you must have a tty to run sudo
```

Способ решения:

Необходимо скорректировать sudoers.

Нужно убрать requiretty в sudoers или поменять местами requiretty и !requiretty. 12. Ошибка при установке СПО в файле installLibs.log: multilib versions: lz4-1.7.5-3.el7.x86_64 != lz4-1.7.5-2.el7.i686

```
Способ решения: Рекомендуется установить пакеты вручную ``` sudo yum -y update sudo yum -y install cyrus-sasl-devel python-devel lz4-devel ```
```

13. В логах ошибка вида unable to get local issuer certificate.

    Способ решения:

    В настройках **proxy_ssl** указать в **ssl_trusted_certificate** цепочку вместе с подписантами.

    Сама конфигурация должна выглядеть приблизительно так:

```
proxy_ssl: ssl_use: {{ gws_fss_ssl_use }} ssl_certificate: {{ gws_fss_ssl_certificate }} ssl_certificate_key: {{ gws_fss_ssl_certificate_key }} ssl_verify: {{ gws_fss_ssl_verify }} ssl_trusted_certificate: {{ gws_fss_trusted_certificate }} ssl_name: {{ gws_fss_hostname }} ssl_server_name: {{ gws_fss_ssl_server_name }}
```

14. При обращении к SOWA возникает ошибка 404 Not Found.

    Способ решения:

    Ошибка воспроизводится с включенной настройкой *strict_hostname_check*.

    Параметр *strict_hostname_check* означает, что профиль будет проверять значение заголовка HOST. Запросы со значениями заголовка, не входящими в список разрешенных, будут отклонены.

Для решения необходимо произвести откат на сборку с выключенной настройкой *strict_hostname_check*.

15. Can't configure profile: Failed to configure profile: [Errno 13] Permission denied: '/etc/systemd/system/sowa-SMIT.service'

    Способ решения:

    Ошибка может возникать после обновления версии ОС в случае, если меняются права на /etc/systemd/system, что приводит к некорректной работе sowa-config.

    Для решения необходимо последовательно выполнить следующие команды:

```
sudo ./install.sh sudo ./installLibs.sh
```

## Чек-лист валидации установки

Для проверки корректности установки SOWA рекомендуется убедиться в корректности выполнения следующих команд:

- команда *sowa-version*;
- команда *sowa-config* под пользователем *sowacfg*.

Для проверки корректности Zabbix необходимо:

- проверить наличие скриптов в */var/lb/zabbix/scripts*;
- убедиться в корректности выполнения команды */var/lib/zabbix/scripts/sowa_discovery.sh profile_list* под пользователем zabbix.

Для проверки корректности настройки SIEM необходимо убедиться в том, что сообщения успешно приходят в хранилище, указанное при настройке.