EASystem

Release 1.0.0

Makar Oleg Y. <oleg.makar90@yandex.ru>

May 17, 2023

Документация:

1. Введение

EASystem создана чтобы улучшить встроенную систему алертинга для ElasticSearch
с помощью добавление возможности отправки уведомлений в Telegram, E-mail, MS Teams
и приведения уведомлений в более информативный и читабельный вид.

Note: Поддерживаемые версии Elastic

7.*, 8.*

---

2. Зависимости

```
certifi==2022.9.24
cffi==1.15.1
charset-normalizer==2.1.1
cryptography==38.0.1
elastic-apm==6.12.0
elasticsearch==7.17.0
idna==3.4
pycparser==2.21
PyYAML==6.0
requests==2.28.1
schedule==1.1.0
urllib3==1.26.12
pydantic==1.10.2
```

Note: Пакетный менеджер `pip` имеет возможность читать файлы с описанием зависимостей и устанавливать их с помощью команды `pip install -r requirements.txt`

---

3. Настройка Python

Note: Рекомендуется использовать виртуальное окружение Python (VENV)

3.1 VENV

Рекомендуется использовать виртуальную среду Python для запуска EASystem, как и для любого другого подобного приложения.

4. Конфигурационный файл

Конфигурационный файл можно найти в директории `function\configs\config.yml`

```yaml
#file (id.log), elk, sqlite3
modules:
  main:
    database.type: sqlite3
    database.fill: false
    database.fill_query_range: 24 #in hours
    interval: 60 #in seconds, minimum 30 seconds
    query_range: 10 #in hours, minimum 1 hour
    include_projects: [ '*' ]
    exclude_projects: [ ]

  find_restarts:
    enabled: true
    time: "300000" #in milliseconds. (system.uptime.duration.ms)
    include_projects: [ '*' ]
    exclude_projects: [ ]

  certificate_expire_date:
    enabled: true
    every: 1 #day(s)
    at: "10:00" #time

encryption:
  include_projects: [ '*' ]
  exclude_projects: [ ]
  telegram: true

debug_mode:
  enabled: true
  silent: false
  #telegram_channel_id:
  #telegram_token:

info_message:
  at_startup: true
  schedule: false
  schedule_timer: 60 #in minutes
  #telegram_channel_id:
  #telegram_token

#Debug, info, warning, error, critical.
logging:
```

(continues on next page)

(continued from previous page)

```
  level: warning
  to_files: true
  to_console: false

logs.directory:
  linux: "/var/log/EASystem/"
  win32: "E:\\EASystem\\logs\\"

config.directory:
  linux: "/usr/share/EASystem/configs/"
  win32: "E:\\EASystem\\configs\\"

passwd.directory:
  linux: "/usr/share/EASystem/passwd/"
  win32: "E:\\EASystem\\passwd\\"

output.elasticsearch:
  hosts: [ "https://localhost:9200" ]
  verify_certs: false
  #certificate: "E:\\EASystem\\elasticsearch-ca.pem"
  certificate: "/usr/share/EASystem/elasticsearch-ca.pem"
  username: ""
  password: ""

output.elasticsearch.apm:
  enabled: false
  service_name: "EASystem"
  server_url: "http://localhost:8200"
  secret_token: ""
  environment: "prd"

connectors:
  e-mail:
    enabled: true
    # Overrides all recipients in any cases.
    redirect:
      enabled: false
      silent: false
      to: [ 'contracted1@contoso.com' ]

  telegram:
    enabled: true
    #default_channel_id:
    #default_token:
    #projects_channel_id:
      #project1:
    #projects_token:
      #project1:

modifiers:
  metrics:
    system.core: [ ]
    system.cpu: [ 'total.norm.pct': 'CPU Usage', 'system.pct': 'CPU pst' ]
    system.diskio: [ ]
    system.entropy: [ ]
    system.filesystem: [ 'used.pct': 'Disk Usage','free': 'Disk free space' ]
    system.fsstat: [ ]
    system.load: [ ]
    system.memory: [ 'actual.used.pct': 'RAM Usage','swap.free': 'Swap free', 'actual.free':
↪'Actual Free RAM' ]
    system.network: [ ]
    system.network_summary: [ ]
```

(continues on next page)

(continued from previous page)

```
    system.process: [ ]
    system.process.summary: [ ]
    system.raid: [ ]
    system.service: [ ]
    system.socket: [ ]
    system.socket.summary: [ ]
    system.uptime: [ ]
    system.users: [ ]
    prometheus.metrics: [ 'node_filesystem_avail_bytes': 'Disk Usage (in bytes)' ]

  alerts:
    #kibana-alert-history-[accepted_projects]
    projects: [ "default", "project1", "project2" ]
    #Accepted Tags for shown as topic
    tags: ["tag1", "tag2"]

  mail_recipients:
      tag1:
          to: [ 'contracted1@contoso.com' ]
      tag2:
          to: [ 'contracted1@contoso.com', 'contracted2@contoso.com' ]
mail_recipients:
    project1:
        enabled: true
        to: [ 'contracted1@contoso.com', 'contracted2@contoso.com' ]

    project2:
        enabled: true
        to: [ 'contracted1@contoso.com', 'contracted2@contoso.com' ]
```

4.1 4.1 Modules

Секция `modules` отвечает за настройку модулей программы:

```
modules:
    main:
        database.type: file
        database.fill: false
        database.fill_query_range: 24 #in hours
        interval: 60 #in seconds, minimum 30 seconds
        query_range: 1 #in hours, minimum 1 hour
        include_projects: ['*']
        exclude_projects: []

    find_restarts:
        enabled: true
        time: "300000" #in milliseconds. (system.uptime.duration.ms)
        include_projects: ['*']
        exclude_projects: []

    certificate_expire_date:
        enabled: true
        every: 1 #day(s)
        at: "10:00" #time
```

4.1.1 4.1.1 Основной модуль (main)

Основной модуль программы ищет в индексах `kibana-alert-history-*` новые алерты и сравнивает их с имеющейся базой данных (см. `database.type`). Если найденного алерта нет в базе данных, то на его основе формируется оповещение с последующим занесением его в базу данных.

database.type
Выбор типа базы данных для записывания ID событий. Принимаемые значения: `file`, `sqlite3`, `elk`
По умолчанию: `sqlite3`

Note:

- Типы баз данных:
  - `file` расположен в файле *id.log* в `logs.directory` (см. раздел конфига *logs.directory*)
  - `elk` все найденные события записываются в индекс с именем *kibana-alert-history-id* (необходимо создать его вручную)
  - `sqlite3` sql база данных расположена в корневой директории в файле *easystem.db*

---

database.fill
Заполнение базы данных позволяет записать все найденные события в индексах `kibana-alert-history-` в базу данных,

без формирования оповещений. Данная опция полезна при длительном простоя программы или при первом запуске. | По умолчанию: `false`

database.fill_query_range: 24
Глубина просмотра при заполнении базы данных (см. **database.fill**).
По умолчанию: `24`. Единицы измерения: часы

interval: 60
Интервал поиска новых событий.
По умолчанию: `60`. Единицы измерения: секунды. Минимальное значение: 30.

query_range: 1
Глубина просмотра при поиске новых событий. Увеличение параметра увеличивает нагрузку на систему.
По умолчанию: 1. Единицы измерения: часы. Минимальное значение: 1.

include_projects: [‘*’]
Если явно указан проект (*например: [‘my-project1’, ‘my-project2’]*), то остальные найденные проекты, при поиске новых событий, будут игнорироваться.
По умолчанию: `['*']` - включены все проекты.

exclude_projects: []
Если указан проект (например: [‘my*project’]), то он будет проигнорирован при поиске новых событий.
По умолчанию: [] - нет исключений проектов из списка поиска новых событий.

4.2 4.2 Encryption

4.3 4.3 Debug mode

4.4 4.4 Info message

4.5 4.5 Logging

4.6 4.6 Directory

4.7 4.7 Output

4.8 4.8 Connectors

4.9 4.9 Modifiers

4.10 4.10 Mail recipients

5. Модули

5.1 5.1 Основной

5.2 5.2 Поиск рестартов

5.3 5.3 Проверка срока истечения SSL сертификата

6

6. Первый запуск

7. Системы получения оповещений

7.1 7.1 Электронная почта

7.2 7.2 Мессенджеры

8. Шифрование чувствительных данных

Шифрует **CHAT_ID** и **BOT_ID** в рандомную строку. С включенной настройкой не нужно указывать эти данные в явном виде в конфиге.

Note: Формат заполнения файлов -100000000000:x:1234456789:AAAAAA_XXXXXXXXXXXXXXXXXXXXXXX
где -100000000000 - CHAT_ID 1234456789:AAAAAA_XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX - BOT_ID.

Для начала необходимо заполнить файл `default_settings.key`, откуда будут браться настройки CHAT_ID и BOT_ID для тех проектов, для которых не указаны другие данные (для которых не определен свой телеграм канал и бот).

Если `connectors.telegram.enabled: true` и `encryption.telegram: true`, но файл `default_settings.key` не заполнен, программа попросит вас его заполнить.

При первом запуске программа создаст файлы с именами <*project*>*.key*, в директории passwd, где <*project*> последняя часть имени индекса алертов (проект).

Для тех проектов, которые имеют номер своего канала в телеграмме для отправки, необходимо заполнить одноименные файлы в директории `passwd` согласно формату, приведенному выше. При следующем запуске программы строка зашифруется.

Если файл `default_settings.key` поврежден или удален, то восстанавливается его предыдущая копия из файла `shadow_copy.key`. Это обычная копия последнего работоспособного файла `default_settings.key`.

Если *.key* файл проекта поврежден, то он перезаписывается настройками из `default_settings.key`.

9. Модификаторы

9.1 9.1 Custom

9.2 9.2 Service

10

10. Дополнительно

10.1 10.1 Elasticsearch APM

10.2 10.2 Режим отладки

10.3 10.3 Информационное сообщение

11. Список терминов и определений

ElasticSearch
: Высокомасштабируемая распределенная поисковая система полнотекстового поиска и анализа данных с веб-интерфейсом, REST API и неформализованными JSON-документами, которая разработана на базе полнотекстового поиска Lucene и работает в режиме реального времени. https://www.elastic.co/elasticsearch/

Виртуальная среда Python (Virtual Environment, VENV)
: Уникальное сочетание интерпретатора Python и набора библиотек, которое не повторяется в других глобальных окружениях. Виртуальное окружение предназначено для конкретного проекта, и данные о нем хранятся в папке проекта. В этой папке содержатся установленные библиотеки окружения и файл pyvenv.cfg, в котором указан путь к базовому интерпретатору, расположенному в другом месте файловой системы.

Алерт
: От англ. Alert - оповещение, уведомление, сигнал

Проект
: Имя проекта определяется по последней части имени индекса с событиями оповещений `kibana*alert*history*[проект]`

12

en

12.1 Введение

EASystem создана чтобы улучшить интегрированную систему алертинга для ElasticSearch.

12.2 Зависимости

```
certifi==2022.9.24
cffi==1.15.1
charset-normalizer==2.1.1
cryptography==38.0.1
elastic-apm==6.12.0
elasticsearch==7.17.0
idna==3.4
pycparser==2.21
PyYAML==6.0
requests==2.28.1
schedule==1.1.0
urllib3==1.26.12
pydantic==1.10.2
```

Note: Пакетный менеджер `pip` имеет возможность читать файлы с описанием зависимостей и устанавливать их с помощью команды `pip install *r requirements.txt`

12.3 Настройка Python

Note: Рекомендуется использовать виртуальное окружение Python

12.3.1 VENV

12.4 Конфигурационный файл

```
#file (id.log), elk, sqlite3
modules:
  main:
    database.type: sqlite3
    database.fill: false
    database.fill_query_range: 24 #in hours
    interval: 60 #in seconds, minimum 30 seconds
    query_range: 10 #in hours, minimum 1 hour
    include_projects: [ '*' ]
    exclude_projects: [ ]

  find_restarts:
    enabled: true
    time: "300000" #in milliseconds. (system.uptime.duration.ms)
    include_projects: [ '*' ]
    exclude_projects: [ ]

  certificate_expire_date:
    enabled: true
    every: 1 #day(s)
    at: "10:00" #time

encryption:
  include_projects: [ '*' ]
  exclude_projects: [ ]
  telegram: true

debug_mode:
  enabled: true
  silent: false
  #telegram_channel_id:
  #telegram_token:

info_message:
  at_startup: true
  schedule: false
  schedule_timer: 60 #in minutes
  #telegram_channel_id:
  #telegram_token

#Debug, info, warning, error, critical.
logging:
  level: warning
  to_files: true
  to_console: false

logs.directory:
  linux: "/var/log/EASystem/"
  win32: "E:\\EASystem\\logs\\"

config.directory:
  linux: "/usr/share/EASystem/configs/"
  win32: "E:\\EASystem\\configs\\"

passwd.directory:
  linux: "/usr/share/EASystem/passwd/"
  win32: "E:\\EASystem\\passwd\\"
```

(continues on next page)

(continued from previous page)

```
output.elasticsearch:
  hosts: [ "https://localhost:9200" ]
  verify_certs: false
  #certificate: "E:\\EASystem\\elasticsearch-ca.pem"
  certificate: "/usr/share/EASystem/elasticsearch-ca.pem"
  username: ""
  password: ""

output.elasticsearch.apm:
  enabled: false
  service_name: "EASystem"
  server_url: "http://localhost:8200"
  secret_token: ""
  environment: "prd"

connectors:
  e-mail:
    enabled: true
    # Overrides all recipients in any cases.
    redirect:
      enabled: false
      silent: false
      to: [ 'contracted1@contoso.com' ]

  telegram:
    enabled: true
    #default_channel_id:
    #default_token:
    #projects_channel_id:
      #project1:
    #projects_token:
      #project1:

modifiers:
  metrics:
    system.core: [ ]
    system.cpu: [ 'total.norm.pct': 'CPU Usage', 'system.pct': 'CPU pst' ]
    system.diskio: [ ]
    system.entropy: [ ]
    system.filesystem: [ 'used.pct': 'Disk Usage','free': 'Disk free space' ]
    system.fsstat: [ ]
    system.load: [ ]
    system.memory: [ 'actual.used.pct': 'RAM Usage','swap.free': 'Swap free', 'actual.free':
↪'Actual Free RAM' ]
    system.network: [ ]
    system.network_summary: [ ]
    system.process: [ ]
    system.process.summary: [ ]
    system.raid: [ ]
    system.service: [ ]
    system.socket: [ ]
    system.socket.summary: [ ]
    system.uptime: [ ]
    system.users: [ ]
    prometheus.metrics: [ 'node_filesystem_avail_bytes': 'Disk Usage (in bytes)' ]

  alerts:
    #kibana-alert-history-[accepted_projects]
    projects: [ "default", "project1", "project2" ]
    #Accepted Tags for shown as topic
    tags: ["tag1", "tag2"]
```

(continues on next page)

(continued from previous page)

```
  mail_recipients:
      tag1:
          to: [ 'contracted1@contoso.com' ]
      tag2:
          to: [ 'contracted1@contoso.com', 'contracted2@contoso.com' ]
mail_recipients:
    project1:
        enabled: true
        to: [ 'contracted1@contoso.com', 'contracted2@contoso.com' ]

    project2:
        enabled: true
        to: [ 'contracted1@contoso.com', 'contracted2@contoso.com' ]
```

12.4.1 1. Modules

12.4.2 2. Encryption

12.4.3 3. Debug mode

12.4.4 4. Info message

12.4.5 5. Logging

12.4.6 6. Directory

12.4.7 7. Output

12.4.8 8. Connectors

12.4.9 9. Modifiers

12.4.10 10. Mail recipients

12.5 Модули

12.5.1 Основной

12.5.2 Поиск рестартов

12.5.3 Проверка срока истечения SSL сертификата

12.6 Первый запуск

12.7 Системы получения оповещений

12.7.1 Электронная почта

12.7.2 Мессенджеры

12.8 Шифрование чувствительных данных

12.9 Модификаторы

12.9.1 Custom

12.9.2 Service

12.10 Дополнительно

12.10.1 Elasticsearch APM

12.10.2 Режим отладки

12.10.3 Информационное сообщение

12.11 Глоссарий

Index

E