SOLAR

Солар Программный Комплекс Обнаружения и Реагирования

Версия 0.4

Инструкция по установке для экспертов

МОСКВА, 2024

Содержание

1. Установка Solar NTA

1.1. Конфигурирование сторонних сервисов

1.1.1. Вводная информация

В данном разделе описан процесс установки / обновления сторонних сервисов, необходимых для корректной работы сервисов Solar NTA.

1.1.2. Требования

- ОС: Debian 12, Debian 11, Debian 10, Astra SE 1.7.3+, RedOS 7+;
- наличие и доступность базовых репозиториев ОС для установки зависимых пакетов;
- привилегии root-пользователя;
- предварительно на виртуальной машине необходимо установить следующие инструменты: **sudo, net-tools**.

1.1.3. Сервисы

Перечень сервисов, которые будут установлены и настроены:

- PostgreSQL;
- Scylla >= 5.4.

1.1.4. Порядок установки Солар ПКОиР для Debian 10|11|12

Конфигурирование **PostgreSQL**:

1. Подключить базовый репозиторий ОС для установки PostgreSQL.

Для этого можно обратиться к официальной инструкции по подключению репозиториев.

Выполнить установку PostgreSQL:

```
sudo apt-get install -y postgresql
```

2. Добавить параметры **statement_timeout и idle_in_transaction_session_timeout** в конфигурационный файл **/etc/postgresql/${POSTGRESQL_VERSION}/main/postgresql.conf**:

```
# Добавить

statement_timeout = 180000   # in milliseconds, 0 is disabled

idle_in_transaction_session_timeout = 60000   # in milliseconds, 0 is
disabled
```

3. Перезагрузить службу **postgresql**:

```
sudo systemctl restart postgresql
```

4. Создать учетную запись и БД для работы сервисов NTA:

```
# Перейти в учетную запись postgres

sudo su postgres

# Создать пользователя nta для работы в БД

psql -v  ON_ERROR_STOP=1 --username postgres -c "CREATE USER nta WITH
PASSWORD '${POSTGRES_NTA_USER_PASSWORD}'"
```

```
# Создать БД nta
psql -v  ON_ERROR_STOP=1 --username postgres -c "CREATE DATABASE nta"
# Выдать права пользователю nta для работы с БД nta
psql -v  ON_ERROR_STOP=1 --username postgres -c "ALTER DATABASE nta OWNER
TO nta"
psql -v  ON_ERROR_STOP=1 --username postgres -c "GRANT ALL PRIVILEGES ON
DATABASE nta TO nta;"
# Выйти из учетной записи postgres
exit
```

где:

POSTGRES_NTA_USER_PASSWORD – пароль от учетной записи пользователя nta.

Конфигурирование **ScyllaDB**:

1. Установка без доступа во внешнюю сеть:

- Открыть браузер на своем рабочем ПК;
- Перейти по адресу https://downloads.scylladb.com/downloads/scylla/relocatable/
- Перейти в каталог с необходимой версией Scylla, например 6.1.
- Скачать архив **scylla-unified** с учетом требуемой архитектуры, например, x86_64.

Внимание!

*Следует обратить внимание на суффикс версии. **-rc** скачивать не надо – это «релиз-кандидаты»*

Пример корректного архива: **scylla-unified-6.1.0-0.20240804.abbf0b24a60c.x86_64.tar.gz**

- Скопировать архив на хост развертывания (используя scp, putty или альтернативный инструмент, позволяющий передать файлы на хост развертывания);
- Подключиться к хосту развертывания по ssh;
- Перейти в каталог, в котором расположен архив;
- Распаковать архив:

```
tar xvfz ${ARCHIVE_NAME}
```

где:

ARCHIVE_NAME – название скачанного архива, например, **scylla-unified-6.1.0-0.20240804.abbf0b24a60c.x86_64.tar.gz**.

- Перейти в каталог с распакованной версией:

```
cd scylla-${SCYLLA_VERSION}
```

где:

SCYLLA_VERSION – версия ScyllaDB, которая была скачана. Например: 6.1.

- Установить **scylla**, **scylla-python3**, **scylla-tools и scylla-cqlsh**:

```
cd scylla && sudo ./install.sh && cd ..
```

```
cd scylla-python3 && sudo ./install.sh && cd ..
cd scylla-tools && sudo ./install.sh && cd ..
cd scylla-cqlsh && sudo ./install.sh && cd ..
```

2. Запустить конфигурирование ScyllaDB:

```
sudo scylla_setup
```

3. Запустить службу ScyllaDB:

```
sudo systemctl start scylla-server
```

1.2. Установка сервисов NTA из deb/rpm пакетов

1.2.1. Вводная информация

Сервисы NTA поставляются в виде deb/rpm-пакетов под различный набор операционных систем.

Пакеты поставляются в виде .tag.gz архива. В состав архива входит:

- deb|rpm пакеты для установки сервисов NTA;
- packages_installer.sh – скрипт для установки deb/rpm пакетов.

1.2.2. Информация о пакетах

Перечень пакетов, которые будут установлены и настроены:

- solar-nta – мета-пакет, позволяющий установить все пакеты-зависимости (all in one);
- solar-config – пакет, устанавливающий конфигурационный файл. Конфигурационные файлы расположены по путям: **/etc/nta/nta.conf** и **/opt/solar/nta/etc/common**;
- solar-nta-server – пакет, позволяющий установить сервис solar-nta-server. Необходимые файлы устанавливаются в каталог **/opt/solar/nta**;
- solar-nta-storage – пакет, позволяющий установить сервис solar-nta-storage. Необходимые файлы устанавливаются в каталог **/opt/solar/nta**;
- solar-nta-broker – пакет, позволяющий установить сервис solar-nta-broker. Необходимые файлы устанавливаются в каталог **/opt/solar/nta**;
- solar-nta-outer-api-interface – пакет, позволяющий установить сервис solar-nta-outer-api-interface. Необходимые файлы устанавливаются в каталог **/opt/solar/nta**;
- solar-nta-aggregator- пакет, позволяющий установить сервис solar-nta-aggregator. Необходимые файлы устанавливаются в каталог **/opt/solar/nta**;
- solar-nta-suricata – пакет, позволяющий установить сервис solar-nta-suricata. Необходимые файлы устанавливаются в каталог **/opt/solar/nta/suricata**;
- solar-nta-tools – пакет, позволяющий установить набор вспомогательных утилит solar-nta-tools. Необходимые файлы устанавливаются в каталог **/opt/solar/nta/service-builder**;

1.2.3. Требования

- ОС: Debian 12, Debian 11, Debian 10;
- наличие и доступность пакетов из базовых репозиториев для операционной системы;
- привилегии root-пользователя.

1.2.4. Порядок установки Солар ПКОиР

1. Скачать архив с ПО Солар ПКОиР.
2. Распаковать его:

```
# распаковка, где ARCHIVE_NAME - название скачанного архива
tar -xvf ${ARCHIVE_NAME}
```

3. Открыть в терминале директорию распакованного архива.
4. Выполнить команду, далее следовать инструкциям:

```
sudo bash packages_installer.sh install | sudo tee -a
/tmp/packages_installer.log
```

В случае если установка прошла успешно, должны появится следующие сервисы:

- solar-nta-broker.service;
- solar-nta-outer-api-interface.service;
- solar-nta-server.service;
- solar-nta-storage.service;
- solar-nta-aggregator.service.

5. После установки необходимо внести изменения в файл **/etc/hosts**:

- открыть файл **/etc/hosts**;
- добавить следующие строки:

```
${SCYLLA_HOST_IP}     scylla scylla1
${POSTGRESQL_HOST_IP}     postgres postgres1
```

где:

SCYLLA_HOST_IP – IP-адрес хоста, на котором развернута ScyllaDB. В случае если ScyllaDB развернута на том же хосте, что и сервисы NTA, необходимо указать IP-адрес: 127.0.0.1.

POSTGRESQL_HOST_IP – IP-адрес хоста, на котором развернута PostgreSQL. В случае если PostgreSQL развернута на том же хосте, что и сервисы NTA, необходимо указать IP-адрес: 127.0.0.1.

6. Выполнить инициализацию PostgreSQL в случае, если PostgreSQL и сервисы NTA развернуты на одном хосте:

```
# Перейти в учетную запись postgres
sudo su postgres
# Выполнить инициализацию БД
PGPASSWORD=${POSTGRES_NTA_USER_PASSWORD} psql -h 127.0.0.1 -U nta "nta" -v
"ON_ERROR_STOP=0" -c "DROP SCHEMA IF EXISTS metadata CASCADE;DROP SCHEMA IF
EXISTS metadata_description CASCADE;" -f /opt/solar/nta/service-
builder/solar-nta/solar-nta-metadata/metadata_types.sql
# Выйти из учетной записи postgres
exit
```

где:

POSTGRES_NTA_USER_PASSWORD – пароль от учетной записи пользователя nta;

7. Выполнить инициализацию ScyllaDB в случае, если ScyllaDB и сервисы NTA развернуты на одном хосте:

```
CQLSH_PORT=${SCYLLA_PORT} CQLSH_HOST=127.0.0.1 cqlsh -e "DROP KEYSPACE IF EXISTS ${SCYLLA_DB}; CREATE KEYSPACE ${SCYLLA_DB} WITH replication = {'class': 'SimpleStrategy', 'replication_factor': '1'}  AND durable_writes = true;"

CQLSH_PORT=${SCYLLA_PORT} CQLSH_HOST=127.0.0.1 cqlsh --keyspace=$SCYLLA_DB -f /tmp/opt/solar/nta/service-builder/solar-nta/solar-nta-packets/database.sql
```

где:

SCYLLA_PORT – порт, на котором запущена ScyllaDB, по умолчанию: 9042;

SCYLLA_DB – название БД ScyllaDB. По умолчанию: nta;

8. Изменить значение параметра **capture.afpacket.deviceName** в конфигурационном файле **/opt/solar/nta/etc/solar-nta-storage.json** на имя сетевого устройства, на котором будет происходить захват. Например, «ens18».

9. Добавить сервисы в автозагрузку

```
# Для одного сервиса

systemctl enable ${SERVICE_NAME}   # SERVICE_NAME - имя сервиса (имена сервисов перечислены в п.3)


# Для всех сервисов

for i in solar-nta-broker.service solar-nta-server.service solar-nta-storage.service solar-nta-outer-api-interface.service solar-nta-aggregator.service; do systemctl enable ${i}; done
```

10. Запустить сервисы:

```
# Для одного сервиса

systemctl start ${SERVICE_NAME}   # SERVICE_NAME - имя сервиса (имена сервисов перечислены в п.3)


# Для всех сервисов

for i in solar-nta-broker.service solar-nta-server.service solar-nta-storage.service solar-nta-outer-api-interface.service solar-nta-aggregator.service; do systemctl start ${i}; done
```

1.2.5. Обновление основных сервисов NTA

1. Скачать архив с ПО Солар ПКОиР.

2. Распаковать его:

```
# распаковка, где ARCHIVE_NAME - название скачанного архива

tar -xvf ${ARCHIVE_NAME}
```

3. Открыть в терминале директорию распакованного архива.

4. Выполнить команду, далее следовать инструкциям:

```
sudo bash packages_installer.sh update | sudo tee -a
/tmp/packages_installer.log
```

1.2.6. Просмотр логов

Файлы логов располагаются в директории **/var/log/solar/nta**.

Посмотреть лог конкретного сервиса можно с помощью команды:

```
journalctl -fu ${SERVICE_NAME}   # SERVICE_NAME - имя сервиса (см. выше)
```

1.2.7. Возможные проблемы и их решения

ScyllaDB

Проблема:

scylla-server не запускается

В некоторых случаях можно столкнуться с проблемой при запуске scylla-server.

В логах появится следующее сообщение:

```
Aug 21 17:20:33 nta-ropo-test scylla[982]:  [shard  0:main] init - Only 462
MiB per shard; this is below the recommended minimum of 1 GiB/shard;
terminating.Configure more memory (--memory option) or decrease shard count
(--smp option).

Aug 21 17:20:33 nta-ropo-test scylla[982]:  [shard  0:main] init - Shutting
down sighup

Aug 21 17:20:33 nta-ropo-test scylla[982]:  [shard  0:main] init - Shutting
down sighup was successful

Aug 21 17:20:33 nta-ropo-test scylla[982]:  [shard  0:main] init - Shutting
down configurables

Aug 21 17:20:33 nta-ropo-test scylla[982]:  [shard  0:main] init - Shutting
down configurables was successful

Aug 21 17:20:33 nta-ropo-test scylla[982]:  [shard  0:main] init - Startup
failed: std::runtime_error (configuration (memory per shard too low))
```

Решение:

уменьшение кол-ва ядер и ОЗУ, используемых scylla-server. Для этого необходимо:

1. Перейти на хост с установленной ScyllaDB

2. Выполнить команды:

```
sudo ./scylla_cpuset_setup --smp ${CPU_CORES_COUNT/2}

sudo ./scylla_memory_setup --lock-memory --memory ${MEMORY_COUNT/2}G
```

где:

CPU_CORES_COUNT – общее количество ядер на хосте;

MEMORY_COUNT – общее количество ОЗУ на хосте (в Гб).

solar-nta-server

Проблема:

Unable to get packets from storage

Под нагрузкой в логах solar-nta-server.service появляется сообщение:

```
[20.05.4024 20:33:42.716'887"7](server.1::api::0x202CA2)<TRACE>:out
{"id":1,"result":{"brokerParameters":{"heartBeatInterval":5,"pollingInterva
l":1000,"defaultParentId":"016b1af4-7d47-698d-be8d-94a0a8c454c0"}}}
[20.05.4024 20:33:42.716'942"8](server.1::api::0x202CA2)<TRACE>:in
{"method":"get_raw_packets","id":2,"params":{"previousPacketId":"71c5a656-
1673-11ef-b7d6-00832111b36c","maximumPacketCount":1000}} [20.05.4024
20:33:42.841'293"0](server.1::api::0x202CA2)<TRACE>:out
{"id":2,"error":{"code":500,"message":"/home/a-dzyuba/service-
builder.release/solar-nta/solar-nta-server/src/api.cpp:1176 'Internal
error'\\n from/home/a-dzyuba/service-builder.release/solar-nta/solar-nta-
server/src/storage/scylla/scylla_storage_adapter.cpp:255 'Unable to get
packets from storage'\\n from/home/a-dzyuba/service-builder.release/solar-
nta/solar-nta-server/common/src/nta/common/cassandra/client.cpp:239 'Unable
to execute query. Operation failed for nta.packets - received 0 responses
and 1 failures from 1 CL=LOCAL_ONE.'"}} [20.05.4024
20:33:42.924'414"9](server.1::api::0x202CA2)<TRACE>:in
{"method":"heartbeat","params":{}} [20.05.4024
20:33:47.721'407"0](server.1::api::0x202CA2)<TRACE>:in
{"method":"heartbeat","params":{}}
```

Решение:

1. Перейти на хост с установленной ScyllaDB.
2. Открыть файл **/etc/scylla/scylla.yaml.**
3. Добавить строки:

Внимание!

Значения параметров указываются в Мб

```
max_memory_for_unlimited_query_soft_limit: 419430400
max_memory_for_unlimited_query_hard_limit: 536870912
```

Тем самым увеличивается размер памяти, выделяемый на запросы типа **non-paged** и **reverse**. Важно использовать оба значения, так как при превышении лимита soft в лог будет выводиться **warning**, а при превышении **hard limit** – память будет жестко ограничиваться.

2. Установка Solar EDR Windows на защищаемое конечное устройство

Сервис

Название: EdrUpdater.

Расположение: C:\Program Files (x86)\SolarUpdaterEDR.

Ключи реестра

[HKLM\Software\SolarUpdaterEDR]:

- XdrServerUrl – URL для соединения с XDR-сервером;
- TenantId.

Для установки Solar EDR Windows необходимо загрузить дистрибутив **EDR_Agent_0.4.0.141.zip** на сервер Solar XDR:

1. Авторизоваться на Swagger XDR Software Update Center (**http://<ip-адрес сервера>:<порт>/swagger-ui/index.html**).

2. Найти операцию «Сохранить бинарный артефакт EDR» на сервере в блоке **Artifact** и нажать **Try it out**.

3. Выбрать дистрибутив Solar EDR в стандартном диалоговом окне.

4. Нажать **Execute**, дождаться завершения загрузки и убедиться, что получен код 201 **Артефакт сохранён**.

5. Перейти на хост, на который требуется установить агент, и выполнить команду установки компонента ADAM:

```
msiexec.exe /i EDR_Updater_[version_updater].msi
UPDATERSERVERNAME="http://[ip:port]" /L*vx msi_updater_install.txt /QN
```

где

version_updater – версия ADAM в релизе,

ip:port – IP-адрес и порт сервера Solar XDR.

Лог установки сохраняется в файле **msi_updater_install.txt**, который создается в том же каталоге, где запущен исполняемый файл.

6. Через 2-5 минут (в зависимости от состояния сети) перейти в раздел **Сеть** веб-интерфейса Solar XDR и убедиться, что статус агента в карточке хоста **Активен**. Также проверить статус установки агента можно по логу установки в папке **C:\Program Files (x86)\SolarUpdaterEDR\update**.

3. Установка Solar XDR

В данном разделе описана пошаговая инструкция по установке Solar XDR на хост без сетевого доступа к репозиториям Solar.

Примечание

Прежде чем приступить к установке ПО, необходимо запросить на support@rt-solar.ru дистрибутивы для вашей ОС

Требования:

- ОС: Debian 12, Debian 11, Debian 10;
- наличие и доступность пакетов из базовых репозиториев для операционной системы;
- привилегии root-пользователя;
- отсутствие установленных систем контейнеризации;
- отсутствие ограничений для штатной работы Docker Engine.

Далее приведена инструкция по установке XDR на хост с ОС Debian 12.

Установка и подготовка Docker

1. Авторизоваться под пользователем root:

```
$ su -
```

2. Распаковать архив и перейти в директорию распакованного архива:

```
# unzip docker-distrs-debian-12-bundle-26.1.4.zip
# cd docker-distrs-26.1.4-debian-12-bundle
```

3. Запустить установку docker & docker-compose:

```
# bash docker_installer.sh update | tee -a /tmp/docker_installer.log
```

Работа с Docker под отдельным пользователем

Примечание

Приведенные далее команды могут меняться в зависимости от ОС и выполняемых задач

Если требуется использовать docker не под root-пользователем, то необходимо:

1. Создать пользователя в системе:

Пример 1:

```
# useradd docker-user
```

Пример 2:

```
# adduser docker-user
```

2. Добавить созданного пользователя в группу docker:

Пример добавления пользователя docker-user в группу docker:

```
# usermod -aG docker docker-user
```

Внимание!

При появлении ошибки о том, что группа docker не существует, необходимо создать группу:

```
# groupadd docker
```

После создания необходимо выполнить команду добавления пользователя в группу повторно.

3. Выйти из системы и войти снова, чтобы членство в группе было пересмотрено.

Установка XDR

Требования:

- наличие docker и docker-compose в системе;
- привилегии root-пользователя (или иного пользователя с правами для работы с docker | docker-compose);
- отсутствие ограничений для штатной работы Docker Engine.

Установка:

1. Скачать архив с ПО Солар ПКОиР.
2. Распаковать его:

```
# tar -xvf ${ARCHIVE_NAME}
```

где ARCHIVE_NAME – название скачанного архива.

3. Открыть в терминале директорию распакованного архива

```
# cd ${DIRECTORY_NAME}
```

где DIRECTORY_NAME - название директорию распакованного архива

4. Загрузить docker-образы в локальное хранилище docker

```
# docker load -i xdr-images.tag.gz
```

5. Создать .env файл, выполнив команду:

```
# cp .env.template .env
```

6. Изменить содержимое файла .env, указав соответствующие серверу значения для представленных переменных:

```
# nano .env
```

Внимание!

*Важно! Значения переменных с логинами (*USER*) изменять нельзя, т.к. сервисы потеряют взаимосвязанность.*
Необходимо изменить значения следующих переменных:

- EXTRENAL_HOST_IP – IP-адрес сетевого интерфейса, на котором будет доступен WEB-интерфейс XDR;
- POSTGRES_PASSWORD – пароль БД Postgres;
- POSTGRES_XDR_PASSWORD – пароль БД XDR;
- POSTGRES_KEYCLOAK_PASSWORD – пароль БД Keycloak;

- CLICKHOUSE_XDR_PASSWORD – пароль Clickhouse;
- KEYCLOAK_ADMIN_PASSWORD – пароль администратора Keycloak;
- NTA_HOST_IP – IP-адрес сервера, на котором работает NTA;
- NTA_PORT – можно оставить по умолчанию или изменить;
- NTA_HTTP_PORT – можно оставить по умолчанию или изменить.

7. Запустить docker-compose:

```
# docker compose up -d
```