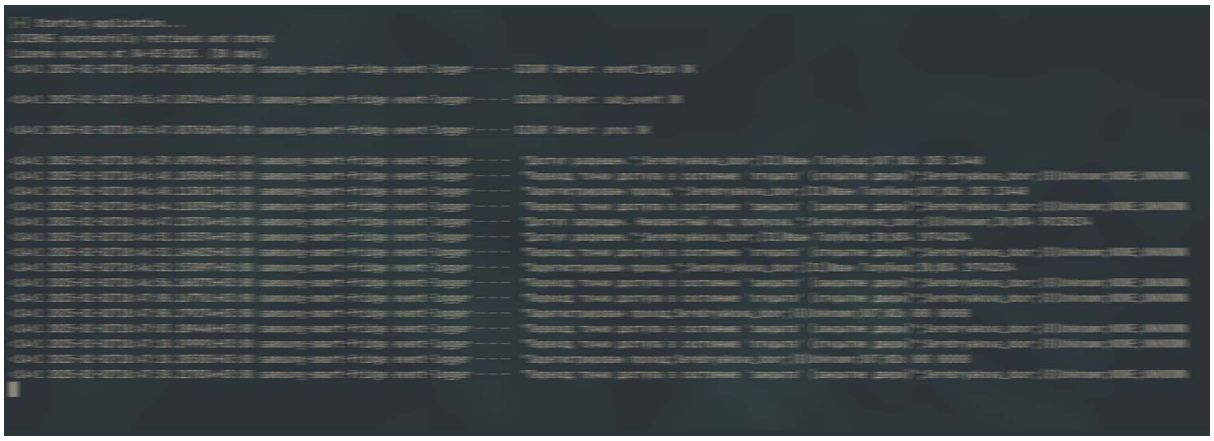
МОДУЛЬ ИНТЕГРАЦИИ SIGUR С SYSLOG



1. О модуле

Syslog - стандартный протокол, используемый для передачи сообщений о системных событиях от устройств и приложений в сети на централизованный сервер.

Интеграция СКУД (системы контроля и управления доступом) с Syslog предоставляет ряд преимуществ:

- Централизованный мониторинг и анализ событий СКУД и других систем в едином хранилище логов.
- Интеграция с SIEM - улучшенная эффективность обнаружения угроз путем сопоставления событий доступа с данными сети, конечных точек и других данных безопасности.
- Увеличение надежности СКУД и связанных систем, обеспеченное механизмами отказоустойчивости Syslog, такими как резервное копирование журналов и возможность обрабатывать большие объемы данных.
- Упрощение устранения неполадок в работе СКУД и смежных систем по логам из разных источников в одном месте.
- Долгосрочное хранение данных может быть полезно для ретроспективного анализа инцидентов и расследования происшествий.

Модуль Syslog для SIGUR - утилита, которая обеспечивает передачу событий, генерируемых системой контроля и управления доступом SIGUR, на удаленный Syslog-сервер. Модуль работает как утилита для платформ Linux/Windows. Он перехватывает события SIGUR, формирует из них сообщения в формате RFC5424 и отправляет их на указанный Syslog-сервер.

2. Поддерживаемые версии Syslog

Модуль поддерживает стандарт RFC 5424 (Syslog Protocol). Может быть использован любой Syslog-сервер. Тестирование утилиты проходило с использованием сервера RSyslog.

3. Настройка Syslog-сервера

Основные принципы настройки Syslog-сервера для приема сообщений утилиты на примере RSyslog

3.1. Включите прием сообщений по сети

- Для UDP:

  ```
  $ModLoad imudp
  $UDPServerRun 514
  ```

- Для TCP:

  ```
  $ModLoad imtcp
  $InputTCPServerRun 514
  ```

3.2. Настройте правила для приема сообщений от утилиты (опционально)

Вы можете создать отдельный файл в директории /etc/rSyslog.d (например, 10-sigur-Syslog.conf) и добавить правила фильтрации и маршрутизации сообщений. Например, для фильтрации по имени процесса:

```
f $programname == 'event-logger' then {
  # Запись в файл event_logger.log
  action(type="omfile" file="/var/log/event_logger.log")
  stop
}
```

Общие рекомендации:

- Убедитесь, что брандмауэр на сервере разрешает входящие соединения на порт 514 (или другой, который вы используете) по протоколу UDP или TCP.
- Вам может потребоваться дополнительная настройка в зависимости от ваших требований и конфигурации Syslog-сервера. Всегда обращайтесь к документации по вашему Syslog-серверу для получения более подробной информации.

4. Конфигурация типов событий

Модуль позволяет настроить, какие типы событий СКУД SIGUR будут отправляться на Syslog-сервер. Настройка осуществляется через файл events.csv в корневой директории утилиты, в котором описаны события согласно протоколу SIGUR OIF. Документацию по этому протоколу следует запросить у поставщика СКУД SIGUR.

5. Примеры логов

Пример сообщения о разрешенном доступе:

<14>1 2024-12-12T12:50:08.933783+03:00 hostname event-logger - - - "Доступ разрешен." Access_Point (69)Иванов Иван IN W34 B2534812

Пример сообщения о проходе без идентификации (например, по кнопке):

<14>1 2024-12-12T12:47:06.801723+03:00 hostname event-logger - - - "Зарегистрирован проход Access_Point (0)Unknown OUT W26 000 00000

Где:

- <14> - Priority Value (user.info);
- `1` - Version;
- `2024-12-12T12:47:06.801723+03:00` - TIMESTAMP;
- `host-name` - HOSTNAME;
- `event-logger` - APP-NAME;
- `-` - PROCID, MSGID, STRUCTURED-DATA;
- `Зарегистрирован проход Access_Point (0)Unknown OUT W26 000 00000` - MSG.

6. Возможные события

Код	Значение
0	(не используется)
1	Зарегистрирован взлом.
2	Зарегистрирован проход в разблокированном режиме.
3	Зарегистрирован проход, санкционированный с кнопки.
4	Зарегистрирован проход.
5	Зарегистрирован проход при открытой двери.
6	Зарегистрирован проезд по путевому листу.
7	(не используется)
8	Доступ запрещен. Введен неверный PIN-код.
9	Доступ запрещен. Контроллер не готов.
10	Доступ запрещен. Неизвестный код пропуска.
11	Доступ запрещен. Режим не позволяет проход.
12	Доступ запрещен. Нет допуска на точку доступа.
13	Доступ запрещен. Нет допуска в это время.
14	Доступ запрещен. Повторный проход.
15	Доступ запрещен. Срок действия ключа истек.

Код	Значение
16	Пожарная тревога! Произведена аварийная разблокировка.
17	Пожарная тревога завершена.
18	Корпус контроллера открыт.
19	Корпус контроллера закрыт.
20	Связь с точкой доступа потеряна.
21	Связь с точкой доступа восстановлена.
22	Закрытие ворот.
23	Открытие ворот.
24	Доступ разрешен.
25	Удержание двери в открытом состоянии начато.
26	(не используется)
27	(не используется)
28	Переход на работу от сети (восстановление питания)
29	Переход на работу от аккумулятора (потеря сетевого питания)
30	Установка режима точки доступа "Нормальный"
31	Установка режима точки доступа "Заблокированный"
32	Установка режима точки доступа "Разблокированный"
33	(не используется

Код	Значение
34	(не используется
35	(не используется)
36	Переход точки доступа в состояние "закрыта" (закрытие двери)
37	Переход точки доступа в состояние "открыта" (открытие двери)
38	Удержание двери в открытом состоянии закончено.
39	Начало ожидания санкции охраны
40	Окончание ожидания санкции охраны
41	Отказ от доступа
42	Ожидание сопровождающего
43	Ожидание ввода PIN кода
44	Ожидание алкотеста
45	Доступ запрещен. Использован основной считыватель (ожидается дополнительный).
46	Доступ запрещен. Использован дополнительный считыватель (ожидается основной).
47	Доступ запрещен. Режимы пересеклись недопустимым способом.
48	Доступ запрещен. Точка доступа заблокирована.
49	Доступ запрещен. Удерживается кнопка блокировки.
50	Доступ запрещен. Другая дверь шлюза сейчас открыта

Код	Значение
51	Доступ запрещен. Превышение числа лиц в зоне.
52	Доступ запрещен. Охранник отказал в доступе.
53	Доступ запрещен. Недопустимое опьянение.
54	Доступ запрещен. Контроллер не готов (код 17).
55	Доступ запрещен. Не дождались результата алкотестирования.
56	Доступ запрещен. Не дождались сопровождающего.
57	Доступ запрещен. Не дождались санкции охраны.
58	Доступ запрещен. Не дождались второго объекта.
59	Доступ запрещен. Обработка предыдущего объекта не завершена (код 22).
60	Доступ запрещен. Обработка предыдущего объекта не завершена.
61	Доступ запрещен. Невозможно списать стоимость выбранной позиции.
62	Доступ запрещен. Не было распознавания гос. Номера.
63	Доступ запрещен. Активно специальное ограничение.
64	Доступ запрещен. Есть не сданные предметы.
65	Неисправность замка. Датчик холла не активен когда должен быть активен.
66	Неисправность замка. Датчик холла активен когда должен быть не активен.
67	Доступ запрещен. Лицо не опознано

Код	Значение
68	Лицо не опознано.
69	Доступ запрещен. Попытка подбора кода. (постановление №969)
70	Ждем сопровождающего, идентифицированный не может выступить в этой роли.
71	Доступ по гос. номеру запрещен согласно режиму.
72	Не удалось получить ответ от внешней системы.
73	Доступ запрещен внешней системой.
74	Лицо распознано.
75	Ожидание лица.
76	Напряжение питания в норме.
77	Напряжение питания ниже нормы.
78	Напряжение питания выше нормы.
79	Доступ запрещен. Нет связи с сервером.
80	Ожидание измерения температуры.
81	Превышен порог предупреждения по температуре.
82	Превышен порог тревоги по температуре.
83	Доступ запрещен. Проверка температуры не пройдена.
84	Доступ запрещен. Верификация не пройдена

Код	Значение
85	Температура в норме.
86	Идентифицирован сопровождающий.
87	Доступ запрещен. Отсутствует лицевая маска.
88	Лицевая маска отсутствует.
89	Успешная проверка лицевой маски.
90	Начата проверка наличия лицевой маски.
91	Результат измерения температуры отсутствует.

7. Лицензирование

Модуль Syslog для SIGUR отдельно лицензируется на каждое устройство, на которое необходимо его установить. Утилита активируется с использованием лицензионного ключа, который потребуется ввести при первом запуске программы.

При работе с подключением к интернету:

1. При первом запуске программа предложит Вам ввести приобретенный лицензионный ключ.
2. Введенный ключ впоследствии хранится локально - в файле `config.conf`.
3. Будет загружен файл `license`, это означает, что утилита активирована и готова к работе.

Если возникли неполадки при работе приложения - обратитесь к нам для получения дополнительной информации.

Оффлайн-активация:

1. Программа предложит вам ввести приобретенный лицензионный ключ.
2. Будет создан файл `failed_auth_[timestamp].json`, содержащий сам ключ и hardware id, необходимые для оффлайн-активации
3. Обратитесь в нашу службу технической поддержки, предоставив данный файл для оффлайн-активации.
4. В ответ вы получите файл активированной лицензии license
5. Поместите полученный файл license в директорию приложения.

⚠	**Лицензия привязана к спецификации машины, используя информацию, такую как MAC-адрес и операционная система. Перемещение приложения на другое устройство потребует повторной активации. Так же при включении/отключении сетевого интерфейса MAC может измениться.**

8. Настройка модуля

- Активировать лицензию.
- Установить модуль Syslog для SIGUR, распаковав модуль в удобную директорию.
- Настроить параметры подключения к Syslog-серверу и серверу СКУД SIGUR. Подробное руководство по настройке поставляется с ПО.
- Запустить ./start.sh / start.bat.
- Проверить поступление логов на Syslog-сервере.

129343, Россия, г. Москва
проезд Серебрякова, д. 8
Тел./Факс: +7 (495) 988-9116

630004, Россия, г. Новосибирск
ул. Ленина д. 21, оф. 230, отель «Азимут»
Тел.: +7 (383) 284-1084

E-mail: **info@agrg.ru**
Web: **www.agrg.ru**
cod.agrg.ru
skud.agrg.ru