УТВЕРЖДЕН
ДБАР.62.01.12.000.183-01 32-ЛУ

ПС «СЕНСОР-ПЛУТОН-М1.0»

Руководство системного программиста

ДБАР.62.01.12.000.183-01 32

Листов 57

Инв.№ подл.	Подп. и дата	Взам.инв.№	Инв.№ дубл.	Подп. и дата

Москва
2018

АННОТАЦИЯ

Документ является руководством системного программиста Программного средства «Сенсор-Плутон-М1.0» ДБАР.62.01.12.000.183-01 (далее – ПС «Сенсор-Плутон-М1.0», ПС Сенсор).

В документе рассмотрены общие сведения о структуре ПС Сенсор, приведено описание процедур сборки, установки, настройки, запуска и проверки ПС Сенсор, типовых приёмов работы с ПС Сенсор и сообщений, выдаваемых ПС Сенсор.

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1 Обозначение и наименование программы

Наименование программы: Программное средство «Сенсор» в составе Программного комплекса «Система обнаружения вторжений «Плутон-М1.0» (далее – ПС «Сенсор-Плутон-М1.0», ПС Сенсор).

Обозначение программы: ДБАР.62.01.12.000.183-01.

1.2 Программное обеспечение, необходимое для функционирования программы

1.2.1 ПС Сенсор функционирует под управлением операционной системы Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

1.2.2 ПС Сенсор для обнаружения сетевых вторжений в контролируемом канале передачи данных сигнатурным методом использует:

– системы обнаружения атак (далее – СОА) Suricata версии 4.0;

– СОА Bro версии 2.5.2;

– утилиту p0f версии 3.09b.

1.2.3 ПС Сенсор использует СОА Bro версии 2.5.2 для обнаружения сетевых вторжений в контролируемом канале передачи данных эвристическим методом обнаружения.

1.2.4 ПС Сенсор использует СУБД ClickHouse версии 1.1.54318 для хранения больших данных о событиях информационной безопасности (далее – СИБ), о журналах событий СОА, о событиях аудита безопасности и статистических данных сетевого трафика.

1.2.5 ПС Сенсор использует СУБД PostgreSQL версии 9.4 для хранения данных об объектах контролируемой системы, справочных данных, решающих правил сигнатурного анализа (РПСА), черных списков, базы уязвимостей и базы GeoIP.

1.2.6 ПС Сенсор использует программу-агент Net-SNMP версии 5.4.3 для мониторинга состояния и работоспособности ПС Сенсор. Пользователь может включить дополнительное средство мониторинга работоспособности компонентов Zabbix версии 2.2.7, входящее в состав поставки ПК СОВ.

1.2.7 ПС Сенсор использует утилиту Afick версии 2.1.3.21.3 для аудита целостности, при котором выявляются несанкционированные изменения объектов ПС Сенсор (ПО, конфигурационных файлов, базы решающих правил сигнатурного анализа, черных списков, программных сценариев эвристического анализа).

1.2.8 ПС Сенсор использует Mosquitto MQTT broker версии 3.1.1/3.1 для передачи данных ПС СУС, расположенному вверх по иерархии.

1.3 Языки программирования, на которых написана программа

ПС Сенсор написано на языках программирования C++ версии 11, Python версии 3.5.3

2 ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1 Назначение программы

ПС Сенсор предназначено для:

– обнаружения компьютерных атак (КА) в сетях передачи данных и аномалий в действиях хостов контролируемой системы;

– накопления статистики сетевого трафика и данных профилей хостов контролируемой системы.

2.2 Область применения

ПС Сенсор используется в составе ПК «СОВ «Плутон-М1.0».

2.3 Решаемые задачи и функции ПС Сенсор

ПС Сенсор выполняет следующие функции:

2.3.1 Регистрация и идентификация сетевых вторжений на основе анализа сетевого трафика, передаваемого по контролируемому каналу связи.

2.3.2 Сбор информации об операционных системах, распределённом программном обеспечении, учётных записях пользователей, сертификатов хостов контролируемой системы.

2.3.3 Обнаружение отклонений от профилей хостов контролируемых систем (обнаружение или изменение операционной системы, распределённого программного обеспечения, учётных записей пользователей, сертификатов).

2.3.4 Накопление информации о выявленных сетевых вторжениях в автономном режиме при отсутствии связи с ПС СУС и передача накопленной информации при восстановлении связи.

2.3.5 Контроль свободного дискового пространства, архивирование и автоматическое удаление устаревшей информации при переполнении жёсткого диска.

2.3.6 Регистрация событий аудита безопасности.

2.3.7 Фиксация, передача и обеспечение гарантированной доставки на ПС СУС:

– данных зарегистрированных сетевых вторжений – событий информационной безопасности;

– статистических характеристик сетевого трафика, передаваемого по контролируемому каналу передачи данных;

– параметров функционирования технических и программных средств ПС Сенсор;

– данных аудита безопасности ПС Сенсор;

– копии трафика;

– данных о сетевых взаимодействиях узлов контролируемых систем;

– данных о распределённом программном обеспечении узлов контролируемых систем.

2.3.8 Агрегация однотипных событий.

2.3.9 Предоставление пользователям возможности настроить ПС Сенсор и изменить его параметры конфигурирования с помощью командной среды операционной системы (ОС).

2.3.10 Выполнение команд, поступающих с ПС СУС.

2.3.11 Регулирование доступа пользователей к функциям ПС Сенсор в соответствии с настройками ролевой модели доступа. В поставке ПК СОВ предусмотрена роль «Администратор безопасности СОВ», которая даёт права доступа к функциям настройки и конфигурирования ПС Сенсор с помощью командной среды ОС.

2.3.12 Идентификация, аутентификация и авторизация пользователей выполняется с помощью операционной системы. При этом:

– для доступа используются логины и пароли пользователей;

– отслеживается выполнение требований, указанных в разделе 4.3, к сложности пароля (длина, специальные символы, цифры, буквы в верхнем и нижнем регистре) и к периодичности смены пароля.

2.3.13 Взаимодействие ПС Сенсор и ПС СУС по защищённому каналу связи. Для исключения несанкционированного доступа во время установки соединения удалённый компонент идентифицируется с помощью проверки цифрового сертификата.

2.3.14 Обновление ПС Сенсор в части базы решающих правил сигнатурного анализа, черных списков, программных сценариев эвристического анализа, справочников, базы уязвимости, базы GeoIP, программного обеспечения.

2.3.15 Маскирование своего функционирования за счёт применения механизмов операционной системы.

2.4 Условия применения

2.4.1 Требования к техническим средствам

2.4.1.1 ПС Сенсор функционирует на ЭВМ с характеристиками производительности не ниже, чем ЭВМ архитектуры x86-64, оснащённой сетевыми интерфейсами, поддерживающими скорость передачи данных до 10 Гбит/с.

2.4.1.2 Для установки и функционирования ПС Сенсор требуется свободное пространство на жёстком диске ЭВМ объёмом не менее 50 Гб.

2.4.1.3 Для обеспечения маскирования работы сенсора сетевой интерфейс, используемый для захвата контролируемого сетевого трафика, должен работать в режиме прослушивания трафика и не должен создавать исходящий трафик в контролируемую систему.

2.4.1.4 Если сетевой интерфейс сенсора подключается в разрыв контролируемого канала, то интерфейс должен обеспечивать работу в режиме bypass для функционирования контролируемой системы при отключении питания, наступлении нештатного или аварийного состояния сетевого интерфейса. Режим bypass обеспечивает сетевой интерфейс с одним основным и одним обводным (bypass) портом. Переключение основного порта на bypass-порт должно происходить автоматически.

2.4.2 Требования к программным средствам

2.4.2.1 ПС Сенсор функционирует под управлением операционной системы Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

2.4.2.2 Для хранения резервных копий базы данных ПС Сенсор рекомендуется использовать внешние хранилища.

2.4.3 Требования к организационной среде эксплуатации

2.4.3.1 Физический доступ в помещение, где функционирует ПС Сенсор, должен быть ограничен.

2.4.3.2 Доступ к ПС Сенсор и право работы с ним должны иметь только зарегистрированные пользователи.

2.4.3.3 Взаимодействие сенсоров с СУС должно выполняться по защищённым каналам связи.

2.4.3.4 Для идентификации и аутентификации ПС Сенсор по умолчанию используется сертификат удостоверяющего центра (УЦ) разработчика. Потребителю рекомендуется заменить сертификат удостоверяющего центра разработчика своим сертификатом.

2.4.4 Требования к среде функционирования

2.4.4.1 ЭВМ, на которых устанавливается ПС Сенсор, должны находиться в закрытых отапливаемых и кондиционируемых помещениях, снабжённых необходимыми средствами пожарной безопасности.

2.4.4.2 ЭВМ должны быть обеспечены бесперебойным электропитанием.

2.4.4.3 ОС Astra Linux должна работать в режиме изолированной среды.

3 СТРУКТУРА ПРОГРАММЫ

Сведения о структуре программы, её составных частях, о связях между составными частями и о связях с другими программами приведены в документе "ПК «СОВ «Плутон-М1.0». Описание программы", ДБАР.62.01.12.000.181-01 13.

4 УСТАНОВКА И НАСТРОЙКА ПРОГРАММЫ

4.1 Установка ПС Сенсор

4.1.1 Среда установки

Административное управление в ОС Astra Linux отделено от общего доступа. пользователей. Поэтому, следующие операции по установке и настройке ПС Сенсор, выполняемые в командной среде ОС Astra Linux, требуют привилегий технологического пользователя root:

- настройка сетевого взаимодействия компонентов;
- установка системного времени;
- монтирование внешних носителей;
- установка ПС Сенсор на ТС;
- перезагрузка системы;
- смена пароля пользователя;
- создание пользователей и настройка их учётных записей;
- регистрация компонентов в ПК СОВ;
- настройка параметров протокола MQTT;
- настройка параметров config.conf;
- настройка параметров контролируемой системы;
- настройка параметров следующих сервисов:
    - pluton-pcap-generator;
    - pluton-stat-collector;
    - pluton-component-status-server
- настройка параметров диагностики состояния сервисов;
- настройка уровня системного журналирования;
- удаление и перезагрузка ПС Сенсор.

ВНИМАНИЕ! После установки ОС интерактивный вход в систему привилегированного технологического пользователя root по умолчанию заблокирован.

Создаваемый при установке операционной системы пользователь включается в группу astra-admin. Пользователям, входящим в названную группу, через механизм sudo предоставляются права на выполнение действий по настройке ОС, требующих привилегий технологического пользователя root.

ВНИМАНИЕ! К паролю пользователей, обладающих административным доступом, предъявляются повышенные требования к качеству и надёжности, указанные в п. 4.3.

ПС Сенсор развёртывается на технических средствах (далее – ТС) с установленной операционной системой семейства Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

ВНИМАНИЕ! На ТС не должно быть установлено ПС ПК СОВ.

Для получения информации об установленной операционной системе, необходимо запустить команду:

```
# uname –vr
```

Примечание: для запуска команды необходимо после ввода команды в командную строку нажать кнопку Enter. Подробное описание выполнения команд приведено в п. 4.4.2.

После выполнения команды в командной строке отобразится сообщение следующего вида с номером релиза и номером версии операционной системы:

```
4.2.0-23-generic #28astra39 SMP Tue Mar 1 17:41:12 MSK 2016
```

4.1.2 Установка ПС Сенсор

Предварительно необходимо выполнить подготовительные операции с техническим средством, на которое будет устанавливаться ПС Сенсор:

1) Проверить правильность подключения клавиатуры и дисплея (KVM-консоли) к ТС.

2) В случае использования KVM-консоли – переключить KVM-консоль на взаимодействие с ТС.

3) Включить ТС.

4) Если внешний носитель с установочными пакетами ПС Сенсор – оптический диск, то при отсутствии в составе ТС оптического привода CD-ROM необходимо подключить переносной CD-ROM-привод к свободному USB-разъёму ТС.

5) Убедиться, что основной порт сетевого интерфейса ПС Сенсор не переключён на bypass-порт.

После выполнения всех указанных выше действий необходимо выполнить подготовительные операции с программными средствами, под функционированием которых работает ПС Сенсор:

1) Настроить в конфигурационном файле /etc/network/interfaces сетевой интерфейс, с помощью которого будет выполняться взаимодействие ПС Сенсор с ПС СУС. Пример настройки выглядит следующим образом:

```
auto eth3
iface eth3 inet static
address 192.168.1.1
netmask 255.255.255.0
gateway 192.168.1.2
```

2) Для генерации корректного SSL-сертификата и настройки протокола HTTPS, который будет поддерживать взаимодействие компонентов, необходимо настроить сетевое взаимодействие ПС Сенсор и вышестоящего ПС СУС в таблице /etc/hosts. Для этого необходимо:

а) запустить команду `hostname -f`, которая вернёт полное доменное имя (FQDN) сервера;

б) использовать полученное полное доменное имя для установки доменного имени сервера в файле /etc/hosts. Для этого запустить команду:

`# ipaddress fqdn hostname`, где

– `ipaddress` – IP-адрес хоста, например, 192.168.1.1;

– `fqdn` – полное доменное имя хоста, полученное командой `hostname -f`, например, pluton-sensor-1.domain.tld;

– `hostname` – доменное имя хоста, например, pluton-sensor-1

Пример команды:

```
192.168.1.1 pluton-sensor-1.domain.tld pluton-sensor-1
```

3) Для генерации корректного SSL-сертификата и настройки протокола HTTPS необходимо настроить системное время. Чтобы узнать точное время с поправкой на часовой пояс, необходимо запустить команду:

```
# date
```

После выполнения команды в командной строке появится сообщение с указанием временной метки и часового пояса:

```
Tue Mar 6 13:20:51 MSK 2018
```

4) Установить пакеты `ifenslave` и `bridge-utils`. Для этого запустить команду:

```
# apt-get install bridge-utils ifenslave
```

5) Настроить сетевые интерфейсы, с помощью которых ПС Сенсор получает сетевой трафик, предназначенный для анализа. ПС Сенсор анализирует сетевой трафик, который направляют на агрегированный виртуальный сетевой интерфейс `bond0`. В `bond0` могут быть объединено несколько физических сетевых интерфейсов. Пример объединения физических интерфейсов в `bond0` представлен на рисунке 1 .

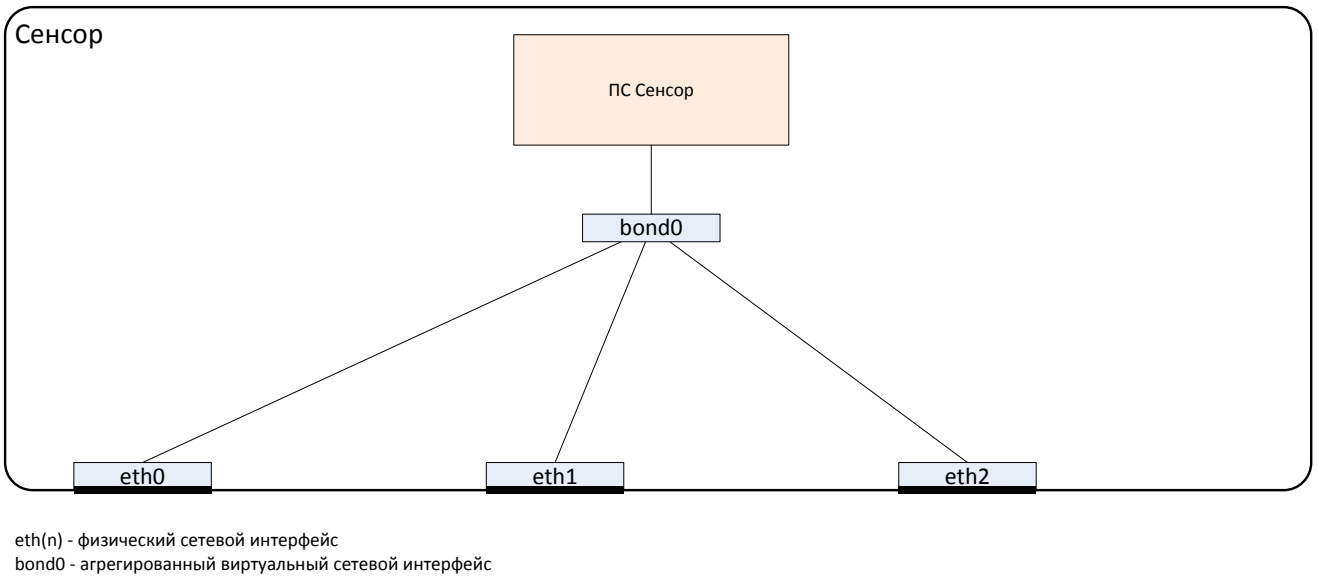


Рисунок 1 – Объединения физических интерфейсов в bond0

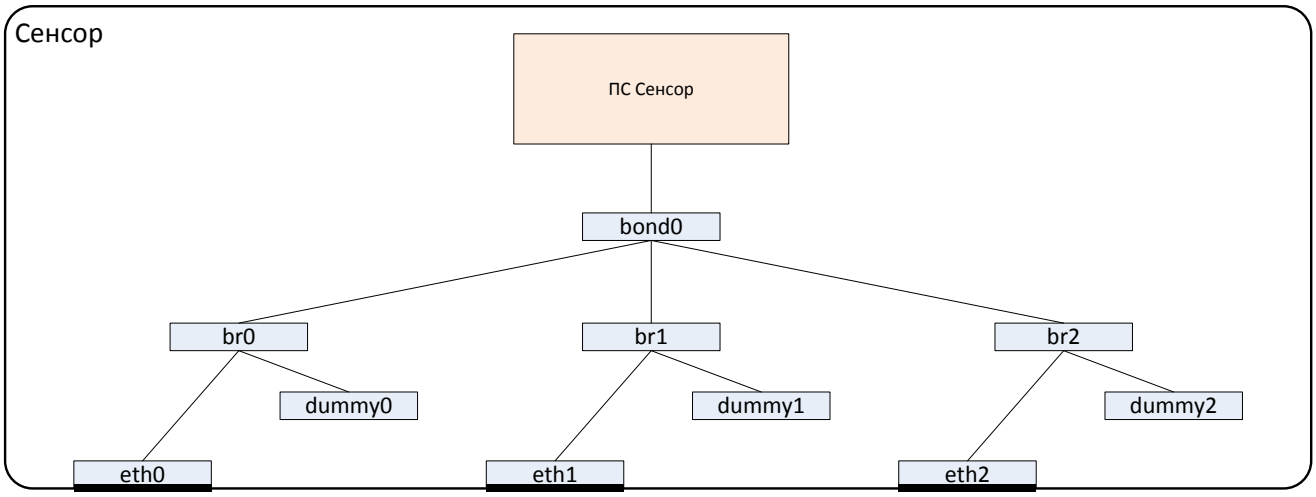
Пример настройки `bond0` в конфигурационном файле /etc/network/interfaces выглядит следующим образом:

```
auto eth0
```

```
iface eth0 inet static
address 0.0.0.0

auto eth1
iface eth1 inet static
address 0.0.0.0

auto eth2
iface eth2 inet static
address 0.0.0.0

auto bond0
iface bond0 inet static
address 0.0.0.0
slaves eth0 eth1 eth2
bond-mode balance-rr
bond-miimon 100
bond-downdelay 200
bond-updelay 200
```

В зависимости от используемых физических сетевых интерфейсов может возникать следующая ситуация: после отсоединении от физического сетевого интерфейса сетевого кабеля `bond0` автоматически не восстанавливает получение сетевого трафика даже после восстановления подключения кабеля.

Для решения этой проблемы можно использовать программный сетевой мост. В этом случае пример объединение физических интерфейсов в `bond0` выглядит следующим образом (см. рисунок 2).



eth(n) - физический сетевой интерфейс
dummy(n) - фиктивный сетевой интерфейс
br(n) - сетевой мост
bond(n) - агрегированный виртуальный сетевой интерфейс

Рисунок 2 - Объединения физических интерфейсов в bond0 с применением сетевых мостов

Пример настройки `bond0` в конфигурационном файле /etc/network/interfaces выглядит следующим образом:

```
auto eth0
iface eth0 inet static
address 0.0.0.0
auto dummy0
iface dummy0 inet static
address 0.0.0.0
pre-up modprobe dummy;:

auto eth1
iface eth1 inet static
address 0.0.0.0
auto dummy1
iface dummy1 inet static
address 0.0.0.0
```

```
pre-up modprobe dummy;:

auto eth2
iface eth2 inet static
address 0.0.0.0
auto dummy2
iface dummy2 inet static
address 0.0.0.0
pre-up modprobe dummy;:

auto br0
iface br0 inet static
bridge_ports eth0 dummy0
address 0.0.0.0

auto br1
iface br1 inet static
bridge_ports eth1 dummy1
address 0.0.0.0

auto br2
iface br2 inet static
bridge_ports eth2 dummy2
address 0.0.0.0

auto bond0
iface bond0 inet static
address 0.0.0.0
```

```
slaves br0 br1 br2
bond-mode balance-rr
bond-miimon 100
bond-downdelay 200
bond-updelay 200
```

6) Убедиться, что на сервере доступен установочный диск с Astra Linux Special Edition «Смоленск» версии не ниже 1.5.

После проведения всех подготовительных действий для установки ПС Сенсор на ТС необходимо выполнить следующие инструкции:

1) Подключить внешний носитель с установочными пакетами и средой функционирования ПК «СОВ «Плутон-М1.0» ДБАР.62.01.12.000.181-01 к ТС одним из следующих способов:

– если внешний носитель – оптический диск, то поместить внешний носитель в оптический привод CD-ROM;

– если внешний носитель – USB-накопитель, то использовать для подключения USB-порт.

2) Нажать на клавиатуре (KVM-консоли) ТС клавиши Ctrl+Alt+F2 и на запрос операционной системы ввести имя и пароль привилегированного технологического пользователя «root».

После ввода учётных данных привилегированного технологического пользователя этот пользователь получит доступ к командной строке операционной системы.

3) Смонтировать внешний носитель. Для этого указать команду:

– для установки через оптический привод CD-ROM:

```
# sudo mount -r -t iso9660 /dev/cdrom /media/cdrom
```

– для установки через USB-порт:

```
# sudo mount -r -t iso9660 /dev/sdb
```

4) Перейти в каталог /media/cdrom. Для этого указать команду:

```
# cd /media/cdrom
```

5) Выполнить команду установки ПС Сенсор. Для этого ввести следующие параметры:

– тип устанавливаемого компонента -- sensor;

– географические координаты ПС Сенсор с ключами --ln (долгота) и --lt (широта);

– IP-адрес сервера синхронизации времени с ключом --ntp;

– путь до оптического диска со средой функционирования ПС СУС -- prt.

Примеры команды:

```
# sudo bash ./pluton_install.sh sensor --ln <долгота ПС Сенсор> --lt <широта ПС Сенсор> --ntp <IP-адрес сервера синхронизации времени> --prt <путь к точке монтирования оптического диска со средой функционирования ПС СУС>
```

При установке ПС Сенсор автоматически создаётся технологический пользователь «admin».

6) По завершении установки указать команду перезагрузки системы:

```
# sudo init 6
```

ВНИМАНИЕ! Выполнение перезагрузки после установки обязательно, в противном случае корректная настройка и запуск ПС Сенсор будут невозможны.

После перезагрузки следует:

1) Переключить основной порт сетевого интерфейса ПС Сенсор на bypass-порт.

2) Нажать на клавиатуре (KVM-консоли) ТС клавиши Ctrl+Alt+F2.

3) Ввести рабочее имя и пароль технологического пользователя (заводская установка – «admin»/ «vP}sW23*»).

После этого будет выполнен вход в командную среду технологического пользователя, предоставляющую доступ к технологическим возможностям ПС Сенсор.

4) Изменить пароль технологического пользователя. Для этого в командной среде технологического пользователя указать команду:

```
# passwd admin
```

5) В ответ на запрос системы дважды ввести новый пароль, удовлетворяющий требованиям, указанным в п. 4.3.

6) Создать при необходимости дополнительных технологических пользователей. Для этого указать команду:

```
# sudo useradd <имя_пользователя>
```

7) Настроить программные средства согласно п. 4.2.

8) Завершить сеанс работы – на клавиатуре KVM-консоли нажать клавиши Ctrl+D.

4.2 Настройка ПС Сенсор

Действия по настройке ПС Сенсор выполняются в командной среде ОС. Процедура входа в командную среду описана в разделе 4.4.1. Настройку ПС Сенсор может проводить только пользователь, обладающий привилегиями технологического пользователя «root».

По окончании внесения изменений следует выйти из режима изменения конфигурационных параметров – нажать клавиши Ctrl+D.

4.2.1 Регистрация сенсора

Для регистрации сенсора необходимо выполнить следующие действия:

1) На регистрируемом сенсоре указать команду:

```
# pluton-register-component host port [info],
```

где

`host` – адрес СУС, в котором регистрируется сенсор,

Примечание: если указывается hostname, то нужно указывать его полностью. При попытке зарегистрировать с сокращённым hostname система выдаст ошибку, так как выполняется проверка на полное соответствие указанного hostname с hostname сертификата.

`port` – порт транспортной системы MQTT (фиксированный параметр, port=8883),

`info` – информационное сообщение (необязательный параметр).

Пример команды:

```
# sudo pluton-register-component 10.31.9.157 8883 Sensor-1
```

2) На СУС, в котором регистрируется сенсор, с использованием графического интерфейса перейти из вкладки меню «Администрирование» в раздел «Журнал регистрации компонентов».

3) Выделить в списке компонентов регистрируемый сенсор правой кнопкой мыши;

4) Подтвердить регистрацию сенсора – нажать кнопку  .

После успешной регистрации статус регистрируемого сенсора должен измениться с «В процессе» на «Подтверждено», в соответствии с рисунком 3.

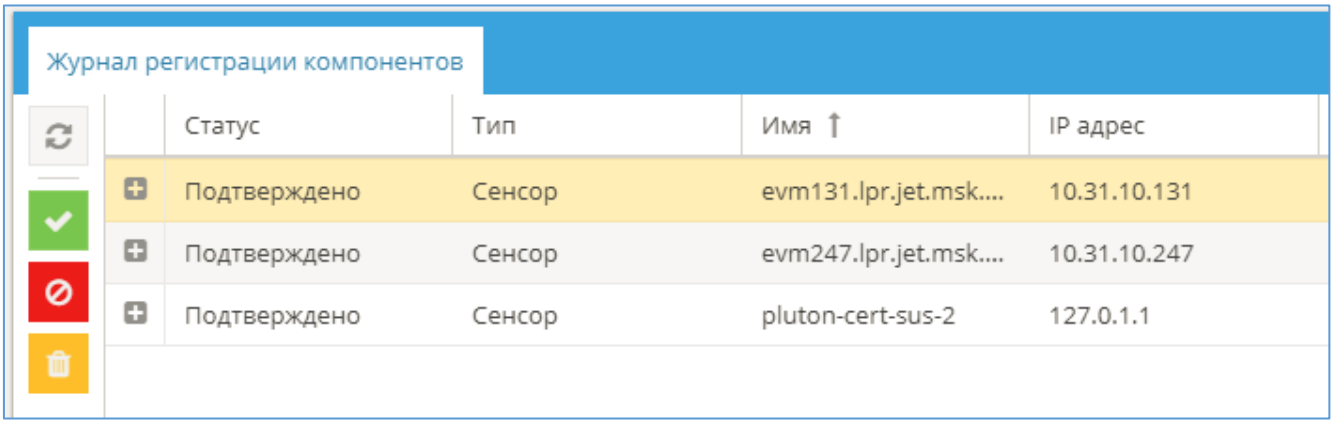


Рисунок 3 – Регистрация компонентов

Для проверки статуса регистрируемого сенсора необходимо указать команду:

```
# pluton-registration-status
```

При успешной регистрации сенсора в командной строке пользователю отобразится сообщение:

```
Компонент зарегистрирован на СУС: fvm91.lpr.jet.msk.su
```

При отклонении вышестоящим СУС заявки на регистрацию сенсора в командной строке пользователя отобразится сообщение:

```
Последний запрос на регистрацию отклонён 2018-03-15 13:31:53+00:00
Desc: ""
Msg: "Заявка на регистрацию отклонена"
ParentComp: fvm91.lpr.jet.msk.su
ParentCompPort: 8883
Компонент не зарегистрирован на СУС
```

4.2.2 Настройка параметров протокола MQTT и соединения с вышестоящим ПС СУС

Для обмена данными с вышестоящим СУС используется Mosquitto MQTT broker версии 3.1.1/3.1.

Сервер Mosquitto принимает сообщения на порту 8883.

Для подключения требуется указать IP-адрес СУС и порт сервера Mosquitto (по умолчанию 8883).

Регистрация сенсора на вышестоящем СУС описана в разделе 4.2.1

4.2.3 Настройка параметров контролируемой системы home_net

Контролируемая система задаётся на сенсоре пользователем, обладающим привилегиями технологического пользователя «root». Для задания контролируемой системы требуется указать команду:

```
# sudo pluton-change-homenet [-n "Имя КС"] [-d "Описание"]
CIDR [CIDR]
```

Пример команды:

```
# sudo pluton-change-homenet -n "Intranet" -d "controlled
network" "192.168.0.0/16, 10.140.31.0/24, 210.0.0.0/8"
```

ВНИМАНИЕ! Настройка параметров контролируемой системы homenet является обязательной! Иначе сервисы pluton-pcap-generator и pluton-stat-collector будут игнорировать сессии.

4.2.4 Настройка параметров сервиса сбора трафика pluton-pcap-generator

Для корректной работы сервиса pluton-pcap-generator, сервиса сбора сетевого трафика, необходимо настроить следующие параметры:

– session_count=18000 – количество кэшируемых сессий;

– packets_count_session=300 – количество захваченных пакетов за время одной сессии;

– packets_around_ise = 10 – количество сохраняемых сетевых пакетов после генерирования СИБ (число сохраняемых пакетов должно быть не менее 10);

– packet_payload=1600 – размер сетевого пакета;

– alert_socket_ip=127.0.0.1 – IP-адрес программного интерфейса сервиса pluton-ise-publisher;

– alert_socket_port=50001 – порт программного интерфейса сервиса pluton-ise-publisher;

– alert_socket_reconnect_time=1 – временной интервал повторного подключения к сервису pluton-ise-publisher;

– alerts_path=/var/spool/pluton/pcap-generator/PCAPs/ – путь к хранилищу файлов с расширением *.pcap;

– affinity="0,1" – ядра процессов, которые использует сервис pluton-pcap-generator.

4.2.5 Настройка параметров сервиса сбора статистики pluton-stat-collector

Для корректной работы сервиса pluton-stat-collector, сервиса сбора статистики по сетевому трафику, необходимо настроить следующие параметры:

– `stat_interval=60` – размер порции накопления статистики, который представляет собой длительность интервала времени в секундах .

4.2.6 Настройка параметров config.conf

Значения всех конфигурационных параметров ПС Сенсор и примеры их задания приведены в таблице 1.

Таблица 1 – Конфигурационные параметры ПС Сенсор

Раздел	Параметр	Описание
`[COMMON]`	`broker_reconnect_interval=60000`	Настройка интервала повторного подключения к MQTT broker
	`interface=bond0`	Имя сетевого интерфейса, прослушиваю щего сетевой трафик
`[COMPONENT]`	`id = 75e51d10-02ff-4733-a32e-c31aaa811c84`	Числовой идентификатор сенсора; должен быть уникальным в пределах множества всех сенсоров, функционирую щих в иерархической структуре ПК СОВ «Плут он-М1.0»
	`type = SENSOR`	Тип компонента (для сенсора всегда `SENSOR`)

Раздел	Параметр	Описание
[DATABASE]	hostname = 127.0.0.1	Имя хоста, который подключается к БД PostgreSQL
	port = 5432	Номер порта, на котором происходит взаимодействие ПС Сенсор с БД PostgreSQL
	name = pluton	Название БД PostgreSQL
	user = pluton	Имя пользователя в БД PostgreSQL
	password = arUw4Tvl	Пароль пользователя БД PostgreSQL
	reconnect_timeout = 5000	Настройка тайм-аута (в мс) на повторное соединение с сервисом БД PostgreSQL после обрыва предыдущего соединения
[CLICKHOUSE]	hostname = 127.0.0.1	Имя хоста, который подключается к БД PostgreSQL
	port = 8123	Номер HTTP-порта, на котором происходит взаимодействие ПС Сенсор с БД PostgreSQL
	native_port = 9000	Номер TCP-порта, на котором располагается ClickhouseClient
	name = default	Название БД ClickHouse

Раздел	Параметр	Описание
	user = default	Имя пользователя в БД ClickHouse
	password = KEIrOvfb	Пароль пользователя БД ClickHouse.
	clickhouse_save_interval=1000	Настройка интервала между запросами к сервису БД Clickhouse. Рекомендуется использовать значение больше чем 10 мс, чтобы не превышать значения 100 запросов в секунду
[PKI]	cafile = /etc/pluton/tls/Pluton-CA.crt certfile = /etc/pluton/tls/evm247.lpr.jet.msk.su.crt keyfile = /etc/pluton/tls/evm247.lpr.jet.msk.su.pem	Цепочка SSL-сертификатов
	updates_signal_topic=sensor/internal/updates-signal	Топик обновлений
[TELEMETRY]	RAM_period = 60	Периодичность обновления данных об использовании ОЗУ в секундах
	RAM_thresholds = 50 80	Пороговые значения для показателя «Процент использования ОЗУ»
	CPU_period = 60	Периодичность обновления данных об использовании ЦПУ в секундах

Раздел	Параметр	Описание
	CPU_thresholds = 70 95	Пороговые значения для показателя «Процент использования ЦПУ»
	SWAP_period = 120	периодичность обновления данных об использовании файле подкачки в секундах
	SWAP_thresholds = 50 80	Пороговые значения для показателя «Процент использования файла подкачки»
	HDD_period = 300	Периодичность обновления данных об использовании НЖМД в секундах
	HDD_thresholds = 60 90	Пороговые значения для показателя «Процент использования НЖМД»
	heartbeat = 60	Периодичность отправки сигнала о работоспособности на вышестоящий компонент в секундах

Раздел	Параметр	Описание
[NOTIFICATION]	alert_caption_template = /etc/pluton/alert-notification/caption_template.txt alert_content_template = /etc/pluton/alert-notification/content_template.txt alert_attr_table = /etc/pluton/alert-notification/attr_table.json audit_caption_template = /etc/pluton/audit-notification/caption_template.txt audit_content_template = /etc/pluton/audit-notification/content_template.txt audit_attr_table = /etc/pluton/audit-notification/attr_table.json	Файлы, содержащие шаблоны почтовых уведомлений
	notify_severity_min = 0	Минимальное пороговое значение критичности, при котором формируется уведомление о появлении СИБ и событий аудита безопасности
	notify_audit_type = 'Создана новая роль'	Имя события аудита безопасности (параметр может использоваться несколько раз)
	notify_event_type = 'Аудит пользователей'	Имя типа события аудита безопасности (параметр может использоваться несколько раз)
	notify_smtp_from = noreply@service.jet.msk.su	Электронный адрес отправителя уведомления
	notify_smtp_server = lab-dns.service.jet.msk.su	Адрес сервера исходящей электронной почты

Раздел	Параметр	Описание
	notify_smtp_port = 25	Порт сервера исходящей электронной почты
	notify_smtp_login =	Учётная запись сервера исходящей электронной почты. Необязательный параметр, при необходимости устанавливается пользователем
	notify_smtp_password =	Пароль учётной записи сервера исходящей электронной почты. Необязательный параметр, при необходимости устанавливается пользователем
	notify_smtp_ssl = False	Параметр защиты соединения
[SURICATA]	install_path=/etc/suricata	Путь к файлам Suricata
	backup_path=/var/spool/pluton/pluton-updater/backup/suricata	Путь к резервным копиям файлов Suricata
	rules_extension=.rules	Расширение файлов с сигнатурами Suricata
[BRO]	blacklist_path=/opt/bro/scripts/pluton install_path=/opt/bro/scripts/pluton	Путь к файлом Bro
	backup_path=/var/spool/pluton/pluton-updater/backup/bro	Путь к резервным копиям файлов Suricata
	rules_extension=.sig	Расширение файлов с сигнатурами Bro

Раздел	Параметр	Описание
[P0F]	udp_port=53412	Номер порта, через который происходит взаимодействие p0f с сервисом, записывающим сгенерированные p0f СИБ в БД
[GEOIP]	install_path=/usr/share/GeoIP city=GeoIPCity.dat locations_csv=GeoLiteCity-Location.csv blocks_csv=GeoLiteCity-Blocks.csv	Пути для GeoIP
[BROCCOLI]	host=127.0.0.1 reconnect_interval=10000 update_interval=1000	Параметры сокета Bro для Broccoli
[PCAP]	session_count=18000	Количество кэшируемых сессий
	packets_count_session=300	Количество захваченных пакетов за время одной сессии
	packets_around_ise = 10	Количество сохраняемых сетевых после генерирования СИБ. Число сохраняемых пакетов должно быть не менее 10
	packet_payload=1600	Размер сетевого пакета
	alert_socket_ip=127.0.0.1	IP-адрес программного интерфейса сервиса pluton-ise-publisher
	alert_socket_port=50001	Порт программного интерфейса сервиса pluton-ise-publisher

Раздел	Параметр	Описание
	alert_socket_reconnect_time=1	Временной интервал повторного подключения к сервису pluton-ise-publisher
	alerts_path=/var/spool/pluton/pcap-generator/PCAPs/	Путь к хранилищу файлов с расширением *.pcap
	affinity="0,1"	Ядра процессов, которые использует сервис pluton-pcap-generator
[STAT_COLLECTOR]	stat_interval=60	Размер порции накопления статистики, который представляет собой длительность интервала времени в секундах
[AUDIT]	logfiles = /var/log/auth.log, /var/log/syslog, /var/log/pluton/scs-web-ui-access.log	Список системных файлов и каталогов, которые содержат данные журнала аудита
	unsent_buffer = 100000 bulk_insert = 1000	Настройки промежуточного хранилища данных сервиса pluton-ise-publisher
[UPDATE_SERVER]	updates_storage_path = /var/spool/pluton/pluton-updater/archives	Пути к архивам полученных обновлений

Раздел	Параметр	Описание
	archive_folder_by_type = SURICATA_UPDATE:suricata GEOIP_UPDATE:geoip BRO_UPDATE:bro CVE_UPDATE:cve SOFTWARE_UPDATE:software BL_UPDATE:bl	Описание структуры пакета обновлений с указанием типов обновлений (обновление Suricata, обновление GeoIP, обновление Bro, обновление базы уязвимостей, обновление ПО, обновление черных списков)
[ISE_CREATION]	unix_socket_reconnect_timeout=1	Временной интервал для повторного соединения сервиса pluton-ise-publisher на UNIX-сокеты (в секундах)
	suricata_alerts_socket=/tmp/ise-log.sock	Путь к сокету, которому соответствует тип СИБ «сигнатура Suricata»
	signature_ise_socket=/tmp/signature-ise.sock	Путь к сокету, которому соответствует тип СИБ «сигнатура Bro»
	blacklist_ise_socket=/tmp/blacklist-ise.sock	Путь к сокету, которому соответствует тип СИБ «черные списки»

Раздел	Параметр	Описание
	profile_ise_socket=/tmp/profile-ise.sock	Путь к сокету, которому соответствует тип СИБ «изменение профиля хоста»
	group_alert_count=0	Количество СИБ для группировки. Если не указано, то работает только ограничение group_time_interval
	group_time_interval=0	Интервал времени в секундах, в течение которого группируются СИБ. Если не указано, то работает только ограничение group_alert_count
	group_cache_reset_interval=3600	Интервал времени в секундах, по истечении которого ПК СОВ выполняет сброс буфера накопленных СИБ. Если не указано или меньше group_time_interval, то буфер сбрасывается только при достижении параметров group_alert_count, group_time_interval
	geoip_db_path=/usr/share/GeoIP/GeoIPCity.dat	Путь к GeoIP

Раздел	Параметр	Описание
	new_host_rediscovery_time=3600	Временной интервал обновления регистрации хоста
[ISE_TRANSMISSION]	max_queue_size=100000	Максимальный размер очереди сгенерированных СИБ для сервиса pluton-ise-publisher
	max_ise_package_size=1000	Количество СИБ в одном пакете
	package_wait_verify_timeout=600000	Тайм-аут на подтверждение от вышестоящего компонента получения пакета с СИБ (мс)
	send_package_interval=4000	Временной интервал отправления пакетов с СИБ на вышестоящий компонент (мс)
	send_ise_request_topic=v1/scs/sendIseRequest accept_read_resp_topic=v1/sensors/%1/iseAcceptReadinessResponse send_ise_resp_topic=v1/sensors/%1/sendIseResponse accept_read_request_topic=v1/scs/iseAcceptReadinessRequest	Топики (%1 – id сенсора)
	crit_prior_intervals="00:00:00-23:59:59" major_prior_intervals="00:00:00-23:59:59" norm_prior_intervals="00:00:00-23:59:59" minor_prior_intervals="00:00:00-23:59:59" info_prior_intervals="00:00:00-23:59:59"	Временные интервалы, за которые происходит передача СИБ указанного приоритета
[COMPONENT_STATUS]	get_status=internal/get_mode service_status=internal/%1/mode general_status=internal/mode	Настройки транспортного протокола MQTT между сервисами ПК СОВ

Раздел	Параметр	Описание
	tmp_path=/var/spool/pluton/pluton-component-status/tmp	Путь к хранилищу временного состояния сервисов ПК СОВ
	process_start_tries_number=3 process_stop_tries_number=3	Количество всех попыток изменения состояния сервисов
	process_change_state_retry_pause_sec=15	Временной интервал между попытками (в секундах)
	creating_profiles_call_timeout_sec=60	Тайм-аут ожидания генерации профилей при выходе из режима обучения
	check_processes_interval_sec=60	Временной интервал запуска проверки работоспособности сервиса
[EVENT_LOGGER_WATCHDOG]	event_logger_process_name=pluton-event-logger	Имя процесса, который записывает сгенерированные СИБ в БД (сервис pluton-event-logger)
	check_processes_interval_sec=30	Временной интервал запуска проверки контролируемых сервисов
	first_bro_worker_port=47763	Первый порт, с которого осуществляется взаимодействие с Broccoli

Раздел	Параметр	Описание
	is_heartbeat_enabled=false	Параметр активации сервиса слежения за состоянием модуля
	heartbeat_interval_sec=30	Временной интервал активации сервиса слежения за состоянием модулей ПК СОВ
	heartbeat_ports_range_starts_with=4433	Первый порт, на котором происходит активация сервиса слежения за состоянием модулей
	heartbeat_timeout_sec=20	Тайм-аут сервиса слежения за состоянием модуля
	heartbeat_host=127.0.0.1	IP-адрес хоста, на котором происходит запуск сервиса слежения за состоянием модулей

4.2.7 Настройка параметров диагностики состояния сервисов и уровня журналирования

Уровни записи в системные журналы файлов с расширением *.log сервисов ПК СОВ настраиваются в конфигурационном файле /etc/pluton/logging.conf и /etc/pluton/loggingCpp.conf

Системные журналы сервисов ПК СОВ записываются и хранятся в системном log-файле /var/log/syslog в формате:

```
[дата] [время] [хост] [идентификатор процесса] – [дата] [время] – [имя сервиса] [уровень журналирования] [сообщение]
```

Пример команды:

```
Mar 10 16:12:26 dvm167 9084 - 2018-03-10 16:12:26,954 -
PlutonComponentStatusServer - INFO - Nothing to stop at
status PASSIVE at "Health check" mode
```

Системные журналы транспортной системы, веб-сервера и системные журналы миграций расположены в файле /var/log/pluton/.

Системные журналы сервисов third-party записываются и хранятся в соответствии с собственными настройками журналирования.

4.2.8 Настройка параметров сервиса pluton-component-status-server. Управление и диагностика

Сервис pluton-component-status-server – сервис, предназначенный для проведения над сервисами ПК СОВ следующих операций:

- контроль состояний;
- запуск и перезапуск;
- остановка.

Сервисы, реализующие функции ПК СОВ, могут находится в одном из следующих состояний:

- «Работает» – сервис загружен в ОЗУ и выполняет свою основную функцию;
- «Остановлен» – сервис выгружен из ОЗУ и не выполняет никаких функций;

ПС Сенсор может находится в одном из следующих функциональных состояний:

- «Инициализация»;
- «Не зарегистрирован»;
- «Не активный»;
- «Обучение»:
  - «Обучение»;
  - «Переобучение»;
  - «Дообучение»;
  - «Коррекция профиля хостов»
- «Обнаружение»;
- «Скомпрометирован».

В таблице 2 установлено соответствие между состоянием ПС Сенсор и состояниями сервисов: в каждом определённом состоянии компонента должны быть запущены и остановлены определённые сервисы. Если сервис находится в состоянии, которое не соответствует состоянию, обозначенному в таблице 2, то сервис работает некорректно.

Таблица 2 – Статусы системных сервисов ПС Сенсор

Статус компонента/ Системный сервис	**Инициализация**	**Не зарегистрирован**	**Неактивный**	**Обучение**	**Обнаружение**	**Скомпрометирован**
Сервисы Python						
pluton-audit-server	Остановлен	Работает	Работает	Работает	Работает	Работает
pluton-homenet-control	Остановлен	Остановлен	Работает	Остановлен	Работает	Остановлен
pluton-job-runner	Остановлен	Остановлен	Работает	Работает	Работает	Работает
pluton-notification-server	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
pluton-suricata-rule-updater*	Остановлен	Остановлен	Остановлен	Работает	Работает	Остановлен
pluton-updater-server	Остановлен	Остановлен	Работает	Работает	Работает	Остановлен
pluton-transport-server	Остановлен	Работает	Работает	Работает	Работает	Работает
pluton-event-logger-watchdog	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
pluton-pcap-server	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
pluton-query-server	Остановлен	Работает	Работает	Работает	Работает	Работает

Статус компонента/ Системный сервис	**Инициали-зация**	**Не зарегистри-рован**	**Неактивный**	**Обучение**	**Обнаруж ение**	**Скомпроме тирован**
pluton-suricata-rule-server	Остановлен	Остановлен	Остановлен	Работает	Работает	Остановлен
pluton-profile-replicator*	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
pluton-component-status-server	Остановлен	Работает	Работает	Работает	Работает	Работает
pluton-health-monitor	Остановлен	Работает	Работает	Работает	Работает	Работает
Сервисы C++						
pluton-ise-publisher	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
pluton-stat-collector	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
pluton-pcap-generator	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
pluton-event-logger	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
Сервисы ПС Сенсор						
Сервис suricata*	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
Сервис pluton-bro	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
Сервис p0f*	Остановлен	Остановлен	Остановлен	Работает	Работает	Работает
MQTT	Остановлен	Остановлен	Работает	Работает	Работает	Работает

Статус компонента/ Системный сервис	**Инициали-зация**	**Не зарегистри-рован**	**Неактивный**	**Обучение**	**Обнаруж ение**	**Скомпроме тирован**
Сервис предотвращения переполнения дискового пространства оперативных данных	Остановлен	Остановлен	Работает	Работает	Работает	Работает
Zabbix	Остановлен	Остановлен	Работает	Работает	Работает	Работает
PostgreSQL	Остановлен	Остановлен	Работает	Работает	Работает	Работает
ClickHouse	Остановлен	Остановлен	Работает	Работает	Работает	Работает
SNMPD	Остановлен	Работает	Работает	Работает	Работает	Работает

Дополнительных настроек сервис pluton-component-status-server не требует.

4.2.9 Настройка учётных записей пользователей

Учётные записи пользователей создаются на корневом СУС и передаются на нижние уровни иерархической модели компонентов. Чтобы активировать учётную запись на подчинённом компоненте, в том числе на сенсоре, необходимо через утилиту useradd указать команду создания пользователя:

```
# sudo useradd <имя_пользователя>
```

Создание и управление учётными записями пользователей реализуются стандартными средствами ОС Astra Linux.

4.2.10 Проверка результатов установки и запуска ПС Сенсор

После проведения подготовительных операций на ТС для установки ПС Сенсор и выполнения действий по установке ПС Сенсор (см. раздел 4.1.2) в командной строке отобразится сообщение с выводом результатов выполнения набора сценариев развёртывания ПС Сенсор, которые содержатся в файле playbook системы Ansible. Результат содержит следующие параметры:

- `ok` – общее количество выполняемых сценариев по установке ПС Сенсор;
- `changed`– количество изменённых состояний на локальном хосте;

– `unreachable` – количество хостов, которые были недоступны во время выполнения набора сценариев (в случае успешного завершения установки ПС Сенсор этот параметр принимает значение 0, в случае завершения установки с ошибкой – значение 1);

– `failed` – количество невыполненных сценариев (в случае успешного завершения установки ПС Сенсор данный параметр принимает значение 0, в случае завершения установки с ошибкой – значение больше нуля).

В случае успешной установки ПС Сенсор в командной строке отобразится сообщение, показанное на рисунке :

Рисунок 4 –Успешное завершение установки ПС Сенсор

В случае возникновения ошибки при установке ПС Сенсор, пользователю в командной строке отобразится сообщение, показанное на рисунке 5:

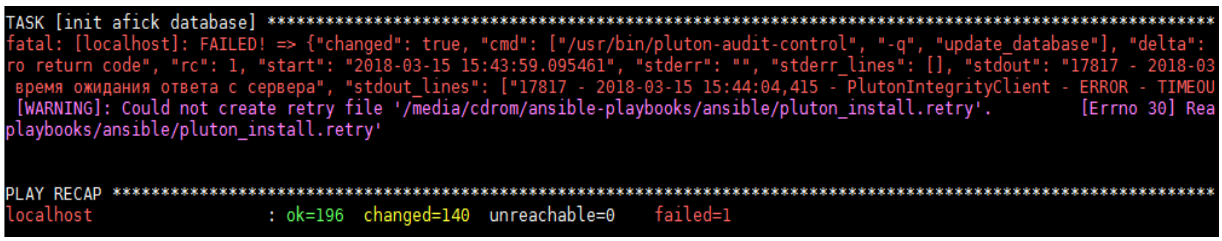


Рисунок 5 – Завершение установки ПС Сенсор с ошибкой

4.2.11 Удаление и перезагрузка ПС Сенсор

Удаление всех установочных пакетов, настроек и данных ПС Сенсор выполняется средствами ОС Astra Linux Special Edition «Смоленск». Операцию удаления может совершать пользователь, обладающий привилегиями технологического пользователя «root». Для удаления ПС Сенсор с ТС необходимо указать команду:

```
# sudo rm -rf --no-preserve-root /
```

Дополнительных сервисов по удалению и перезагрузке ПС Сенсор не предусмотрено.

4.3 Парольная политика

Пароли учётных записей пользователей должны удовлетворять следующим требованиям сложности:

а) срок действия пароля составляет не более 90 дней;

б) длина пароля не менее восьми символов;

в) пароль должен содержать как цифровые, так и буквенные символы, минимально две цифры и минимально две буквы;

г) пароль должен содержать минимально два нецифровых и небуквенных символа;

д) пароль должен содержать буквенные символы в верхнем и нижнем регистре, минимально одну букву в верхнем регистре;

е) каждый обновлённый пароль должен отличаться от четырёх предыдущих;

ж) каждый обновлённый пароль должен отличаться минимум на три символа от предыдущего.

Выполнение требований к сложности пароля (длина, специальные символы, цифры, буквы в верхнем и нижнем регистре) и к периодичности смены пароля отслеживается механизмами операционной системы.

4.4 Использование командной среды ПС Сенсор

Для начальной настройки, проверки и восстановления работоспособности ПС Сенсор используется командная среда операционной системы Astra Linux, предоставляющая доступ к возможностям диагностики и настройки ПС Сенсор.

4.4.1 Вход в командную среду ПС Сенсор

Чтобы войти в командную среду ПС Сенсор с локальной консоли (KVM-консоли), необходимо:

– нажать на клавиатуре (KVM-консоли) клавиши Ctrl+Alt+F2.

На экране появится запрос на ввод рабочего имени и пароля пользователя;

– ввести имя и пароль технологического пользователя «admin».

Чтобы войти в командную среду ПС Сенсор по сети с удалённого узла (при наличии такой возможности), необходимо на удалённом узле, функционирующем под управлением операционной системы Astra Linux Special Edition «Смоленск» версии не ниже 1.5, указать команду:

```
# ssh <ip-адрес сенсора>,
```

где в качестве параметра `<ip-адрес сенсора>` задать ip-адрес сенсора. В ответ на запрос необходимо ввести имя и пароль технологического пользователя «admin».

4.4.2 Выполнение команд

Для выполнения команды можно либо набрать её на клавиатуре полностью, либо набрать несколько первых символов команды и нажать клавишу Tab. Если набранным первым символам соответствует несколько команд, появится подсказка с возможными вариантами, после чего можно набранную команду откорректировать. Если набранным первым символам соответствует одна команда, введённое начало команды в строке ввода автоматически будет дополнено недостающими символами.

Большинство команд требует задания одного или нескольких параметров. Для просмотра списка требуемых параметров после набора команды также можно нажать клавишу Tab для вывода необходимых параметров команды. Если команда требует параметр, значение которого выбирается из списка, по нажатии клавиши Tab появится список возможных значений параметра. Для вывода подсказки, поясняющей действие, выполняемое командой, необходимо после набора команды ввести с клавиатуры символ «?».

Для выполнения набранной команды следует нажать клавишу Enter.

Команды, выполняющие логически связанные действия, логически объединяются в группы. Команды в группе начинаются с одного и того же слова или нескольких слов. Это позволяет выполнять нескольких команд одной группы, не набирая каждую из них полностью: достаточно ввести общие начальные слова для группы команд и нажать клавишу Enter, в результате чего произойдёт переход в режим выполнения команд данной группы. В этом режиме требуется вводить только завершающую часть команд, опуская общее для группы команд начало. Для возврата из режима выполнения команд той или иной группы в режим ввода команд полностью следует нажать клавиши Ctrl+D.

Если выводимые в результате выполнения команды сообщения не помещаются на экране, для прокрутки экрана можно использовать комбинации клавиши Shift+PageUp и Shift+PageDown.

Для повторного заполнения строки ввода ранее выполненной командой используются клавиши «↑» и «↓».

Для завершения сеанса работы в командной среде изделия следует нажать клавиши Ctrl+D.

4.5 Создание резервной копии данных ПС Сенсор на внешнем носителе

ПС Сенсор позволяет создавать и сохранять резервные копии своей БД на внешнем носителе информации. Резервное копирование выполняется по команде администратора безопасности СОВ.

Для создания резервной копии БД ПС Сенсор необходимо:

– при отсутствии в составе технического средства, на котором установлено ПС Сенсор, записывающего CD/DVD-привода – подключить переносной записывающий CD/DVD-привод к свободному USB-разъёму технического средства;

– вставить чистый компакт-диск в CD/DVD-привод;

– нажать на клавиатуре (KVM-панели) клавиши Ctrl+Alt+F2 и на запрос операционной системы ввести имя и пароль пользователя, обладающего привилегиями технологического пользователя «root».

– после ввода учётных данных пользователь получит доступ к командной строке операционной системы.

4.5.1 Создание резервной копии файлов *.conf

Для создания резервной копии файлов *.conf пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС указать команду:

```
# pluton guard backup config <путь к хранилищу>
```

Для выполнения команды необходимо указать путь к хранилищу созданных резервных копий.

4.5.2 Создание резервной копии файлов *.pcap

Для создания резервной копии файлов *.pcap пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС указать команду:

```
# pluton guard backup pcap <путь к хранилищу>
```

Для выполнения команды необходимо указать путь к хранилищу созданных резервных копий.

4.5.3 Создание резервной копии данных БД PostgresSQL

Для создания резервной копии данных БД PostgresSQL пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС указать команду:

```
# pluton guard backup postgresql <путь к хранилищу>
```

Для выполнения команды необходимо указать путь к хранилищу созданных резервных копий (значение по умолчанию – /backup/postgres).

Созданная резервная копия данных БД PostgreSQL сохраняется в директории YYYY/MM/DD. Эта директория автоматически создаётся внутри дискового раздела, указанного при первоначальной настройке резервного копирования.

4.5.4 Создание резервной копии данных для БД ClickHouse

Для создания резервной копии данных БД ClickHouse пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС указать команду:

```
# pluton guard backup clickhouse <путь к хранилищу>
```

Для выполнения команды необходимо указать путь к хранилищу созданных резервных копий (значение по умолчанию – /backup/clickhouse).

Созданная резервная копия данных БД PostgreSQL сохраняется в директории YYYY/MM/DD. Эта директория автоматически создаётся внутри дискового раздела, указанного при первоначальной настройке резервного копирования.

Созданная резервная копия данных БД Clickhouse сохраняется в директории YYYY/MM/DD. Данная директория автоматически создаётся внутри дискового раздела, указанного при первоначальной настройке резервного копирования.

4.5.5 Создание резервной копии всех данных ПС Сенсор

Для создания резервной копии файлов *.conf,*.pcap, данных БД PostgeSQL, данных БД ClickHouse пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС указать команду:

```
# pluton guard backup all <путь к хранилищу>
```

Для выполнения команды необходимо указать путь к хранилищу созданных резервных копий.

4.6 Восстановление данных ПС Сенсор из резервной копии с внешнего носителя

Для восстановления данных ПС Сенсор из резервной копии следует:

– при отсутствии в составе технического средства, на котором установлено ПС Сенсор, CD/DVD-привода – подключить переносной CD/DVD-привод к свободному USB-разъёму технического средства;

– вставить оптический диск с резервной копией данных в CD/DVD-привод;

– нажать на клавиатуре (KVM-консоли) клавиши Ctrl+Alt+F2 и на запрос операционной системы ввести имя и пароль пользователя, обладающего привилегиями технологического пользователя «root»;

После ввода учётных данных пользователя, обладающего привилегиями технологического пользователя «root» такой пользователь получит доступ к командной строке операционной системы.

4.6.1 Восстановление файлов *.conf

Для восстановления файлов *.conf пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС указать команду:

```
# pluton guard restore config <путь к файлу резервного копирования>
```

Для выполнения команды необходимо указать путь к файлу резервного копирования.

4.6.2 Восстановление файлов *.pcap

Для восстановления файлов *.pcap пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС указать команду:

```
# pluton guard restore pcap <путь к файлу резервного копирования>
```

Для выполнения команды необходимо указать путь к файлу резервного копирования. Путь к директории, в которую происходит восстановление файлов *.pcap, указан в файле config.confd, в значении параметра:

alerts_path=/var/spool/pluton/pcap-generator/PCAPs (см. раздел 4.2.6)

4.6.3 Восстановление данных БД PostgreSQL

Для восстановления данных БД PostgreSQL пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС выполнить следующие действия:

1) Указать команду соединения с сервером PostgreSQL:

```
# psql -U pluton
```

2) В ответ на предложение ввести пароль, ввести пароль, указанный в параметре `password` в файле config.conf (см. раздел 4.5.4).

3) После получения доступа к БД PostgreSQL указать команду удаления БД:

```
# DROP DATABASE
```

4) Указать команду останова сервиса БД PostgreSQL:

```
# service postgresql stop
```

5) Указать команду восстановления данных БД PostgreSQL. Для этого указать путь к файлу резервного копирования, дату восстанавливаемой резервной копии в формате YYYYMMDD и путь к директории, в которую должно происходить восстановление:

```
# pluton guard restore postgresql <путь к файлу резервного копирования> <дата восстанавливаемой резервной копии> <путь к директории, в которую происходит восстановление>
```

Рекомендуется в качестве параметра `<путь к директории, в которую происходит восстановление>` указывать каталог `/var/lib/postgresql/9.4/main`.

Пример команды для восстановления резервной копии БД PostgreSQL из директории `/b1/postgres` с датой создания копии 22 декабря 2017:

```
# pluton guard restore postgresql /b1/postgres 20171222 /var/lib/postgresql/9.4/main
```

Примечание. После восстановления резервной копии данных БД PostgreSQL нумерация WAL-файлов продолжится с номера, актуального на момент резервного копирования, а в директории архивных логов `/var/lib/postgres/archivelog` уже могут находится файлы с такими же или большими номерами. В этом случае необходимо перенести резервные копии, хранящиеся в `/var/lib/postgres/archivelog/`, в другую директорию и затем указать команду перезапуска БД PostgreSQL.

4.6.4 Восстановление данных БД ClickHouse

Для восстановления данных БД ClickHouse используется команда:

```
# pluton guard restore clickhouse
```

Команда выполняется со следующими параметрами:

`restore_mode` – режим восстановления, один из вариантов: `all|table|all_tab_partition|table_partition;`

`all` – все таблицы,

`table` – одна конкретная таблица,

`all_tab_partition` – одна секция для всех таблиц,

`table_partition` – одна секция одной таблицы

`backup_date` – дата резервной копии, с которой требуется начать восстановление. Задаётся либо словом "last" (для восстановления последней резервной копии), либо датой в формате YYYYMMDD, где YYYY – год, MM– месяц, DD – день;

`backup_directory` – директория с сохранёнными резервными копиями;

`restore_dir` – директория, в которую восстанавливаются секционированные таблицы. Рекомендуется использовать в качестве значения параметра директорию var/lib/clickhouse/data;

`table_name` – имя восстанавливаемой таблицы (только для режимов `table` и `table_partition`);

`partition_name` – имя восстанавливаемой секции (только для режимов `all_tab_partition` и `table_partition`). Формат имени секции: YYYYMMDD, где YYYY – год, MM – номер месяца, DD – число.

4.6.4.1 Восстановление данных БД ClickHouse за период

Для восстановления данных БД ClickHouse за определённый период времени пользователю, обладающему привилегиями технологического пользователя «root», необходимо в командной строке ОС выполнить следующие действия:

1) Указать команду соединения с сервисом clickhouse-client. с указанием пароля пользователя в качестве параметра команды (пароль указан в параметре `password` в файле config.conf (см. раздел 4.5.4)):

```
# clickhouse-client --password <пароль пользователя>
```

2) Указать команду восстановления данных БД ClickHouse.

```
# pluton guard restore clickhouse
```

Пример команды:

```
# pluton guard restore clickhouse table_partition last
/b1/clickhouse /var/lib/clickhouse/data/ alert 20171201,
```

где

- `restore_mode = table_partition;`
- `backup_date = last;`
- `backup_directory = /b1/clickhouse;`
- `restore_dir = /var/lib/clickhouse/data/;`
- `table_name = alert;`
- `partition_name = 20171201.`

4.6.4.2 Восстановление данных БД ClickHouse после потери файлов данных

В случае потери всех имеющихся данных в БД ClickHouse пользователю, обладающему привилегиями технологического пользователя «root», необходимо в командной строке ОС выполнить следующие действия:

1) Указать команду соединения с сервисом clickhouse-client. с указанием пароля пользователя в качестве параметра команды (пароль указан в параметре `password` в файле `config.conf` (см. раздел 4.5.4)):

```
# clickhouse-client --password <пароль пользователя>
```

2) Указать команду удаления БД ClickHouse:

```
# DROP DATABASE
```

3) Указать команду восстановления данных БД ClickHouse:

```
# pluton guard restore clickhouse
```

Для этого указать следующие значения параметров:

- `restore_mode = table_partition` (фиксированный параметр);
- `backup_date = last` (фиксированный параметр);
- `backup_directory` (указывает пользователь);

– `restore_dir` (указывает пользователь).

5 ПРОВЕРКА ПРОГРАММЫ

Для проверки основных функций ПС Сенсор, а также корректности настройки ПС Сенсор предусмотрены операции самотестирования с получением отчётов о состоянии.

5.1 Генерация тестовых атак

Для генерации тестовых атак и записи их в БД ПС Сенсор пользователь должен указать команду:

```
# pluton-check-analyzer
```

После выполнения команды (может занять некоторое время) в командной строке отобразится отчёт о результатах добавления тестовых данных в БД ПС Сенсор, а также табличный список событий информационной безопасности, которые были получены в результате воздействия на ПС Сенсор тестовых атак.

5.2 Проверка работоспособности сервисов ПС Сенсор

Для проверки работоспособности сервисов ПС Сенсор пользователь должен указать команду:

```
# pluton-check-monitoring
```

В ходе выполнения команды происходят следующие действия:

1) команда передаёт список сервисов ПС Сенсор утилите `service`;
2) утилита в ответ передаёт состояние указанных сервисов;
3) полученные состояния сервисов отображаются в командной строке пользователя;
4) команда передаёт сервису `pluton-component-status-server` команды для запуска следующих сервисов:

- `pluton-ise-handler`;
- `pluton-ise-publisher`

5) команда передаёт утилите `service` следующие сервисы:

- `pluton-ise-handler`;
- `pluton-ise-publisher`

6) утилита в ответ передаёт состояние двух указанных сервисов;

7) полученные состояния двух указанных сервисов отображаются в командной строке пользователя;

8) команда передаёт сервису `pluton-component-status-server` команды для остановки следующих сервисов:

– `pluton-ise-handler`;

– `pluton-ise-publisher`

9) команда выводит в командную строку пользователя сообщение о результатах завершения тестирования сервисов ПС Сенсор.

5.3 Получение отчёта о состоянии компонента

Для получения отчёта о состоянии компонента пользователь должен указать команду:

```
# pluton-component-status-report
```

Дождитесь выполнения команды. После выполнения в командной строке отобразится отчёт о состоянии компонента.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД	База данных
КА	Компьютерная атака
НЖМД	Накопитель на жёстких магнитных дисках
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПК	Программный комплекс
ПО	Программное обеспечение
ПС	Программное средство
РПСА	Решающие правила сигнатурного анализа
СИБ	Событие информационной безопасности
СОА	Система обнаружения атак
СОВ	Система обнаружения вторжений
СУБД	Система управления базой данных
ТС	Технические средства
ЭВМ	Электронно-вычислительная машина
CEF	Common Event Format – формат, который применяется к данным, поступающим в SIEM-систему
MQTT	Message Queue Telemetry Transport –сетевой протокол, работающий поверх TCP/IP, применяемый для взаимодействия между устройствами (machine-to-machine)
SIEM	Security information and event management – класс ПО, который обеспечивает собор в одном месте событий, генерируемых различными системами информационной безопасности и корреляционный анализ событий в реальном времени

ПЕРЕЧЕНЬ ТЕРМИНОВ

Администратор безопасности СОВ	Уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию СОВ
Компонент	Сенсор – компонент регистрации событий. СУС – компонент анализа событий и управления сенсорами
Контролируемая система	Сегмент вычислительной сети, захват и анализ трафика которой выполняет сенсор
Корневой СУС	СУС, не имеющий вышестоящего СУС
Политика безопасности ОО	Совокупность правил, регулирующих управление, защиту и распределение информационных ресурсов, контролируемых ОО
Протокол	Стандарт передачи данных
Профиль хоста	Обобщённая информация о хосте, включающая в себя: – тип, имя, адрес, статус, важность, контролируемую систему; – показатели сетевой активности и статистику сетевого трафика; – установленные программные продукты и связанные с ними уязвимости; – перечень пользователей; – историю изменений.
Сенсор	Программный или программно-технический компонент СОВ, предназначенный для сбора и первичного анализа данных о событиях контролируемой системы
Сигнатура	Характерные признаки вторжения (атаки), используемые для его (её) обнаружения

Система обнаружения вторжения	Программное или программно-техническое средство, реализующие функции автоматизированного обнаружения (блокирования) действий в информационной системе, направленных на преднамеренный доступ к информации, специальные воздействия на информацию (носители информации) в целях её добывания, уничтожения, искажения и блокирования доступа к ней
События СОА	Дополнительные данные, которые предоставляет СОА Bro в результате обработки сетевого трафика, позволяющие предоставить расширенную информацию для анализа СИБ. События СОА содержат данные о сетевых соединениях, сеансах протоколов прикладного уровня, уведомлениях о потенциально опасных событиях
Хост	Компьютер или сервер, подключённый к сегменту вычислительной сети контролируемой системы
Afick	Утилита аудита целостности, при котором осуществляется выявление несанкционированных изменений объектов ПК СОВ (ПО, конфигурационных файлов, базы решающих правил сигнатурного анализа, чёрных списков, программных сценариев эвристического анализа)
Ansible	Программная система управления конфигурациями, которая использует декларативный язык разметки для описания конфигураций. Применяется для автоматизации настройки и развёртывания программного обеспечения
Bro	Сетевая система обнаружения вторжения. Является свободным программным обеспечением
C++	Компилируемый, статически типизированный язык программирования общего назначения

ESMA Script	Встраиваемый расширяемый язык программирования, не имеющий средств ввода-вывода, используемый в качестве основы для построения других скриптовых языков. Одним из расширений языка ESMA Script является JavaScript
GeoIP	База данных географического местоположения IP-адресов
HTTP-запрос	HTTP (HyperText Transfer Protocol) — протокол прикладного уровня передачи данных по технологии «клиент-сервер». Клиент инициирует соединение и посылает запрос серверу
HTTPS	HTTPS (HyperText Transfer Protocol Secure) – расширение протокола HTTP для поддержки шифрования в целях повышения безопасности
IP-адрес	Уникальный сетевой адрес хоста в компьютерной сети, построенной на основе стека протоколов TCP/IP
JavaScript	Язык сценариев. Применяется для разработки графического пользовательского интерфейса
MD5-хеш	«Отпечаток» сообщения произвольной длины, созданный с помощью 128-битного алгоритма хеширования. Применяется для проверки целостности информации и хранения хешей паролей
Mosquitto MQTT broker	Брокер сообщений, который реализует протокол MQTT версии и обеспечивает выполнения обмена сообщениями с использованием модели публикации/подписки
p0f	Утилита пассивного определения версии операционной системы на удалённом хосте с использованием метода сигнатурного анализа
Python	Высокоуровневый язык программирования общего назначения
Suricata	Сетевая система обнаружения и предотвращения вторжения. Является свободным программным обеспечением

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	Номер документа	Входящий номер сопроводительного документа	Подпись	Дата
	изме-ненных	заменен-ных	новых	аннулиро-ванных					