

Содержание

| | |
|--|---|
| 1 Введение | 2 |
| 2 Управление | 3 |
| 2.1 Изменение адреса назначения syslog-сообщений | 3 |
| 2.2 Загрузка и обновление шаблонов | 3 |
| 2.3 Передача сообщений в вышестоящую систему мониторинга | 4 |
| 2.3.1 Формат нормализованных сообщений | 4 |
| 2.3.2 Формат сообщений о подтверждении или закрытии нормализованных сообщений..... | 4 |
| 3 Конфигурирование ПК | 5 |
| 3.1.1 Конфигурирование ds-logger | 5 |
| 3.1.2 Конфигурирование ds-click | 7 |

1 Введение

Программное обеспечение комплекса «Диагностическая станция ПТК АСУТП» представляет собой решение, предназначенное для формирования и передачи нормализованной информации об инцидентах информационной безопасности или иной информации, не содержащей сведений, составляющих государственную тайну, соответствующих требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2018), в вышестоящие системы мониторинга.

Программное обеспечение «Диагностическая станция ПТК АСУТП» реализует функцию передачи нормализованных журнальных сообщений из ПАК «ИК.ДС», а также осуществляет установку шаблонов в формате XML из интерфейса командной строки, что позволяет эффективнее интегрировать информацию в вышестоящие системы мониторинга.

Программное обеспечение состоит из:

- ds-logger: Программа, которая передает журнальные сообщения из ПАК «ИК.ДС» в формате Syslog RFC3164 или RFC5424.
- ds-click: Программа, которая выполняет административные задачи обслуживания ПАК «ИК.ДС» через командный интерфейс.

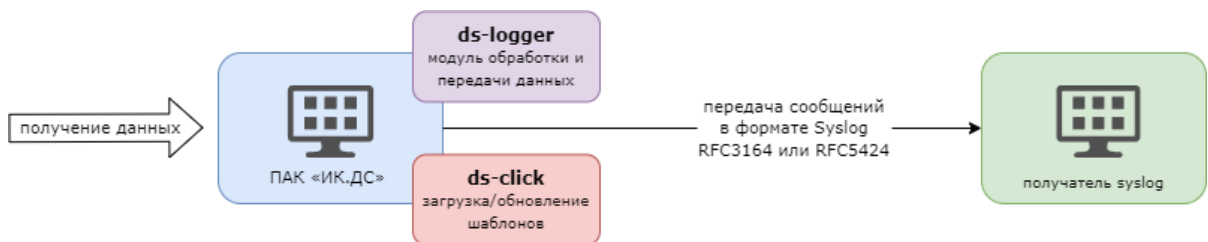


Рисунок 1 – Структура взаимодействия компонентов

2 Управление

2.1 Изменение адреса назначения syslog-сообщений

Адрес назначения syslog-сервера, для передачи syslog сообщений, указан как символьное имя syslog-dest в файле /etc/hosts. Символьное имя **не подлежит изменению**, при необходимости указания IP-адреса следует изменять только его.

Пример изменения адреса назначения представлен на рисунке 2.

```
127.0.0.1      localhost
127.0.1.1     ds-incont
10.39.99.51   syslog-dest
# The following lines are desirable for IPv6 capable hosts
::1          localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters
```

Рисунок 2 – Пример изменения адреса назначения

2.2 Загрузка и обновление шаблонов

Директория с шаблонами, которые предназначены для загрузки, указывается в конфигурационном файле appsetting.json в параметре template_upd_dir, файл расположен в директории с ds-click - /opt/ic-ds/ds-click/. Используемые параметры описаны в таблице 2.

Для загрузки шаблонов следует перейти в директорию, в которой расположен ds-click и запустить его с помощью команды:

```
sudo ./ds-click
```

Далее шаблоны будут загружены и на экране появится следующая информация (см. рисунок 3), в зависимости от выбранного параметра log_level:

```
[icadmin@ds-incont ds-click]$ sudo ./ds-click
[sudo] password for icadmin:
[2024-07-15 10:56:52.580640 +02:00] INFO [src/main.rs:44] Версия: 0.1.0
[2024-07-15 10:56:53.204154 +02:00] INFO [src/main.rs:52] Открыта API сессия, id: af59b206beabf485a9a04f517ba46e30
[2024-07-15 10:56:53.204225 +02:00] INFO [src/main.rs:54] Директория /opt/ic-ds/TemplatesUpdate/ формат xml
[2024-07-15 10:56:53.755481 +02:00] INFO [src/main.rs:75] Шаблон /opt/ic-ds/TemplatesUpdate/_MOXA_PT-7828.xml успешно импортирован
[2024-07-15 10:56:54.120802 +02:00] INFO [src/main.rs:75] Шаблон /opt/ic-ds/TemplatesUpdate/_SNMPv2 Common.xml успешно импортирован
[2024-07-15 10:56:54.280044 +02:00] INFO [src/main.rs:95] Закрыта API сессия, id: af59b206beabf485a9a04f517ba46e30
```

Рисунок 3 – Результат работы ds-click

Описание информации, при загрузке шаблонов, при выбранном параметре log_level – **info**:

- *Версия* – версия ds-click;
- *Открыта API сессия, id: <id-сессии>* – открытие API сессии;
- *Директория <директория> формат <формат>* – указывает директорию, из которой происходит загрузка шаблонов и формат шаблонов. Директория и формат указываются в файле конфигурации appsetting.json;
- *Шаблон <путь до директории, из которой загружается шаблон/шаблон> успешно импортирован* – отображает шаблон, который был загружен и статус загрузки;
- *Закрыта API сессия, id: <id-сессии>* – закрытие API сессии.

В случае успешной загрузки шаблонов они будут доступны в меню ПАК «ИК.ДС» «Настройка» – «Шаблоны» (см. рисунок 4).

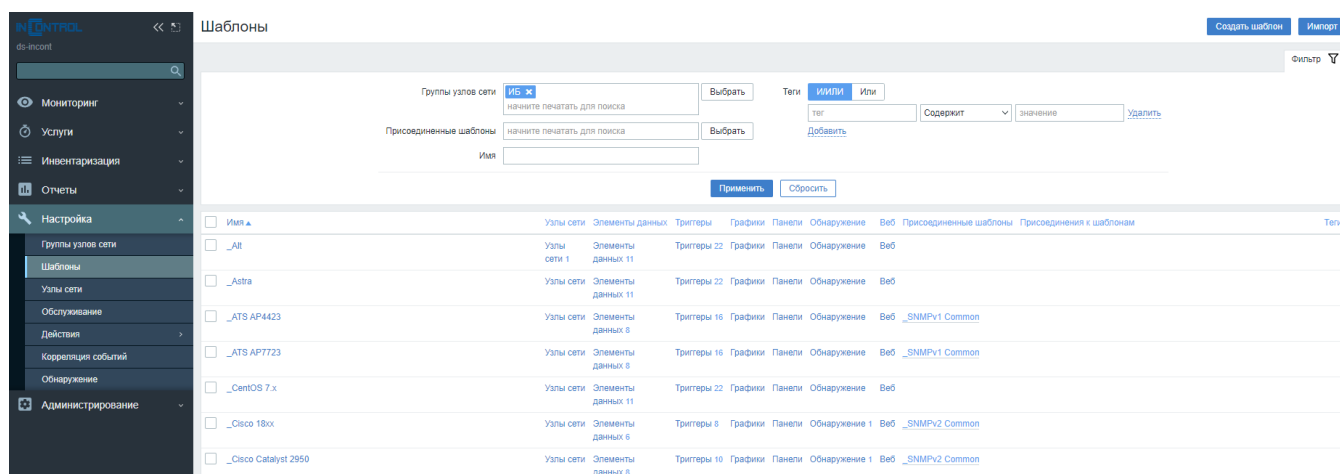


Рисунок 4 – Загруженные шаблоны

2.3 Передача сообщений в вышестоящую систему мониторинга

2.3.1 Формат нормализованных сообщений

{ALERT.SENDTO} – ip-адрес удаленного сервера syslog-dest;

{ALERT.SUBJECT} – глобальный тег ZBX;

{ALERT.MESSAGE} – тело сообщения следующего формата:

ID:{EVENT.ID}; – уникальный ID события;

{EVENT.TAGS}; – теги сигнализации;

Time:{EVENT.DATE}{EVENT.TIME}; – метка времени возникновения события в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС;

IP:{HOST.IP}; – ip-адрес узла, на котором возникла сигнализация;

Host:{HOST.NAME}; – символьное имя узла, на котором возникло событие;

Problem:{EVENT.NAME}; – событие (имя проблемы);

Severity:{TRIGGER.SEVERITY}; – важность события.

2.3.2 Формат сообщений о подтверждении или закрытии нормализованных сообщений

{ALERT.SENDTO} – ip-адрес удаленного сервера syslog-dest;

{ALERT.SUBJECT} – глобальный тег ZBX;

{ALERT.MESSAGE} – тело сообщения следующего формата:

ID:{EVENT.ID}; – уникальный ID события (совпадает с EVENT.ID события активной сигнализации);

ACK:{EVENT.ACK.STATUS}; – бинарный статус подтверждения события; (Подтверждено\ Не подтверждено)

STATUS:{EVENT.STATUS}; – бинарный статус состояния события (Активно\Решено).

3 Конфигурирование ПК

3.1.1 Конфигурирование ds-logger

Описание конфигурационного файла appSetting.json представлено в таблице 1.

Таблица 1 – Описание файла appSetting.json

| Параметр | Описание параметра | Значение | Описание возможного значения |
|------------|--|--------------|--|
| rfc | Определение формата сообщений syslog | RFC5424 | Использует структурированный формат сообщения, состоящий из ключевых слов и значений, согласно RFC5424 |
| | | RFC3164 | Использует неструктурированный формат сообщения, согласно RFC3164 |
| facility | Значение facility в конфигурации syslog указывает на источник сообщения журнала. | LOG_KERN | Ядро системы |
| | | LOG_USER | Пользовательские процессы |
| | | LOG_MAIL | Сообщения, связанные с системой электронной почты |
| | | LOG_DAEMON | Сообщения от фоновых процессов |
| | | LOG_AUTH | Сообщения авторизации |
| | | LOG_SYSLOG | Сообщения о внутренних событиях службы syslog |
| | | LOG_LPR | Сообщения, связанные с системой печати |
| | | LOG_NEWS | Сообщения, связанные с новостными сервисами |
| | | LOG_UUCP | Сообщения, связанные с системой UUCP (Unix-to-Unix Copy) |
| | | LOG_CRON | Задания cron |
| | | LOG_AUTHPRIV | Частные сообщения авторизации |
| | | LOG_FTP | Сообщения, связанные с сервером FTP |
| | | LOG_LOCAL0 | Пользовательские значения |
| | | LOG_LOCAL1 | |
| | | LOG_LOCAL2 | |
| LOG_LOCAL3 | | | |
| LOG_LOCAL4 | | | |
| LOG_LOCAL5 | | | |
| LOG_LOCAL6 | | | |
| LOG_LOCAL7 | | | |

| Параметр | Описание параметра | Значение | Описание возможного значения |
|-----------------|--|-------------|------------------------------|
| level | Значение <code>level</code> в конфигурации <code>syslog</code> | LOG_EMERG | Критическая ошибка |
| | | LOG_ALERT | Серьезная ошибка |
| | | LOG_CRIT | Критическое состояние |
| | | LOG_ERR | Ошибка |
| | | LOG_WARNING | Предупреждение |
| | | LOG_NOTICE | Уведомление |
| | | LOG_INFO | Информационное сообщение |
| | | LOG_DEBUG | Отладочное сообщение |
| socket | Тип сокета в конфигурации <code>syslog</code> | UNIX | Локальный сокет |
| | | UDP | UDP протокол |
| | | TCP | TCP протокол |
| port | Определяет номер порта, который будет использоваться для отправки сообщений журнала. | 514 | - |
| udp_bind | Используется только при использовании сокета UDP. Определяет локальный IP-адрес и порт, на котором программа будет ожидать запросы на отправки сообщений журнала. "0.0.0.0:0" означает, что программа будет слушать на всех доступных интерфейсах и любом свободном порте. | 0.0.0.0:0 | - |

3.1.2 Конфигурирование ds-click

Описание конфигурационного файла appsetting.json представлено в таблице 2, файл расположен в папке /opt/ic-ds/ds-click/.

Таблица 2 – Описание конфигурационного файла appsetting.json

| Параметр | Описание параметра | Значение по умолчанию |
|------------------------------|---|-----------------------|
| logger | Объект с настройками логирования | - |
| log_level | Уровень логирования <i>Возможные значения:</i> info – информационное сообщение; debug – отладочное сообщение; warning – предупреждение; error – ошибка | info |
| path | Путь к директории для лог-файлов | ./log |
| file_size_limit_bytes | Максимальный размер лог-файла в байтах | 1048576 |
| max_rolling_files | Максимальное количество сохраняемых лог-файлов | 10 |
| zbc | Способ передачи параметров zbusser_api и zbpaspass_api. <i>Возможные значения:</i> true : значения параметров zbusser_api и zbpaspass_api считаются зашифрованными; false : значения параметров zbusser_api и zbpaspass_api используются в открытом виде | true |
| | | false |
| zbusser_api | Имя пользователя для доступа к API | - |
| zbpaspass_api | Пароль для доступа к API | - |
| url_api | URL API-сервиса | - |
| template_upd_dir | Путь к директории, содержащей шаблоны | - |
| format | Формат передаваемых шаблонов. <i>Возможные значения:</i> null : выбран формат шаблонов по умолчанию – xml; XML : передача шаблонов в формате xml; JSON : передача шаблонов в формате json | null |
| | | XML |
| | | JSON |
| rules | Правила, каким образом необходимо импортировать новые и существующие объекты. Параметр rules детально описан в конфигурационном файле custom.json | null |

Описание конфигурационного файла custom.json представлено в таблице 3, файл расположен в папке /opt/ic-ds/ds-click/.

Таблица 3 – Описание конфигурационного файла custom.json

| Параметр | Описание параметра | Значение |
|------------------------|--|---|
| discoveryRules | Правила, каким образом импортировать LLD правила | <p><i>Возможные значения:</i> createMissing: создать отсутствующие объекты; updateExisting: обновить существующие объекты; deleteMissing: удалить отсутствующие объекты. Для использования значения указывается параметр <i>true</i>, для отключения – <i>false</i>.</p> |
| graphs | Правила, каким образом импортировать график | |
| groups | Правила, каким образом импортировать группы узлов сети | |
| hosts | Правила, каким образом импортировать узлы сети | |
| httptests | Правила, каким образом импортировать web-сценарии | |
| images | Правила, каким образом импортировать изображения | |
| items | Правила, каким образом импортировать элементы данных | |
| maps | Правила, каким образом импортировать карты сетей | |
| templateLinkage | Правила, каким образом импортировать соединения с шаблонами | |
| templates | Правила, каким образом импортировать шаблоны | |
| triggers | Правила, каким образом импортировать триггеры | |
| valueMaps | Правила, каким образом импортировать преобразования значений | |