Создание Custom Alert Action для Splunk Enterprise

VolgaBlob

Об этом мастер-классе

- Структура приложений alert action
- Использование Splunk Add-On Builder
- Применяемые технологии:
  - немного python
- Дополнительно: взаимодействие со Splunk с помощью REST API

https://www.gotomeet.me/vbtrend-alert

Custom Alert Action API

- Custom alert action API для создания приложений типа alert action
- Позволяет распространять их через Splunkbase
- Пользователи получают возможность использования и конфигурирования новых alert action через Splunk Web

Структура директорий

```
[app_name]
    appserver
        static
            [app_icon].png                  // Картинка иконки с логотипом
    bin
        [custom_alert_action_script] *      // Логика: скрипт или исполняемый файл
    default
        alert_actions.conf *                // Конфигурация: Объявление custom alert action
        app.conf *                          // Конфигурация приложения
        restmap.conf                        // Правила валидации пользовательских параметров
        setup.xml                   // Страница для настройки глобальных параметров
        data
            ui
                alerts
                    [custom_alert_action].html * // Интерфейс пользователя для
                                                 // установки значений параметров
    metadata
        default.meta                // Экспорт
    README
        alert_actions.conf.spec     // Описание глобальных параметров
        savedsearches.conf.spec     // Описание пользовательских параметров
```

alert_actions.conf

is_custom	boolean	Индикатор того, что в приложении реализуется custom alert action (устанавливается в 1)
label	text	Отображаемое в интерфейсе имя action
icon_path	text	Относительное расположение файла appIcon.png иконки аддона ($SPLUNK_HOME$/etc/[app]/appserver/static/), рекомендуется 48 x 48 px PNG
alert.execute.cmd	text	Имя/расположение скрипта или исполняемого файла, запускаемого при срабатывании
payload_format	(xml | json)	Формат передачи параметров в скрипт
param.[param_name]		Пользовательские параметры, значения которых передаются в скрипт

Дополнительные параметры: http://docs.splunk.com/Documentation/Splunk/7.0.0/Admin/Alertactionsconf

alert_actions.conf

```
$SPLUNK_HOME$/etc/apps/[name]/default/alert_actions.conf

[logger]
is_custom = 1
label = My Alert Action
icon_path = myicon.png
payload_format = json
disabled = 0
# Custom params
param.foo = bar
param.param1 = I can use a toker
```

```
<alert>
    <server_host>localhost:8089</server_host>
    <server_uri>https://localhost:8089</server_uri>
    <session_key>1234512345</session_key>
    <results_file>
      /opt/splunk/var/run/splunk/129387182931 23.121/results.csv.gz
    </results_file>
    <results_link>
       http://splunk.server.local:8000/en-US/app/search?sid=12341234.123
    </results_link>
    <sid>12341234.123</sid>
    <search_name>My Saved Search</search_name>
    <owner>admin</owner>
    <app>search</app>
    <configuration>
        <stanza name="[my_custom_alert]">
            <param name="[param_name_1]">[some value]</param>
            <param name="[param_name_2]">[other value]</param>
        </stanza>
    </configuration>
</alert>
```

[custom_alert_action_script]

Windows platforms

filename.bat
filename.cmd
filename.py
filename.js
filename.exe

*Nix platforms

filename.sh
filename.py
filename.js
filename (executable file without an extension)

- Расположение файла: $SPLUNK_HOME$/etc/apps/[myapp]/bin/
- Имя скрипта следует называть также, как конфигурацию в alert_action.conf

savedsearches.conf

- Содержат значения пользовательских параметров конкретного alert action
- Имеют приоритет над значениями параметров в alert_action.conf

alert_actions.conf.spec, savedsearches.conf.spec

- Содержат описание параметров, настраиваемых в alert_actions.conf и savedsearches.conf
- Spec-файлы служат для документирования и валидации конфигурационных файлов

restmap.conf

- Содержат правила валидации для параметров
- Проверяются значения параметров, если условия не выполнены, отображается сообщение

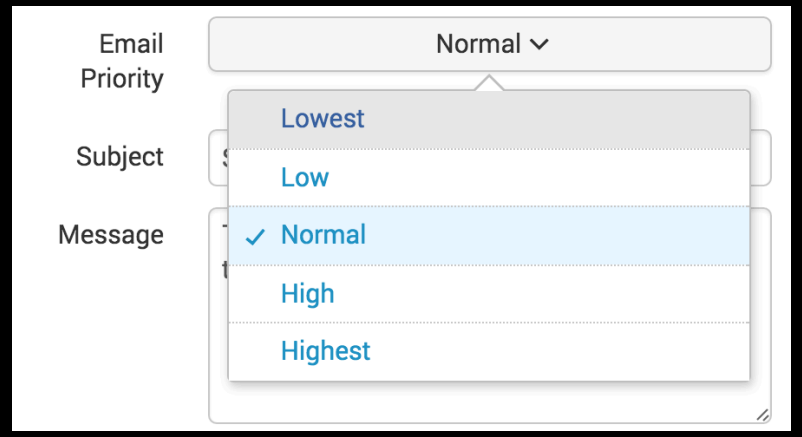
```
1  [validation: savedsearches]
2  action.webhook.param.url = validate( match('action.webhook.param.url', "^https?://[^\s]+$"), "Webhook URL is invalid")
```

Дополнительная информация:
http://docs.splunk.com/Documentation/Splunk/7.0.0/AdvancedDev/CustomAlertOptionalItems

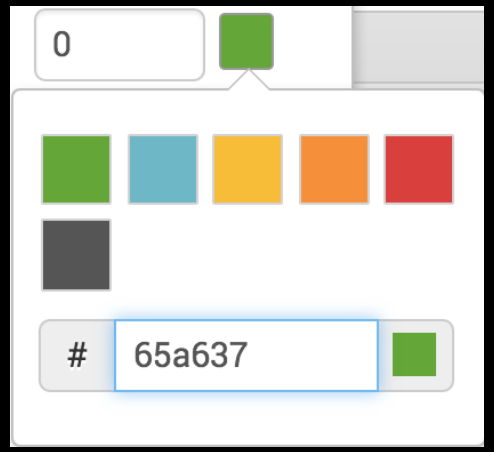
Определяется в HTML-файле: [custom_alert_action].html
Расположение:
$SPLUNK_HOME/etc/apps/[custom_alert_action_app_name]/default/data/ui/alerts/

Интерфейс

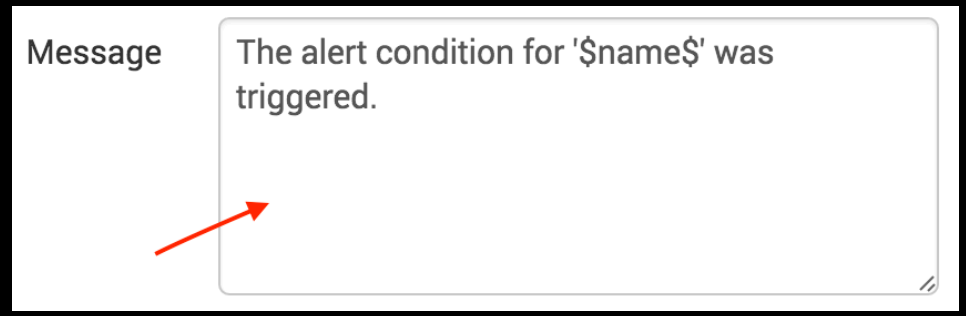
splunk-select



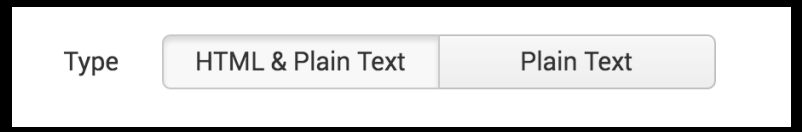
splunk-color-picker



splunk-text-area



splunk-radio-button



splunk-text-input


```
1   <div class="control-group">
2       <label class="control-label" for="my_text_area">Message</label>
3
4       <div class="controls">
5           <input type="text" name="action.myalert.param.message" id="my_text_area" />
6           <span class="help-block">
7             Text of the message to be sent
8           </span>
9       </div>
10  </div>
```

Дополнительная информация:
http://docs.splunk.com/Documentation/Splunk/7.0.0/AdvancedDev/CustomAlertUI

Процесс создания

Custom Alert Action

- Объявляем alert action и его свойства
- Определяем параметры и формируем пользовательский интерфейс
- Скрипт с логикой реакции

Telegram

Bots – стороннее приложение, работающее внутри Telegram. Пользователи могут взаимодействовать с ботоами, отправляя им сообщени и команды. Бота можно контролировать, используя HTTPS запросы к bot API.

Bot API – HTTP-based интерфейс, созданный для разработчиков ботов Telegram.

Channels – средство для широковещательной рассылки сообщений определенной аудитории.

Параметры

Token	для программного взаимодействия с Bot API
ChatId	идентификатор канала, в который необходимо отправлять сообщения
Message	отправляемое сообщение
Disable notification	пользователи будут получать сообщения без звукового сигнала

Add-on Builder

Splunk Add-on Builder – приложение для создания TA для Splunk Enterprise.

- Мастер, проводящий по всем шагам создания addon
- Уменьшает время разработки
- Помогает следовать Best Practice и Naming Conventions
- Позволяет создавать Alert Action и Modular Input

Splunk Add-on Builder: https://splunkbase.splunk.com/app/2962/