УТВЕРЖДЕН
ДБАР.62.01.12.000.182-01 32-ЛУ

ПС «СУС-ПЛУТОН-М1.0»

Руководство системного программиста

ДБАР.62.01.12.000.182-01 32

Листов 47

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

Москва
2018

АННОТАЦИЯ

Документ является руководством системного программиста Программного средства «СУС-Плутон-М1.0» ДБАР.62.01.12.000.182-01 (далее – ПС «СУС-Плутон-М1.0», ПС СУС).

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

СОДЕРЖАНИЕ

1 ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1 Обозначение и наименование программы

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

Обозначение программы: ДБАР.62.01.12.000.182-01.

1.2 Языки программирования, на которых написана программа

ПС СУС написано на языках программирования C++ версии 11, Python версии 3.5.3, ECMA Script 5.

2 ФУНКЦИОНАЛЬНОЕ НАЗНАЧЕНИЕ

2.1 Назначение программы

ПС СУС предназначено для:

– выполнения анализа данных о компьютерных атаках (КА) и аномалиях в действиях хостов контролируемой системы;

– поддержка иерархической модели подчинения ПС СУС и ПС Сенсор и управление сенсорами.

2.2 Область применения

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

2.3 Решаемые задачи и функции ПС СУС

ПС СУС выполняет следующие функции:

2.3.1 Поддержка иерархической модели подчинения компонентов ПС СУС и ПС Сенсор.

2.3.2 Предоставление пользователю возможности анализировать данные: как поступающие с подчинённых компонентов, так и генерируемые самим ПС СУС с помощью графического пользовательского интерфейса.

2.3.3 Приём от ПС Сенсор, хранение и передача на вышестоящий ПС СУС:

– СИБ;

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

– параметров функционирования своих технических и программных средств подчинённых компонентов;

– данных аудита безопасности – своих и подчинённых компонентов;

– копий трафика;

– данных о распределённом программном обеспечении узлов контролируемых систем.

2.3.4 Накопление информации о профилях хостов контролируемых систем и передача их на ПС Сенсор.

2.3.5 Регистрация событий аудита безопасности.

2.3.6 Предоставление пользователям возможности настроить ПС СУС и подчинённые компоненты и изменить параметры их конфигурации с помощью командной среды ОС и графического пользовательского интерфейса.

2.3.7 Выполнение команд, поступающих с вышестоящего ПС СУС.

2.3.8 Регулирование доступа пользователей к функциям ПС СУС в соответствии с настройками ролевой модели доступа. В поставке ПК СОВ предусмотрены:

– роль «Администратор безопасности СОВ», которая даёт права доступа к функциям настройки ПС СУС и подчинённых компонентов и изменению параметров конфигураций с помощью командной среды ОС и графического пользовательского интерфейса;

– роль «Оператор визуального контроля СОВ», которая даёт права доступа к функциям:

а) анализа СИБ;

б) анализа собственных событий аудита безопасности и событий аудита безопасности подчинённых компонентов;

в) анализа собственного состояния и состояний подчинённых компонентов;

г) настройки решающих правил сигнатурного анализа.

2.3.9 Идентификация, аутентификация и авторизация пользователей выполняется через механизмы 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.

2.3.10 Взаимодействие программных средств ПК СОВ по защищённому каналу связи. Для исключения несанкционированного доступа во время установки соединения удалённый компонент идентифицируется с помощью проверки цифрового сертификата.

2.3.11 Взаимодействие с внешней системой обновлений.

2.3.12 Обновление ПС СУС в части базы решающих правил сигнатурного анализа, чёрных списков, справочников, базы уязвимости, базы GeoIP, данных картографии, программного обеспечения и передача обновлений на подчинённые компоненты.

2.3.13 Представление данных СИБ в формате CEF (Common Event Format) для передачи во внешние SIEM-системы.

2.4 Условия применения

2.4.1 Требования к техническим средствам

2.4.1.1 ПС СУС функционирует на ЭВМ с характеристиками производительности не ниже, чем ЭВМ архитектуры x86-64, оснащённой сетевыми интерфейсами, поддерживающими скорость передачи данных до 1 Гбит/с.

2.4.1.2 Для установки и функционирования ПС СУС требуется свободное пространство на жёстких магнитных дисках, объединённых в RAID-массив объёмом не менее 24 Тбайт.

2.4.2 Требования к программным средствам

2.4.2.1 ПС СУС 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 СУС рекомендуется использовать внешние хранилища.

2.4.3 Требования к организационной среде эксплуатации

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

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

2.4.3.3 Взаимодействие ПС СУС с подчинёнными компонентами должно выполняться по защищённым каналам связи.

2.4.3.4 Для идентификации и аутентификации ПС СУС 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 СУС, 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 СУС

4.1.1 Среда установки

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

- настройка сетевого взаимодействия компонентов;
- установка системного времени;
- монтирование внешних носителей;
- установка ПС СУС на ТС;
- перезагрузка системы;
- создание пользователей и настройка их учётных записей;
- регистрация компонентов в ПК СОВ;
- настройка параметров протокола MQTT;
- настройка параметров config.conf;
- настройка параметров сервиса pluton-component-status-server
- настройка параметров диагностики состояния сервисов;
- настройка параметров соединения ПС СУС с внешними SIEM-системами;
- настройка параметров соединения ПС СУС с почтовым сервером;
- настройка параметров соединения ПС СУС с севером обновлений;
- установка и замена на ПС СУС цифрового сертификата;
- удаление и перезагрузка ПС СУС.

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.

Установка ПС СУС развёртывается на технических средствах (далее – ТС) с установленной операционной системой 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: команду:

```
# uname –vr
```

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

После выполнения команды пользователю 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 СУС

Перед установкой необходимо выполнить следующие подготовительные операции с техническим средством, на которое устанавливается ПС СУС:

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 СУС – 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 СУС не переключён на bypass-порт.

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

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

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

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

а) указать 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 указать следующую 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 для настройки протокола HTTPS, необходимо настроить системное время. Чтобы узнать точное время с поправкой на часовой пояс, необходимо указать команду:

```
# date
```

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

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

4) 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 СУС 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, выполнив команду:

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

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

– тип устанавливаемого компонента -- scs;

– географические координаты ПС СУС 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 scs --ln <долгота ПС СУС> --lt <широта ПС СУС> --ntp <IP-адрес сервера синхронизации времени> --prt <путь к точке монтирования оптического диска со средой функционирования ПС СУС>
```

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

По завершении установки необходимо указать команду перезагрузки системы:

```
# sudo init 6
```

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

После перезагрузки следует:

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

2) Ввести рабочее имя и пароль технологического пользователя (заводская установка – «admin»/ «fL9B}3&wq»).

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

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

```
# passwd admin
```

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

5) Создать при необходимости дополнительных технологических пользователей – указать команду:

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

6) Настроить программные средства согласно разделу 4.2.

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

4.2 Настройка ПС СУС

Действия по настройке ПС СУС выполняются в командной среде ОС. Процедура входа в командную среду описана в разделе 4.4.1. Настройку ПС СУС 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 компонента

Для регистрации компонента необходимо выполнить следующие действия:

1) На регистрируемом компоненте указать команду:

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

где

`host` – адрес вышестоящего СУС, в котором регистрируется СУС;

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 SCS-1
```

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

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

4) Подтвердить регистрацию компонента – нажать кнопку  ;

5) После успешной регистрации статус регистрируемого компонента должен измениться с «В процессе» на «Подтверждено», в соответствии с рисунком 1.

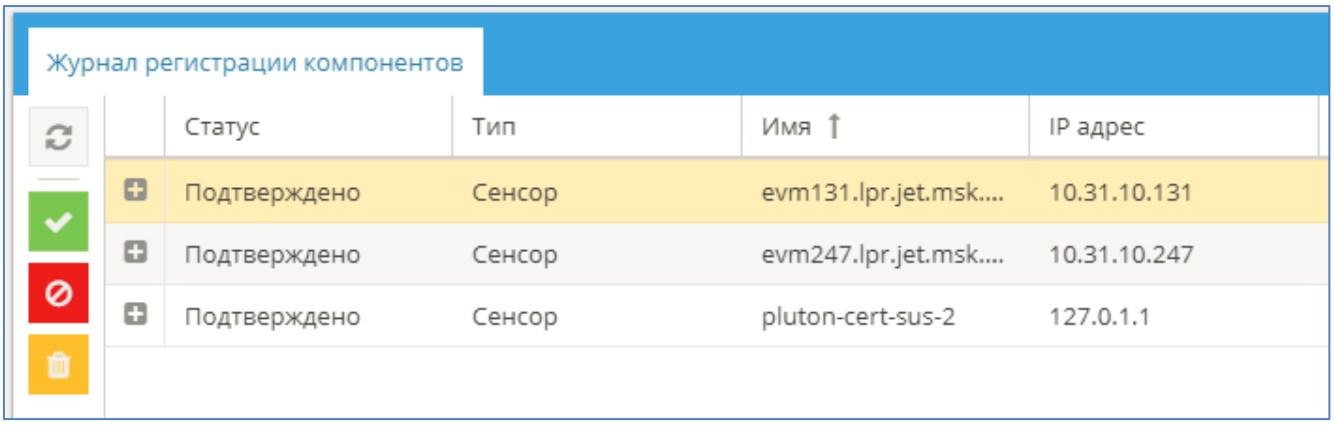

Рисунок 1 – Регистрация компонентов

Для проверки статуса регистрируемого сенсора необходимо указать команду:

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

При успешной регистрации СУС в командной строке пользователю отобразится сообщение:

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

При отклонении вышестоящим СУС заявки на регистрацию СУС 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.

Интеграция СУС с вышестоящим СУС описана в разделе 4.2.1

4.2.3 Настройка параметров соединения с SIEM

Настройка с SIEM выполняется в файле /etc/rsyslog.conf.

Пример настройки:

```
LOCAL0.notice   @10.31.10.105
LOCAL0.notice   /var/log/pluton/pluton-cef.log
```

Максимальная длинна сообщений задаётся в конфигурационном файле /etc/pluton/config.conf, в блоке [SIEM]:

```
alert_max_size=960
```

4.2.4 Настройка параметров соединения с почтовым сервером

Для отправки диагностических сообщений пользователю используется средства электронной почты. Рассылка запускается по факту появлений СИБ в ПС Сенсор и событий аудита безопасности ПС СУС.

Параметры подключения к почтовому серверу задаются в конфигурационном файле /etc/pluton/config.conf, в блоке [NOTIFICATION]. Список возможных параметров:

– шаблоны для почтовых уведомлений:

а) alert_caption_template = /etc/pluton/alert-notification/caption_template.txt – шаблон заголовка уведомления о появлении СИБ;

б) alert_content_template = /etc/pluton/alert-notification/content_template.txt – шаблон тела уведомления о появлении СИБ;

в) alert_attr_table = /etc/pluton/alert-notification/attr_table.json – матрица транслирования имён полей данных в имена атрибутов для СИБ;

г) audit_caption_template = /etc/pluton/audit-notification/caption_template.txt – шаблон заголовка уведомления о появлении событий аудита безопасности;

д) audit_content_template = /etc/pluton/audit-notification/content_template.txt – шаблон тела уведомления о появлении событий аудита безопасности;

е) audit_attr_table = /etc/pluton/audit-notification/attr_table.json – матрица транслирования имён полей данных в имена атрибутов для событий аудита безопасности.

– минимальное пороговое значение критичности, при котором формируется уведомление о появлении СИБ и событий аудита безопасности:

```
notify_severity_min = 0
```

– электронный адрес отправителя уведомления :

```
notify_smtp_from = noreply@service.jet.msk.su
```

– адрес сервера исходящей электронной почты:

```
notify_smtp_server = lab-dns.service.jet.msk.su
```

– порт сервера исходящей электронной почты :

```
notify_smtp_port = 25
```

– учётная запись сервера исходящей электронной почты

```
notify_smtp_login =
```

– пароль учётной записи сервера исходящей электронной почты

```
notify_smtp_password =
```

– параметр защиты соединения:

```
notify_smtp_ssl = False
```

4.2.5 Настройка параметров соединения с сервером обновлений

С сервером обновлений в ПК СОВ взаимодействует только компонент, являющийся корневым СУС. Все остальные компоненты запрашивают обновления через вышестоящие компоненты.

Взаимодействие сервера обновлений с корневым СУС должно осуществляться по защищённому протоколу HTTPS. Корневой СУС проверяет достоверность сервера обновлений на основании SSL-сертификата сервера, который предоставляется Потребителем заранее для интеграции этого сертификата в ПК СОВ.

Параметры подключения к серверу обновлений задаются в конфигурационном файле /etc/pluton/config.conf, в блоке [UPDATE_SERVER]. Список возможных параметров:

– адрес сервера обновлений:

```
host = 10.31.10.126
```

– имя профиля компонента на сервере обновлений:

```
updates_system_name=Pluton2Sens
```

путь к хранилищу обновлений, загруженных на компонент:

```
updates_storage_path = /var/spool/pluton/pluton-
updater/archives
```

– типы обновлений, находящиеся внутри загружаемого пакета с обновлениями:

archive_folder_by_type = SURICATA_UPDATE:suricata GEOIP_UPDATE:geoip BRO_UPDATE:bro CVE_UPDATE:cve SOFTWARE_UPDATE:software BL_UPDATE:bl, где

а) SURICATA_UPDATE:suricata – обновление правил Suricata;

б) GEOIP_UPDATE:geoip – обновление GeoIP;

в) BRO_UPDATE:bro – обновление правил Bro;

г) CVE_UPDATE:cve – обновление базы уязвимостей;

д) SOFTWARE_UPDATE:software – обновление ПО;

е) BL_UPDATE:bl – обновление черных списков.

– ключ для доступа к API сервера обновлений (предоставляется пользователю от сервера обновлений по электронной почте):

apikey=2

4.2.6 Настройка параметров config.conf

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

Таблица 1 – Конфигурационные параметры ПС СУС

Раздел	Параметр	Описание
[COMMON]	broker_reconnect_interval=60000	Настройка интервала повторного подключения к MQTT broker
[COMPONENT]	id = 38c97566-06c9-4b60-9599-ea7ca28dd0ab	Числовой идентификатор сенсора; должен быть уникальным в пределах множества всех сенсоров, функционирующих в иерархической структуре ПК СОВ «Плутон-М1.0»
	type = SCS	Тип компонента (для СУС всегда SCS)

Раздел	Параметр	Описание
	hostname = 127.0.0.1	Имя хоста, который подключается к БД PostgreSQL
[DATABASE]	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 = BnzaoxIC	Пароль пользователя БД PostgreSQL
	reconnect_timeout = 5000	Настройка тайм-аута (в мс) на повторное соединение с сервисом БД PostgreSQL после обрыва предыдущего соединения
	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
[CLICKHOUSE]	name = default	Название БД ClickHouse
	user = default	Имя пользователя в БД ClickHouse
	password = kvsnDkri	Пароль пользователя БД ClickHouse

Раздел	Параметр	Описание
	clickhouse_save_interval=1000	Настройка интервала между запросами к сервису БД Clickhouse. Рекомендуется использовать значение больше чем 10 мс, чтобы не превышать 100 запросов в секунду
[PKI]	cafile = /etc/pluton/tls/Pluton-CA.crt certfile = /etc/pluton/tls/dvm166.lpr.jet.msk.su.crt keyfile = /etc/pluton/tls/dvm166.lpr.jet.msk.su.pem	Цепочка SSL-сертификатов
[SERVER]	activation_code_expiring_period = 2	Временной период окончания действия кода регистрации ПС СУС (в днях)
[UPDATES]	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
	CPU_thresholds = 70 95	Пороговые значения для показателя «Процент использования ЦПУ»

Раздел	Параметр	Описание
	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
[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

Раздел	Параметр	Описание
	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
	notify_smtp_port = 25	Порт сервера исходящей электронной почты
	notify_smtp_login =	Учётная запись сервера исходящей электронной почты;. Необязательный параметр, при необходимости устанавливается пользователем

Раздел	Параметр	Описание
	notify_smtp_password =	Пароль учётной записи сервера исходящей электронной почты. Необязательный параметр, при необходимости устанавливается пользователем
	notify_smtp_ssl = False	Параметр защиты соединения
[SIEM]	alert_max_size=960	Максимальный размер сообщений, отправляемых во внешние SIEM-системы
[SURICATA]	rules_extension=.rules	Расширение файлов с сигнатурами Suricata
[BRO]	rules_extension=.sig	Расширение файлов с сигнатурами Bro
[GEOIP]	install_path=/usr/share/GeoIP city=GeoIPCity.dat locations_csv=GeoLiteCity-Location.csv blocks_csv=GeoLiteCity-Blocks.csv	Пути для GeoIP
[UPDATE_SERVER]	host = 10.31.10.126	IP-адрес хоста, подключаемого к серверу обновлений
	version_ok_message = Версия системы актуальна	Текст сообщения о соответствии версии ПС
	scs_system_name = Pluton2SUS	Название профиля корневого СУС на сервере обновления
	updates_storage_path = /var/spool/pluton/pluton-updater/archives	Путь 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)
	update_url = /agent/update.json report_url = /agent/report.json create_url = /agent/create.json	URL файлов на сервере обновления, содержащих информацию об обновлениях
	cafile = /etc/pluton/pluton-updater/update-server-CA.crt auth = YWdlbnQ6YWdlbnQ=	Цепочка SSL-сертификатов для сервера обновлений
[PCAP]	alerts_path=/var/spool/pluton/pcap-generator/PCAPs/	Путь к хранилищу файлов с расширением *.pcap
[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)

Раздел	Параметр	Описание
	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
	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
[COMPONENT_STATUS]	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)

Раздел	Параметр	Описание
	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

4.2.7 Описание УЦ сертификата. Установка и замена сертификата

SSL-сертификаты генерируются при установке компонента. Расположение сертификатов указано в файле/etc/pluton/config.conf, в блоке [PKI]:

```
cafile = /etc/pluton/tls/Pluton-CA.crt
certfile = /etc/pluton/tls/dvm167.lpr.jet.msk.su.crt
keyfile = /etc/pluton/tls/dvm167.lpr.jet.msk.su.pem
```

ВНИМАНИЕ! Не стоит менять эти настройки, а также пытаться прописать в указанный файл другие сертификаты. Эти настройки не наследуются сторонними компонентами, использующими ssl/tls. Если требуется заменить сертификаты, необходимо заменить имеющиеся файлы сертификатов новыми сертификатами.

4.2.8 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, необходимо через утилиту useradd указать команду создания пользователя:

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

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

4.2.9 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 СУС может находится в одном из следующих функциональных состояний:

– «Инициализация»;

– «Неактивный»;

– «Обнаружение»;

– «Скомпрометирован».

В таблице Таблица 2 установлено соответствие между состоянием компонента 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 данный сервис работает некорректно.

Таблица 2 – Статусы системных сервисов ПС СУС

Статус компонента/ Системный сервис	**Инициализация**	**Неактивный**	**Обнаружение**	**Скомпрометирован**
Сервисы Python				
pluton-audit-server	Остановлен	Работает	Работает	Работает
pluton-homenet-control	Остановлен	Работает	Работает	Остановлен
pluton-job-runner	Остановлен	Работает	Работает	Работает
pluton-notification-server	Остановлен	Остановлен	Работает	Работает
pluton-registration-server	Остановлен	Остановлен	Работает	Остановлен
pluton-updater-server	Остановлен	Работает	Работает	Остановлен
pluton-transport-server	Остановлен	Работает	Работает	Работает

Статус компонента/ Системный сервис	**Инициализация**	**Неактивный**	**Обнаружение**	**Скомпрометирован**
pluton-event-logger-watchdog	Остановлен	Остановлен	Работает	Работает
pluton-query-server	Остановлен	Работает	Работает	Работает
pluton-profile-handler	Остановлен	Остановлен	Работает	Работает
pluton-component-status	Остановлен	Работает	Работает	Работает
pluton-health-monitor	Остановлен	Работает	Работает	Работает
Сервисы C++				
pluton-ise-handler	Остановлен	Остановлен	Работает	Работает
Сервисы ПС СУС				
MQTT	Остановлен	Работает	Работает	Работает
Сервис предотвращения переполнения дискового пространства оперативных данных	Остановлен	Работает	Работает	Работает
Zabbix	Остановлен	Работает	Работает	Работает
PostgreSQL	Остановлен	Работает	Работает	Работает
ClickHouse	Остановлен	Работает	Работает	Работает
SNMPD	Остановлен	Работает	Работает	Работает

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

4.2.10 Проверка результатов установки и запуска ПС СУС

После проведения подготовительных операций на ТС для установки ПС СУС и выполнения действий по установке ПС СУС (см. раздел 4.1), в командной строке отобразится сообщение с выводом результатов выполнения набора сценариев по установке ПС СУС, которые содержатся в файле playbook системы Ansible. Результат содержит следующие параметры:

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

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

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

В случае успешной установки ПС СУС, пользователю в командной строке отобразится сообщение, показанное на рисунке 2:

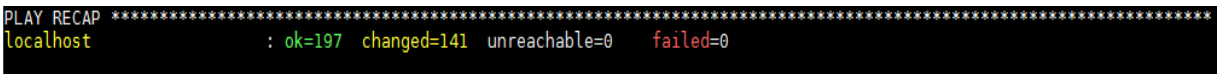

Рисунок 2 –Успешное завершение установки ПС СУС

В случае возникновения ошибки при установке ПС СУС, пользователю в командной строке отобразится сообщение, показанное на рисунке 3:

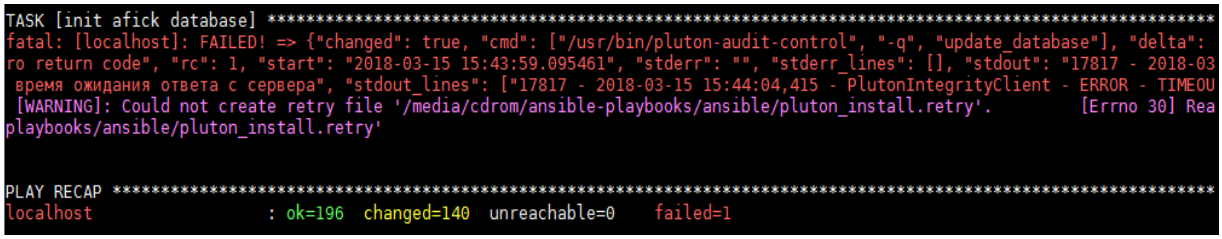

Рисунок 3 – Завершение установки ПС СУС с ошибкой

4.2.11 Удаление и перезагрузка ПС СУС

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

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

Дополнительных сервисов по удалению и перезагрузке ПС СУС не предусмотрено.

4.3 Парольная политика

Пароли учетных записей пользователей должны удовлетворять следующим требованиям к сложности:

а) срок действия пароля составляет не более 90 дней;

б) длина пароля не менее 8 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 1 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 СУС

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

4.4.1 Вход в командную среду ПС СУС

Чтобы войти в командную среду ПС СУС 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 СУС 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 СУС>,
```

где в качестве параметра `<ip-адрес СУС>` задать ip-адрес СУС. 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 откорректировать набранную команду. 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 клавиш Shift+PageUp и Shift+PageDown.

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

Для завершения сеанса работы в командной среде ПС СУС 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 двумя способами:

– периодически через заданный интервал времени (настраивается пользователем, обладающим привилегиями технологического пользователя «root»);

– по команде оператора ПК 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>
```

При выполнении 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. Данная 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>
```

При выполнении 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. Данная 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 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 компакт-диск с резервной копией настроек в CD/DVD-привод;

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

– после ввода учётных данных привилегированного технологического пользователя 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. п 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 производится восстановление секционированных таблиц. 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 пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС:

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. п 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 пользователь, обладающий привилегиями технологического пользователя «root», должен в командной строке ОС выполнить следующие действия:

3) 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>
```

4) Указать команду удаления БД ClickHouse:

```
# DROP DATABASE
```

5) 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).

Необходимо сохранить файл структуры данной таблицы из каталога /var/lib/clickhouse/metadata/default/ и удалить файл таблицы из каталога /var/lib/clickhouse/metadata/default.

Таким образом для таблицы alert_transfer_status необходимо скопировать файл alert_transfer_status.sql в другую директорию, например, /var/tmp, для этого указать команду `cp`

Затем удалить файл из исходного каталога, указать команду `rm`.

6) Запустить БД Clickhouse, если она не была запущена (в случае п. 2)
7) Запустить утилиту восстановления из резервной копии.

5 ПРОВЕРКА ПРОГРАММЫ

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

5.1 Генерация тестовых атак

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

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

Дождитесь выполнения команды. После выполнения в командной строке отобразится отчёт о результатах добавления тестовых атак в MQTT broker, а также табличный список событий информационной безопасности, которые были получены в результате воздействия на ПС СУС тестовых атак.

5.2 Проверка работоспособности сервисов ПС СУС

Для проверки работоспособности сервисов ПС СУС пользователь должен указать команду:

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

В ходе выполнения команды происходят следующие действия:

1) команда передаёт список сервисов ПС СУС 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 СУС.

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
СИБ	Событие информационной безопасности
СОА	Система обнаружения атак
СОВ	Система обнаружения вторжений
СУБД	Система управления базой данных
ТС	Технические средства
УЦ	Удостоверяющий центр
ЦПУ	Центральное процессорное устройство
ЭВМ	Электронно-вычислительная машина
CEF	Common Event Format – формат данных, 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 сбор 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
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)
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
Python	Высокоуровневый язык программирования общего назначения

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (стр.) в документе	Номер документа	Входящий номер сопроводительного документа	Подпись	Дата
	измененных	замененных	новых	аннулированных					