Система предупреждений

Система предупреждений

Вернуться в оглавление Документации Pandora FMS

Конфигурация предупреждений в Pandora FMS

Введение

Предупреждение - это реакция Pandora FMS на неправильное значение Модуля. Эта реакция настраивается и может состоять из всего, что может быть вызвано *скриптом*, настроенным в операционной системе, в которой работает сервер Pandora FMS, обрабатывающий модуль.

Существует несколько типов предупреждений:

- Простые предупреждения.
- Предупреждения о событиях.
- Предупреждения о *ловушках* SNMP.

В этой главе рассматривается система предупреждений в совокупности, особое внимание уделяется первым двум.

Введение в систему предупреждений

В Pandora FMS предупреждения работают посредством определения некоторых условий срабатывания, некоторых действий, выбранных для этого предупреждения, и, наконец, выполнения некоторых команд на сервере Pandora FMS, который будет отвечать за выполнение настроенных действий.

Общая система предупреждений ассоциирует одно предупреждение для каждого модуля, а это предупреждение , в свою очередь, может выполнять одно или несколько действий.

Более подробную информацию вы можете найти в обучающем видео «Без паники: давайте поговорим о системах предупреждения».

Структура предупреждения

Предупреждения состоят из:

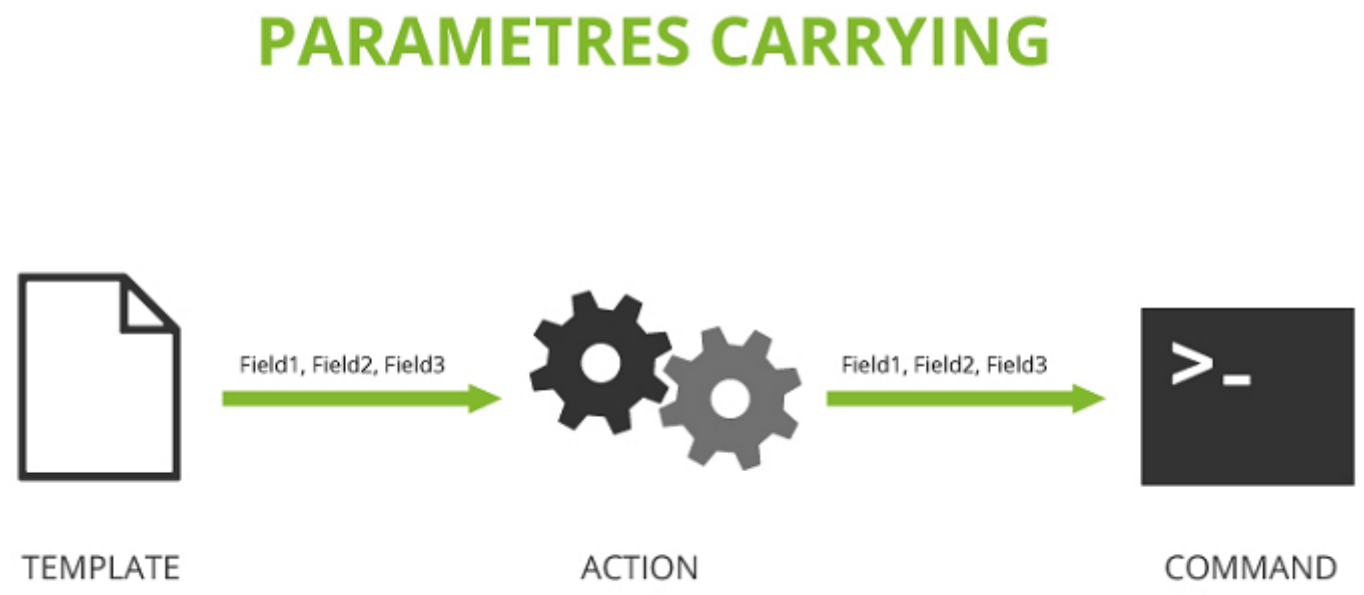
- Команды: Укажите *что будет сделано*; это будет действие, которое сервер Pandora FMS выполнит при подаче предупреждения. Это может быть запись в *журнал*, отправка электронного письма или текстового сообщения (SMS), выполнение *скрипта* и т.д.
- Действия: Они указывают *как это будет сделано*, они являются настройками скриптов команды, они позволяют настроить выполнение как таковое, передавая команде определенные параметры, такие как имя Модуля, Агент и т.д.
- Шаблоны: Они указывают *когда это будет сделано*, определяют условия для запуска действия или действий. Например: когда Модуль переходит в критическое состояние.

Информационный поток в системе предупреждений

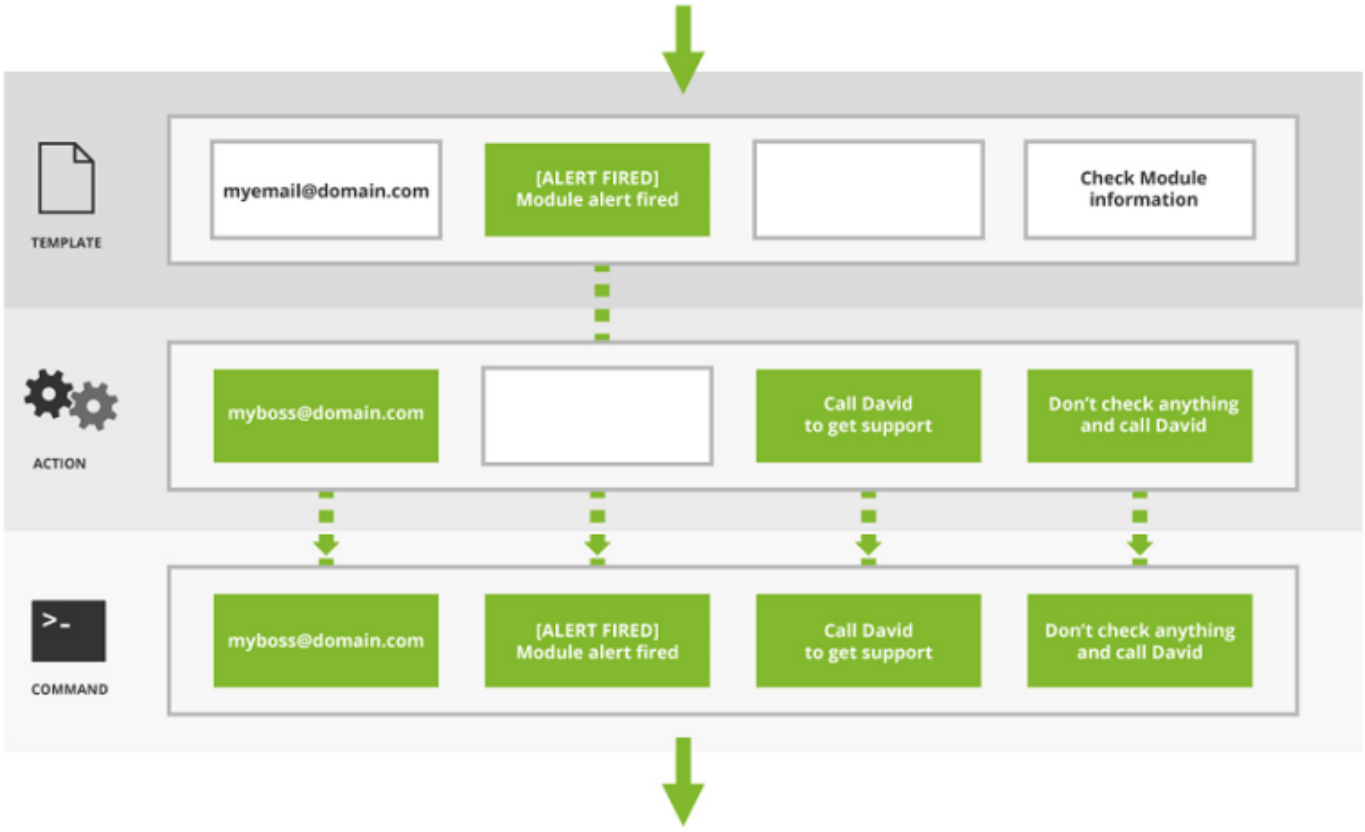
При настройке шаблонов и действий, оба имеют ряд генеративных полей, называемых `Field1` , `Field2` , `Field3`, (...) , `Fieldn`, которые используются для передачи информации от *шаблона* к *действию* и от *действия* к *команде*, и, наконец, используется в качестве параметров при выполнении этой команды.

Эта информация передается всегда, когда следующий шаг еще не имеет информации, определенной в его полях `Fieldn`. То есть, в случае перекрывающихся полей или параметров, действие перезаписывается в шаблон (например, если в шаблоне определено `Field1` и действие тоже, то `Field1` действия имеет приоритет).

На следующей схеме показана передача параметров из шаблона в команду:



Пример того, как перезаписать значения шаблона с помощью значений действия:



Например, шаблон, который запускает предупреждение и отправляет сообщение электронной почты со следующими полями:

- Шаблон:
  - Field1: myemail@domain.com
  - Field2: [Alert] The alert was fired
  - Field3: The alert was fired!!! SOS!!!

- Действие:
  - Field1: myboss @domain.com
  - Field2: <blank>
  - Field3: <blank>

Значения, которые будут достигнуты командой, будут следующими:

- Команда:
  - Field1: myboss@domain.com
  - Field2: [Alert] The alert was fired
  - Field3: The alert was fired!!! SOS!!!

Для полей `Field2` и `Field3` сохраняются значения, определенные в шаблоне, но для поля `Field1` используется значение, определенное в действии.

Команда предупреждения

Введение

Действия, которые Pandora FMS выполняет при возникновении тревожных ситуаций, в конечном итоге переводятся в исполнение на сервере в виде команд.

ALERTS » ALERT COMMANDS

Total items: 14

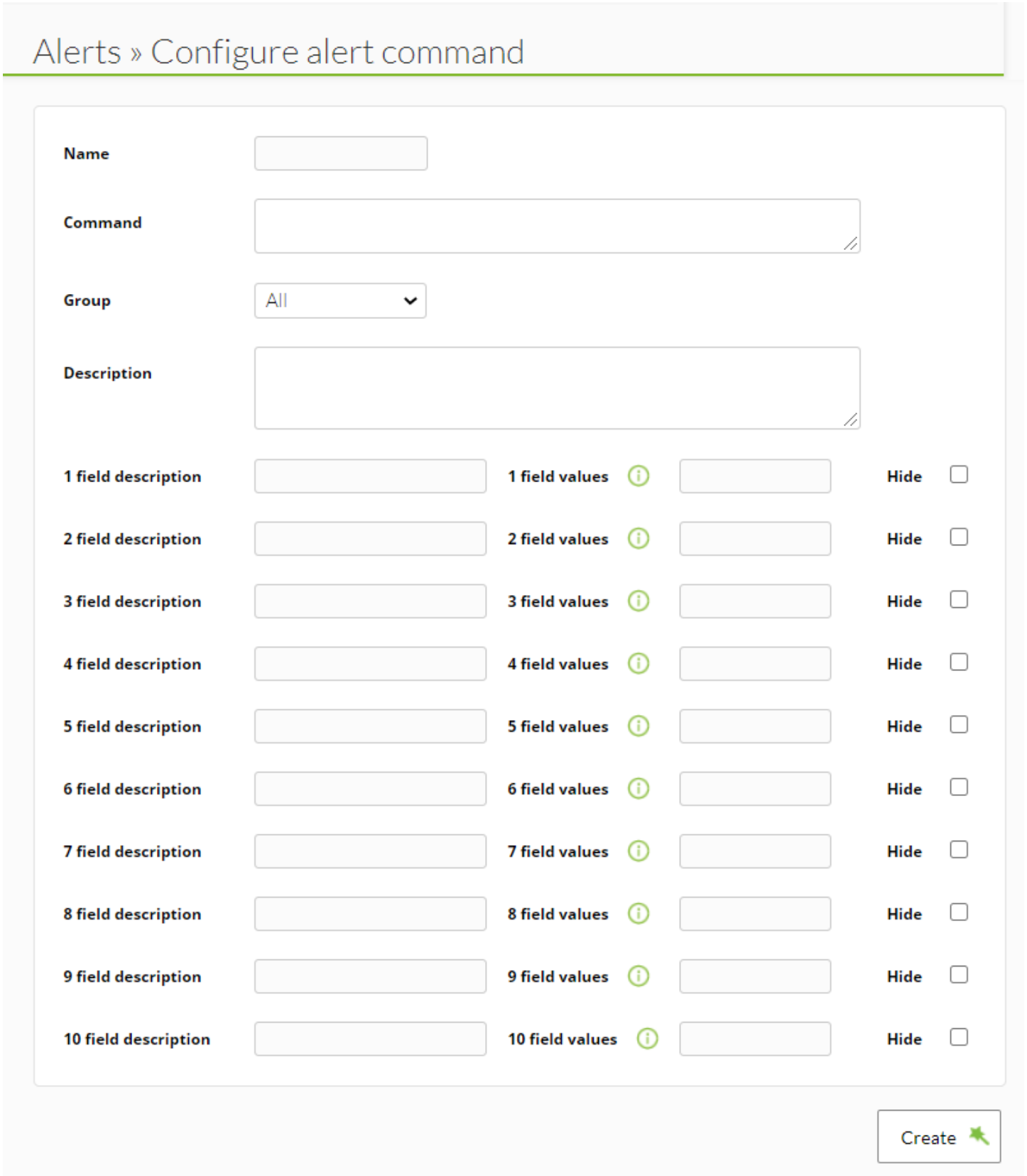
Name	ID	Group	Description	Actions
eMail	1		This alert send an email using internal Server SMTP capabilities (defined in each server, using: _field1_ as destination email address, and _field2_ as subject for message. _field3_ as text of message. _field4_ as content type (plain/text or html/text).	
Internal Audit	2		This alert save alert in internal audit system. Fields are static and only _field1_ is used.	
Monitoring Event	3		This alert create an special event into event manager.	
Alertlog	4		This is a default alert to write alerts in a standard ASCII plaintext log file in /var/log /pandora/pandora_alert.log	
SNMP Trap	5		Send a SNMPTRAP to 192.168.0.4. Please review config and adapt to your needs, this is only a sample, not functional itself.	
Syslog	6		Uses field1 and field2 to generate Syslog alert in facility daemon with "alert" level.	
Sound Alert	7			
Jabber Alert	8		Send jabber alert to chat room in a predefined server (configure first .sendxmpprc file). Uses field3 as text message, field1 as useralias for source message, and field2 for chatroom name	
SMS	9		Send SMS using the standard SMS device, using smstools. Uses field2 as text message, field1 as destination phone (include international prefix!)	
Validate Event	10		This alert validate the events matched with a module given the agent name (_field1_) and module name (_field2_)	
Remote agent control	12		This command is used to send commands to the agents with the UDP server enabled. The UDP server is used to order agents (Windows and UNIX) to "refresh" the agent execution: that means, to force the agent to execute and send data	
Generate Notification	13		This command allows you to send an internal notification to any user or group.	
Send report by e-mail	14		This command allows you to send a report by email.	
Send report by e-mail (from template)	15		This command allows you to send a report generated from a template by email.	

Total items: 14

Create

Создание команды для оповещения

Нажав на кнопку Create в предыдущем разделе:



Name

Название команды, краткое и описательное.

Command

Команда, которая будет выполнена при срабатывании предупреждения. Можно использовать макросы (см. следующий раздел) для замены параметров, заданных в объявлении предупреждений.

Необходимо учитывать, что команды для предупреждений, выполняемые сервером Pandora FMS, выполняются с такими же привилегиями пользователя, которые выполняет сервер Pandora FMS.

Рекомендуется проверить из командной строки, является ли выполнение команды успешным и приводит ли она к желаемому результату (отправка электронного письма, создание записи в файле журнала и т.д.).

Group: Это определяет, с какой группой предупреждений можно связать команду. Вы можете назначить группу, к которой принадлежит пользователь, создающий команду предупреждения, только если этот пользователь явно не принадлежит к группе ВСЕ (ALL).

Field description и Field values: Для каждого пользовательского поля можно выполнить настройку:

- Описание поля: Это будет метка рядом с текстовым полем в форме конфигурации действия, в котором используется эта команда.
- Доступные значения поля: набор возможных значений для данного поля. Если это поле установлено (не пустое), то поле будет не текстовым, а комбинированным. Комбинированный параметр должен иметь для каждого возможного значения метку (видимый вариант) и значение (отправляемый вариант). Синтаксис следующий:

```
значение1,метка1;значение2,метка2;значение3,метка3
```

- Hide: Если поле содержит пароль, эта опция скрывает его содержимое с помощью звездочек.

Начиная с версии 6.0, можно отображать редактор HTML-кода в поле команды при создании или редактировании действия в предупреждении, если это поле команды имеет в качестве специального значения *token*. `_html_editor_`

После того как вы должным образом заполнили все параметры, нажмите на кнопку Create

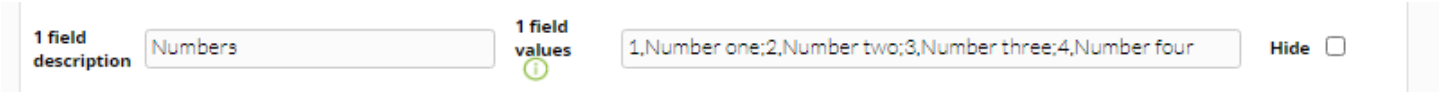
для сохранения.

Пример

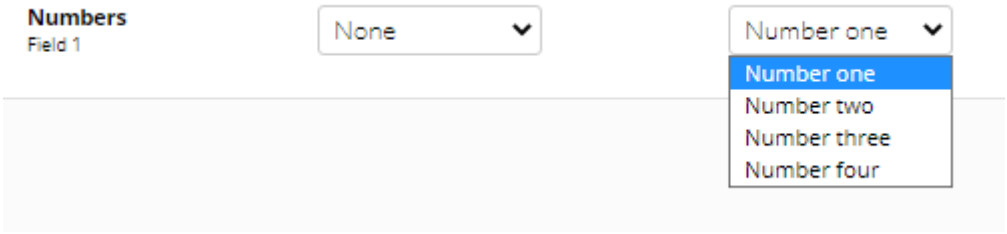
Простое поле, в котором можно будет выбирать между первыми четырьмя числами:

```
1,Число один;2,Число два;3,Число три;4,Число четыре
```

Поле должно быть установлено в команде:



Когда мы перейдем к действию, мы увидим его следующим образом:



Командные макросы

Макросы, которые можно использовать в конфигурации команды, можно найти в списке макросов в конце этой главы.

Предопределенные команды

Существует ряд заранее определенных команд, готовых к использованию в системе предупреждений Pandora FMS.

eMail

Отправляет электронное письмо с сервера Pandora FMS. Сообщения электронной почты отправляются в формате HTML, что позволяет создавать визуально привлекательные шаблоны. Обратите внимание, что получатель должен иметь доступ к ресурсам, используемым в шаблоне, например, к изображениям.

Internal audit

Генерирует запись в системе внутреннего аудита Pandora FMS. Хранится в базе данных

Pandora FMS и может быть проверен с помощью программы просмотра событий с консоли.

Monitoring Event

Создает пользовательское событие в консоли событий Pandora FMS.

Pandora FMS Alertlog

Это предопределенное предупреждение, которое записывает предупреждения в обычном формате ASCII в файл *журнала* `/var/log/pandora/pandora_alert.log` .

SNMP Trap

Отправляет настроенную SNMP *ловушку* с указанием используемых скриптов.

Syslog

Отправляет предупреждение в системный реестр с помощью системной команды. logger.

Sound Alert

Воспроизводит звук в звуковой консоли событий при возникновении предупреждения.

Jabber Alert

Отправляет предупреждение Jabber в чат на заранее определенный сервер (сначала необходимо настроить файл .sendxmpprc). Введите в `field1` алиас пользователя, в `field2` - имя чат-комнаты и `field3` - текстовое сообщение.

SMS Text

Отправляет SMS на определенный мобильный телефон. Сначала необходимо определить предупреждение и настроить шлюз отправки SMS, доступный с сервера Pandora FMS. Вы также можете установить его с помощью Gnokii для отправки SMS, непосредственно используя телефон Nokia с помощью USB-кабеля. Процесс описан ниже.

Validate Event

Проверяет все события, связанные с модулем. Сюда передастся имя агента и название модуля.

Remote agent control

Отправляет команды агентам с включенным сервером UDP. Сервер UDP используется для упорядочивания агентов (Windows и UNIX)б которые «обновляют» выполнение агента: то есть, заставляет агента выполнить и отправить данные.

Generate Notification

Позволяет отправить внутреннее уведомление любому пользователю или группе.

Редактирование команды для предупреждения

Перейдите на ►Alerts → Command:

ALERTS » ALERT COMMANDS

Total items: 14

Name	ID	Group	Description	Actions
eMail	1		This alert send an email using internal Server SMTP capabilities (defined in each server, using: _field1_ as destination email address, and _field2_ as subject for message. _field3_ as text of message. _field4_ as content type (plain/text or html/text).	
Internal Audit	2		This alert save alert in internal audit system. Fields are static and only _field1_ is used.	
Monitoring Event	3		This alert create an special event into event manager.	
Alertlog	4		This is a default alert to write alerts in a standard ASCII plaintext log file in /var/log /pandora/pandora_alert.log	
SNMP Trap	5		Send a SNMPTRAP to 192.168.0.4. Please review config and adapt to your needs, this is only a sample, not functional itself.	
Syslog	6		Uses field1 and field2 to generate Syslog alert in facility daemon with "alert" level.	
Sound Alert	7			
Jabber Alert	8		Send jabber alert to chat room in a predefined server (configure first .sendxmpprc file). Uses field3 as text message, field1 as useralias for source message, and field2 for chatroom name	
SMS	9		Send SMS using the standard SMS device, using smstools. Uses field2 as text message, field1 as destination phone (include international prefix!)	
Validate Event	10		This alert validate the events matched with a module given the agent name (_field1_) and module name (_field2_)	
Remote agent control	12		This command is used to send commands to the agents with the UDP server enabled. The UDP server is used to order agents (Windows and UNIX) to "refresh" the agent execution: that means, to force the agent to execute and send data	
Generate Notification	13		This command allows you to send an internal notification to any user or group.	
Send report by e-mail	14		This command allows you to send a report by email.	
Send report by e-mail (from template)	15		This command allows you to send a report generated from a template by email.	

Total items: 14

Create

Чтобы отредактировать команду предупреждения, просто нажмите на название команды.

ALERTS » CONFIGURE ALERT COMMAND

Name Jabber Alert

Command echo _field3_ | sendxmpp -r _field1_ --chatroom _field2_

Group All

Description Send jabber alert to chat room in a predefined server (configure first .sendxmpprc file). Uses field3 as text message, field1 as useralias for source message, and field2 for chatroom name

1 field description	User alias	**1 field values**		**Hide**	☐
2 field description	Chatroom name	**2 field values**		**Hide**	☐
3 field description	Message	**3 field values**		**Hide**	☐
4 field description		**4 field values**		**Hide**	☐
5 field description		**5 field values**		**Hide**	☐
6 field description		**6 field values**		**Hide**	☐
7 field description		**7 field values**		**Hide**	☐
8 field description		**8 field values**		**Hide**	☐
9 field description		**9 field values**		**Hide**	☐
10 field description		**10 field values**		**Hide**	☐

Update

После изменения выбранного предупреждения нажмите на кнопку Update.

Команды `eMail`, `Internal Audit` и `Monitoring Event` не могут быть изменены или удалены.

Операции команды предупреждения

ALERTS » ALERT COMMANDS

Total items: 14

Name	ID	Group	Description	Actions
eMail	1		This alert send an email using internal Server SMTP capabilities (defined in each server, using: _field1_ as destination email address, and _field2_ as subject for message. _field3_ as text of message. _field4_ as content type (plain/text or html/text).	
Internal Audit	2		This alert save alert in internal audit system. Fields are static and only _field1_ is used.	
Monitoring Event	3		This alert create an special event into event manager.	
Alertlog	4		This is a default alert to write alerts in a standard ASCII plaintext log file in /var/log/pandora/pandora_alert.log	
SNMP Trap	5		Send a SNMPTRAP to 192.168.0.4. Please review config and adapt to your needs, this is only a sample, not functional itself.	
Syslog	6		Uses field1 and field2 to generate Syslog alert in facility daemon with "alert" level.	
Sound Alert	7			
Jabber Alert	8		Send jabber alert to chat room in a predefined server (configure first .sendxmpprc file). Uses field3 as text message, field1 as useralias for source message, and field2 for chatroom name	
SMS	9		Send SMS using the standard SMS device, using smstools. Uses field2 as text message, field1 as destination phone (include international prefix!)	
Validate Event	10		This alert validate the events matched with a module given the agent name (_field1_) and module name (_field2_)	
Remote agent control	12		This command is used to send commands to the agents with the UDP server enabled. The UDP server is used to order agents (Windows and UNIX) to "refresh" the agent execution: that means, to force the agent to execute and send data	
Generate Notification	13		This command allows you to send an internal notification to any user or group.	
Send report by e-mail	14		This command allows you to send a report by email.	
Send report by e-mail (from template)	15		This command allows you to send a report generated from a template by email.	

Total items: 14

Create

Удалено: Чтобы удалить предупреждение, нажмите на серую корзину справа от предупреждения.

Скопировано: Оповещения можно копировать. Особенно полезно при генерировании команд, похожих на существующие, изменяя некоторые детали.

Примеры Команд

Отправка предупреждений с помощью Jabber

Очень полезно настроить Pandora FMS на отправку предупреждений на Jabber-сервер. Jabber может быть системой предупреждений в реальном времени, которая остается исторической и которая позволяет одной группе пользователей одновременно получать предупреждения.

Установка служб Jabber

Со стороны клиента:

1. Установить клиента Jabber, например, *Gaim* (сейчас *Pidgin*).
2. Зарегистрируйте учетную запись (в *Pidgin*: создайте учетную запись, нажав на кнопку регистрации учетной записи).
3. Войдите в свою учетную запись.

Со стороны сервера Pandora FMS:

1. Установить sendxmpp. С помощью этого инструмента вы можете отправлять сообщения Jabber.
2. Создайте файл в каталоге `/home` с именем `.sendxmpprc`.
3. Отредактируйте файл и введите следующие данные (замените их настоящими учетными данными):

```
useraccount@jabber.org password
```

1. Предоставить права доступа к файлу:

```
chmod 0600 .sendxmpprc
```

Теперь можно отправлять личные сообщения, например, через командную строку:

```
$ echo "Hello" | sendxmpp -s pandora useracount@jabber.org
```

Чтобы зарегистрировать предупреждение в консоли Pandora FMS, добавьте новую команду и настройте переменные команды наиболее удобным способом. Очень полезно это сделать следующим образом:

- Field_1> Адрес Jabber.
- Field_2> Отправляемый текст.

Таким образом, предупреждение определяется как:

```
echo _field2_ | sendxmpp -s pandora _field1_
```

Другие примеры использования Jabber

Отправить в чат:

```
 $ echo "Dinner Time" | sendxmpp -r TheCook --chatroom
test2@conference.jabber.org
```

Отправить строки журнала в том виде, в котором они появляются, в пункт назначения Jabber:

```
 $ tail -f /var/log/syslog | sendxmpp -i sysadmin@myjabberserver.com
```

ПРИМЕЧАНИЕ: Будьте осторожны, чтобы не перегрузить публичные Jabber-серверы, иначе вы будете отключены.

Отправка электронных писем с помощью Expect

Иногда для отправки электронной почты необходимо использовать аутентифицированный SMTP. Pandora FMS имеет все необходимое для отправки обычных электронных писем в в общей конфигурации консоли, и даже там вы можете отправить электронное сообщение для тестирования механизма отправки. Но для использования аутентифицированного SMTP, вероятно, проще и универсальнее использовать простой *скрипт* с Expect вместо настройки sendmail.

Expect - это инструмент для автоматизации интерактивных приложений, таких как telnet, ftp, passwd, fsck, rlogin, tip и др. Expect делает этот процесс простым и также полезен для тестирования этих же приложений. Expect может упростить все виды задач, которые непомерно сложны при использовании любого другого инструмента. Expect станет для вас бесценным инструментом, вы сможете автоматизировать задачи, которые раньше никогда не выполняли. Вы сможете настроить автоматизацию задач быстро и легко.

В этом примере Expect используется для отправки электронной почты с помощью сервера MS Exchange®.

Создание файла под названием `/etc/expect_smtp` следующего содержания:

```
#!/usr/bin/expect -f
set arg1 [lindex $argv 0]
set arg2 [lindex $argv 1]
set arg3 [lindex $argv 2]
set timeout 1
spawn telnet myserver.com 25
expect "220"
send "ehlo mymachine.mydomain.com\r"
expect "250"
send "AUTH login\r"
expect "334"
send "2342348werhkwjernsdf78sdf3w4rwe32wer=\r"
expect "334"
send "YRejewrhneruT==\r"
expect "235"
send "MAIL FROM: myuser@domain.com\r"
expect "Sender OK"
send "RCPT TO: $arg1\r"
expect "250"
send "data\r"
expect "354"
send "Subject: $arg2\r"
send "$arg3 \r\r"
send ".\r"
expect "delivery"
send "quit"
quit
```

Измените права доступа к файлу, чтобы разрешить его запуск:

```
chmod 700 /etc/expect_smtp
```

Сначала проверьте, что `/usr/bin/expect` работает правильно, вы можете скопировать, сохранить, дать право на выполнение следующему скрипту:

```
 #!/usr/bin/expect -f

 spawn date
 sleep 20
 expect
```

Чтобы использовать эту функцию в Pandora FMS, необходимо создать новую команду (или изменить существующую для отправки предупреждений по электронной почте) и указать следующие поля в определении команды предупреждения Pandora FMS. В поле Command напишите:

```
/etc/expect_smtp _field1_ _field2_ _field3_
```

Скрипт может быть расположен в любом месте системы, только имейте в виду, что *скрипт*

предупреждения запускается сервером, который обрабатывает данные: если это сетевые данные, то их будет обрабатывать Сетевой сервер, если это данные, поступающие от Агента, через файл данных XML, то их будет обрабатывать Сервер данных.

Если у вас разные физические серверы, вам может понадобиться скопировать один и тот же *скрипт* в одно и то же место, с одинаковыми разрешениями и одним и тем же пользователем-владельцем во всех системах, где у вас есть сервер Pandora FMS, на котором вы хотите выполнять это предупреждение. Также обратите внимание, что сетевые серверы Pandora FMS должны быть запущены от имени пользователя root (чтобы иметь возможность проводить тесты задержки ICMP), а серверы данных могут быть запущены от непривилегированного пользователя.

Предупреждение будет выполнено пользователем, который выполняет процесс сервера Pandora FMS.

Отправка SMS с помощью Gnokii

Для использования Gnokii вам необходимо использовать телефон Nokia или телефон, совместимый с Gnokii (проверьте совместимое оборудование на странице проекта Gnokii). Вам также понадобится USB-кабель для передачи данных, с помощью которого вы сможете подключить свой мобильный телефон к серверу Pandora FMS, отправляющему SMS-предупреждения.

Gnokii поддерживает широкий спектр телефонов Nokia (и некоторых других производителей). В принципе, с его помощью вы можете отправлять SMS из командной строки, непосредственно с сервера Pandora FMS, избегая использования *gateways* для отправки SMS через Интернет или очень дорогих аппаратных решений GSM для отправки сообщений.

Пример отправки SMS с помощью Gnokii из командной строки:

```
echo "PANDORA: Server XXXX is down at XXXXX" | gnokii --sendsms 555123123
```

Gnokii не может отправлять MMS с прикрепленными изображениями, но он может отправить URL HTTP/WAP, который будет отображаться при получении сообщения, например:

```
echo "Image capture sample" | gnokii --sendsms 555123123 -w
http://artica.homelinux.com/capture.jpg
```

Вы можете отправить URL-адрес изображения или URL-адрес, ведущий на облегченную версию консоли, чтобы получить доступ к консоли с мобильного устройства и

проанализировать данные.

Команда разработчиков протестировала отправку SMS с телефона Nokia 6030, отправляя SMS-предупреждения при недоступности интернет-соединения. Nokia 6030 использует определение модуля 6510 в файле `.gnokiirc`, и отправка SMS занимает около четырех секунд.

Другой альтернативой использованию Gnokii является проект Gammu. С помощью такого программного обеспечения можно реализовать более мощный шлюз.

Выполнение удаленной команды на другой системе (UNIX)

Иногда бывает необходимо выполнить команду на другой системе, для этого используется команда ssh. Система, на которой выполняется команда, должна быть UNIX и иметь установленный, запущенный и доступный демон ssh.

Чтобы избежать необходимости использовать пароль доступа к машине, выполняющей команду в Pandora Console, вам следует скопировать открытый ключ сервера, на котором вы хотите выполнить удаленную команду, в сервер Pandora FMS.

Как только это будет сделано, выполните команду:

```
ssh user@hostname [_field1_]
```

Установив `_field1_` в качестве переменной, можно выполнить команду, необходимую для предупреждения.

Действие

Введение

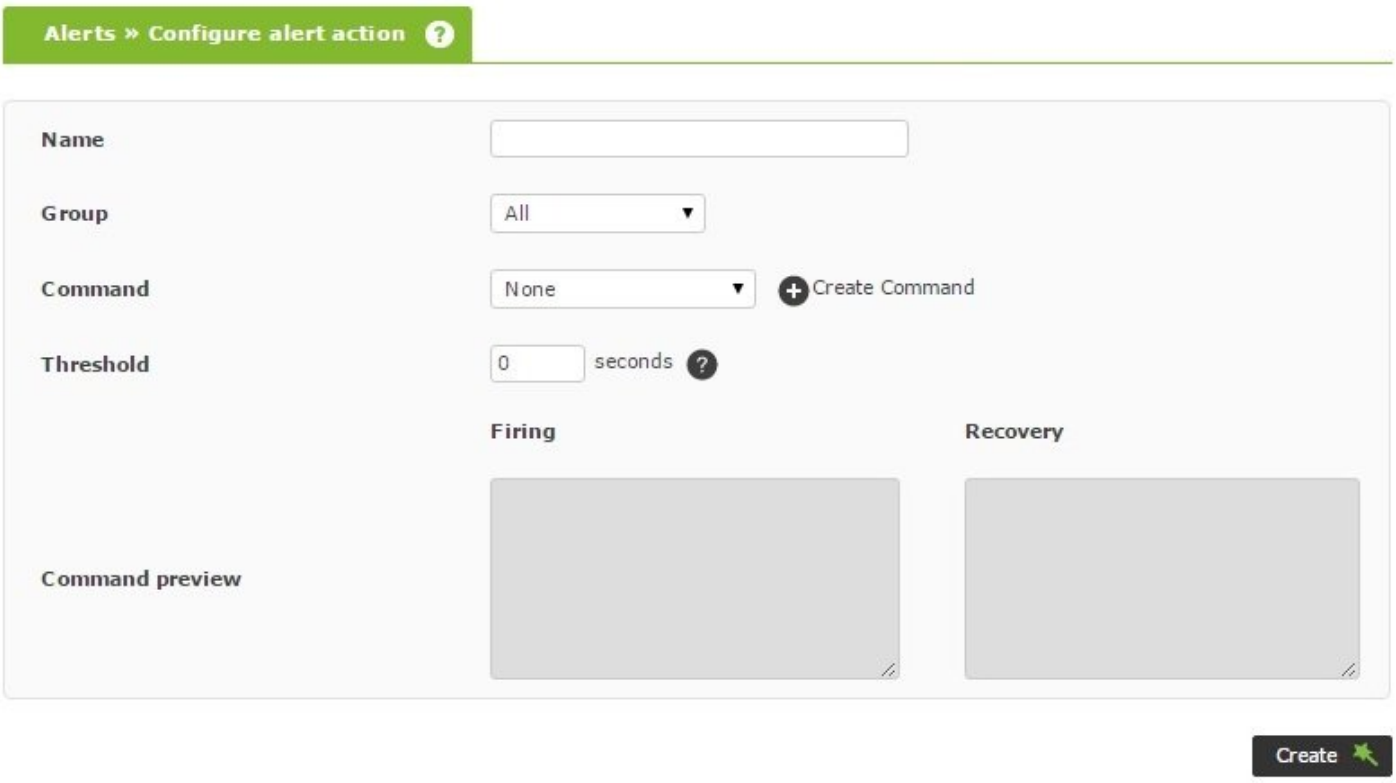
Действия - это компоненты предупреждений, в которых команда связана с общими переменными `Field 1`, `Field` , ... , `Field 10`.

Действия позволяют определить *как* запустить команду.

Создание действия

В меню выберите Alerts > Alert actions > Create:

Появится следующая форма:



Name

Имя действия.

Group

Группа действия. Вы можете назначить группу, к которой принадлежит пользователь, создающий команду предупреждения, только если этот пользователь не будет принадлежать к группе ВСЕ (ALL). Если связанная команда имеет группу, отличную от *All*, в качестве группы действия может быть установлена только группа, связанная с командой,

или группой *All*. Если по какой-то причине это не так, вы увидите предупреждающее сообщение для быстрого исправления пользователем с необходимыми правами.

Command

Команда, которая будет использоваться в случае выполнения предупреждения. Можно выбрать из различных предопределенных Команд, которые содержатся в en Pandora FMS.

Threshold

Порог выполнения действия.

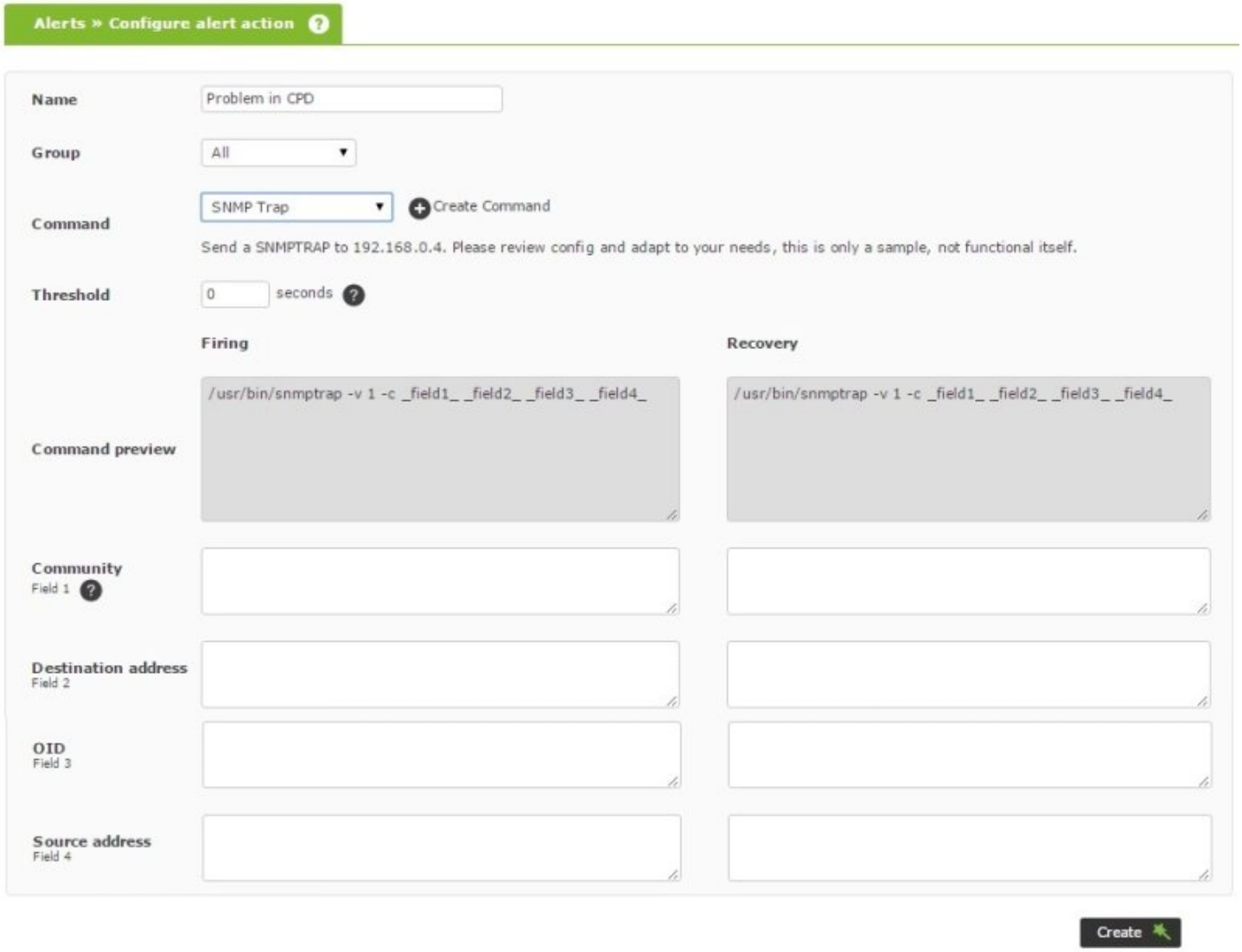
Command Preview

В этом *не редактируемом* поле автоматически отображается команда, которая должна быть выполнена в системе.

Field 1 ~ Field 10

В этих полях определяются значения макросов с `_field1_` по `_field10_`, которые будут использоваться в команде, если это необходимо. При должной настройке эти поля могут быть текстовыми или комбинированными.

После того как поля будут заполнены должным образом, сохраните их с помощью кнопки Create.



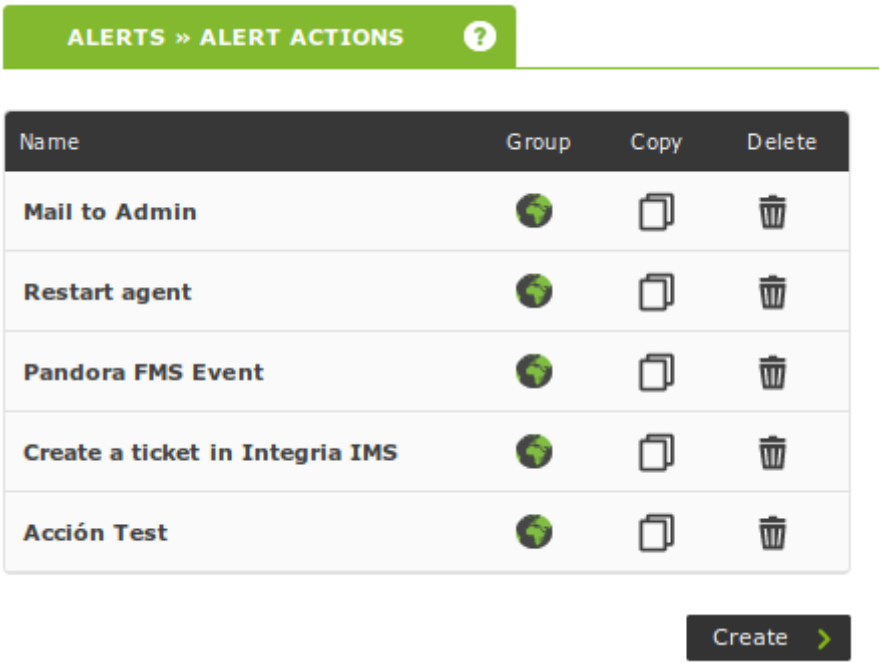
Затем в меню Actions > Alerts вы можете редактировать созданные действия.

Когда мы присваиваем значение полям (Field) в разделе Firing, по умолчанию они будут иметь те же значения для восстановления, если мы не присвоим им другое значение.

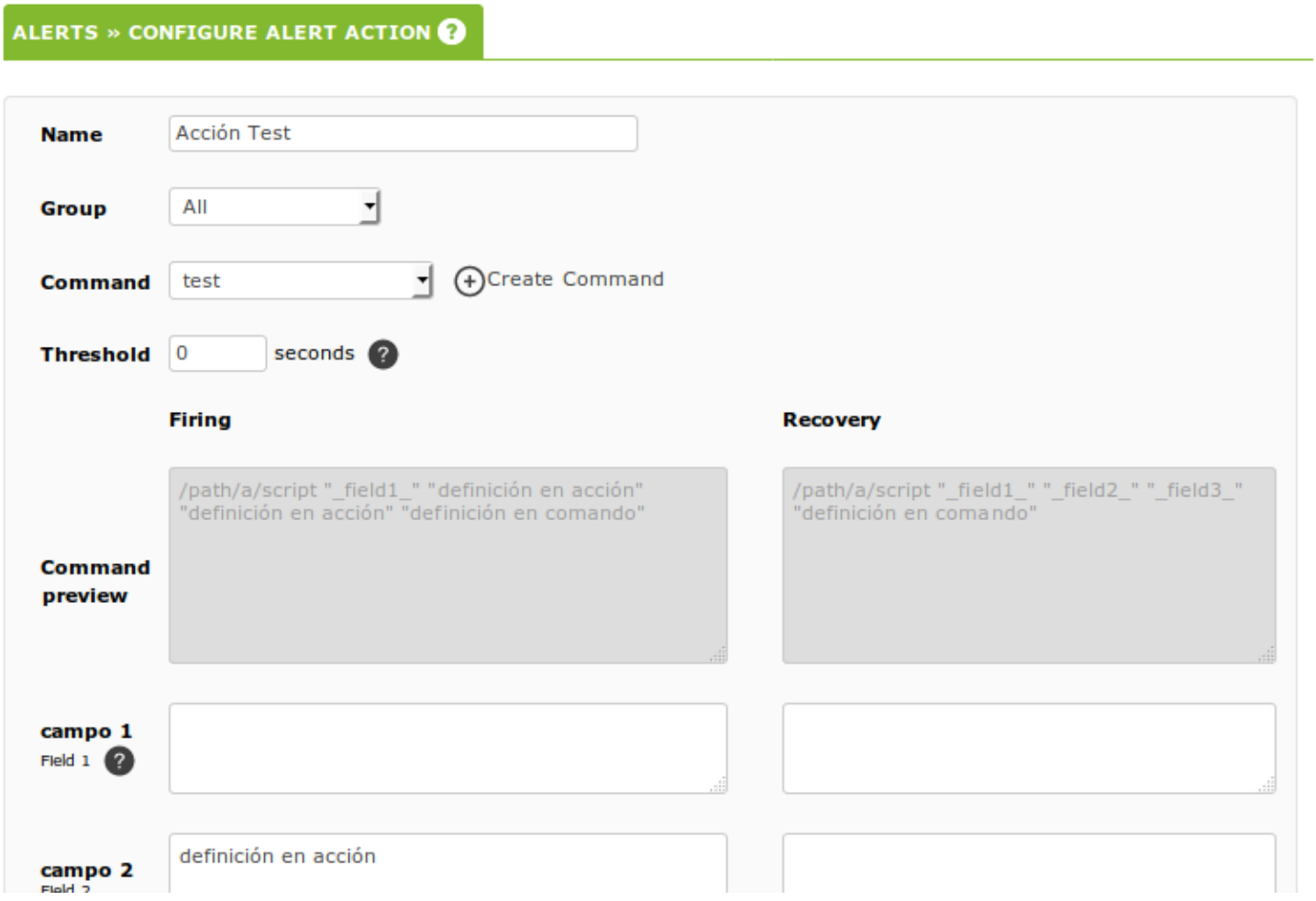
Макросы действий

Макросы, которые можно использовать в конфигурации действия, перечислены в разделе Список_макросов в конце этой главы.

Редактирование действия



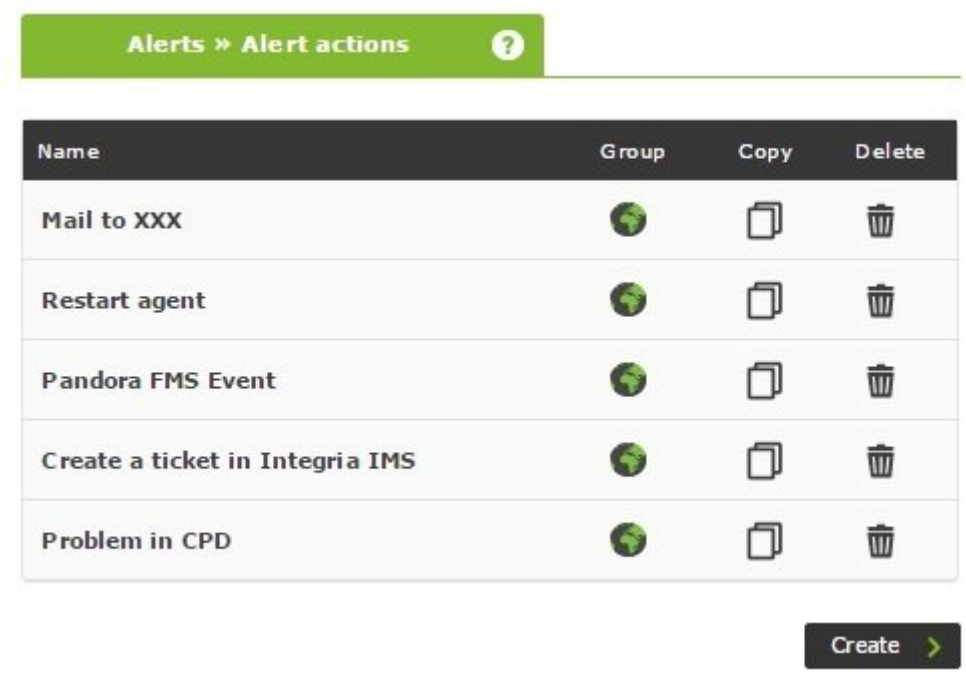
Чтобы отредактировать действие, просто нажмите на его имя.



Когда вы закончите, вы можете сохранить свои изменения, нажав на кнопку «Обновить».

Удалить действие

Вы можете удалить действие, нажав на значок корзины (колонка Delete).



Шаблон предупреждения

Введение

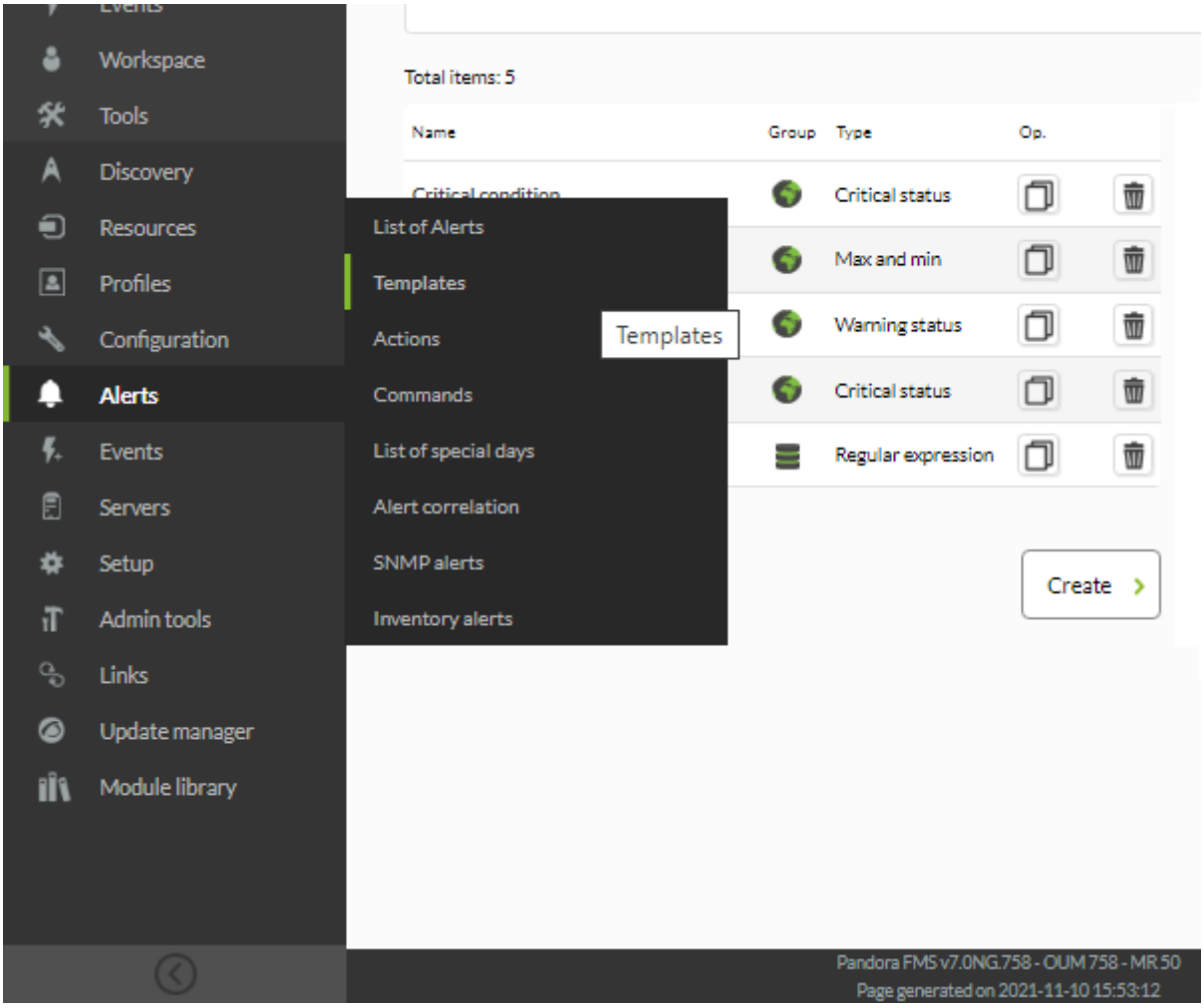
Шаблоны определяют условия срабатывания предупреждения (*когда* выполнять действие).

Шаблоны предупреждений связаны с модулями таким образом, что при выполнении условий шаблона выполняется соответствующее действие (действия).

Его структура позволяет генерировать уменьшенную группу типовых шаблонов, которые можно использовать для большинства возможных случаев в Pandora FMS.

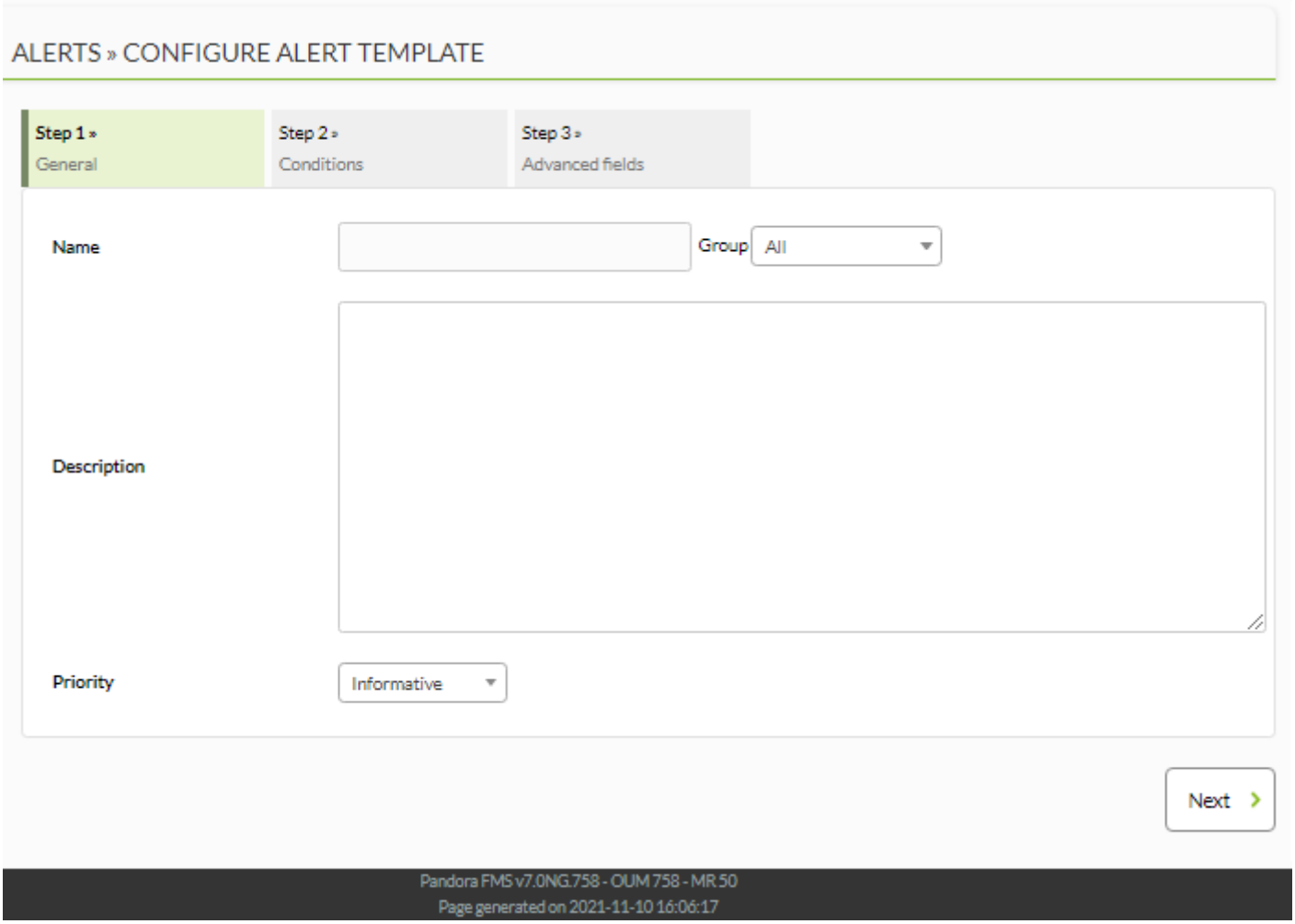
Создание шаблона

Перейдите в меню Alerts → Templates → Create.



Затем выполните три следующих шага.

Шаг 1: Общее



В этом мастере шаблонов (*wizard*) укажите:

Name

Имя шаблона, обязательно.

Group

Группа, к которой будет применен шаблон. Вы можете назначить группу, к которой будет принадлежать пользователь, создающий шаблон, только если этот пользователь явно не принадлежит к группе ВСЕ (ALL).

Описание

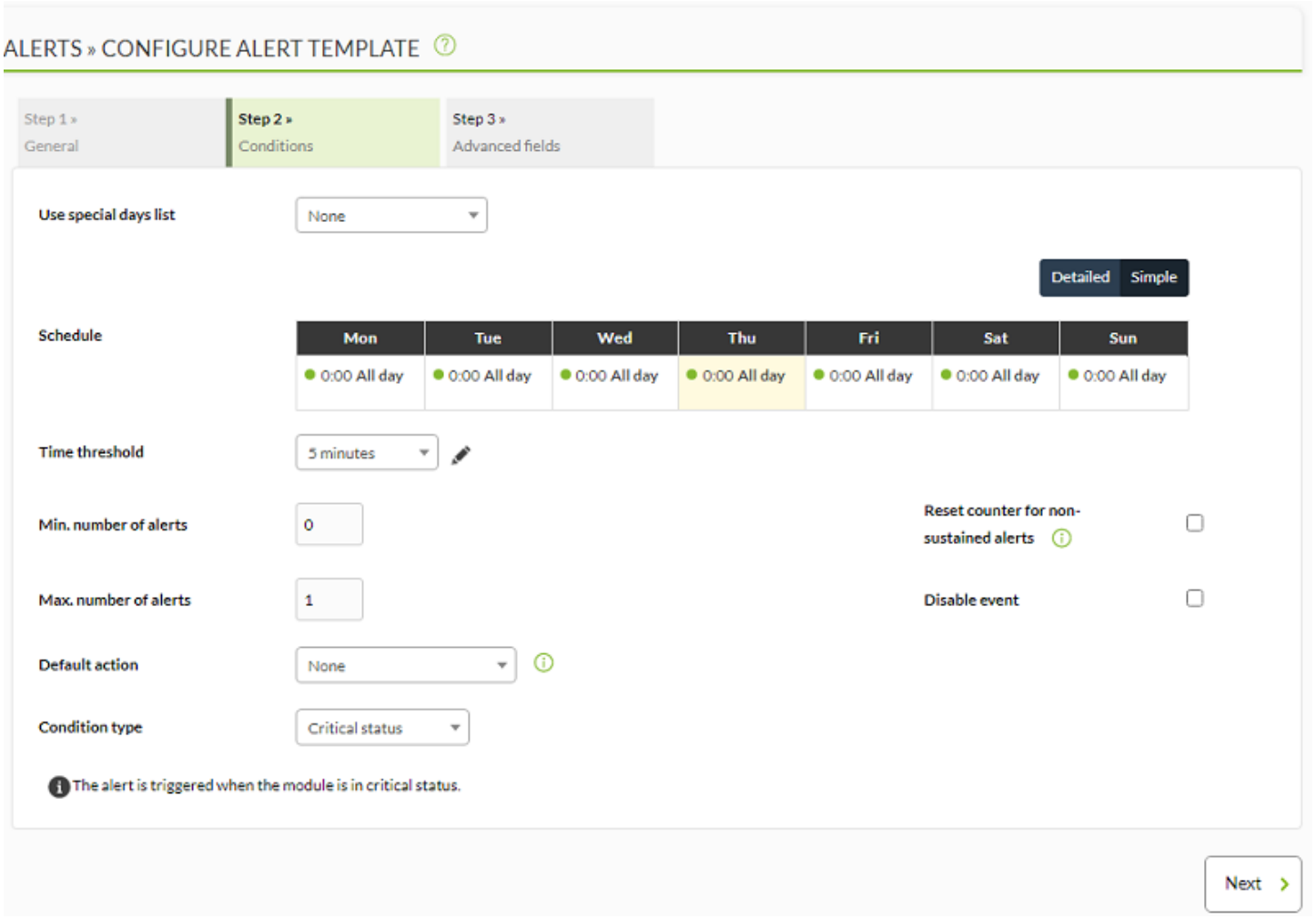
Описывает функцию шаблона и полезен для идентификации шаблона (например, в общем обзоре предупреждений).

Priority

Информационное поле о предупреждении. Событие, генерируемое при срабатывании предупреждения, наследует ее приоритет. Приоритет также очень полезен для фильтрации при поиске предупреждений. Вы можете выбрать один из следующих приоритетов:

- Maintenance.
- Informational.
- Normal.
- Warning.
- Critical.

Шаг 2: Условия



Use special days list

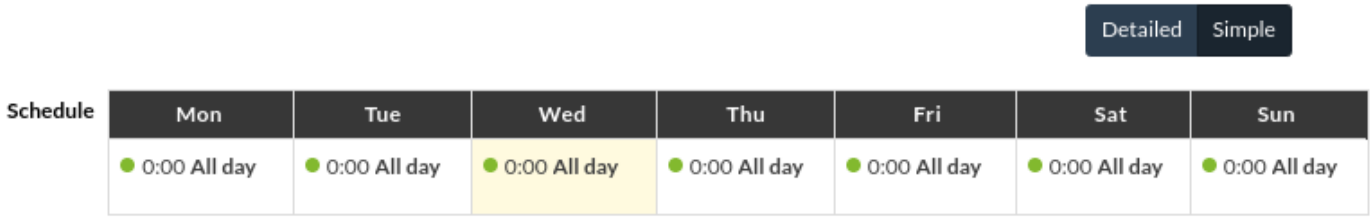
Устанавливает календарь особых дней, который будет использоваться в шаблоне.

Schedule

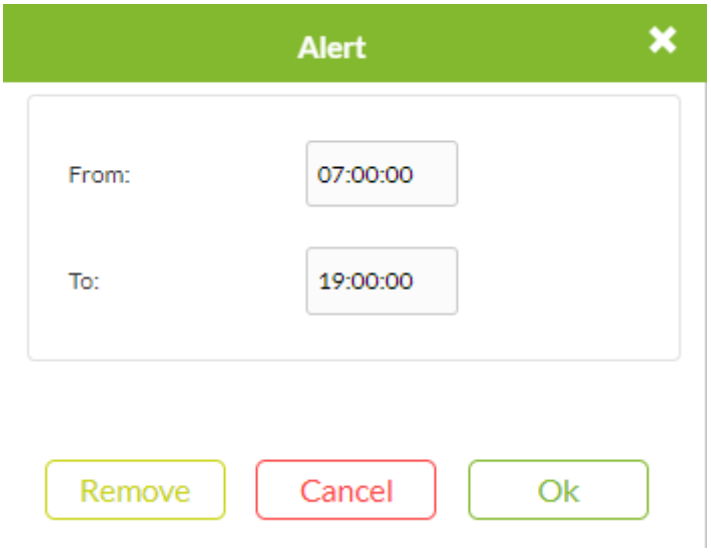
Установите дни, в которые может срабатывать оповещение.

Версия 760 или более поздняя.

Можно просмотреть и настроить, когда оповещение будет активно в каждый день недели, благодаря встроенному редактору, который по умолчанию отображается в простом режиме.

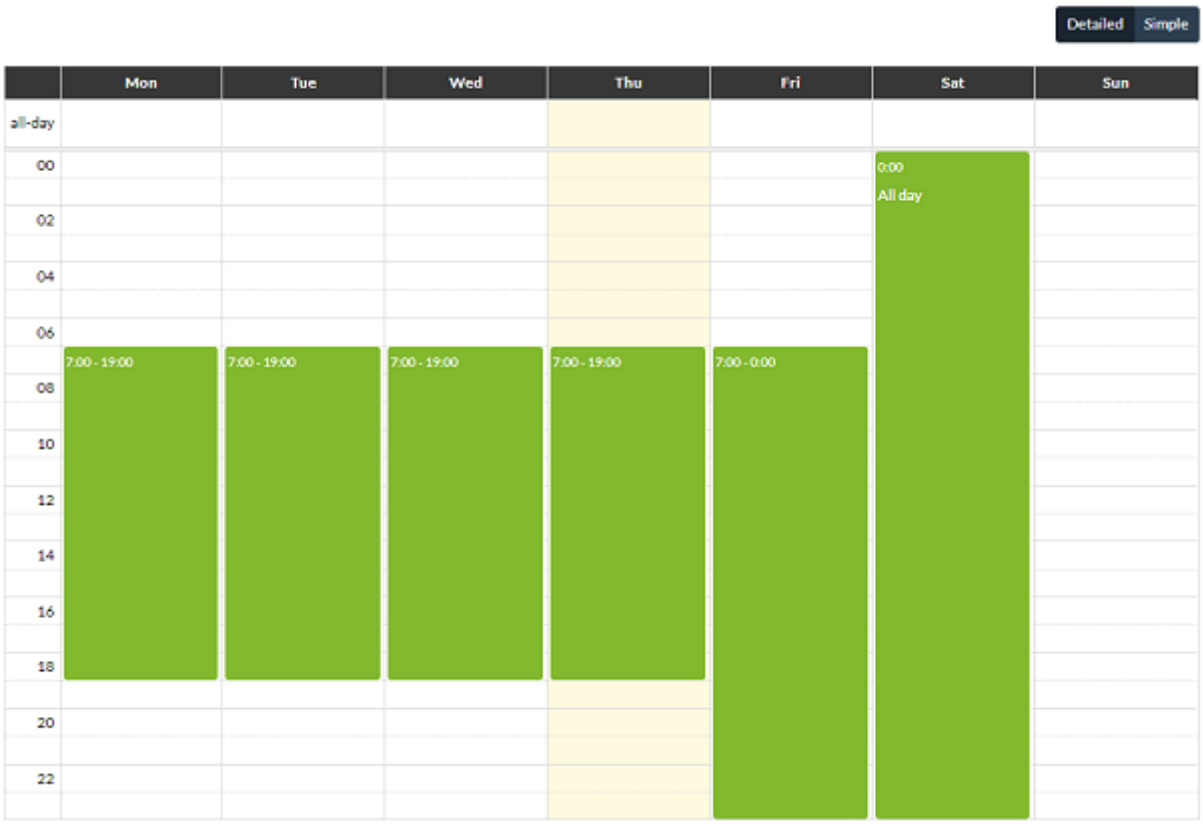


В этом простом режиме их можно настроить, щелкнув на периоде будильника каждого дня и установив время начала или окончания во всплывающей форме. Вы можете использовать кнопку Remove для удаления выбранного периода сигнала, кнопку Cancel для отмены изменений или кнопку Ok для обновления календаря.



Кроме того, перейдя в подробный режим, вы можете более точно настроить расписания. В этом режиме вы также можете использовать всплывающую форму для настройки времени или:

- Щелкните каждый день периода сигнала тревоги и перетащите верхний или нижний край, чтобы продлить период времени сигнала тревоги.
- Для перемещения щелкните в середине каждого дня периода сигнала и перетащите его туда, куда нужно. Вы увидите, что время меняется по мере того, как вы тащите.
- Чтобы добавить новый период сигнала тревоги, щелкните в пустой ячейке, и в ней будет отмечена продолжительность времени. Вы можете перемещать или изменять, как описано в предыдущих двух шагах.



Вы можете добавить столько периодов времени, сколько вам необходимо. Когда вы вернетесь в простой режим, вы получите что-то вроде следующего:

Time Threshold

Время, которое должно пройти до сброса счетчика предупреждений. Определяет интервал времени, в течение которого гарантируется, что предупреждение не будет срабатывать больше раз, чем количество предупреждений, установленное в параметре Максимальное количество предупреждений. По истечении заданного интервала счетчик сбрасывается. При извлечении предупреждения после получения успешного значения, перезапуск счетчика триггеров не запустится, если только Получение оповещения будет включено, в этом случае счетчик сбрасывается сразу после получения успешного значения.

Min number of alerts

Минимальное количество раз, которое должна произойти ситуация, определенная в

шаблоне (всегда отсчитывается от числа, определенного в параметре FlipFlop модуля), чтобы началось оповещение. Значение по умолчанию равно 0, что означает, что оповещение будет запущено при поступлении первого значения, удовлетворяющего условию. Он работает как фильтр, полезный для игнорирования ложных срабатываний.

Max number of alerts

Максимальное количество предупреждений, которые могут быть отправлены подряд в один и тот же временной интервал (Time Threshold). Это максимальное значение счетчика предупреждений. За один временной интервал не должно поступать больше предупреждений, чем указано в этом поле.

Reset counter for non-sustained alerts

Его активация зависит от того, будет ли число, указанное в Min. number of alerts больше 0. Активация этого *токена* сбрасывает счетчик предупреждений, когда указанное условие не повторяется подряд. Например, если поле Min. number of alerts имеет значение 2, это означает, что модуль должен пройти 3 раза через состояние, назначенное в Condition type, чтобы вызвать оповещение. Есть два сценария с этим последним *токеном*:

- При нажатии *токена* сброса необходимо, чтобы количество критических состояний было последовательным, иначе счетчик будет сброшен.

```
нормальное -> критическое -> критическое -> критическое
```

- Если *токен* сброса не отмечен, предупреждение будет срабатывать после альтернативной или непрерывной последовательности критических состояний:

```
нормальное -> критическое -> нормальное -> критическое -> нормальное -> критическое
```

Disable event

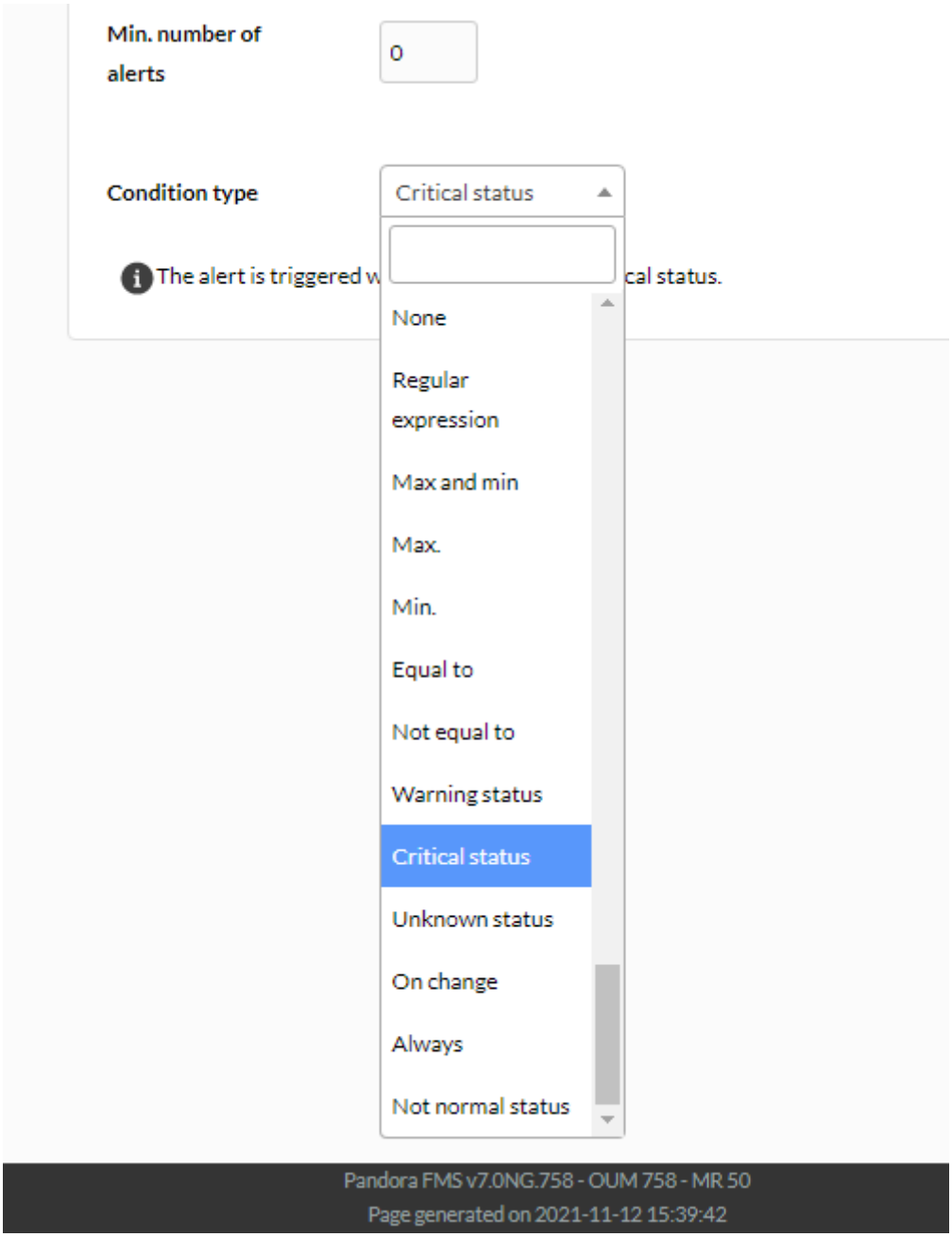
При проверке этого *токена* событие, сгенерированное в просмотре событий срабатывания предупреждения, не будет создано.

Default Action

В этой комбинации вы определяете действие по умолчанию, которое будет у шаблона. Это действие, которое автоматически создается при назначении шаблона модулю. Разместите одно действие или ни одного, однако по умолчанию вы не можете разместить несколько действий.

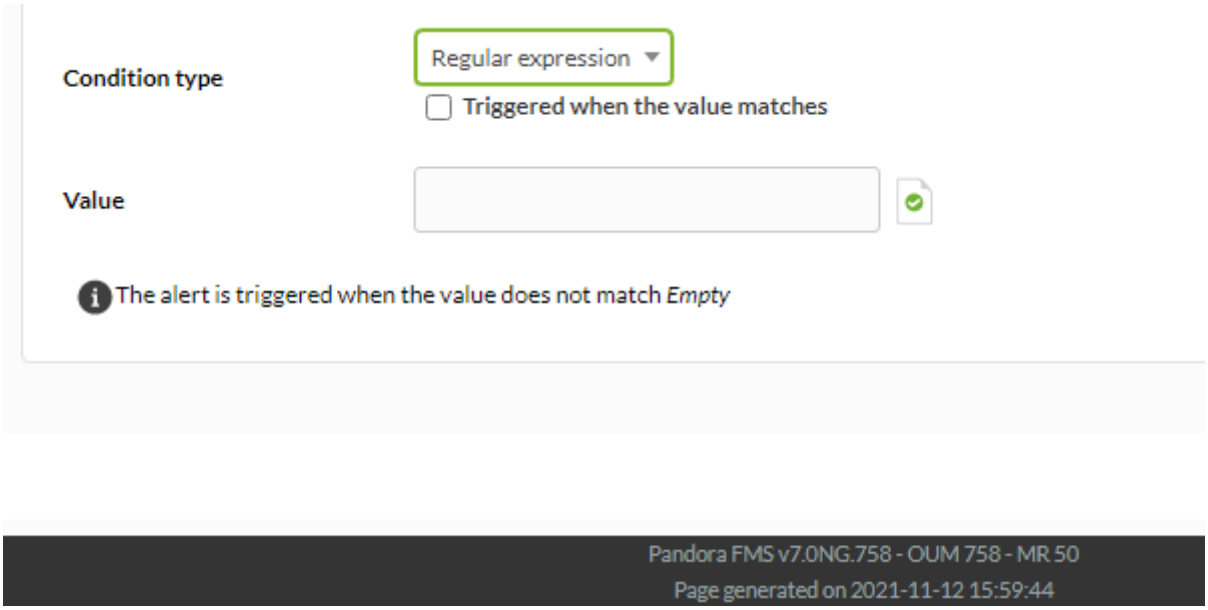
Condition Type

Поле, в котором задается тип условия, применяемого к предупреждению.

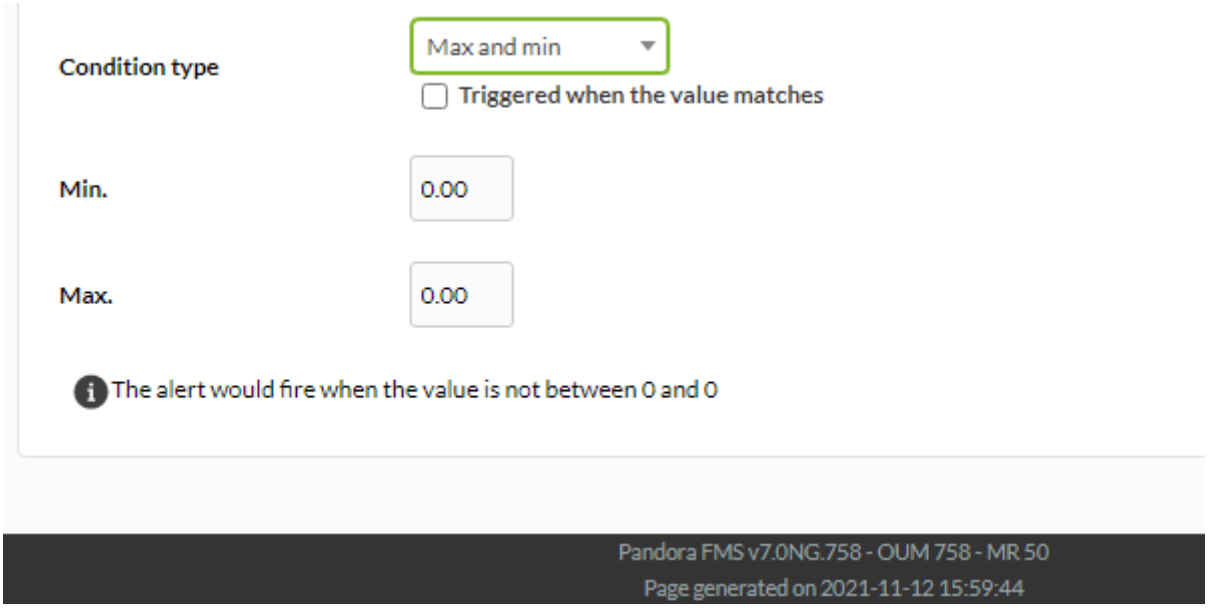


В зависимости от выбранного типа добавляются следующие виды комбинаций:

- Regular Expresion: Используется регулярное выражение. Предупреждение срабатывает, когда значение модуля соответствует заданному условию. При выборе регулярного условия у вас есть возможность установить флажок Triggered when the value matches. Когда вы отметите это флажком, предупреждение будет срабатывать при совпадении значения и наоборот.

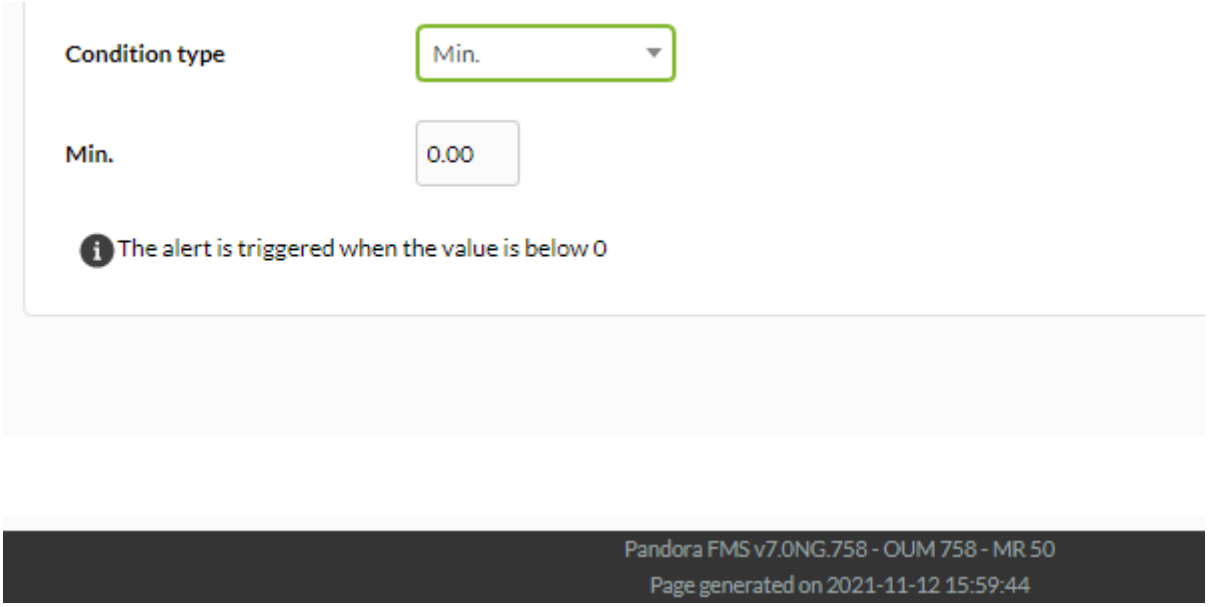


- Max and Min: Числовой интервал ограничен. При выборе флажка Trigger when matches the value предупреждение будет подано, если значение находится в пределах указанного диапазона между максимумом и минимумом, и, если флажок не установлен, предупреждение будет подано, только если значение находится за пределами указанного диапазона.

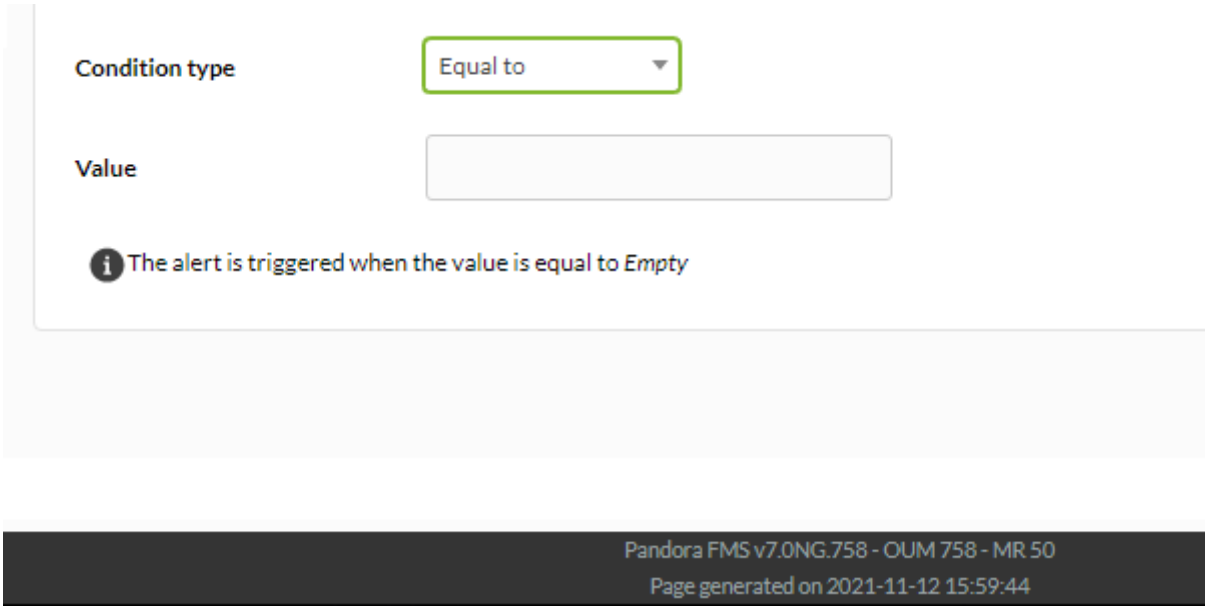


- Max: Используется максимальное значение. Предупреждение срабатывает, когда значение модуля превышает отмеченное максимальное значение.

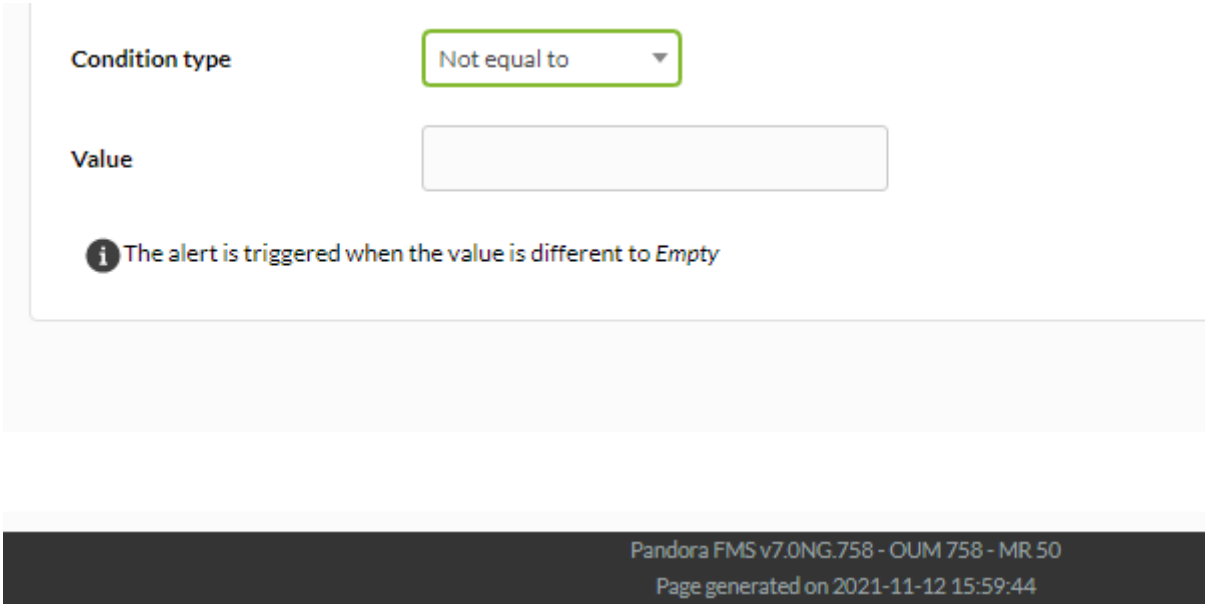
- Min: Используется минимальное значение. Предупреждение срабатывает, когда значение модуля меньше отмеченного минимального значения.



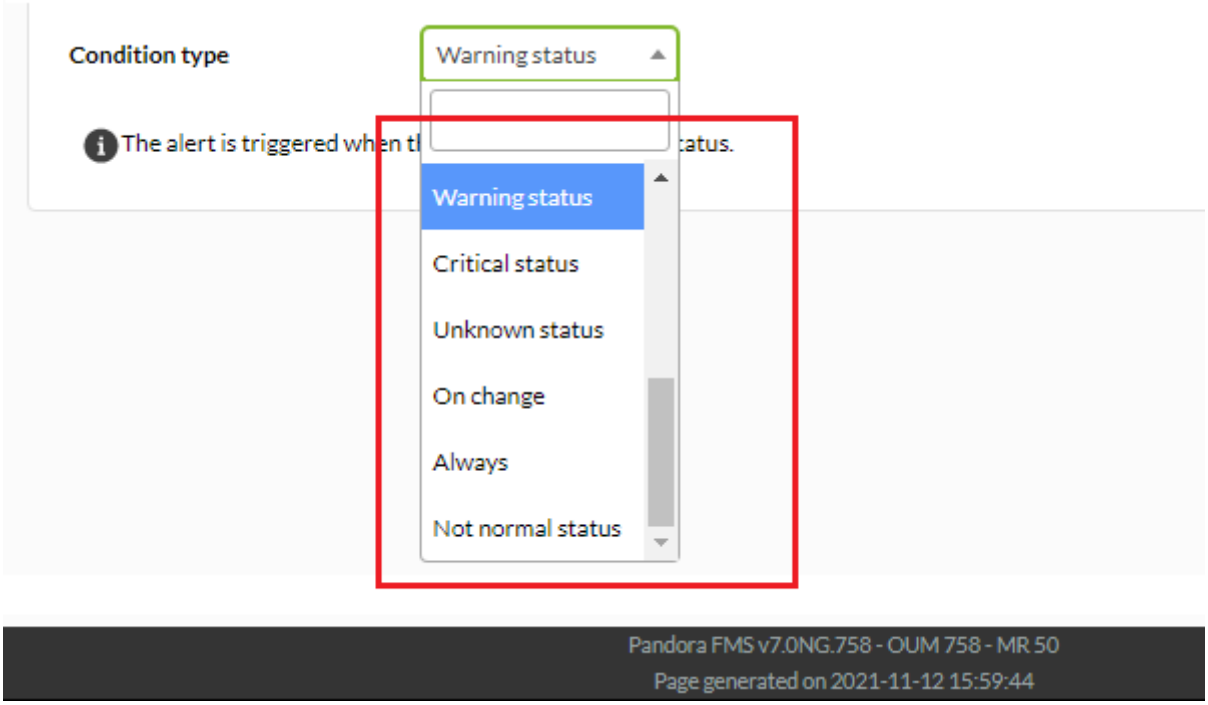
- Equal to: Используется для запуска предупреждения. Когда предоставляется значение, оно должно быть равно полученным данным.



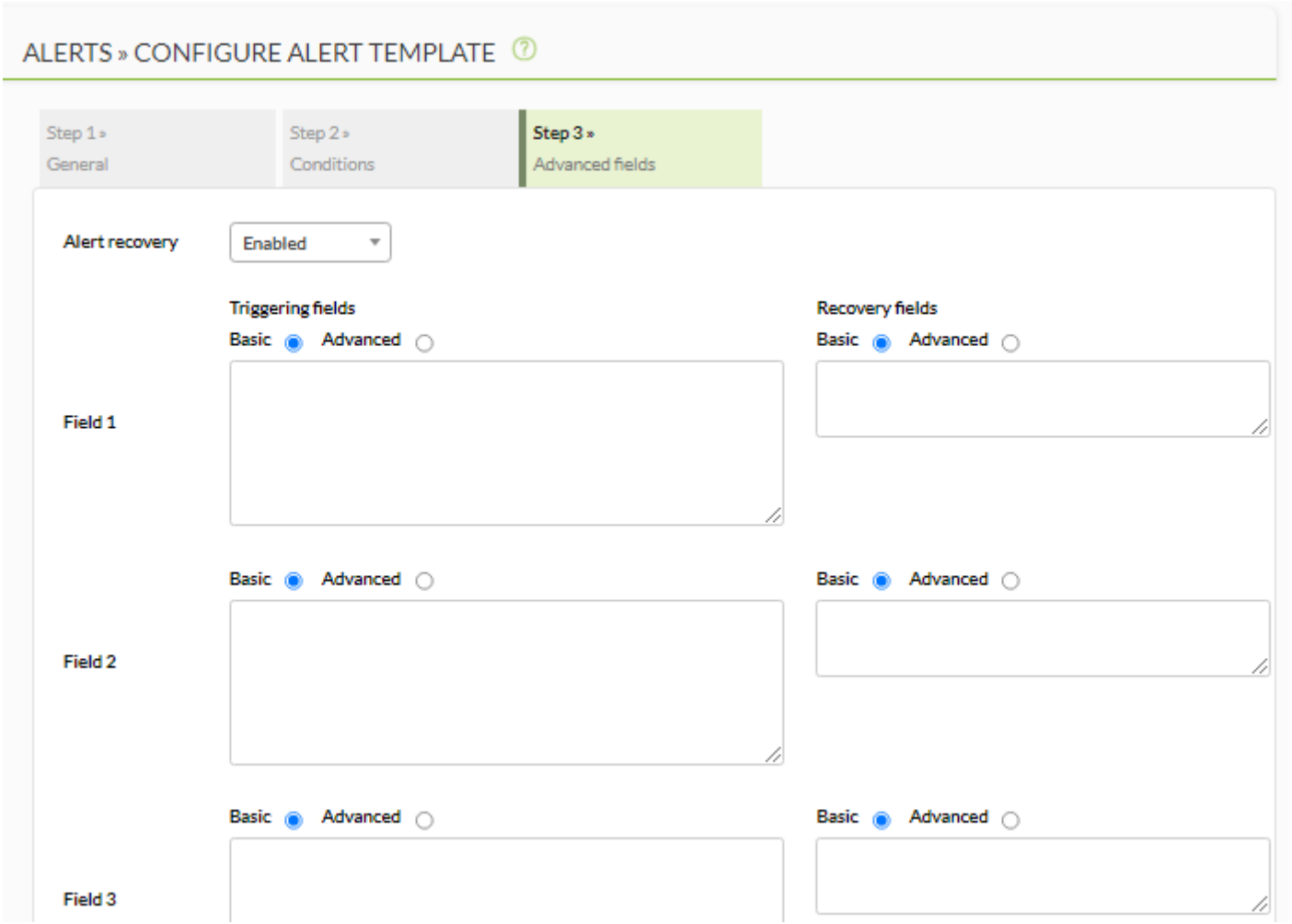
- Not Equal to: То же, что и выше, но отрицание условия (логический оператор NOT).



- Module status: Модуль используется, будь то его статус (Critical status, Warning status, Unknown status, Not normal status), либо изменение его значения (On change, однако снятие флажка подтверждения Triggered when the value matches позволяет выполнять запуск, *если значение остается неизменным*) или просто всегда (Always), если это необходимо.



Шаг 3: Расширенные поля



Alert recovery

Комбинация, где вы можете определить, нужно ли включить возвращение

предупреждений. При включении возвращения предупреждений, когда модуль больше не удовлетворяет условиям, указанным в шаблоне, должно быть выполнено действие, связанное с скриптами, указанными полями *field*, определенными в этой колонке.

Field 1 ~ Field 10

Здесь вы можете использовать ряд макросов, описанных ниже.

При окончании конфигурации закончите ее, нажав на кнопку Finish.

Заменяемые макросы в полях Field1 ~ Field10

Во всех экземплярах полей `field1` ... `field10` как в шаблоне оповещения, так и в команде и в действии) вы можете использовать список макросов, приведенный в конце этой главы, которые представляют собой ключевые слова, заменяемые в момент выполнения на значение, которое меняется в зависимости от времени, значения, Агента, вызывающего предупреждение, и т.д.

Полный пример предупреждения с заменой макроса

Создание записи в LOG, где каждая строка имеет следующий формат:

```
2009-12-24 00:12:00 pandora [CRITICAL] Agent <agent_name> Data <module_data>
Module <module_name> in CRITICAL status
```

Command Configuration

```
echo _timestamp_ pandora _field2_>> _field1_
```

Action Configuration

```
Field1 = /var/log/pandora/pandora_alert.log
Field2 = <Белым>
Field3 = <Белым>
```

Template Configuration

```
Field1 = <Белым>
Field2 = [CRITICAL] Agent _agent_ Data _data_ Module _module_ in CRITICAL status
Field3 = <Белым>
```

В разделе восстановления:

```
Field2 = [RECOVERED] [CRITICAL] Agent _agent_ Data _data_ Module _module_ in
CRITICAL status
Field3 = <Белым>
```

Таким образом, при выполнении предупреждения следующая строка будет помещена в LOG:

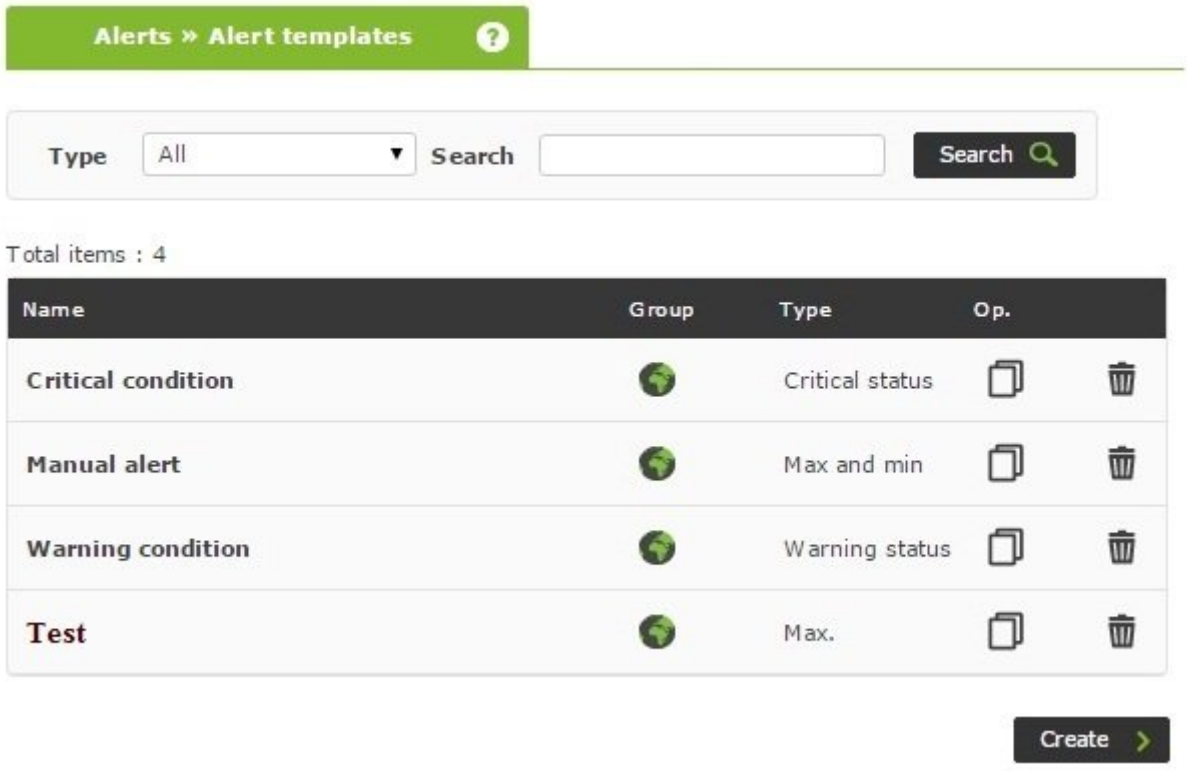
```
2009-10-13 13:37:00 pandora [CRITICAL] Agent raz0r Data 0.00 Module Host Alive
in CRITICAL status
```

И следующая строка для восстановления предупреждения:

```
2009-10-13 13:41:55 pandora [RECOVERED] [CRITICAL] Agent raz0r Data 1.00 Module
Host Alive in CRITICAL status
```

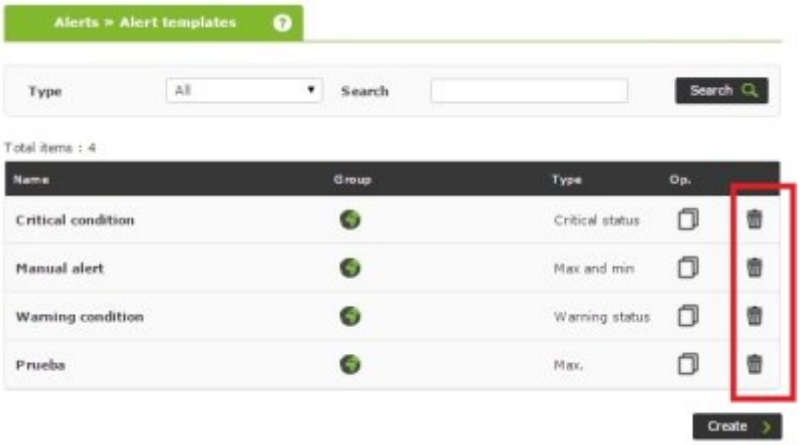
Редактирование шаблона

Перейдите в меню Alerts > Templates и нажмите на имя шаблона для редактирования.



Удалить шаблон

Чтобы удалить шаблон, нажмите на значок серой корзины справа от предупреждения.



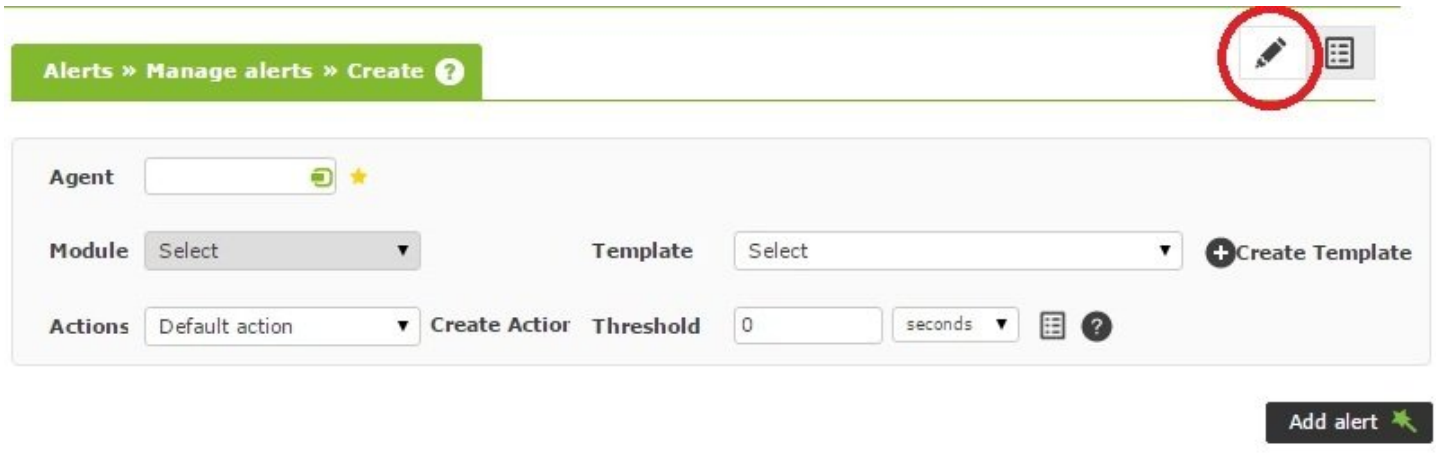
Назначение шаблонов предупреждений модулям

Возможные способы назначения предупреждений модулям обсуждаются в следующих разделах.

Управление предупреждениями из подменю предупреждений

Назначение предупреждений из подменю предупреждений

Vaya a Alerts > List of alerts. В этом разделе вы можете создать новые предупреждения, нажав на значок карандаша (*Builder alert*), перейти к настройке полей:



Agent

Автозаполнение для выбора агента

Module

Список модулей ранее выбранного Агента.

Actions

Действие, которое будет выполнено при срабатывании предупреждения. Если шаблон уже имеет действие по умолчанию, его можно оставить установленным на Default.

Template

Шаблон, содержащий условия срабатывания предупреждения.

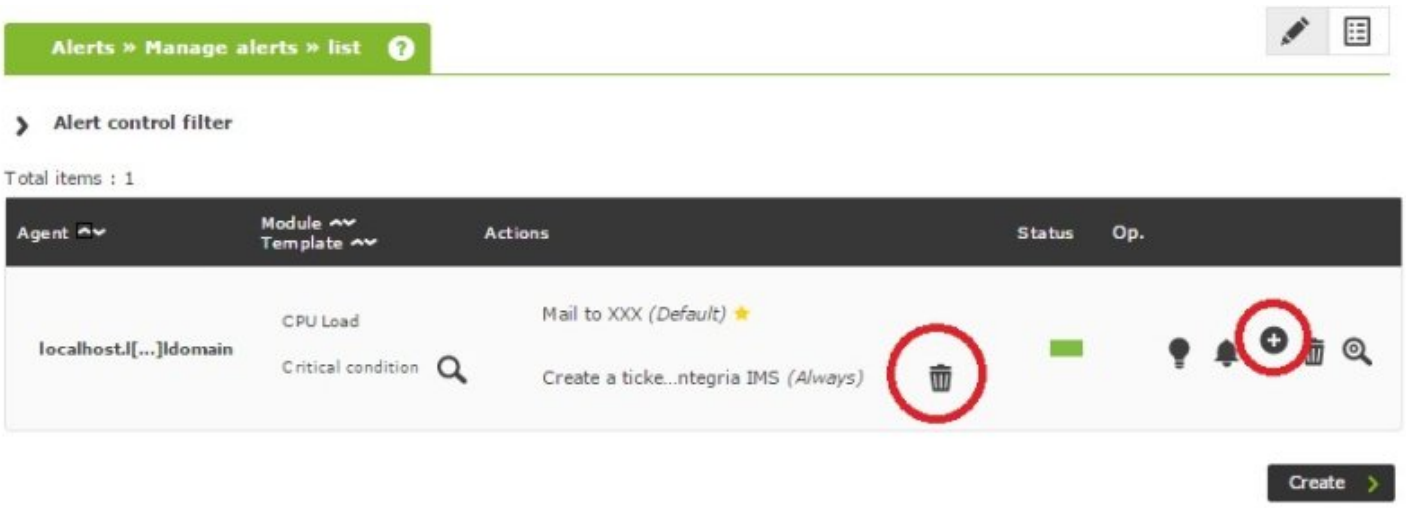
Threshold

Действие предупреждения не должно выполняться чаще, чем раз в `action_threshold` секунд, независимо от количества срабатываний предупреждения.

Изменение предупреждений из подменю предупреждения

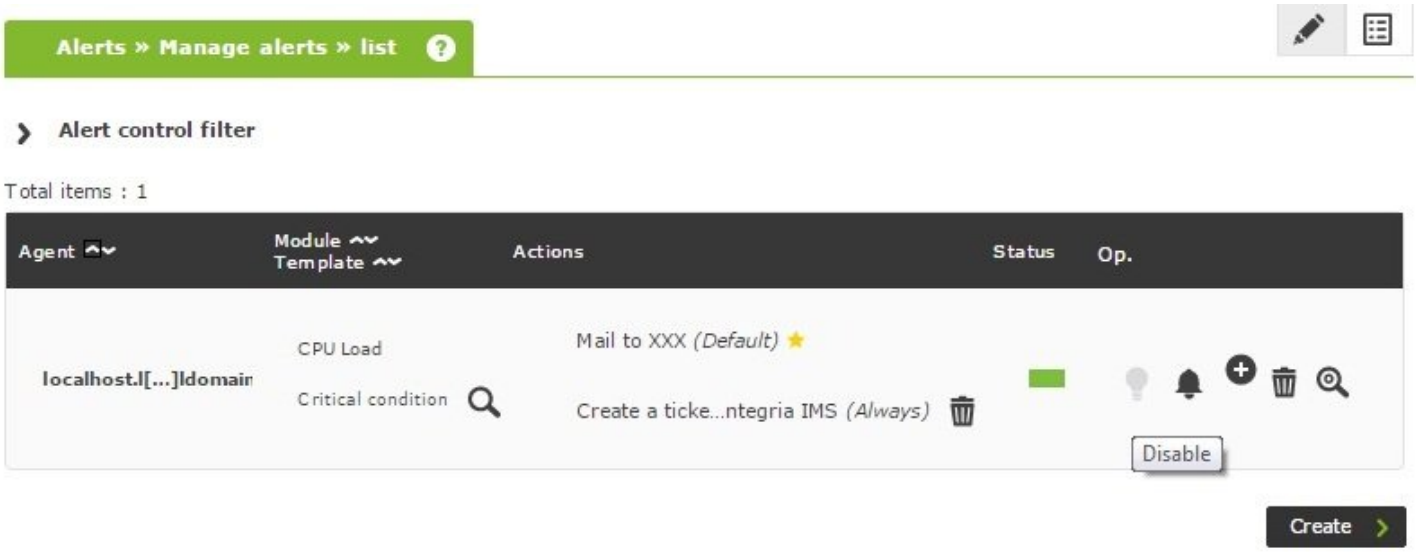
После создания предупреждения можно будет изменить только те действия, которые были добавлены к действию в шаблоне.

Также можно отменить действие, которое было выбрано при создании предупреждения, нажав на значок серой корзины справа от действия, или добавить новые действия, нажав на кнопку «Добавить».



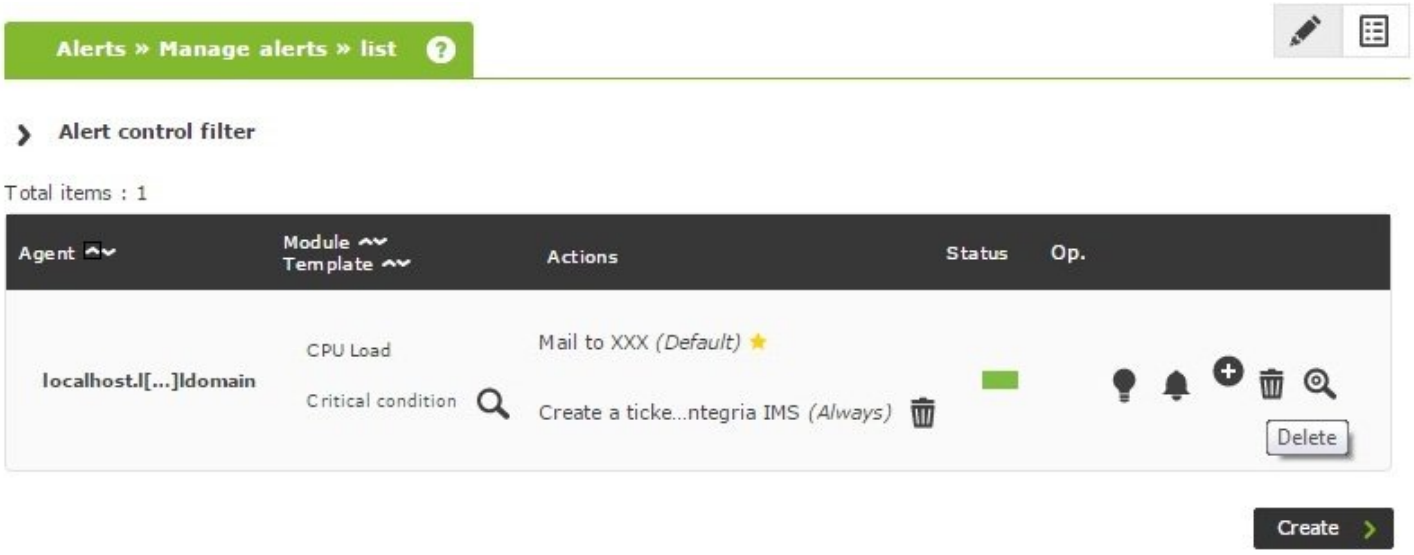
Отключение предупреждений из подменю предупреждения

После создания предупреждения его можно деактивировать, нажав на значок лампочки справа от имени предупреждения



Удалить предупреждение из подменю предупреждения

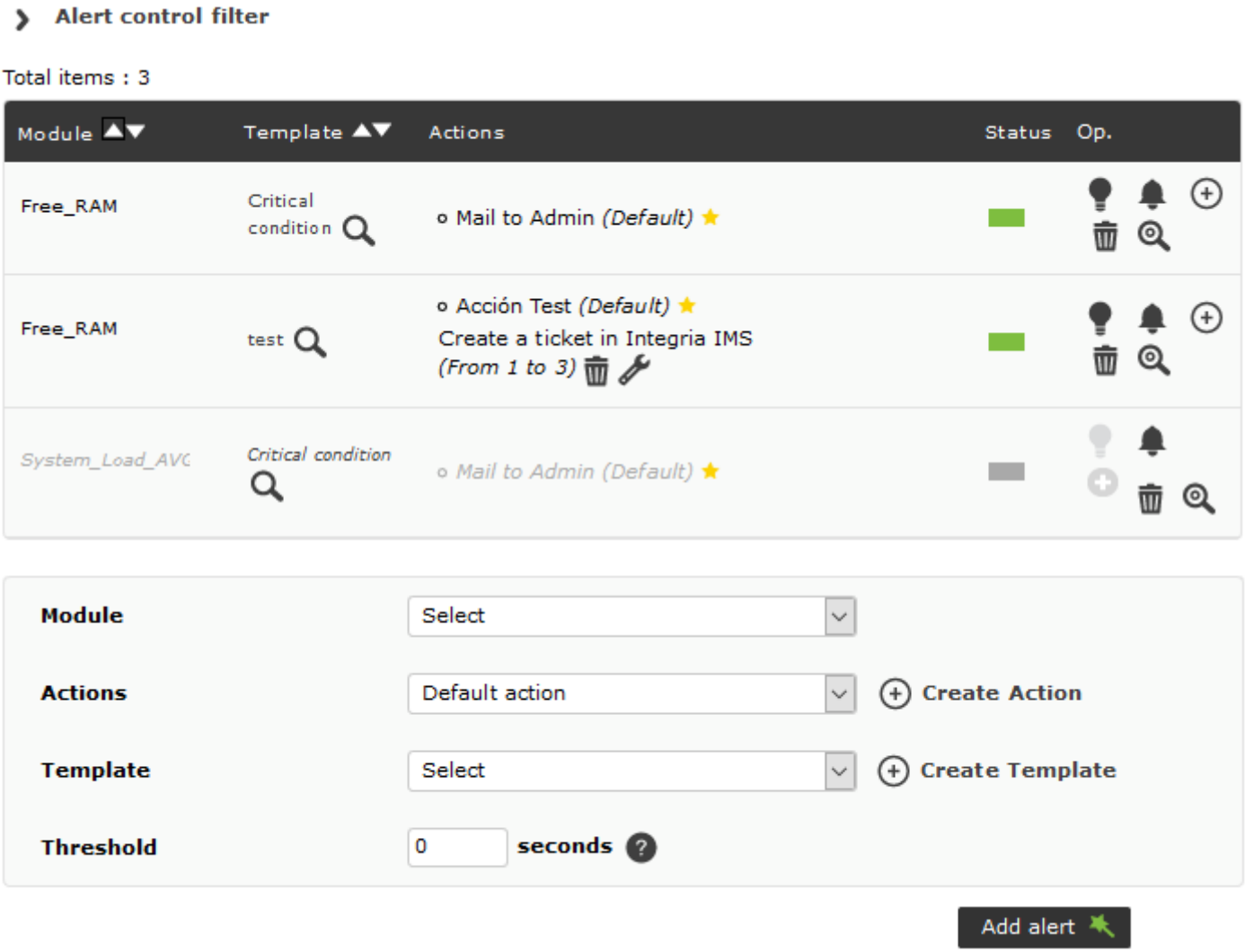
Любое предупреждение можно удалить, нажав на корзину справа от предупреждения.



Управление предупреждениями от агента

Назначение предупреждений от агента

В разделе администрирования агента вы можете добавить новые предупреждения, перейдя на соответствующую вкладку:



Module

Список модулей агента.

Actions

Действие, которое будет выполнено при срабатывании предупреждения. Если шаблон уже имеет действие по умолчанию, его можно оставить установленным на Default.

Template

Шаблон, содержащий условия срабатывания предупреждения.

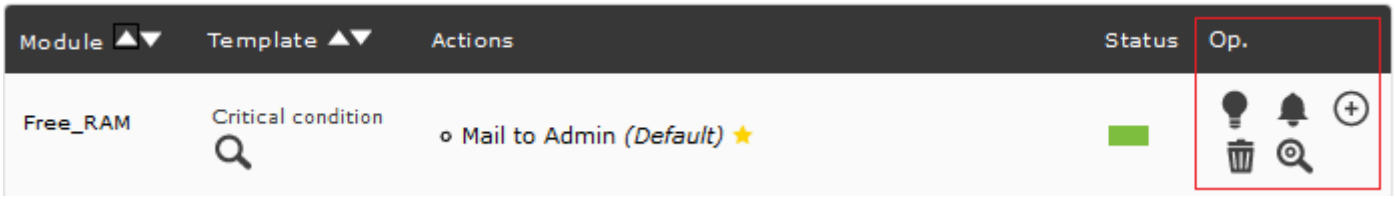
Threshold

Действие предупреждения не должно выполняться чаще, чем раз в `action_threshold` секунд, независимо от количества срабатываний предупреждения.

Изменение предупреждений из агента

После создания предупреждения можно изменять только те действия, которые были добавлены к действию в шаблоне.

Можно удалить действие, которое было выбрано для создания предупреждения, нажав на значок корзины справа от действия, или добавить новые действия, нажав на кнопку «Добавить».



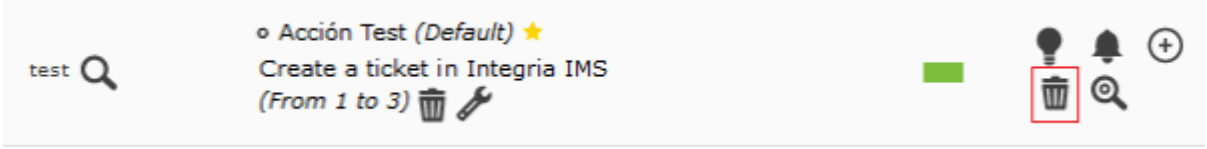
Деактивировать предупреждения от Агента

После создания предупреждения его можно будет деактивировать, нажав на значок лампочки справа от названия предупреждения.

На изображении примера второе предупреждение отключено (обратите внимание, что цвет шрифта и значок отключенного предупреждения светло-серый).

Удаление предупреждений из агента

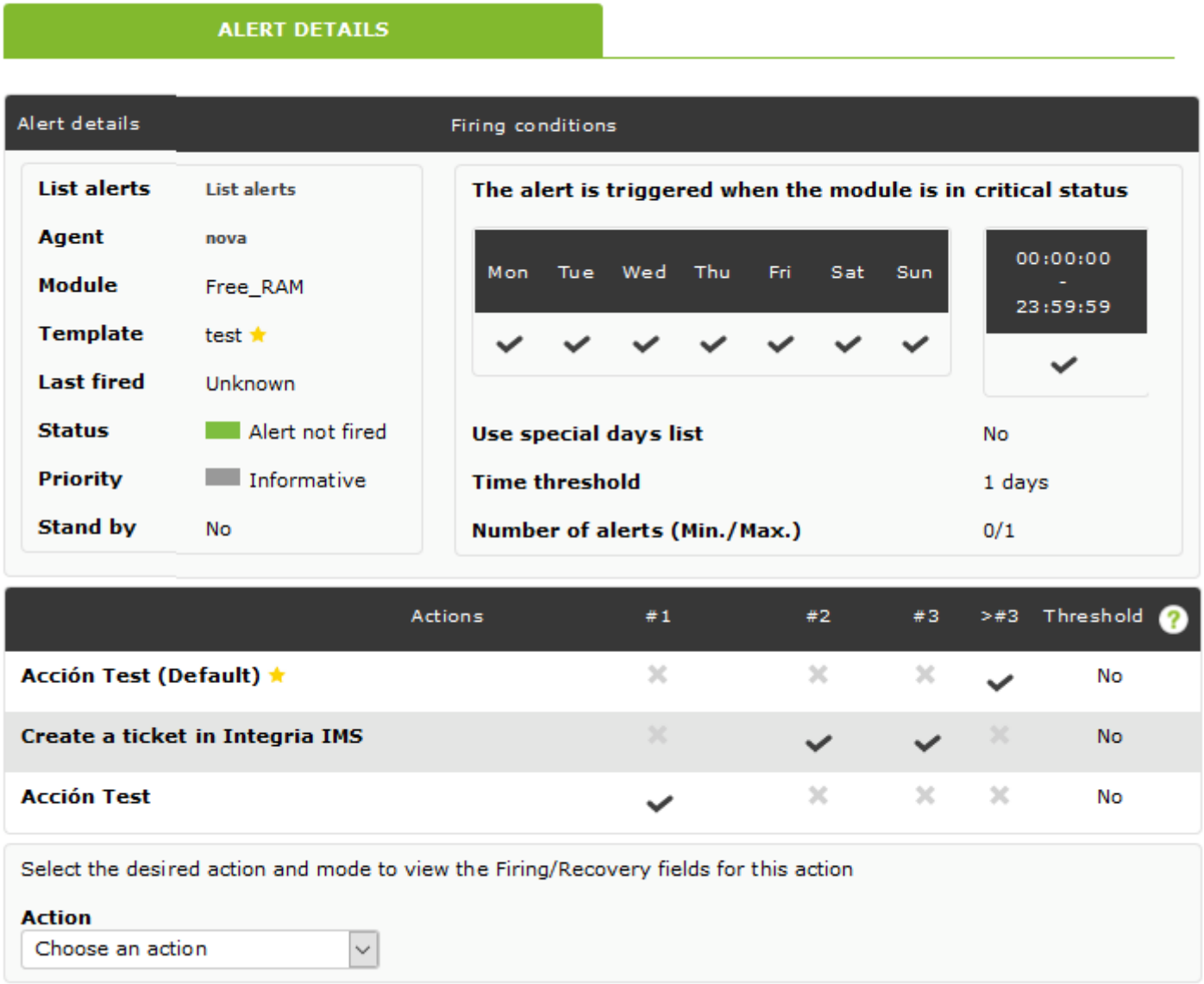
Можно удалить любое предупреждение, нажав на значок корзины справа от предупреждения.



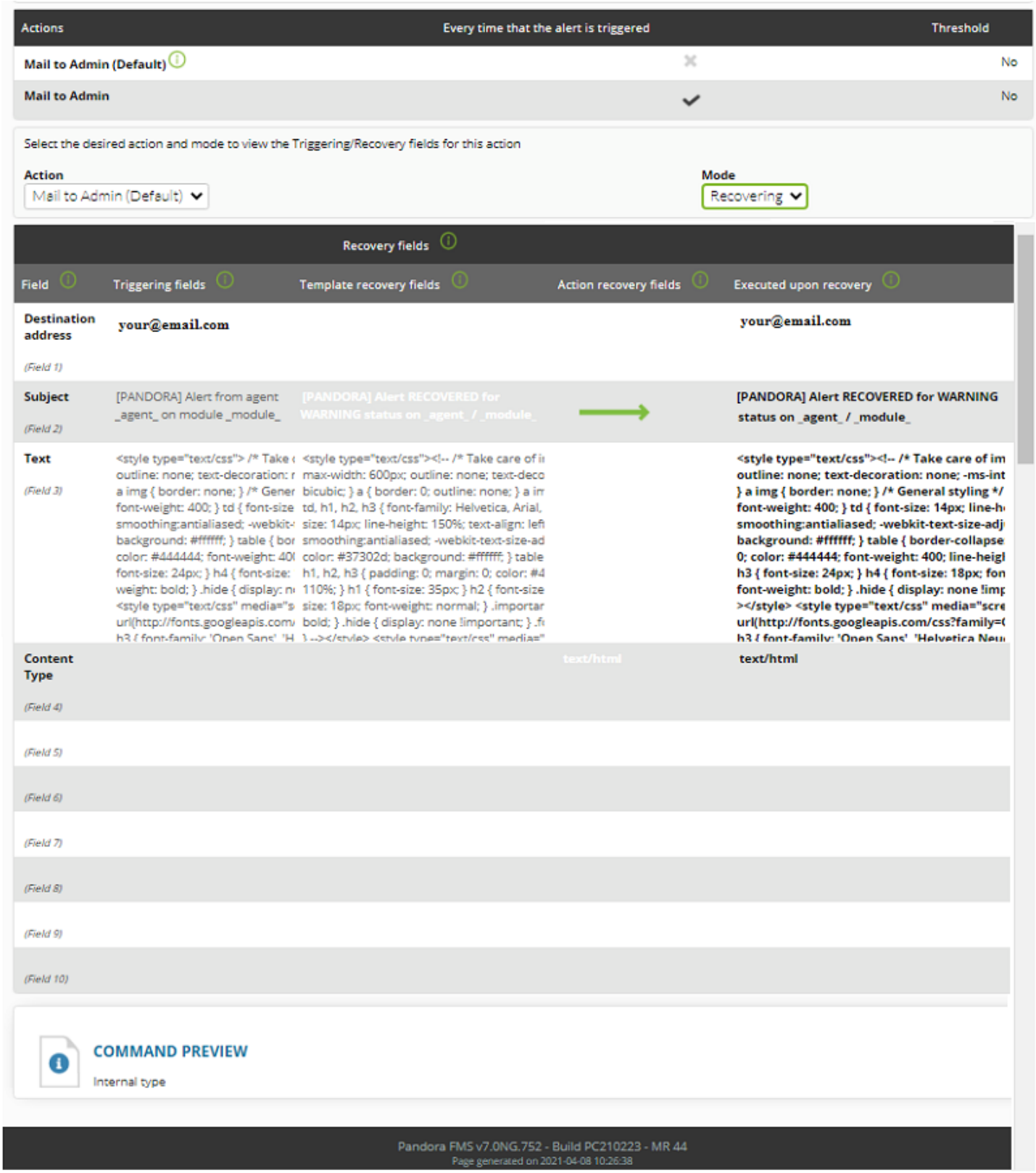
Детали предупреждений

Нажав на значок лупы на панели параметров предупреждений, можно перейти на страницу сводки действующих настроек предупреждений.

На этом экране вы можете подтвердить все настройки, выбранные для предупреждения:



Выберите конкретное действие из раскрывающегося списка действий, чтобы увидеть пример конечной команды:

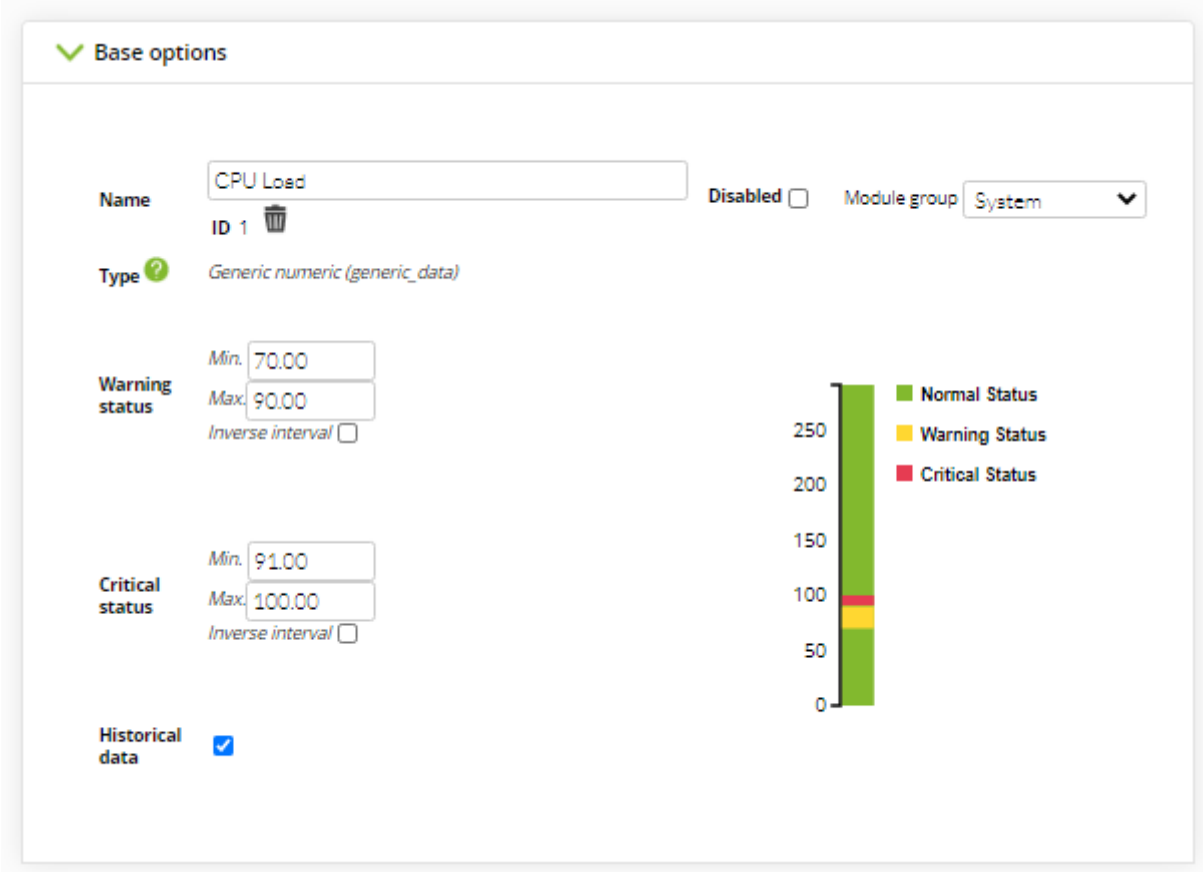


Обзор предупреждения

Определение порога

Для модуля под названием CPU Load определены критический и предупреждающий пороги.

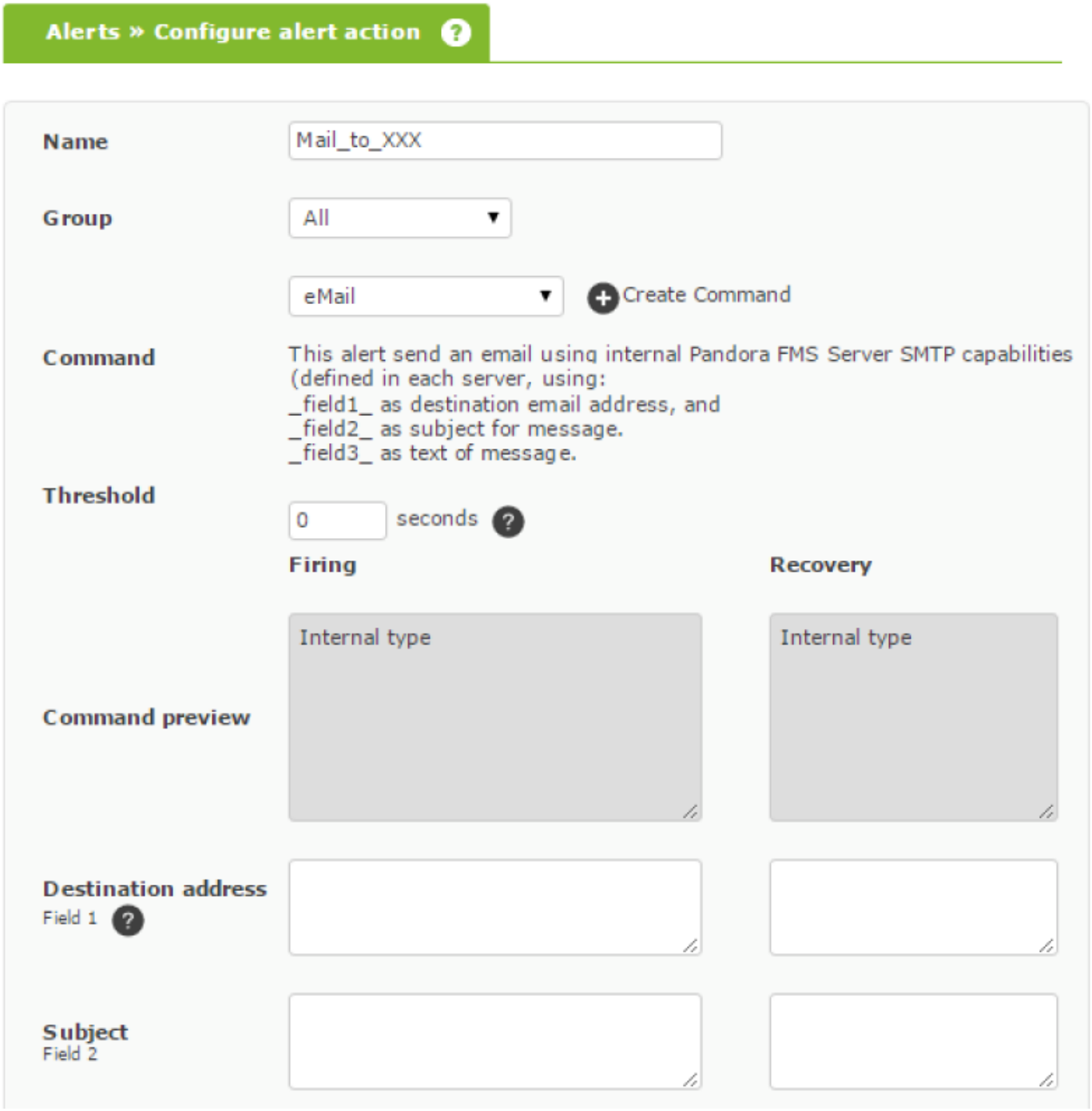
Зайдите в форму редактирования модуля, чтобы установить следующие пороговые значения:



Мы принимаем и сохраняем модификацию. Теперь, когда значение модуля *CPU Load* находится между 70 и 90, его статус становится WARNING, а между 91 и 100 он становится CRITICAL, отображая свой статус красным цветом:

Настройка действия

Чтобы создать действие, состоящее в отправке электронного письма оператору, войдите в меню Alerts > Actions и нажмите на кнопку создания нового действия Create:

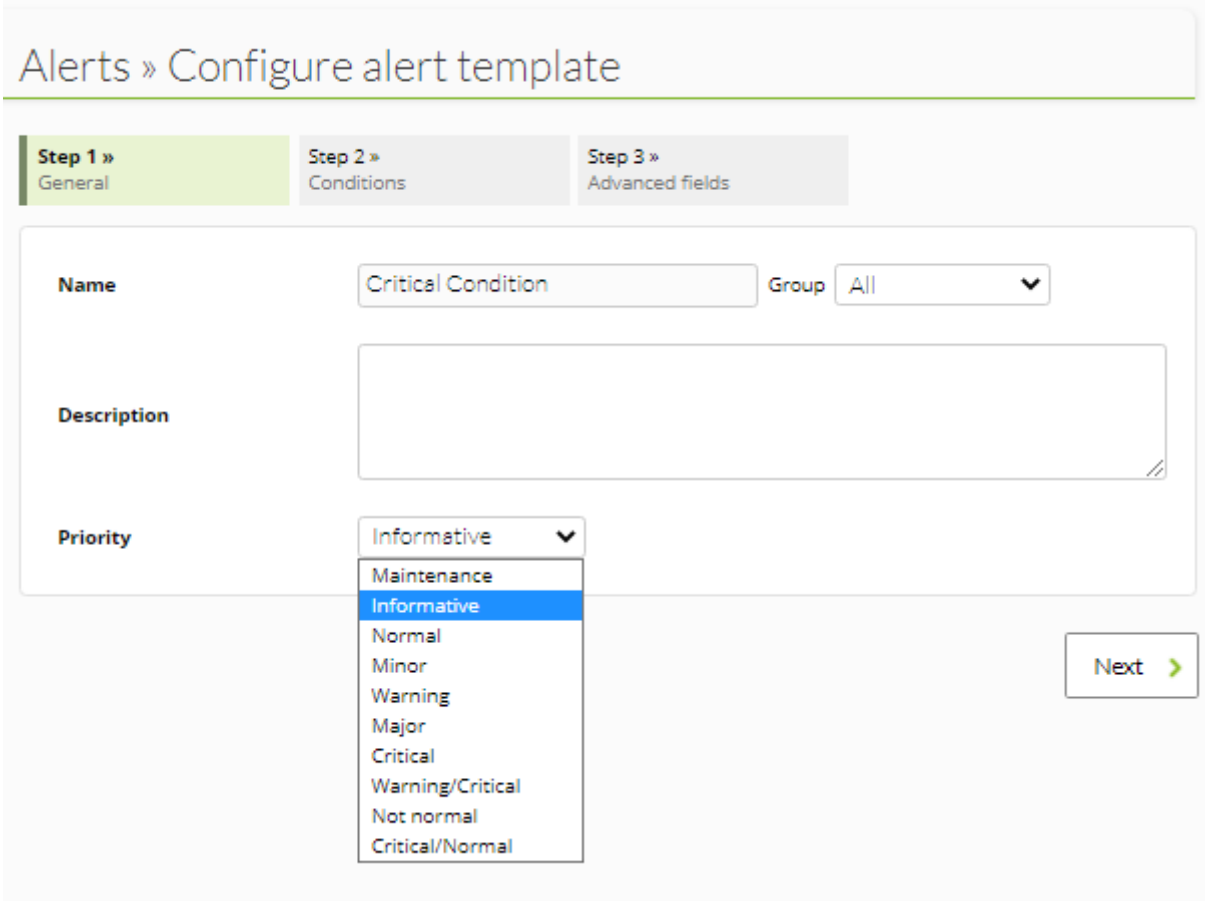


Это действие будет использовать команду eMail, а его поля `Field 1`, `Field 2` и `Field 3` соответствуют адресу назначения, теме письма и телу сообщения.

Настройка шаблона

Чтобы создать общий шаблон предупреждения для любого модуля в критическом состоянии (его действие по умолчанию будет заключаться в уведомлении по электронной почте группы операторов), необходимо зайти в раздел *Templates*.

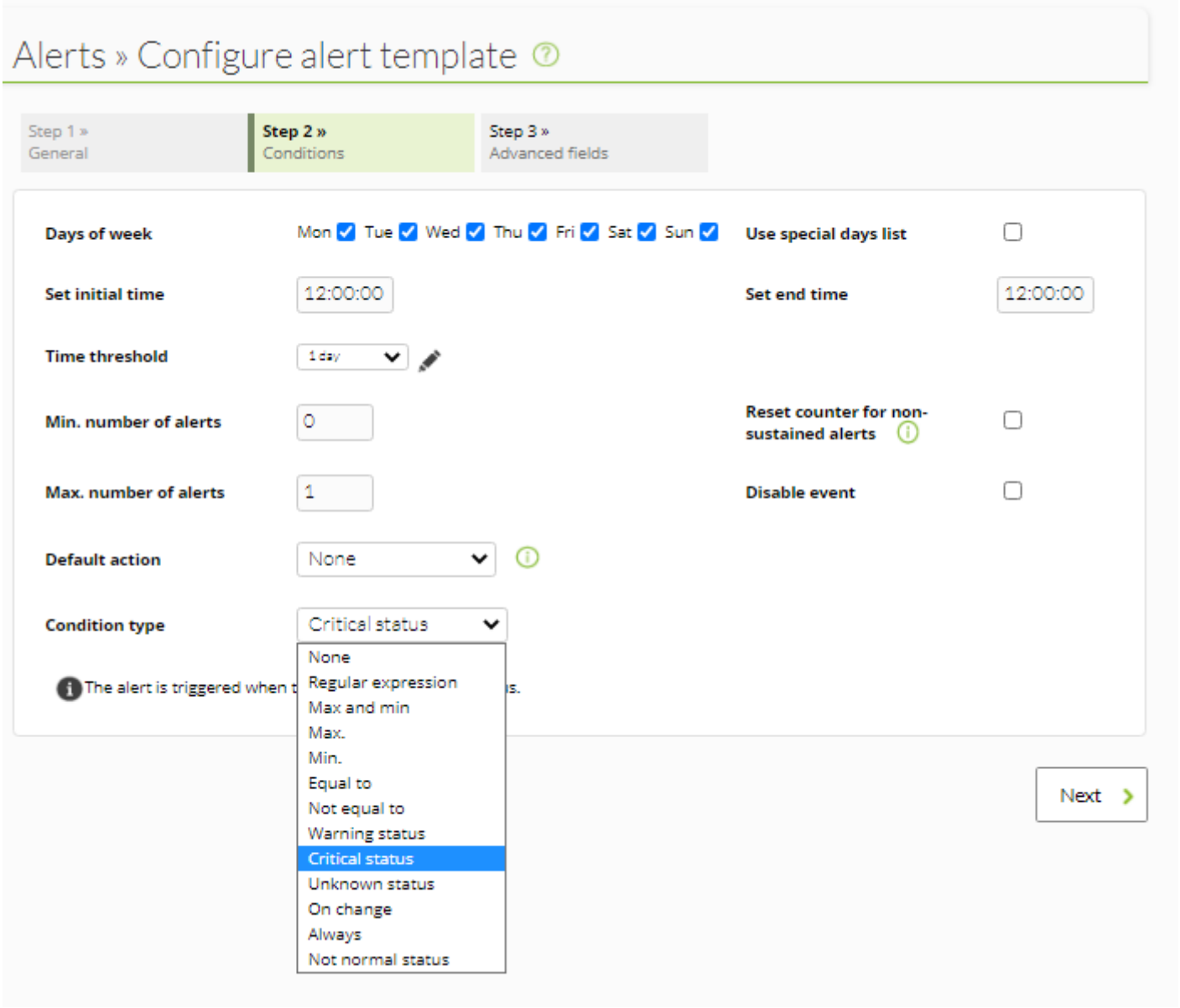
Шаг 1:



Определенный здесь приоритет (Informative) будет использоваться для отображения события определенным цветом при срабатывании предупреждения.

В шаге 2 необходимо задать параметры, определяющие конкретные условия срабатывания, например, состояние, в котором должен находиться модуль, или временные интервалы, в которых будет работать шаблон.

Шаг 2:



Condition Type

Определяет, вызвано ли предупреждение изменением состояния, изменением значения и т.д. Это самый важный параметр для того, чтобы предупреждение функционировало должным образом. В этом примере используется условие Critical status, чтобы предупреждение срабатывало, когда модуль находится в критическом состоянии.

Default Action

(Необязательно) действие по умолчанию, выполняемое при срабатывании предупреждения.

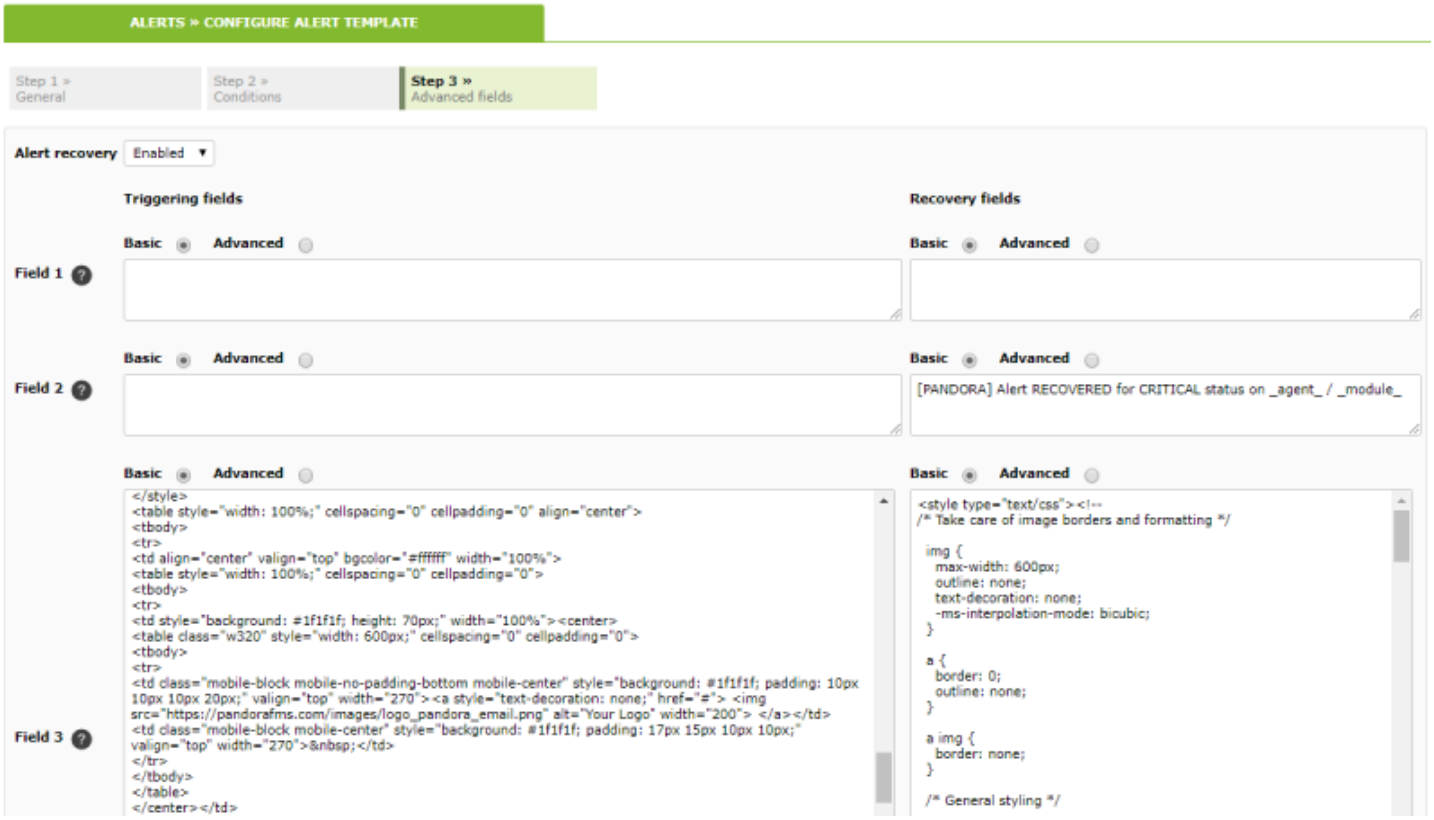
Time Threshold

Время, в течение которого предупреждение не должно повторяться, если неправильное состояние сохраняется постоянно. Например, если установлено значение один день (24 часа), то предупреждение будет отправляться только раз в 24 часа, даже если модуль будет находиться в неправильном состоянии дольше.

Min, Max

Количество предупреждений, минимальное и максимальное количество раз, когда условие (в данном случае, что модуль находится в состоянии `critical`) должно быть задано, прежде чем Pandora FMS выполнит действия, связанные с шаблоном предупреждения. При минимальном значении, равном нулю (0), при первой неисправности модуля сработает предупреждение.

Шаг 3:

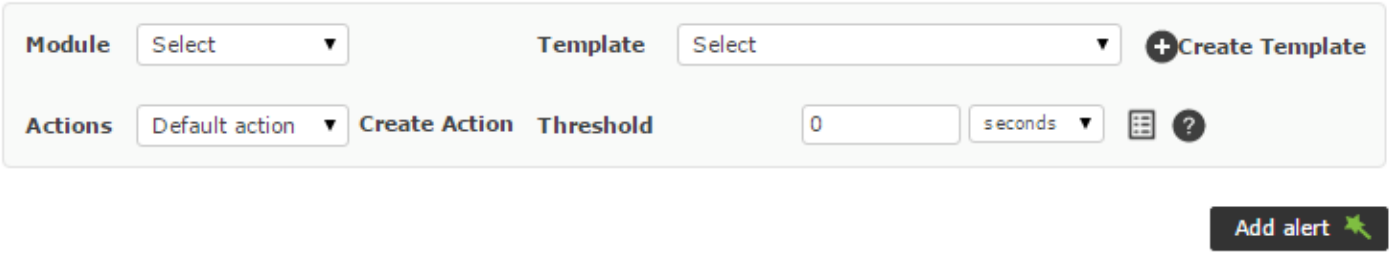


Третья секция включает поля `Field1`, `Field2`, `Field3` и т.д., описанные в предыдущих разделах: они служат для передачи параметров из шаблона в действие и из действия в команду.

Кроме того, в этом разделе можно включить или отключить восстановление предупреждения, которое заключается в выполнении другого действия, когда проблемная ситуация возвращается в нормальное состояние.

Привязка предупреждения к модулю

После того как все необходимые ресурсы собраны, вам остается только связать шаблон предупреждения с модулем. Для этого перейдите на вкладку предупреждений в агенте, где находится модуль:

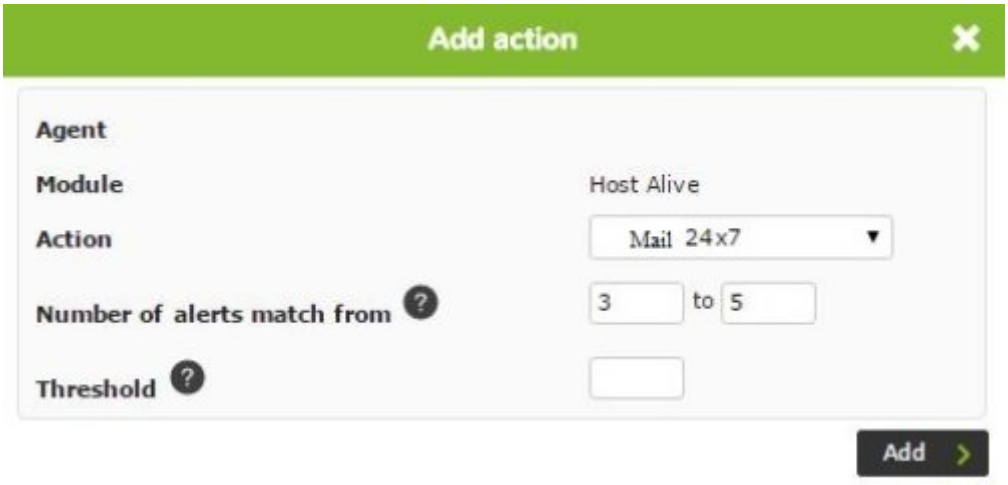


Таким образом, создание ассоциации между модулем `cpu_user` и шаблоном предупреждения Critical condition завершено. По умолчанию он отобразит действие, определенное в этом шаблоне «*Отправить письмо на XXX*».

Эскалация предупреждений

Эскалация предупреждений - это дополнительные действия, которые выполняются, если предупреждение повторяется определенное количество раз подряд (сначала вы должны связать полное предупреждение с Модулем, как объяснялось в предыдущих разделах).

Вам нужно только добавить дополнительные действия и определить, между какими последовательными повторениями оповещения вы будете выполнять это действие. Пример:



При восстановлении предупреждения все действия, которые были выполнены до этого момента, будут выполнены повторно, а не только те, которые соответствуют текущей конфигурации Number of alerts match from.

Дополнительно можно установить порог (Threshold) в качестве второго параметра, с помощью которого предупреждение не сможет сработать более одного раза в течение этого интервала.

Отправка предупреждающих сообщений через систему мгновенного обмена сообщениями

1. Telegram - это платформа мгновенного обмена сообщениями, через которую можно получать предупреждающие сообщения от Pandora FMS. Вы можете узнать больше из обучающего видеоролика «Предупреждения в Telegram: интеграция с Pandora FMS». В этом обучающем видеоролике вы сможете попрактиковаться в создании и настройке всех компонентов предупреждения PFMS в управляемом режиме (начиная с третьей минуты).

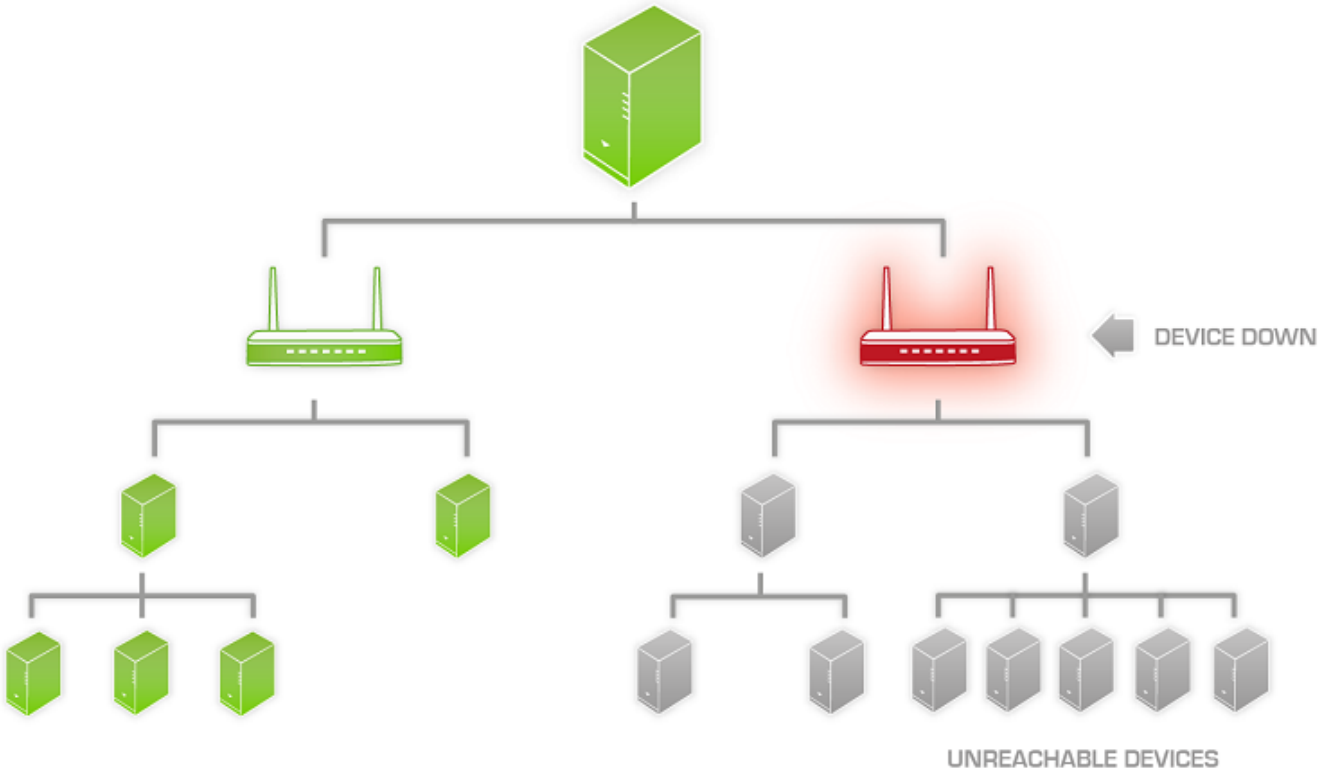
Предупреждение в режиме Standby

Предупреждения могут быть включены, выключены или находиться в режиме ожидания (*standby*). Разница между отключенными предупреждениями и предупреждениями в режиме *standby* заключается в том, что отключенные предупреждения просто не будут работать и поэтому не будут отображаться при просмотре предупреждений. Вместо этого предупреждения в режиме *standby* будут отображаться при просмотре предупреждений и будут работать но только на уровне визуализации. То есть, они будут показывать, сработали предупреждения или нет, *но не будут выполнять запрограммированные действия или генерировать события*.

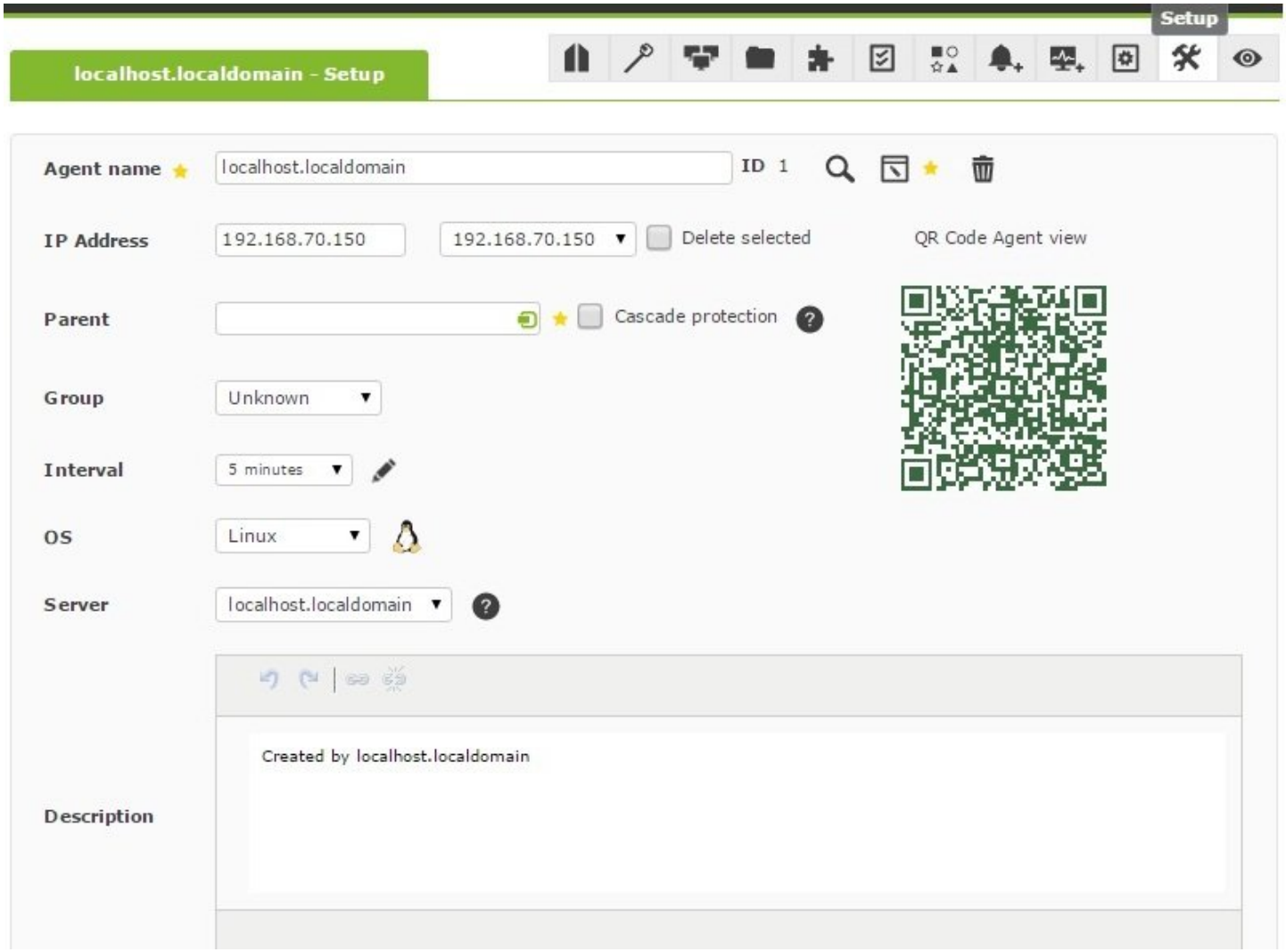
Предупреждения в режиме *standby* полезны, чтобы иметь возможность просматривать их, не мешая другим аспектам.

Каскадная защита

Каскадная защита - это функция Pandora FMS, которая позволяет избежать массированной бомбардировки предупреждениями, когда группа Агентов недоступна из-за отказа основного соединения. Это происходит, когда промежуточный элемент сети, такой как *маршрутизатор* или *коммутатор*, выходит из строя и оставляет большую часть сети, управляемой Pandora FMS, недоступной. Поскольку в этом сценарии проверка сети не сработает, предупреждения об отключенных устройствах начнут срабатывать, не соответствуя действительности.



Каскадная защита активируется из конфигурации агента. Нажмите на опцию Cascade protection.



Для того чтобы агент с активированной каскадной защитой работал, родительский агент, от которого он зависит, должен быть правильно настроен. *Если у родительского агента в настоящее время сработало какое-либо предупреждение о модуле в критическом состоянии, нижестоящий агент с каскадной защитой не будет выполнять свои предупреждения.*. Это не относится к предупреждениям модулей в статусе `warning` или `unknown`.

Примеры

У нас есть следующие Агенты:

- Router: модуль ICMP check и модуль SNMP check, использующие стандартный OID для проверки состояния порта ATM. Вы также можете проверить задержку до *маршрутизатора* вашего провайдера./li>
- Web server: Он имеет несколько модулей, выполняемых агентом: проверка процессов CPU, памяти, Apache. Он также имеет четырехступенчатую проверку WEB-задержки.
- Database server: Он состоит из нескольких модулей, выполняемых агентом: проверка процессов CPU, памяти, MySQL. Он также имеет некоторые дополнительные проверки целостности базы данных. В нем также есть проверка удаленного подключения к другой базе данных с помощью специального *плагина*, который аутентифицируется (*login*), делает запрос (*query*) и выходит, измеряя общее затраченное время.

В WEB SERVER и DATABASE SERVER мы определяем ROUTER в качестве родителя. Активируйте флажок *cascade protection* в WEBSERVER и DATABASE SERVER.

В этом сценарии вы можете определить несколько предупреждений:

- ROUTER

SNMP Check / CRITICAL → Action, send MAIL. Latency > 200ms / WARNING → Action, send MAIL.

- WEB SERVER

CPU / WARNING MEM / WARNING PROCESS / CRITICAL → Action, send MAIL. HTTP LATENCY / CRITICAL → Action, send MAIL.

- DATABASE SERVER

CPU / WARNING MEM / WARNING PROCESS / CRITICAL → Action, send MAIL. SQL LATENCY / CRITICAL > Action, send MAIL.

Если соединение ROUTER, через которое Pandora FMS подключается к WEB SERVER и DATABASE, не работает:

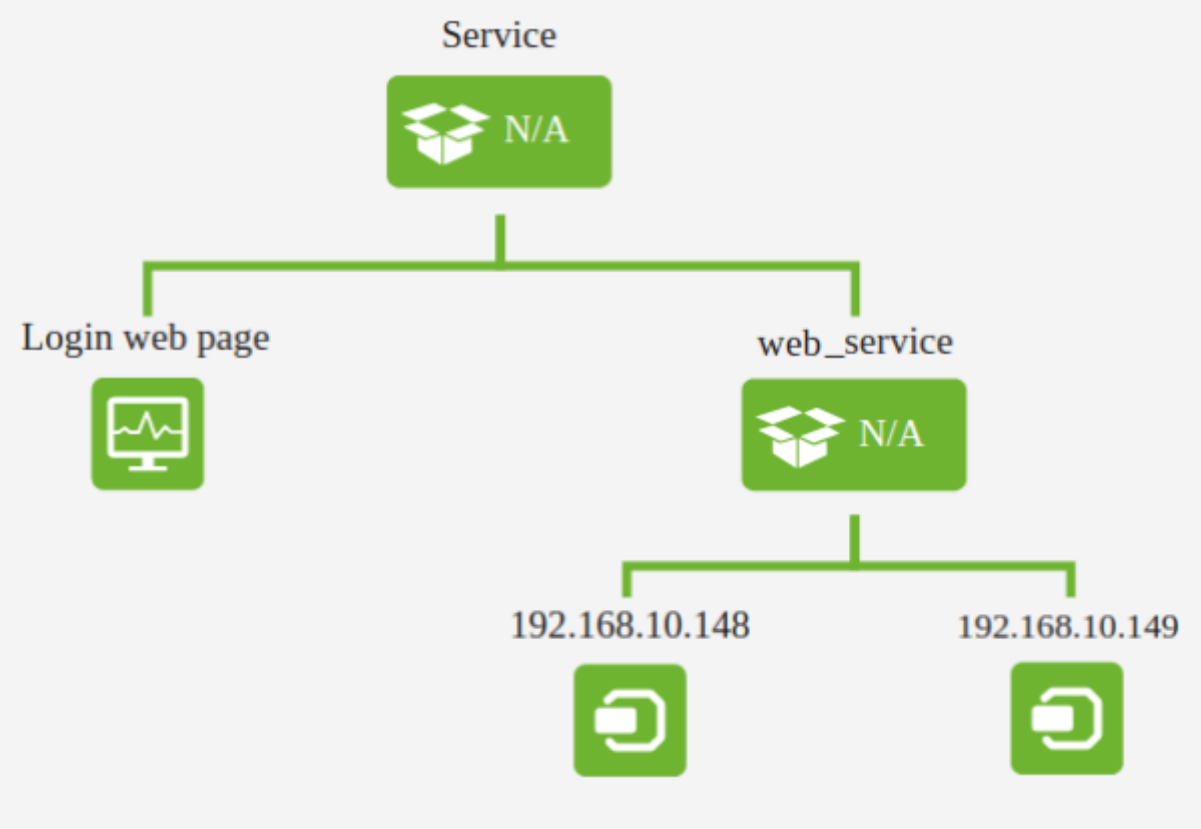
- Не активируя каскадную защиту, вы будете получать шесть предупреждений, которые умножаются на количество серверов (представьте, например, 200). Этот эффект известен как «шторм событий»; в худшем случае он может вывести из строя ваш почтовый сервер, сервер мониторинга и ваш собственный мобильный телефон, наводнив каждый из них сотнями (или даже тысячами) сообщений.
- При включенной каскадной защите вы получите только одно предупреждение, указывающее на то, что интерфейс ATM ROUTER вышел из строя. Однако элементы WEBSERVER и DATABASE SERVER будут отображаться красным цветом, но соответствующие им предупреждения не будут приходить.

Каскадная защита на основе услуг

Версия NG 727 или выше.

Возможно использование служб, чтобы предотвратить поступление предупреждений из нескольких источников, сообщающих об одном и том же инциденте.

Если вы включите каскадную защиту на основе служб, элементы службы (Агенты, Модули или другие сервисы) не будут сообщать о проблемах, но сама служба будет предупреждать от имени пострадавшего элемента.

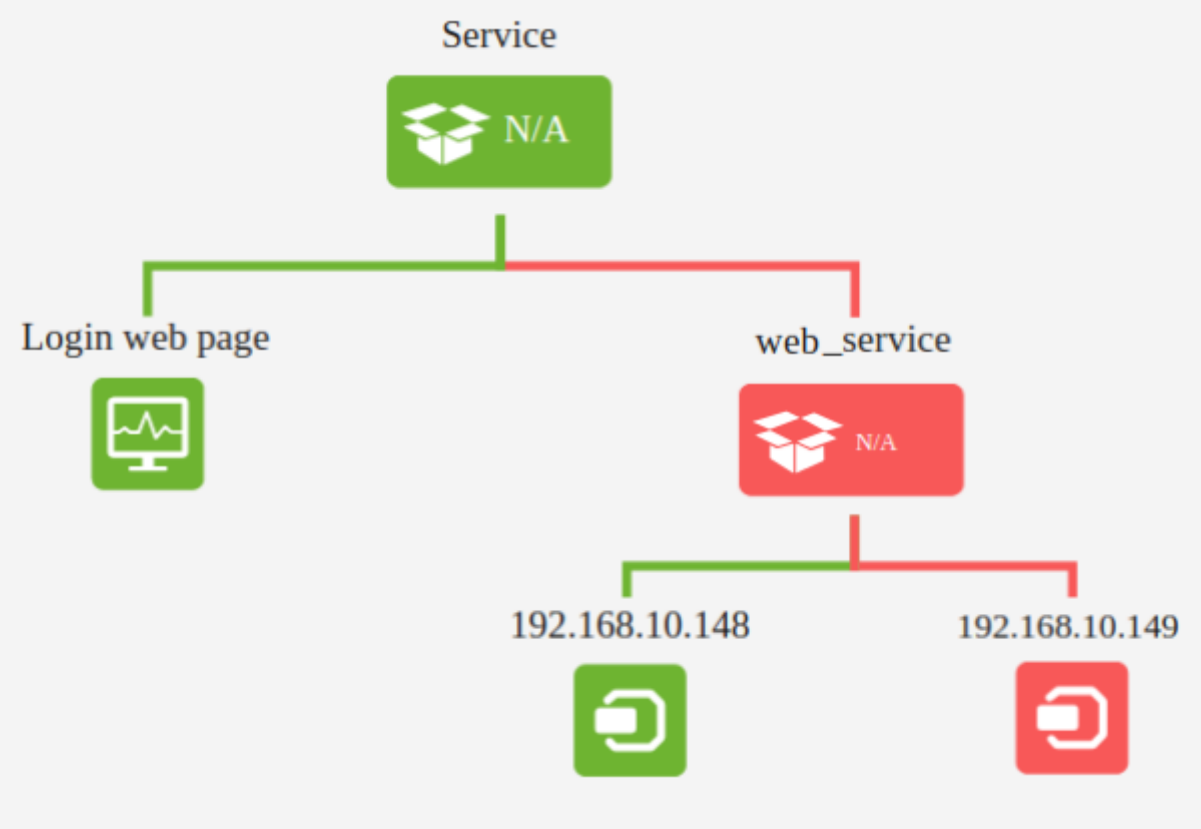


Если элемент `192.168.10.149` станет критическим, не влияя на остальную часть службы, оператор получит предупреждение о том, что `192.168.10.149` не работает, но служба функционирует нормально.

Чтобы получить эту информацию, необходимо отредактировать или создать новый шаблон оповещения, используя макрос `_rca_` для анализа первопричины (*root cause analysis*).

```
_rca_
```

Этот макрос должен предоставить оператору информацию о 'пути', затронутом в сервисе.



Например, значение макроса `_rca_`, соответствующее статусу службы на изображении, будет:

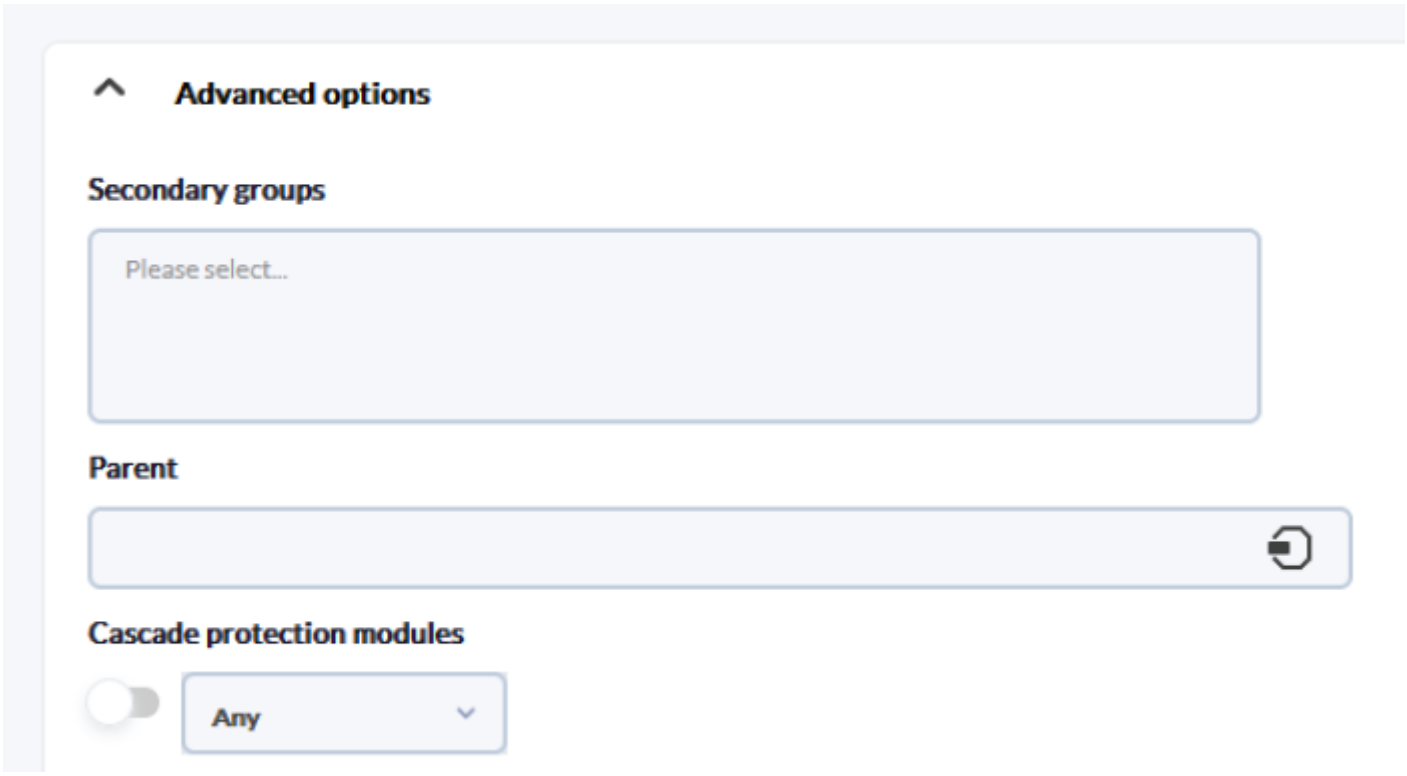
```
[Service -> web_service -> 192.168.10.149]
```

Хотя статус службы будет правильным, так как он не превышает 50% компонентов в критическом состоянии (подробнее об этом можно узнать в разделе Сервисы).

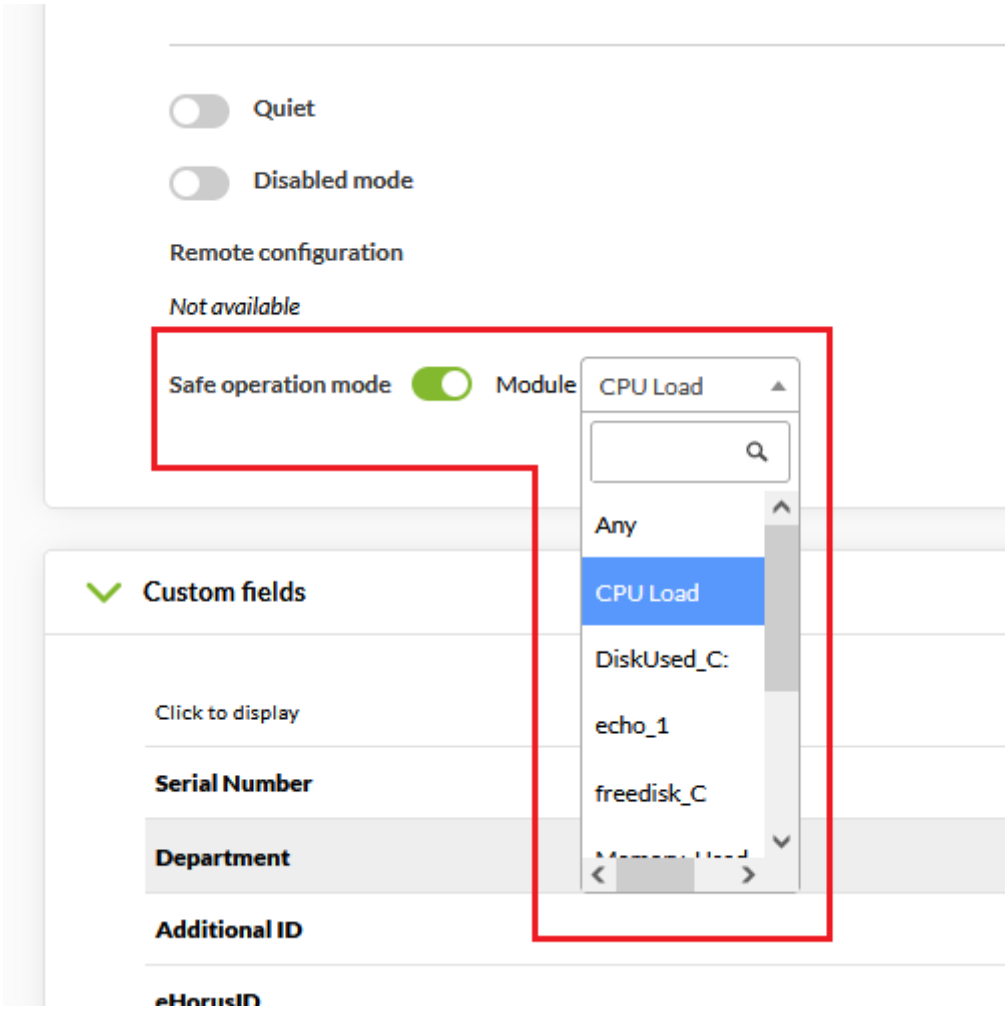
Наблюдение: Цепочка событий, изображенная в анализе первопричины, представляет элементы, находящиеся в критическом состоянии в рамках службы, позволяя увидеть, какие элементы влияют на эту службу.

Каскадная защита на основе модулей

Вы можете использовать статус модуля родительского агента, чтобы запретить ему отправлять предупреждения агентам в случае, если он станет критическим.



Безопасный режим работы



Безопасный режим работы можно включить в расширенных параметрах конфигурации

агента.

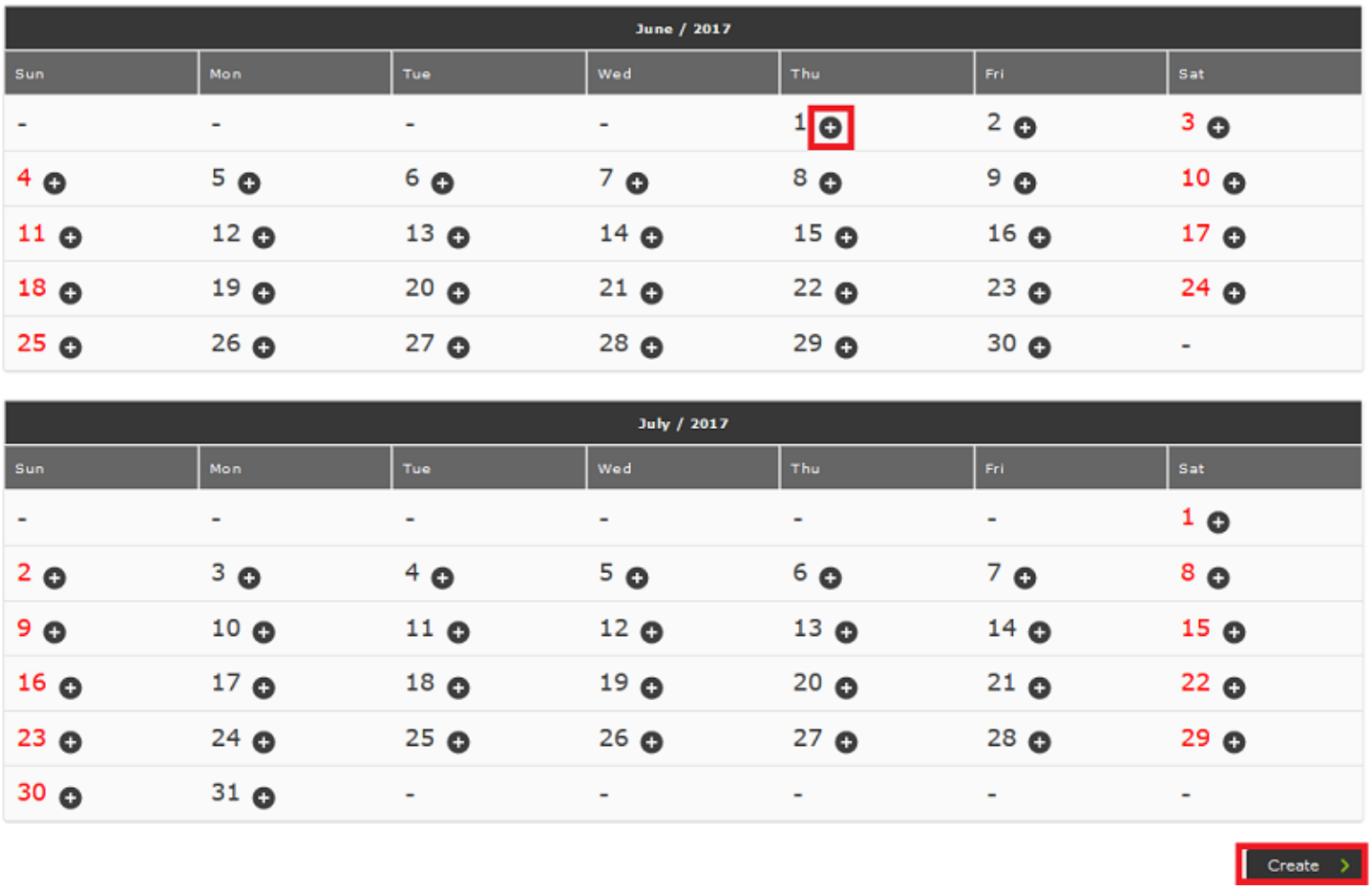
Если статус выбранного модуля переходит в `critical`, все остальные модули Агента отключаются, пока он снова не вернется в `normal` или `warning`. Это позволяет, например, отключать удаленные модули при потере связи.

Список специальных дней

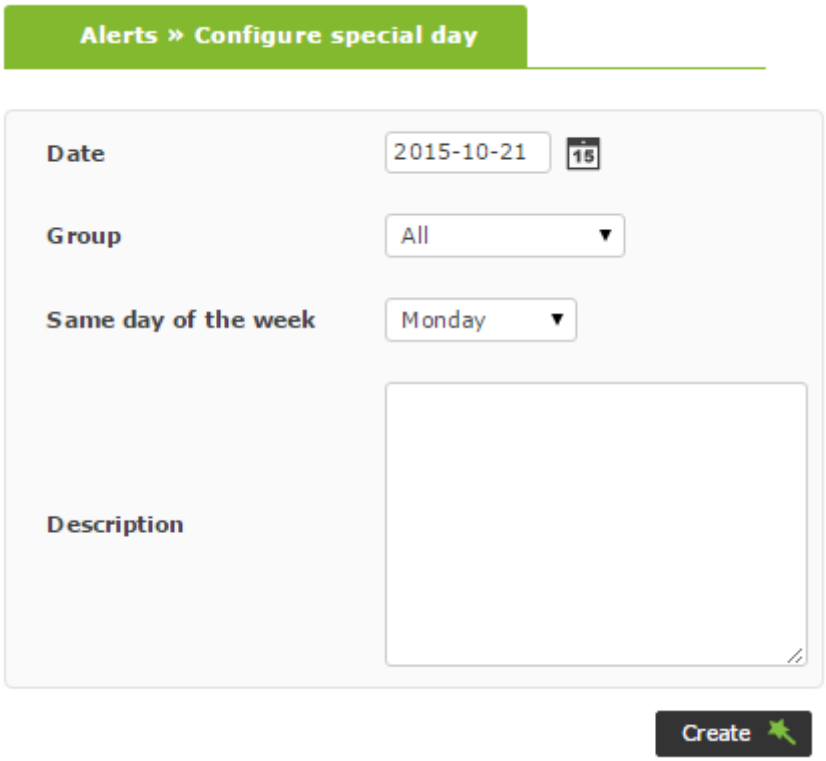
Pandora FMS позволяет определить список специальных дней для праздников и выходных, которые можно использовать в конфигурации шаблона, чтобы в эти дни оповещения не срабатывали.

Создание специального дня

Новые специальные дни создаются в разделе Alerts → List of special days нажатием на кнопку Create под календарем.



После нажатия на одну из них заполните следующие параметры:



Date

Дата специального дня. В формате `YYYY-MM-DD`. Чтобы установить один и тот же день каждый год, вы можете использовать `*-MM-DD`.

Group

Выберите группу, к которой относится специальный день. Вы можете назначить группу, к которой принадлежит пользователь, создающий специальный день, только если этот пользователь не принадлежит к группе ВСЕ (ALL).

Same day of the week

Дата в разделе Date будет рассматриваться так же, как этот день недели, независимо от того, какой это день недели на самом деле.

После того как поля будут выбраны, нажмите на кнопку Create.

Практический пример 1:

Предположим, вы выбрали 1 мая 2021 года как специальный день. Если `2021-05-01` имеет значение воскресенье, этот день будет рассматриваться как воскресенье, а не как соответствующий будний день в календаре.

Практический пример 2:

Предположим, вы выбрали 1 мая всех последующих лет как специальный день. Если

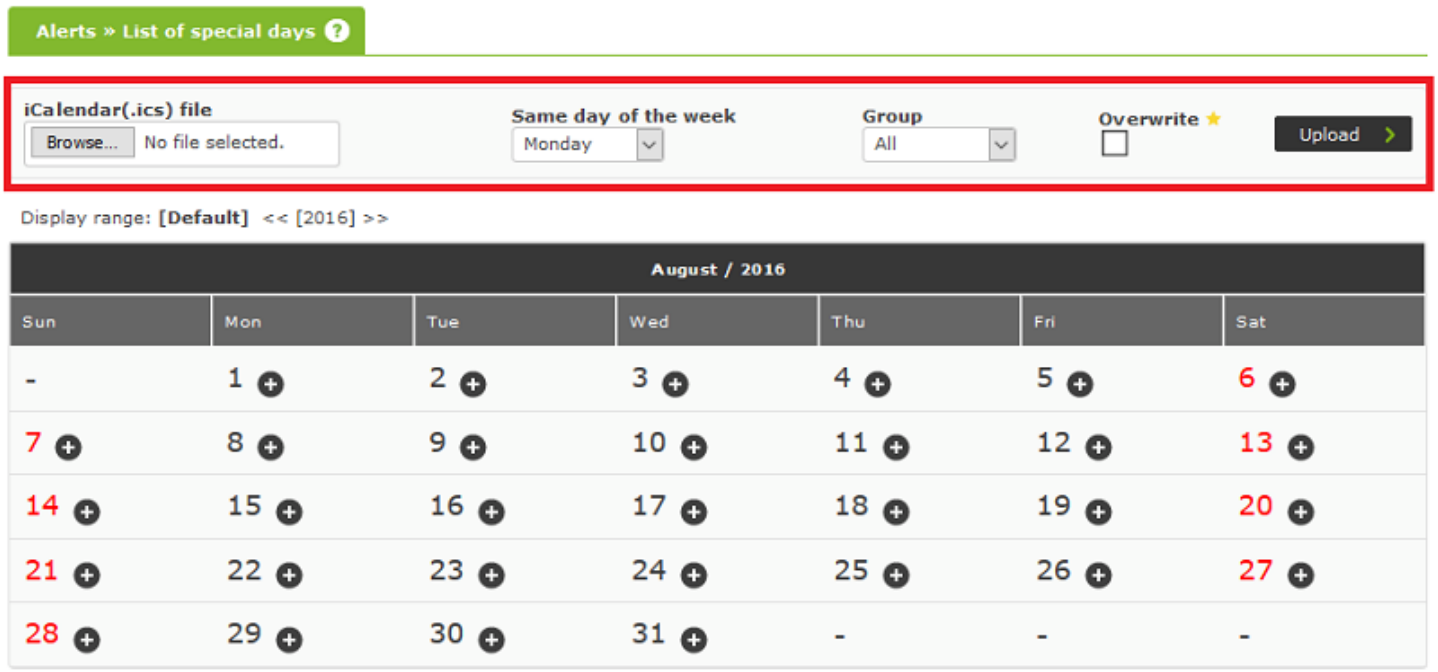
`*-05-01` имеет значение воскресенье, то этот день будет рассматриваться как воскресенье, а не как соответствующий будний день в календаре.

Практический пример 3:

Создан и настроен шаблон, который оповещает только с понедельника по пятницу с 8 до 18 часов. По субботам и воскресеньям этот шаблон не будет вызывать никаких предупреждений. 4 ноября - четверг и является государственным праздником, поэтому мы создадим его как особый день и в поле *Same day of the week* выберем либо субботу, либо воскресенье, таким образом, мы не получим предупреждения о какой-либо проблеме 4 ноября, поскольку это будет рассматриваться как день (суббота или воскресенье), в который шаблон не настроен для запуска предупреждений.

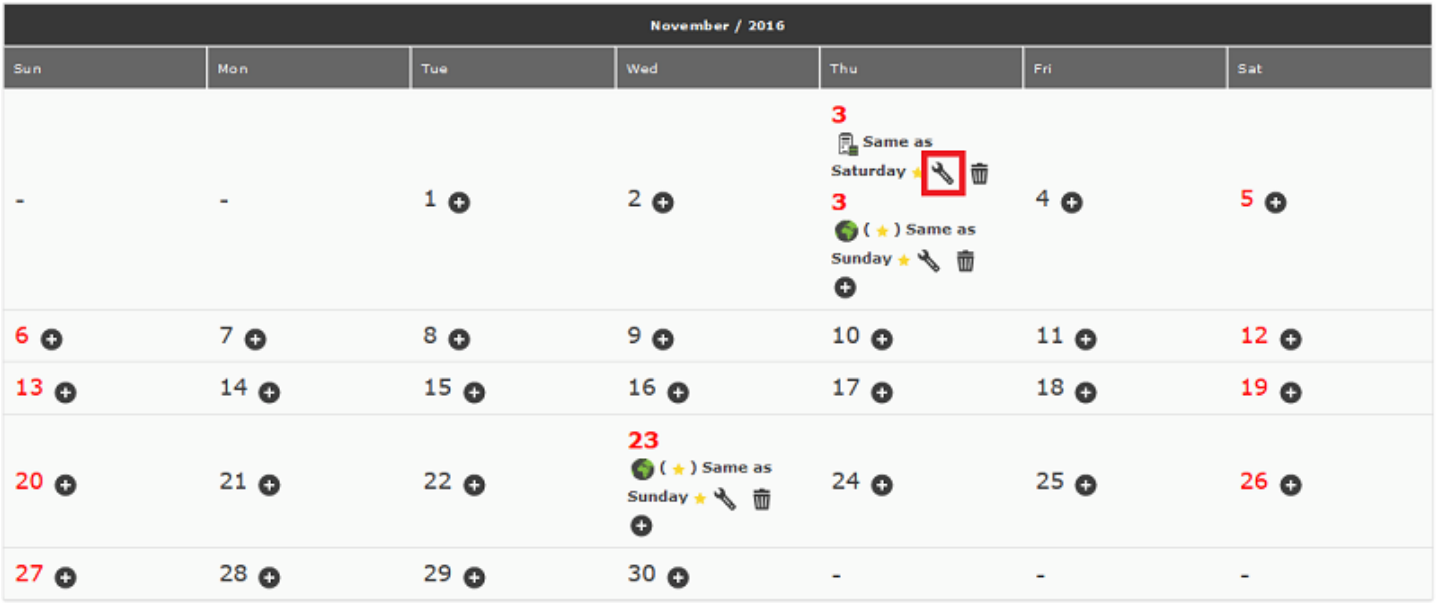
Массовое создание специальных дней с помощью файла .ics

Специальные дни можно также создать с помощью файла iCalendar (.ics). Их можно импортировать в верхней части окна. После импорта соответствующие данные будут записаны в текущем месяце.

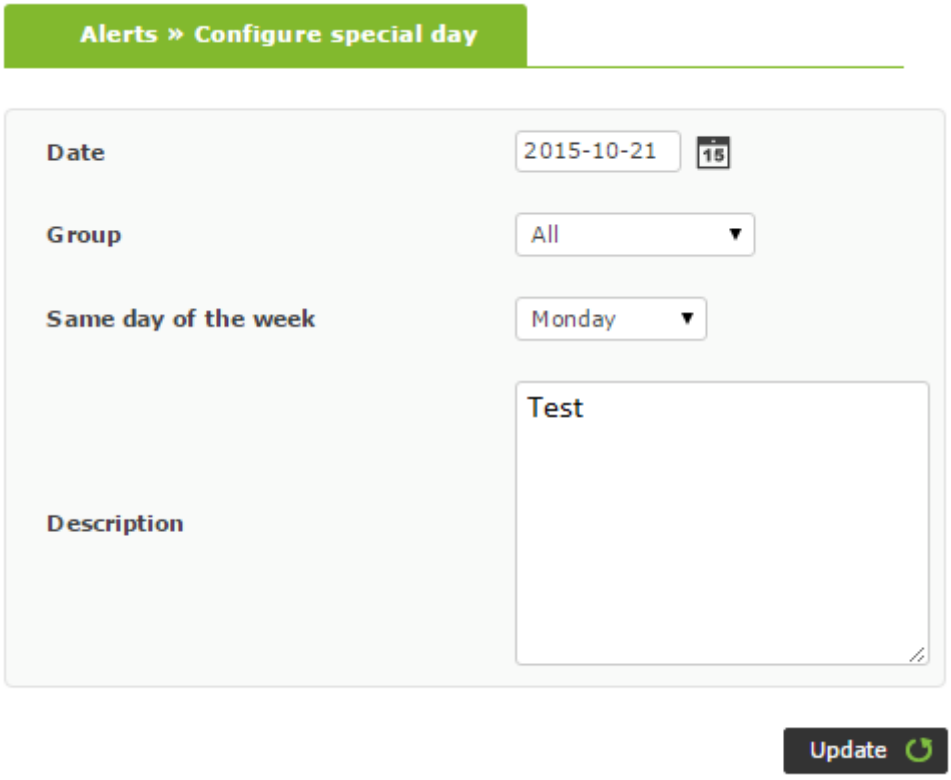


Редактирование специального дня

Можно создать специальные дни, созданные в опции List of special days в разделе Alerts.



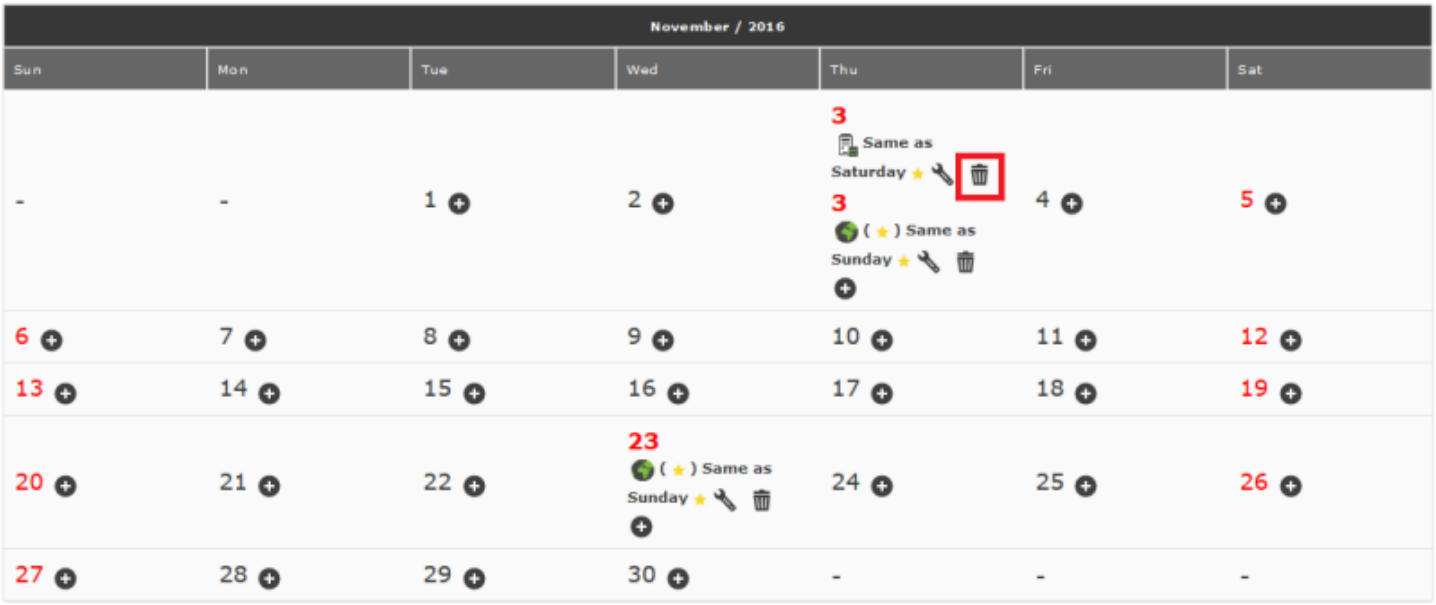
Чтобы отредактировать специальный день, нажмите на значок гаечного ключа рядом с соответствующим специальным днем.



После внесения изменений нажмите кнопку Update, чтобы подтвердить их.

Удалить специальный день

Чтобы удалить специальный день, нажмите на значок корзины рядом со значком гаечного ключа для специального дня.



Примеры полных предупреждений

Отправка предупреждений по SMS

У вас должен быть установлен инструмент, позволяющий отправлять SMS, например smstools.

После того как вы настроили учетную запись SMS, выполните команду:

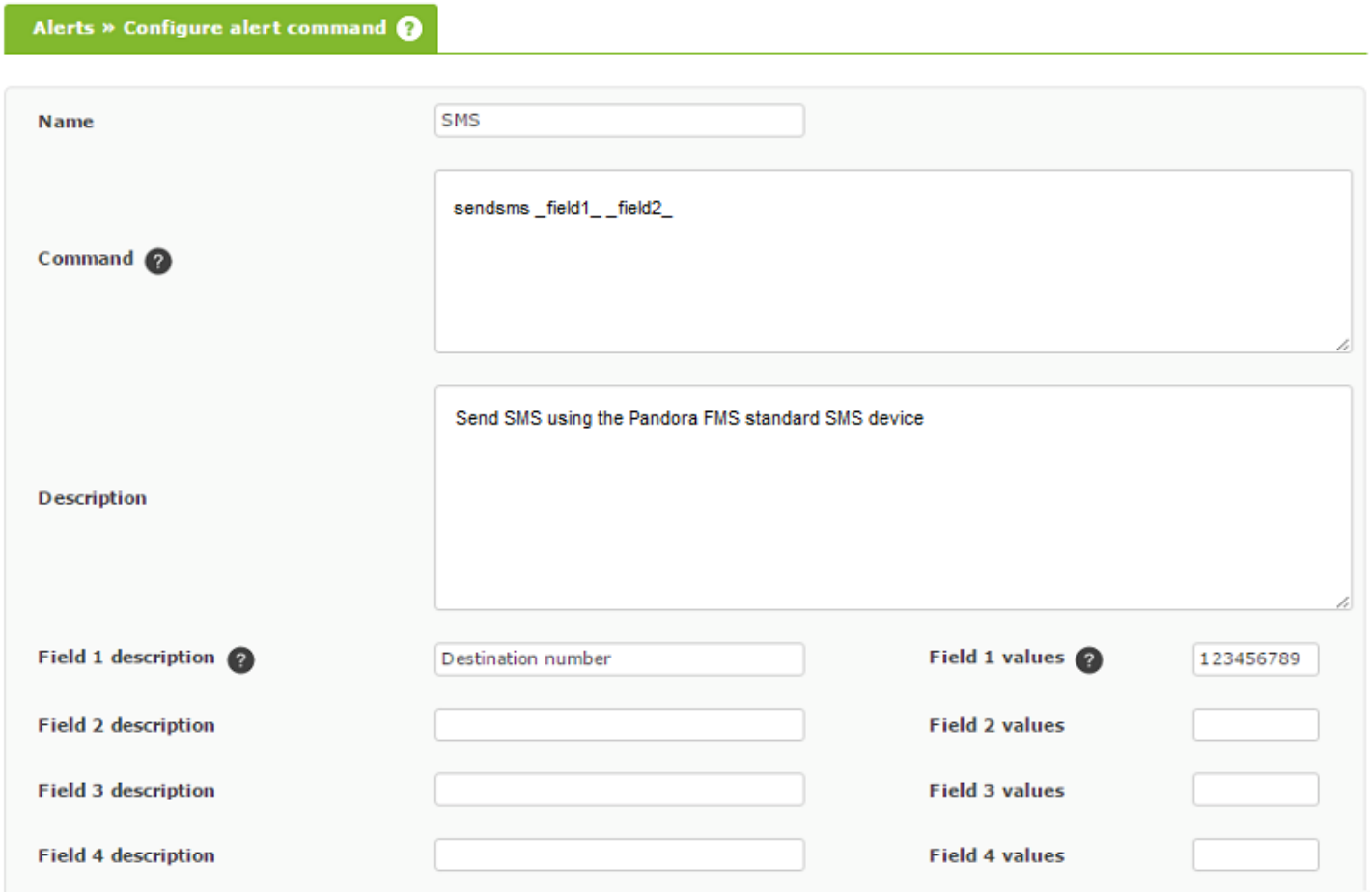
```
> sendsms
```

Вы должны указать два параметра, адрес назначения и сообщение:

```
<destination> 'Full message'
```

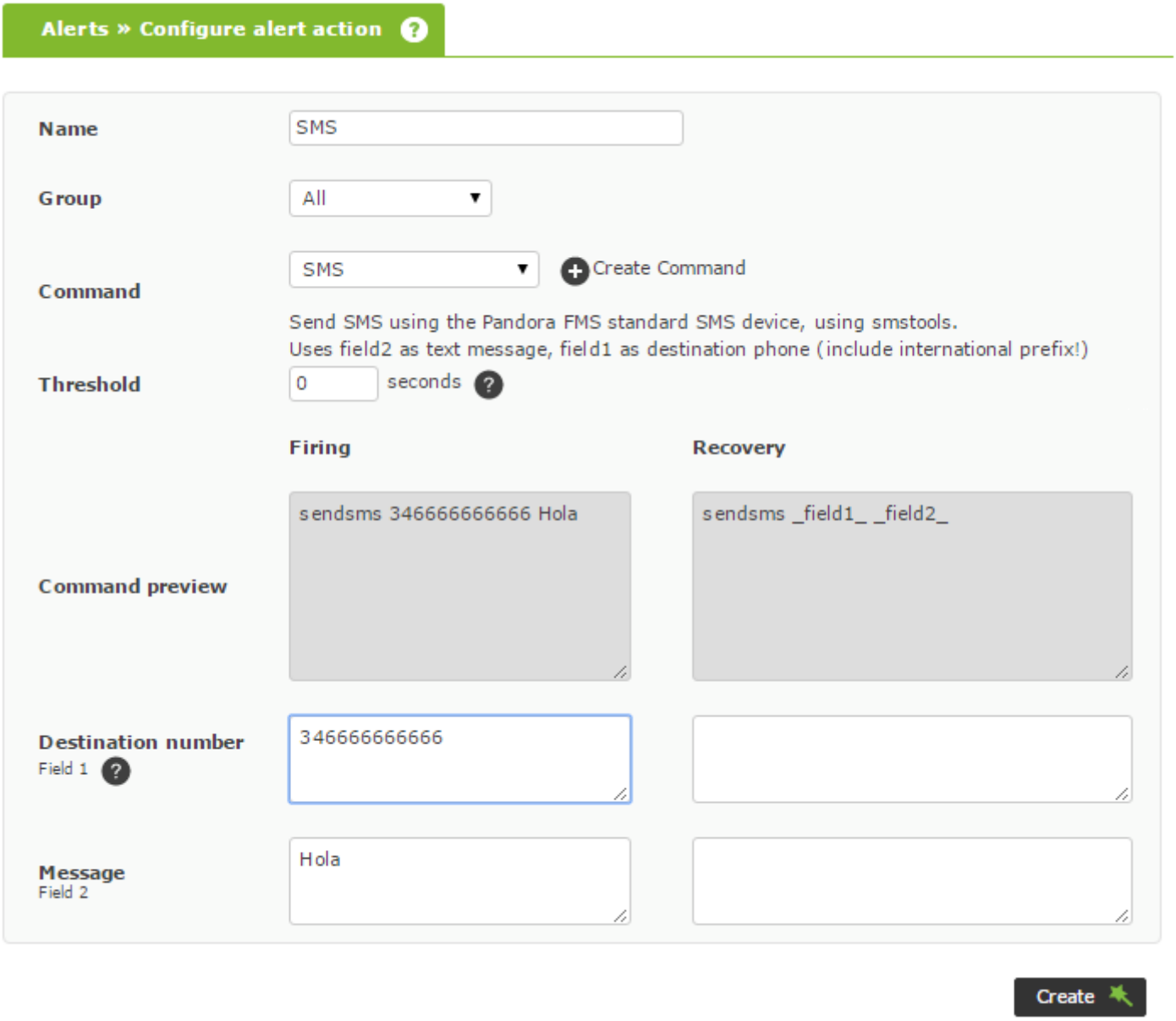
Введите номер назначения полностью (например, 79991234567 для телефонов в РФ) и текст сообщения в простых кавычках (' и ').

Таким образом, вы можете использовать команду для создания предупреждения в административном интерфейсе Pandora FMS.



Для этой команды поле 1 `Field 1` будет телефонным номером назначения, а поле 2 `Field 2` - самим сообщением, его текстом. Помните, что эти поля будут «переданы» в предупреждение и что их значения вполне могут быть взяты или заменены, поэтому на изображении выше номер назначения для примера - «123456789».

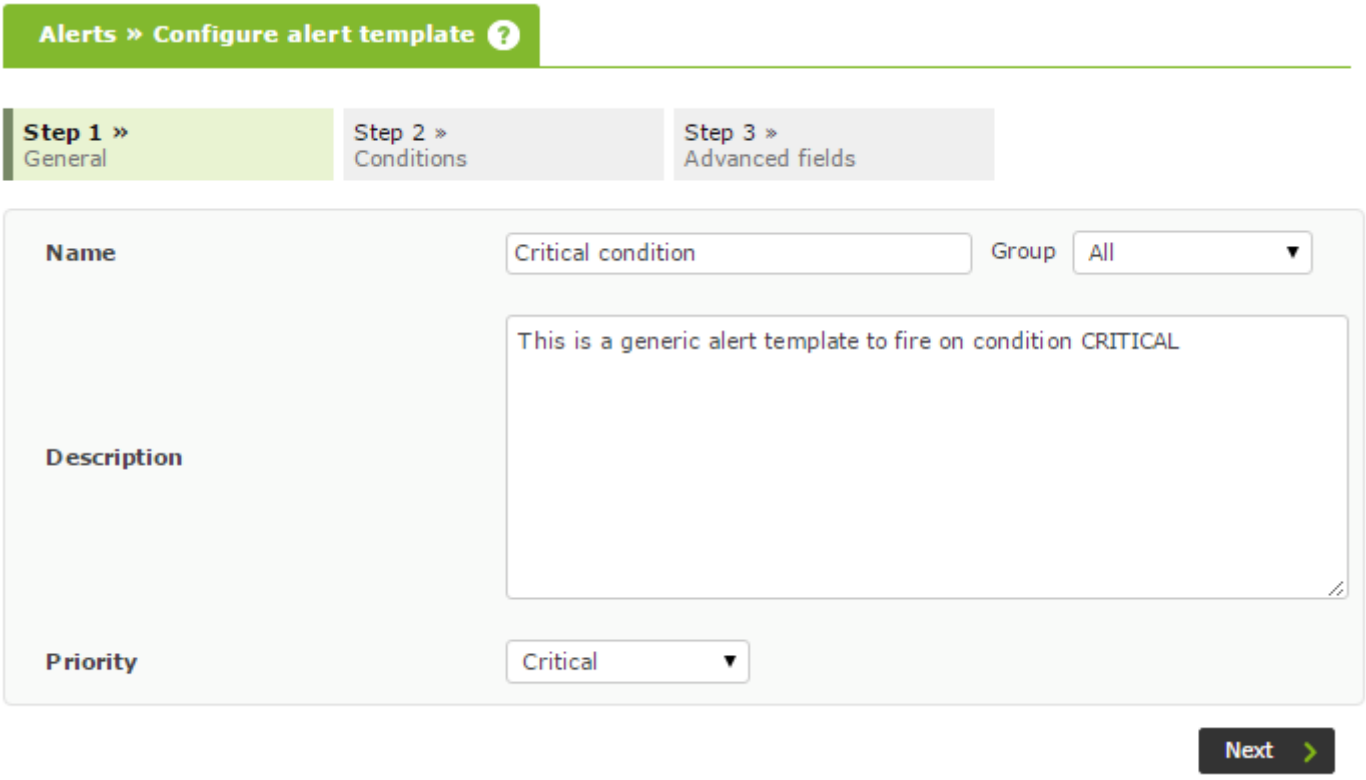
Теперь настройте действие для этой команды:



Это действие выполняет ранее определенную команду, заменяя `Field 1` и `Field 2` пользовательскими значениями. `Field 1` будет телефонным номером назначения («346666666666» как в предыдущем примере), и `Field 2` - текстом, определенным для этого действия («Hola» в примере предыдущего рисунка).

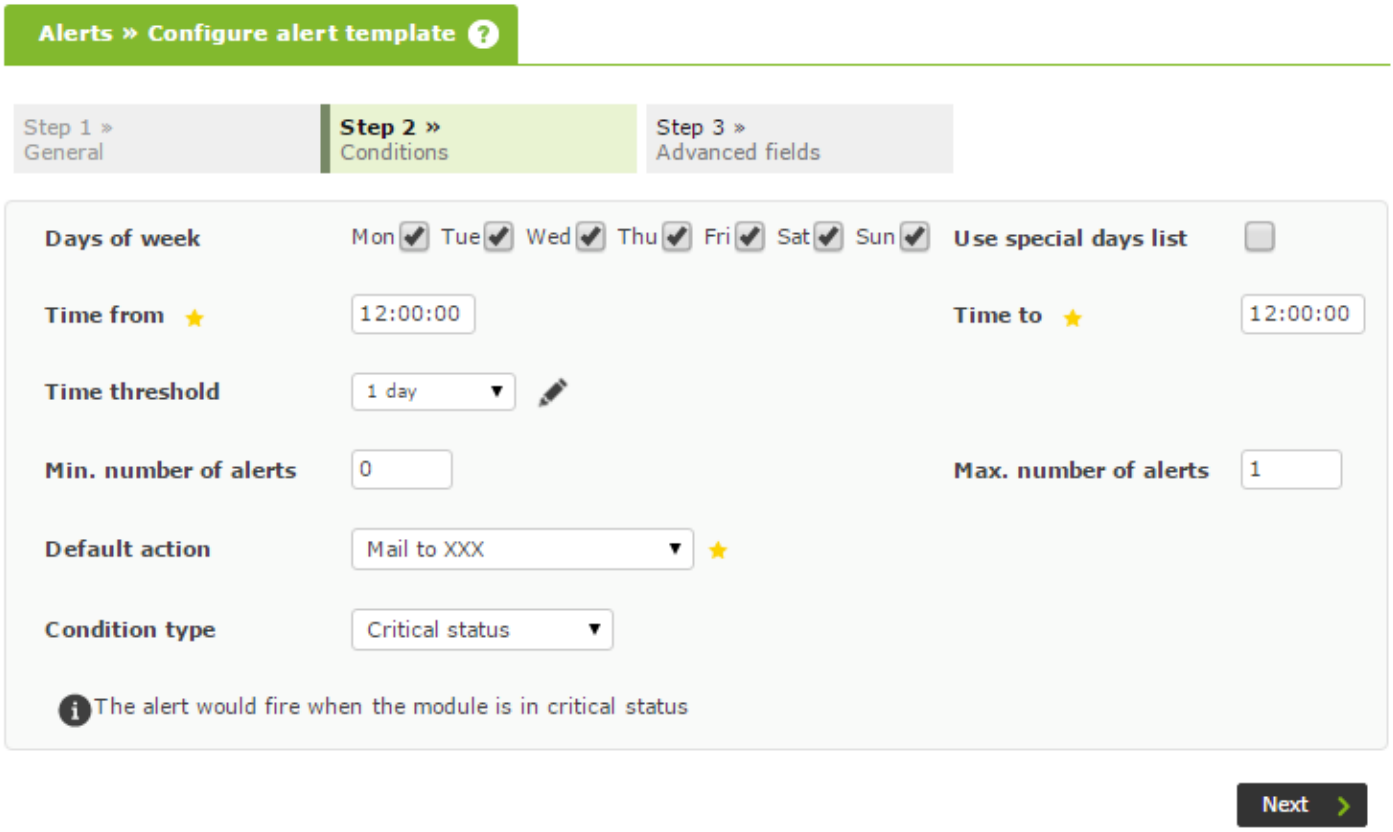
В Pandora FMS вы можете использовать (буквенно-цифровое) слово для номера телефона назначения, но имейте в виду, что некоторые операторы мобильной связи плохо обрабатывают буквенно-цифровые указания.

В следующем шаге вы можете использовать существующий шаблон оповещения или создать новый:

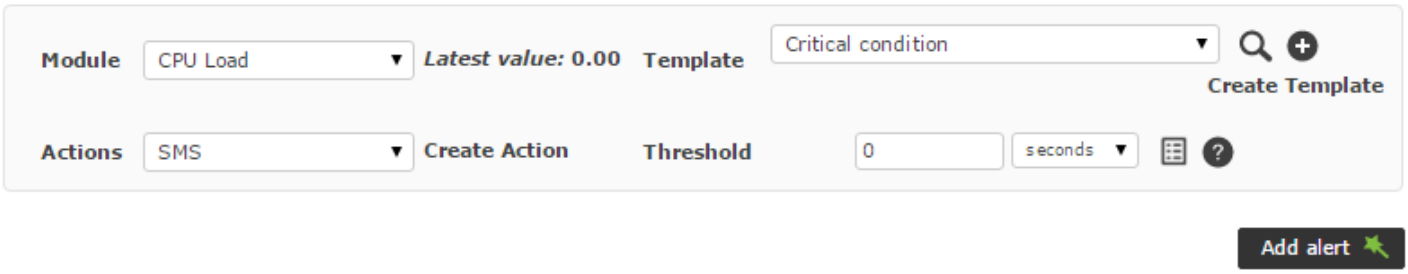


En este caso, la plantilla de alerta solo se activará cuando el módulo esté en estado `critical`.

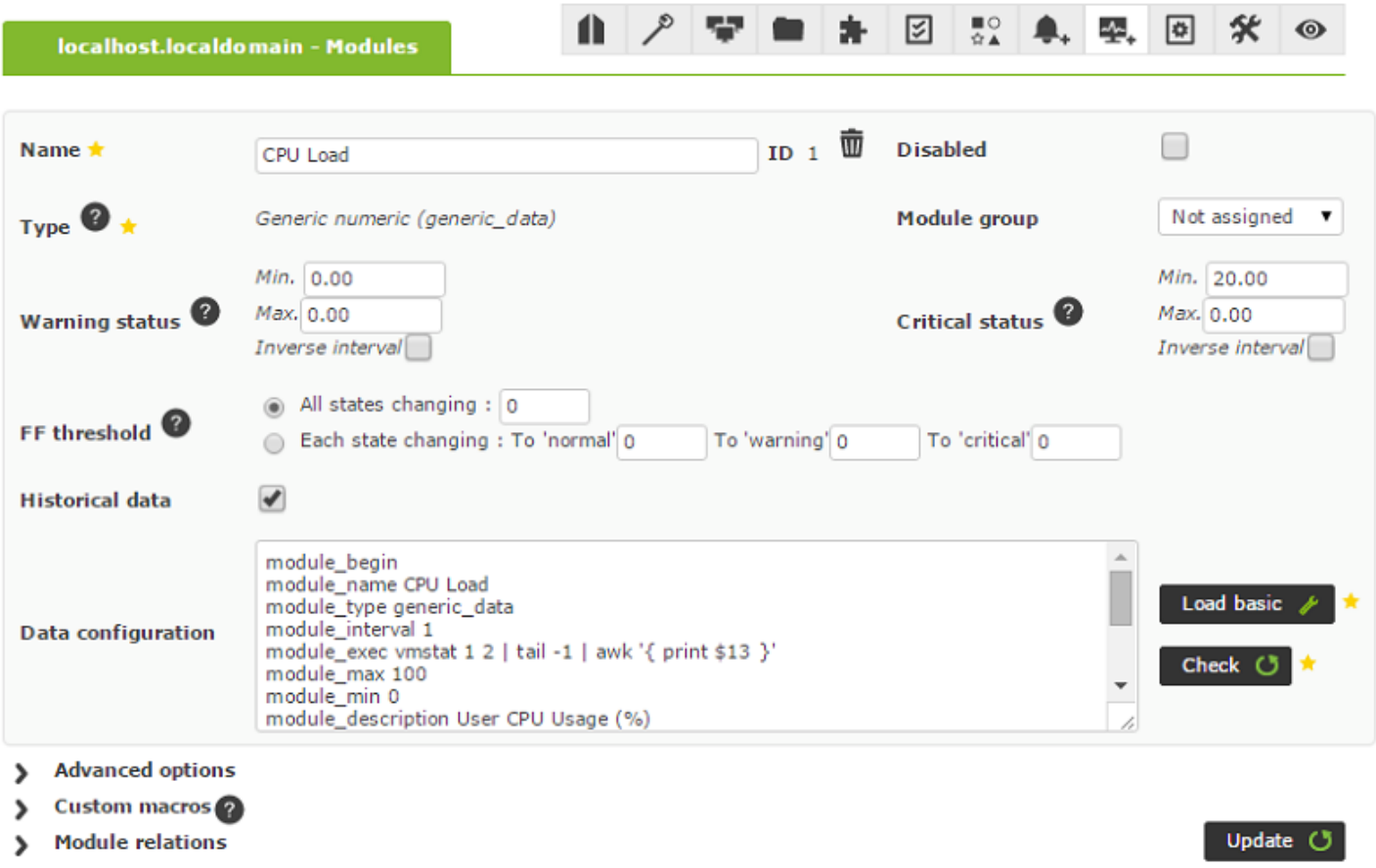
Después de definir este parámetro, configure la alerta para que se active como máximo una vez al día, pero si se recupera, se activará cada vez que se recupere y se active de nuevo; ver figura a continuación.



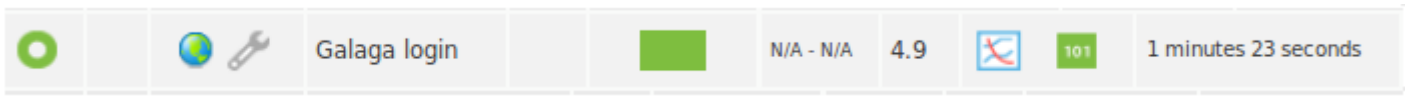
Теперь остается только назначить модуль шаблоном предупреждения и действием предупреждения:



На модуле рабочей нагрузки процессора установите низкое значение 20 для проверки отправки сообщений, см. скриншот ниже:



Наконец, вы можете «принудительно» выполнить предупреждение, то есть выполнить предупреждение агента немедленно; перейдите к просмотру предупреждения агента и нажмите на зеленый круглый значок.



На мобильный телефон должно прийти SMS-сообщение, как показано на изображении ниже. Обратите внимание, что тестовое сообщение было изменено на текст «aeryn», также

значение загрузки процессора показывает «N/A», потому что принудительное предупреждение не получает никаких реальных данных от модуля, *поскольку он не успел собрать никаких значений*.

Использование команд предупреждений, отличных от электронной почты

Pandora FMS характеризуется своей гибкостью, благодаря чему она может быть полезна всегда и в любое время. Следующий процесс более усовершенствован и всегда должен восприниматься как исключение из правил. В некоторых случаях вам может пригодиться знание о том, как он устроен.

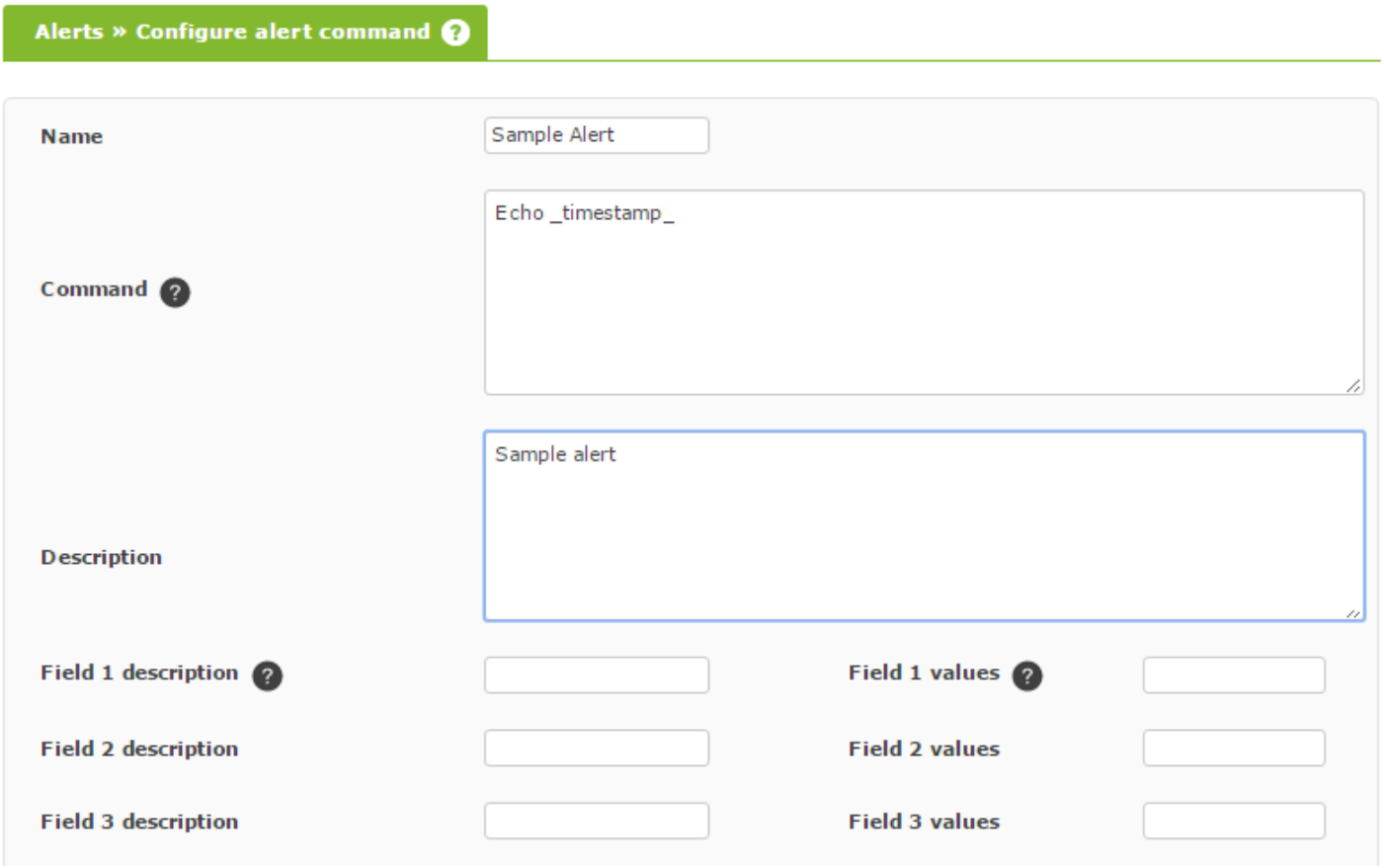
email, как команда, является внутренней для Pandora FMS и не может быть настроена, то есть `Field 1`, `Field 2` и `Field 3` - это определенные поля, которые используются в качестве адресата, темы и текста сообщения. Что если вам нужно выполнить другое, пользовательское действие?

Допустим, вам нужно генерировать файл *log* с каждым предупреждением, обнаруженным Pandora FMS. Формат этого файла *log* будет примерно следующим:

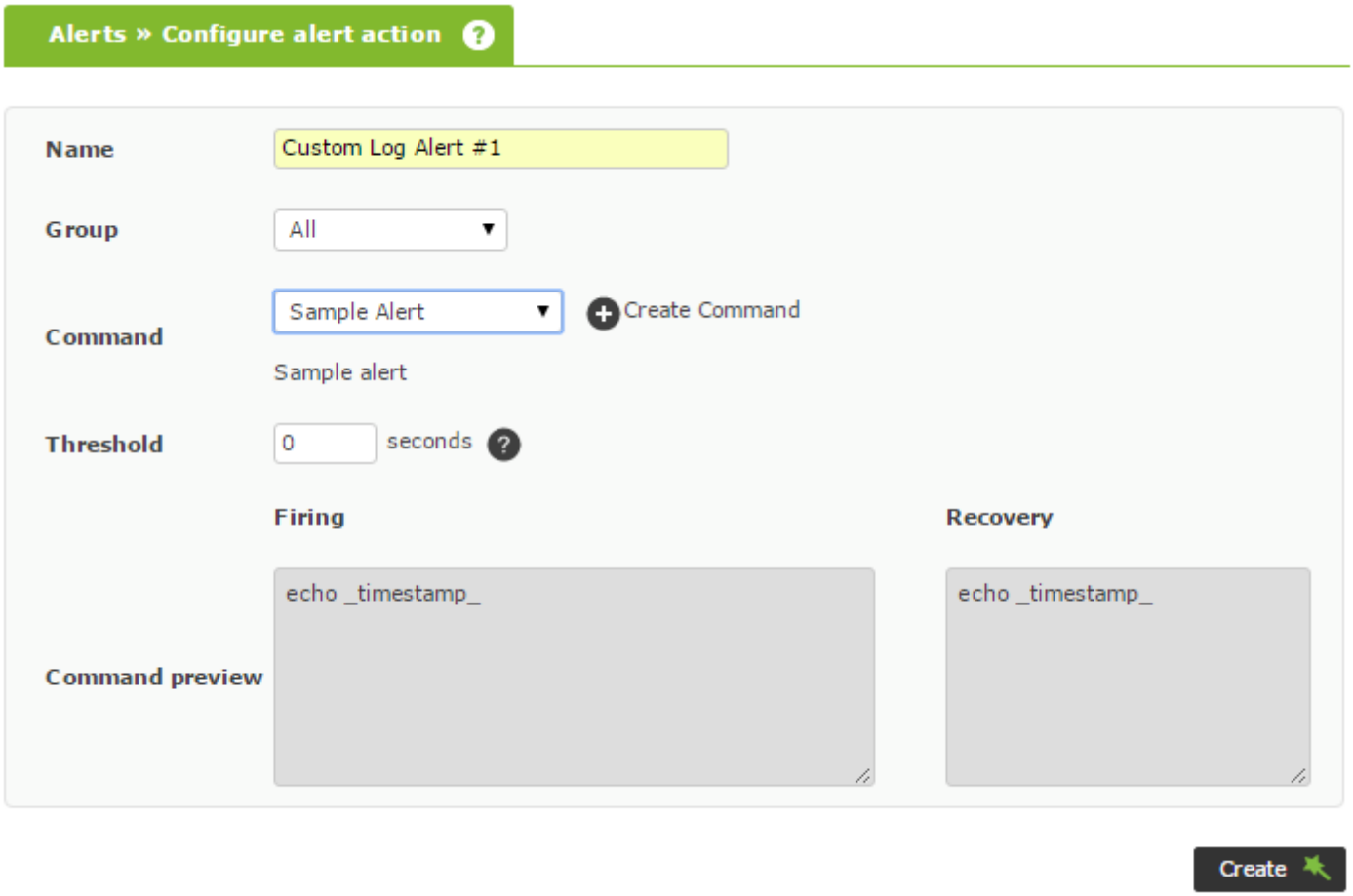
```
ДАТА_ВРЕМЯ - ИМЯ_АГЕНТ - ИМЯ_МОДУЛЬ - ЗНАЧЕНИЕ - ОПИСАНИЕ ПРОБЛЕМЫ
```

Где ЗНАЧЕНИЕ - это значение модуля в этот момент. Будет создано несколько файлов *log*, в зависимости от действия, вызывающего команду. Действие определяет описание и файл, в который отправляются события.

Для этого сначала необходимо создать команду следующим образом:



И определить действие для этого же:



После выполнения аварийных сигналов созданный вами файл *log* может выглядеть примерно так:

```
2010-05-25 18:17:10 - farscape - cpu_user - 23.00 - Custom log alert #1
```

Для данного примера оповещение сработало в 18:17:10 в агенте ««farscape», в модуле «cpu_sys» с данными «23.00» и с описанием, которое было размещено при определении действия.

Выполнение команды, порядок полей и другие моменты могут привести к тому, что мы не будем знать, как на самом деле выполняется команда. Для этого проще всего активировать *debug* трассы сервера Pandora (verbose 10) в файле конфигурации сервера Pandora в `/etc/pandora/pandora_server.conf`. Затем перезапустите сервер командой `/etc/init.d/pandora_server restart` и изучите файл `/var/log/pandora/pandora_server.log`, чтобы найти точную строку с выполнением команды предупреждения, которую вы определили.

Начиная с версии NG 754 и выше, доступны дополнительные опции по ручному запуску и выключению сред высокой доступности (HA).

Полный пример предупреждения с макросами подстановки

Предположим, вам нужно создать запись в LOG, где каждая строка имеет следующий формат:

```
2009-12-24 00:12:00 pandora [CRITICAL] Agent <agent_name> Data <module_data>
Module <module_name> in CRITICAL status
```

Настройка команды

```
echo _timestamp_ pandora _field2_>> _field1_
```

Настройка действий

```
 Field1 = /var/log/pandora/pandora_alert.log
 Field2 = <Белым>
 Field3 = <Белым>
```

Настройка шаблона

```
Field1 = <Белым>
Field2 = [CRITICAL] Agent _agent_ Data _data_ Module _module_ in CRITICAL status
Field3 = <Белым>
```

В разделе восстановления:

```
Field2 = [RECOVERED] [CRITICAL] Agent _agent_ Data _data_ Module _module_ in
CRITICAL status
Field3 = <Белым>
```

Таким образом, при выполнении предупреждения в LOG будет вставлена следующая строка:

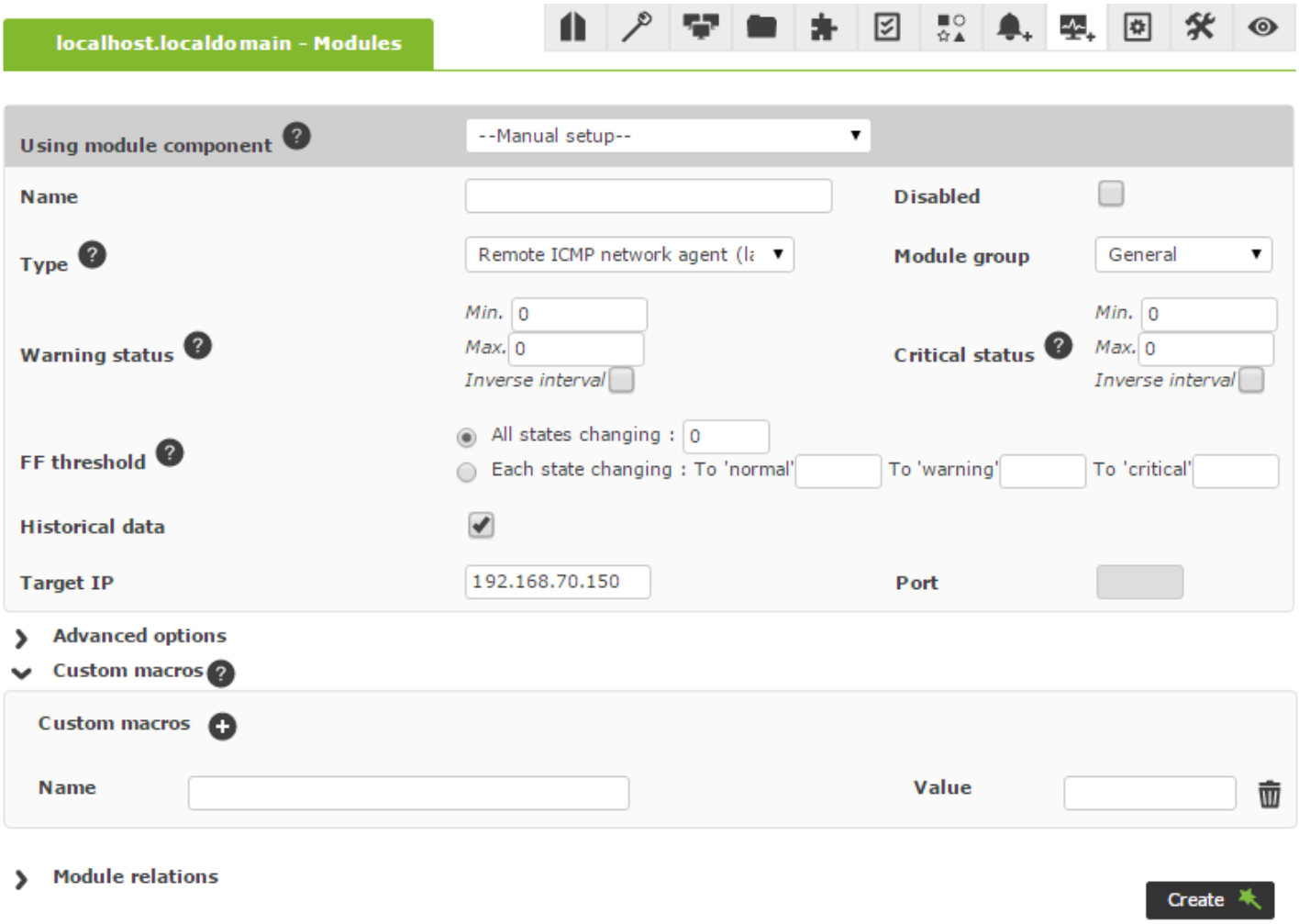
```
2009-10-13 13:37:00 pandora [CRITICAL] Agent raz0r Data 0.00 Module Host Alive
in CRITICAL status
```

И следующая строка при извлечении предупреждения:

```
2009-10-13 13:41:55 pandora [RECOVERED] [CRITICAL] Agent raz0r Data 1.00 Module
Host Alive in CRITICAL status
```

Настраиваемые макросы предупреждения модуля

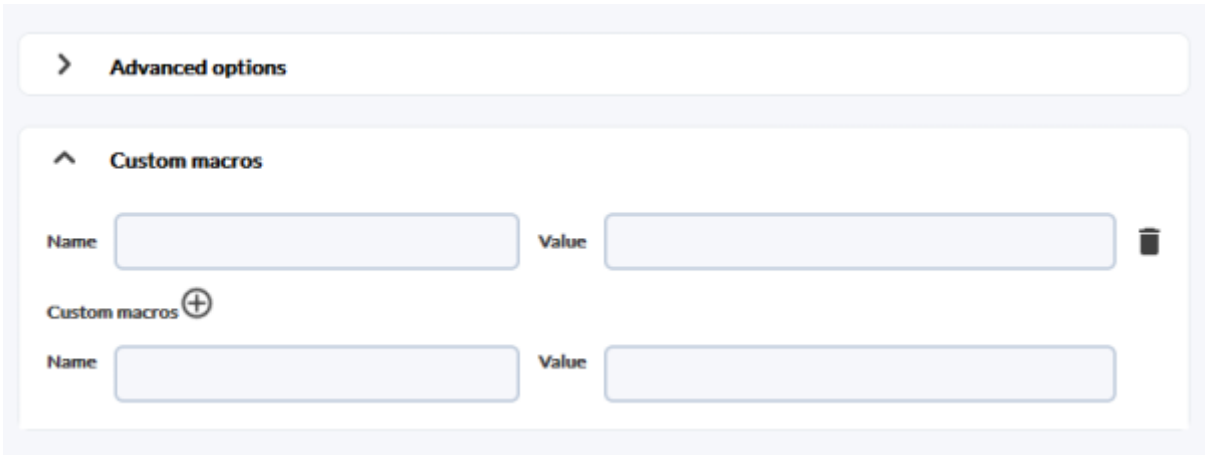
В модуль агента можно добавить любое количество макросов (Custom macros).



Эти пользовательские макросы имеют следующие характеристики:

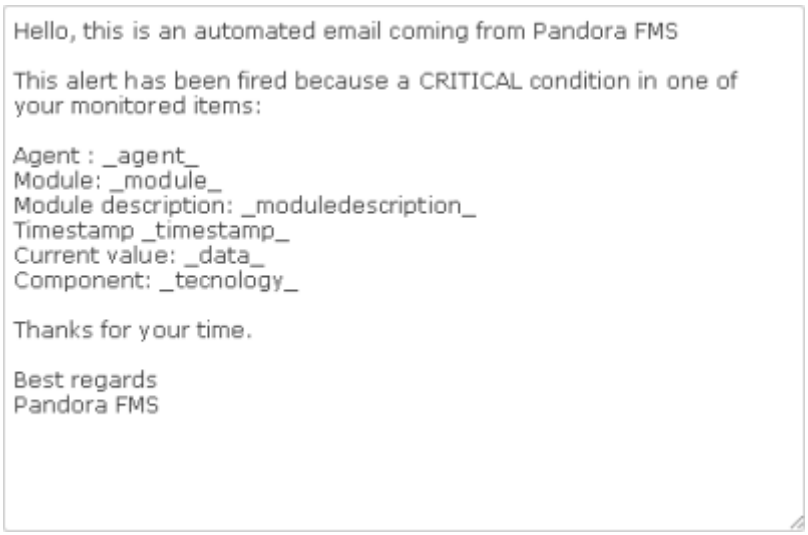
- Они определяются в модуле.
- Они хранят данные в базе данных.
- Они могут иметь любое название, напрмер: `_masha`.
- Не отражаются в локальной конфигурации (`.conf`).
- Они используются исключительно для предупреждений.
- Они не могут быть определены на уровне компонентов.
- Они могут быть определены в политиках.

Эти специфические макросы можно добавить, расширив раздел макросов любого модуля.



Установленные значения можно использовать как часть полей в определении предупреждений.

Например: Чтобы включить макрос в действие отправки письма, необходимо настроить поле тела сообщения следующим образом:



Если модуль добавлен в это оповещение без настроенного макроса, раздел, в котором значение макроса должно появиться в действии, будет пустым.

Настройка электронной почты для предупреждений в Pandora FMS

Pandora FMS сама по себе имеет возможность отправлять электронные письма, как объясняется в разделе Общяя конфигурация Консоли..

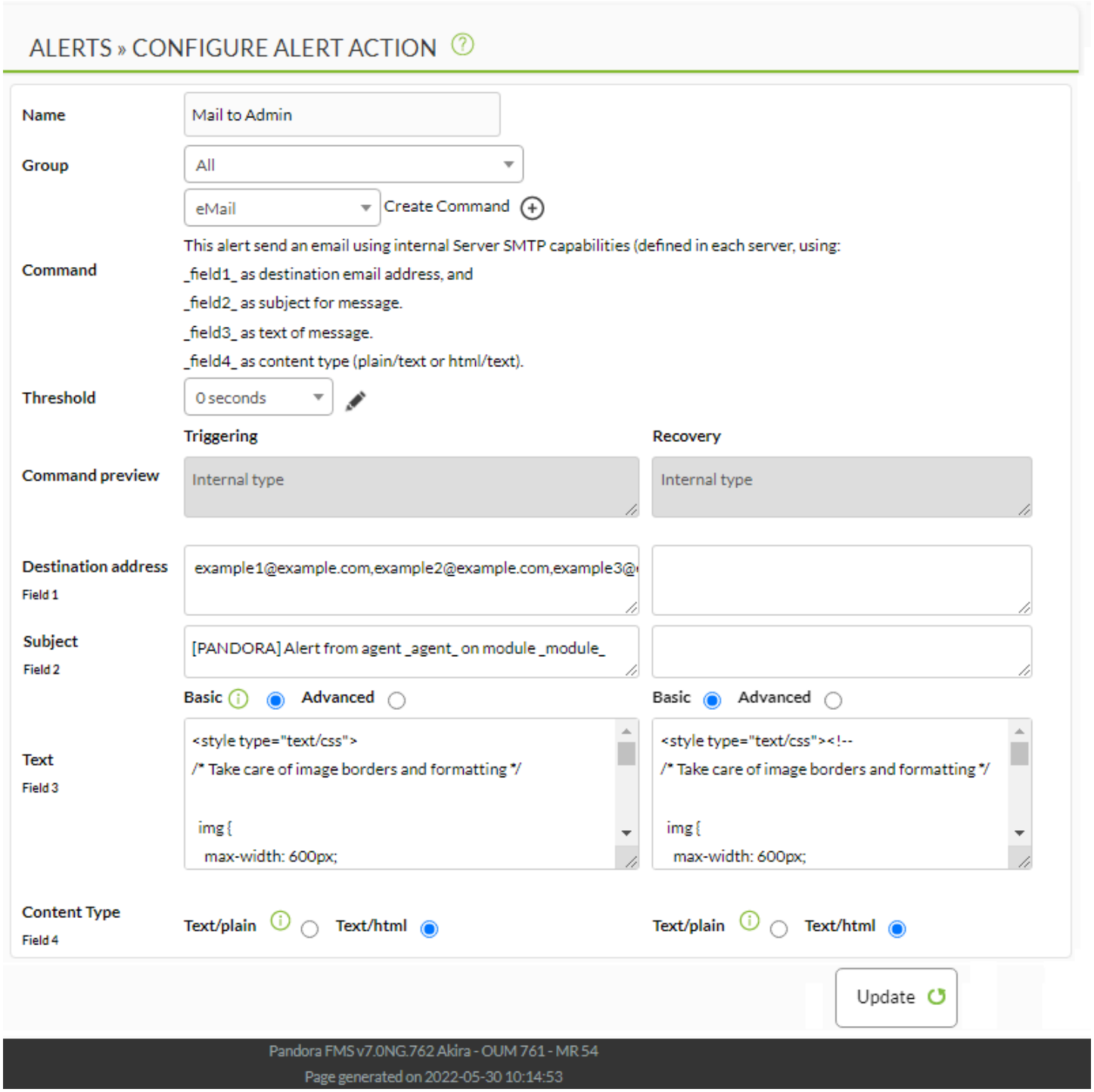
Однако ее гибкость позволяет использовать различные платформы электронной почты.

Настройка почты с помощью учетной записи Gmail

Чтобы сервер Pandora FMS мог отправлять предупреждения через электронную почту аккаунта Google Mail (Gmail) перейдите к к общей конфигурации консоли или к конфигурации сервера Pandora FMS и введите свои учетные данные (веб-домен Office365, имена пользователей, пароль и т.д.).

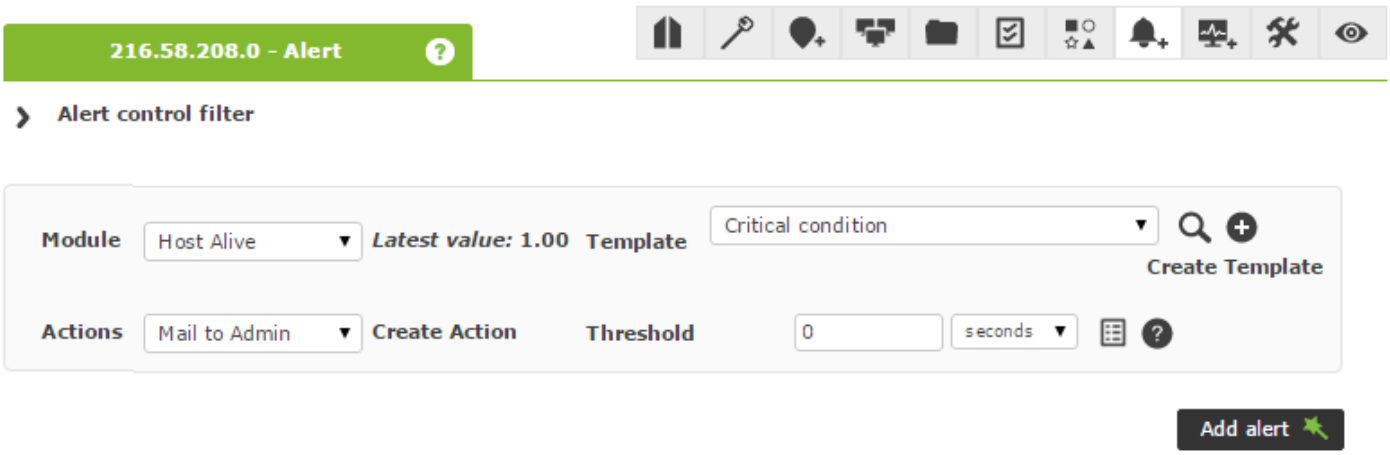
Конфигурация действий

Добавьте действие, например, с именем Mail to Admin, а для настройки получателя сообщения используйте команду eMail:

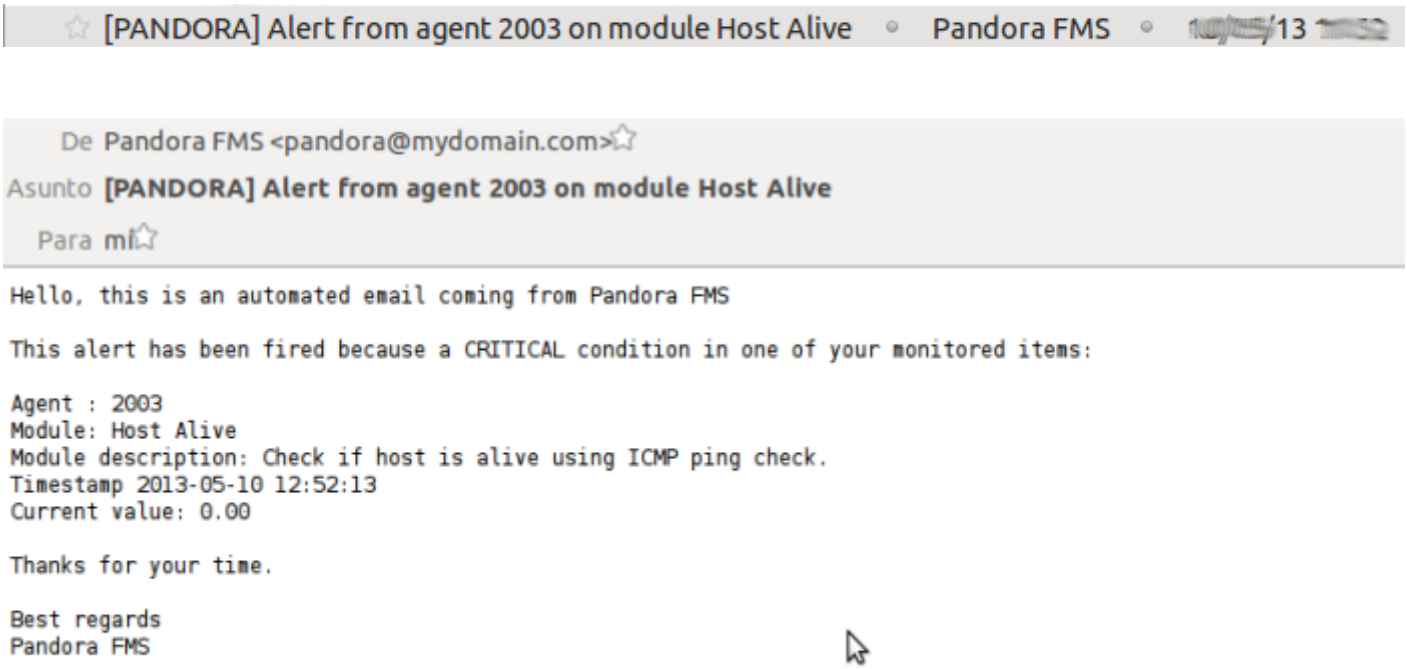


Настройки предупреждения

В этом случае в конфигурации *Модуль* > *Предупреждения* было сгенерировано новое предупреждение со следующим модулем:



Как только предупреждение будет запущено, вы сможете проверить, как оно поступит на выбранный адрес электронной почты в действии:



Конфигурация почты с учетной записью Office365

Pandora FMS может использовать Office365 с помощью следующей конфигурации:

- У вас должна быть создана учетная запись в Office365.
- Перейдите к общей конфигурации консоли или конфигурации сервера Pandora FMS и введите свои учетные данные (веб-домен Office365, имена пользователей, пароль и т.д.).

Корреляция предупреждений: предупреждения в событиях и журналах

Версия NG 741 или выше.

С помощью Pandora FMS вы можете создавать предупреждения на основе полученных событий или на основе данных, собранных с помощью системы сбора журналов. Можно построить простые или более сложные предупреждения, основанные на наборе правил с логическими связями. Эта функция заменяет предыдущую функцию предупреждения о событиях.

Этот тип предупреждения позволяет работать более гибко, поскольку оповещения генерируются не на основе статуса конкретного модуля, а на основе события, которое могло быть сгенерировано несколькими различными модулями, от различных агентов.

Предупреждения о событиях и/или *логи* основаны на правилах фильтрации с использованием следующих логических операторов:

- `and`
- `or`
- `xor`
- `nand`
- `nor`
- `nxor`

Эти логические операторы используются для поиска событий/выражений в *журналах*, которые соответствуют настроенным правилам фильтрации, и если совпадения найдены, срабатывает предупреждения.

Они также используют шаблоны для определения некоторых параметров, например, дней, в которые будет запущено предупреждение; однако в этом случае шаблоны не определяют, когда будет запущено предупреждение, но именно с помощью правил фильтрации осуществляется поиск и запуск предупреждений о соответствующих событиях.

Рекомендуется использовать новый редактор правил, который позволяет строить правила визуально, но некоторое время вы еще можете использовать старый редактор предупреждений о событиях. Вы можете узнать больше из обучающего видеоролика «Выпуск обновлений 741 Pandora FMS».

Учитывая большое количество событий, которое может вместить база данных Pandora FMS, сервер работает в максимальном окне событий, которое определяется в конфигурационном файле `pandora_server.conf` с помощью параметров `event_window` и `log_window`. События, сгенерированные вне этого временного окна, не будут обработаны сервером, поэтому не имеет смысла указывать в правиле временное окно больше,

чем то, которое настроено на сервере.

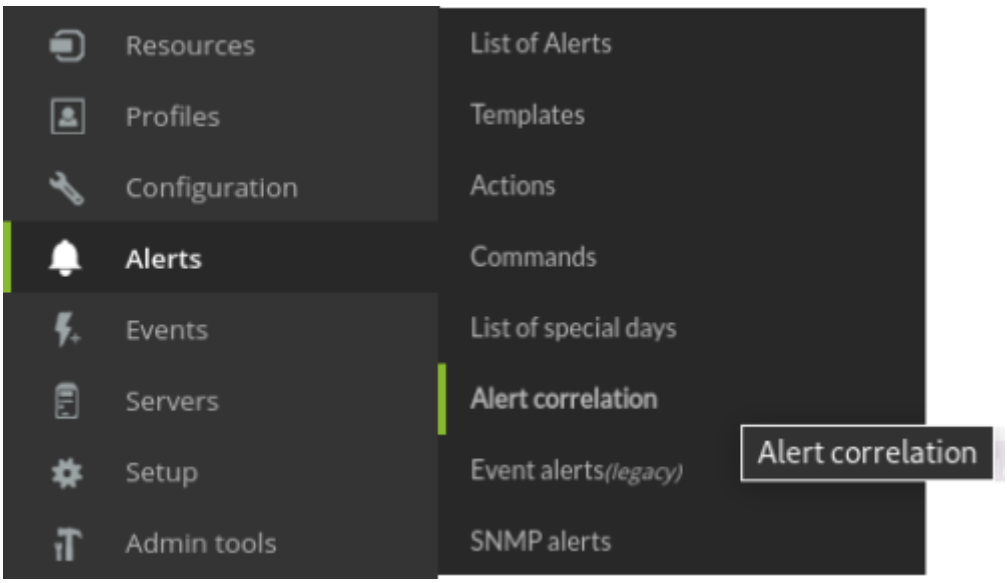
При определении предупреждений о событиях необходимо указать параметры агент, модуль и событие.

Создание корреляционных предупреждений

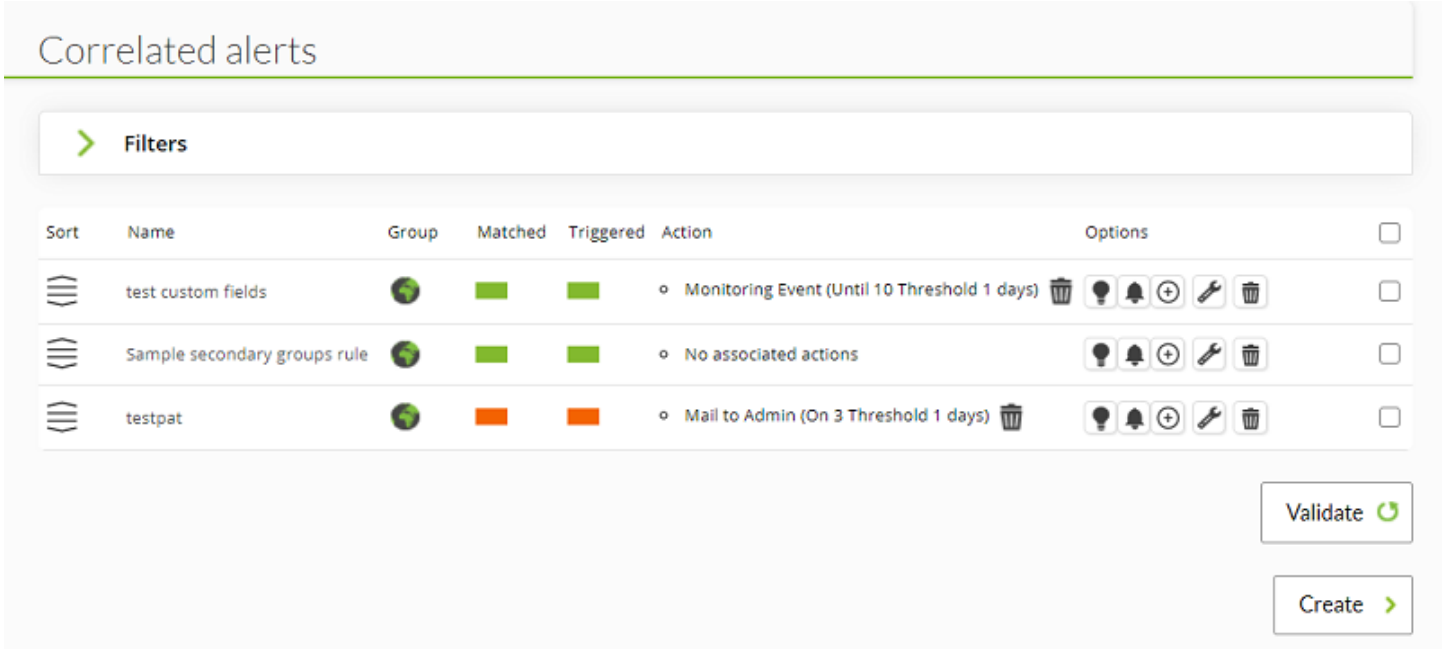
Чтобы предупреждения о корреляции событий работали, необходимо активировать сервер корреляции событий с помощью параметра `eventserver 1` в файле конфигурации сервера Pandora FMS.

Предупреждения о корреляции и шаблоны

Чтобы настроить предупреждения о корреляции, войдите в раздел Alert correlation через меню.



В этом общем виде мы можем наблюдать поля:



Sort

Устанавливает порядок оценки коррелированных предупреждений, оценивая, настроен ли он как pass или drop. Чем выше в списке оно находится, тем быстрее будет оценена тревога.

Name

Имя предупреждения.

Group

Группа, в которой оно было создано. Пользователь сможет увидеть группу, к которой он будет принадлежать, только если этот пользователь не принадлежит к группе ВСЕ (ALL).

Matched

Сколько раз событие, соответствующее правилу запуска, было обнаружено в текущем threshold.

Triggered

Сколько раз срабатывало предупреждение в настроенном threshold.

Action

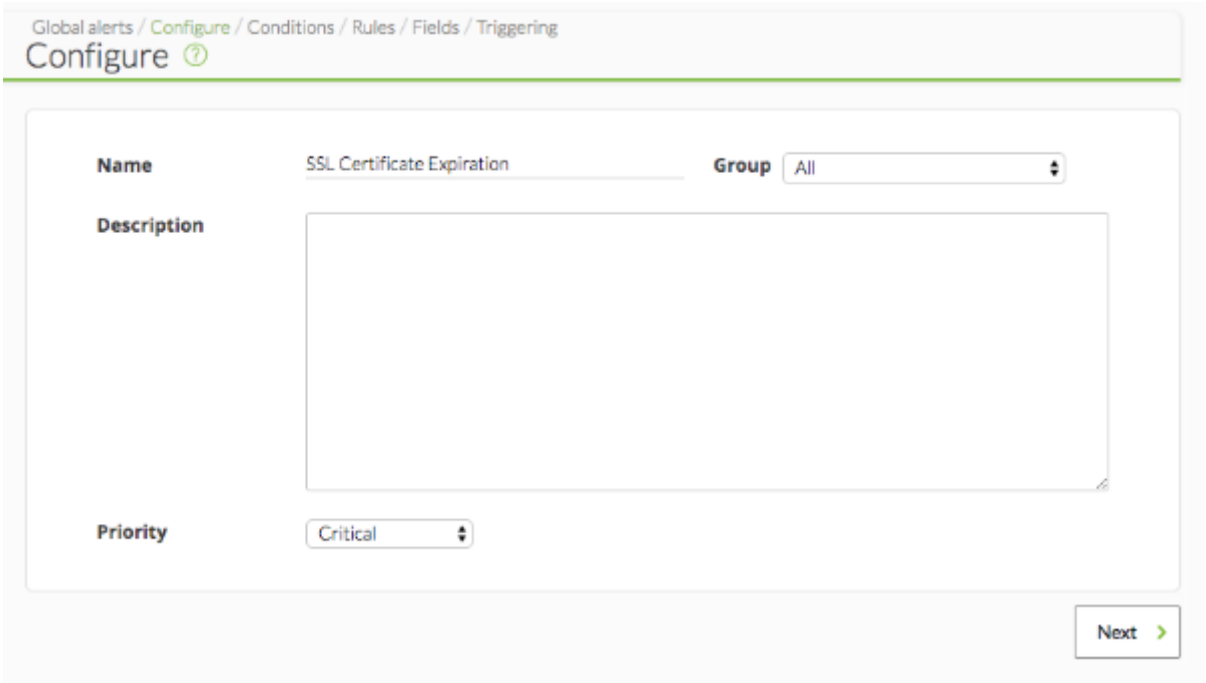
Отображает действия, настроенные в предупреждении.

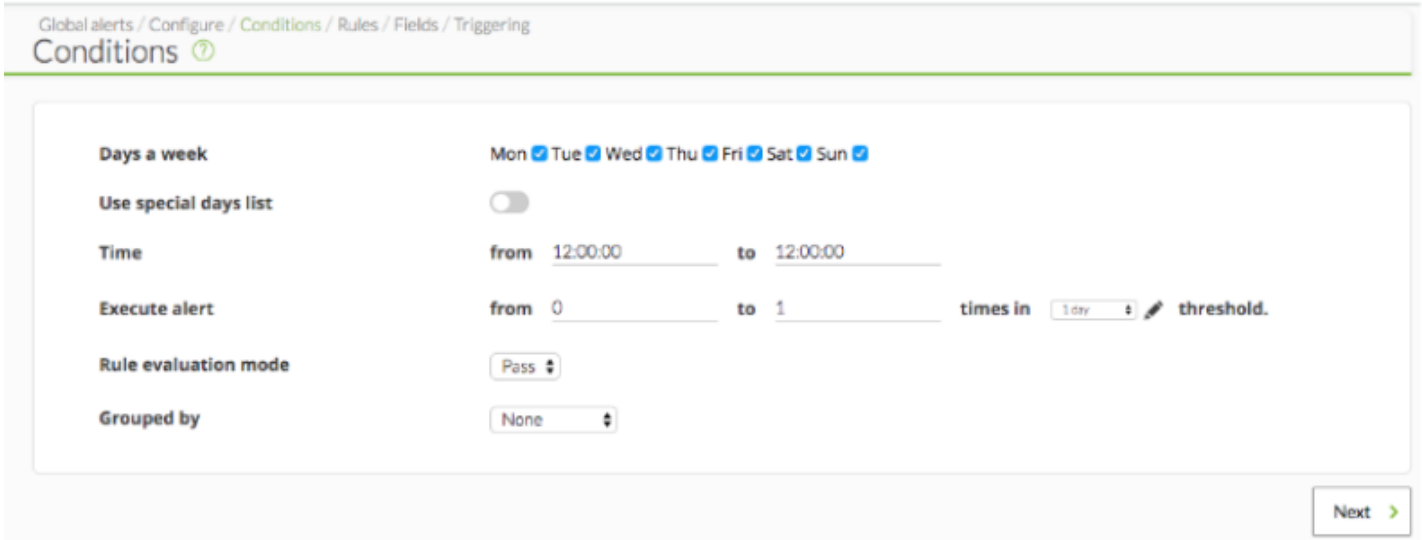
Options

Позволяет работать с отключенным действием, в режиме ожидания, добавлять

дополнительные действия, редактировать или удалять коррелированное предупреждение.

Приступайте к созданию правила и определению его поведения (процесс аналогичен созданию Alert Templates):





Параметры конфигурации шаблонов корреляционных предупреждений аналогичны параметрам конфигурации предупреждений модуля. Есть только два специфических параметра предупреждения о событиях:

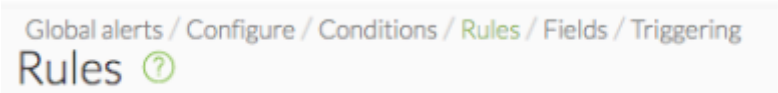
- Режим оценки правила («Rule evaluation mode»): может быть Pass или Drop. Первый означает, что в случае, если событие совпадает с сигналом тревоги, все остальные сигналы тревоги подвергаются дальнейшей оценке. Drop означает, что если событие совпадает с каким-либо предупреждением, оно не оценивается в других предупреждениях.
- Группировка («Group by»): Позволяет группировать правила по агентам, модулям, оповещениям или группам. Например, если правило настроено на срабатывание при

получении двух критических событий и сгруппировано по агентам, два критических события должны поступать от одного и того же агента. Можно деактивировать.

В случае предупреждений, содержащих правила *logs*, это влияет только на группировку по агенту. Если вы выберете другую группировку, оповещения, основанные на записях журнала, никогда не будут выполнены.

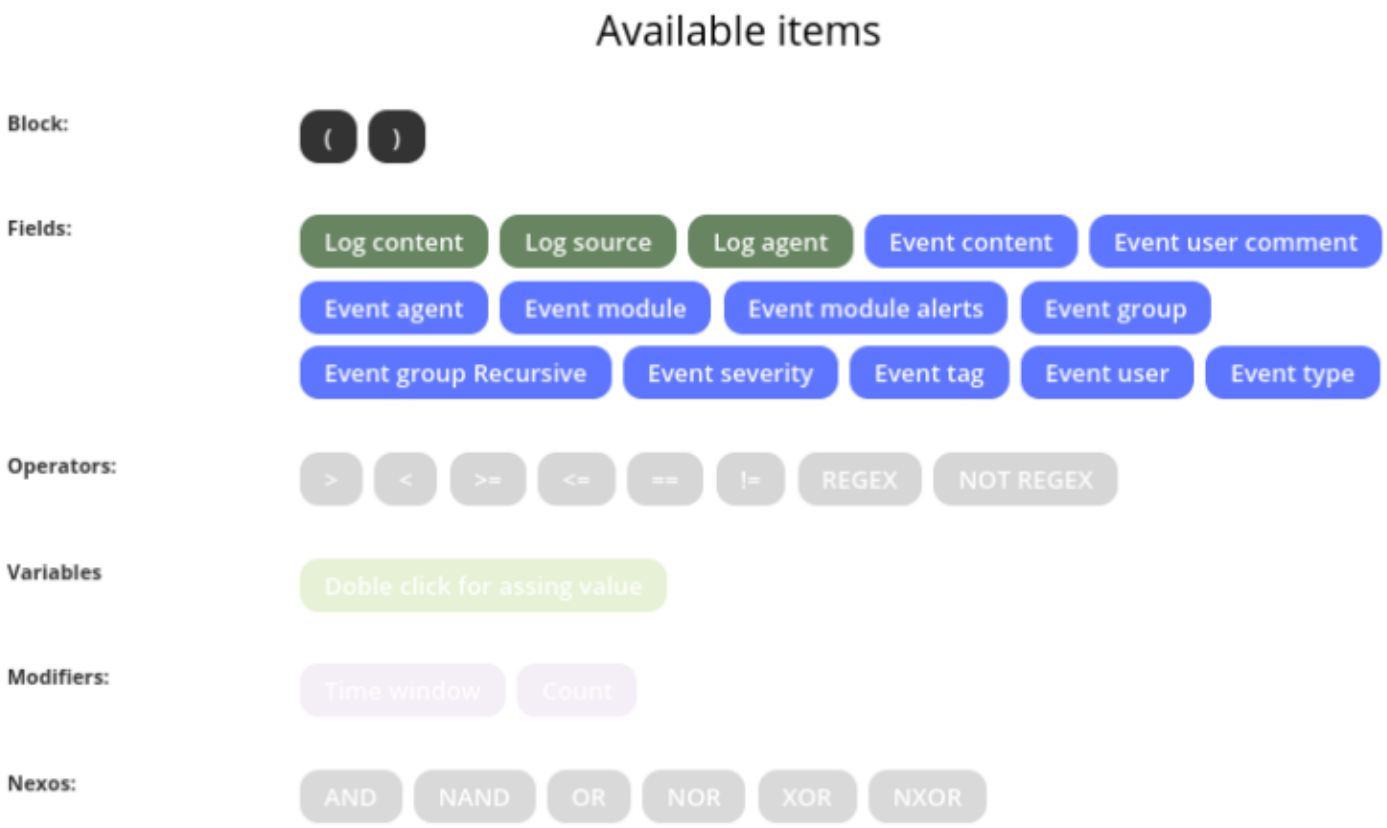
Каждое правило настроено на срабатывание при определенном типе события или *соответствии лога*; при выполнении логического уравнения, определенного правилами и их операторами, срабатывает предупреждение.

Правила внутри корреляционного предупреждения



Чтобы определить правила оповещения, вам нужно перетащить элементы с левой стороны в drop area с правой стороны, чтобы построить свое правило.

Доступные элементы конфигурации:

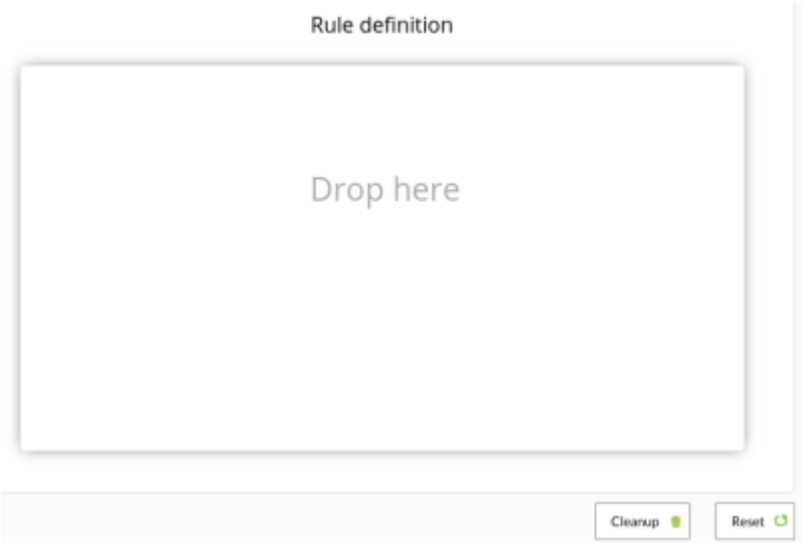


Эти элементы будут постепенно включаться, чтобы направлять пользователя в соблюдении грамматики правила. Ниже приводится упрощенное объяснение грамматики, которую следует использовать:

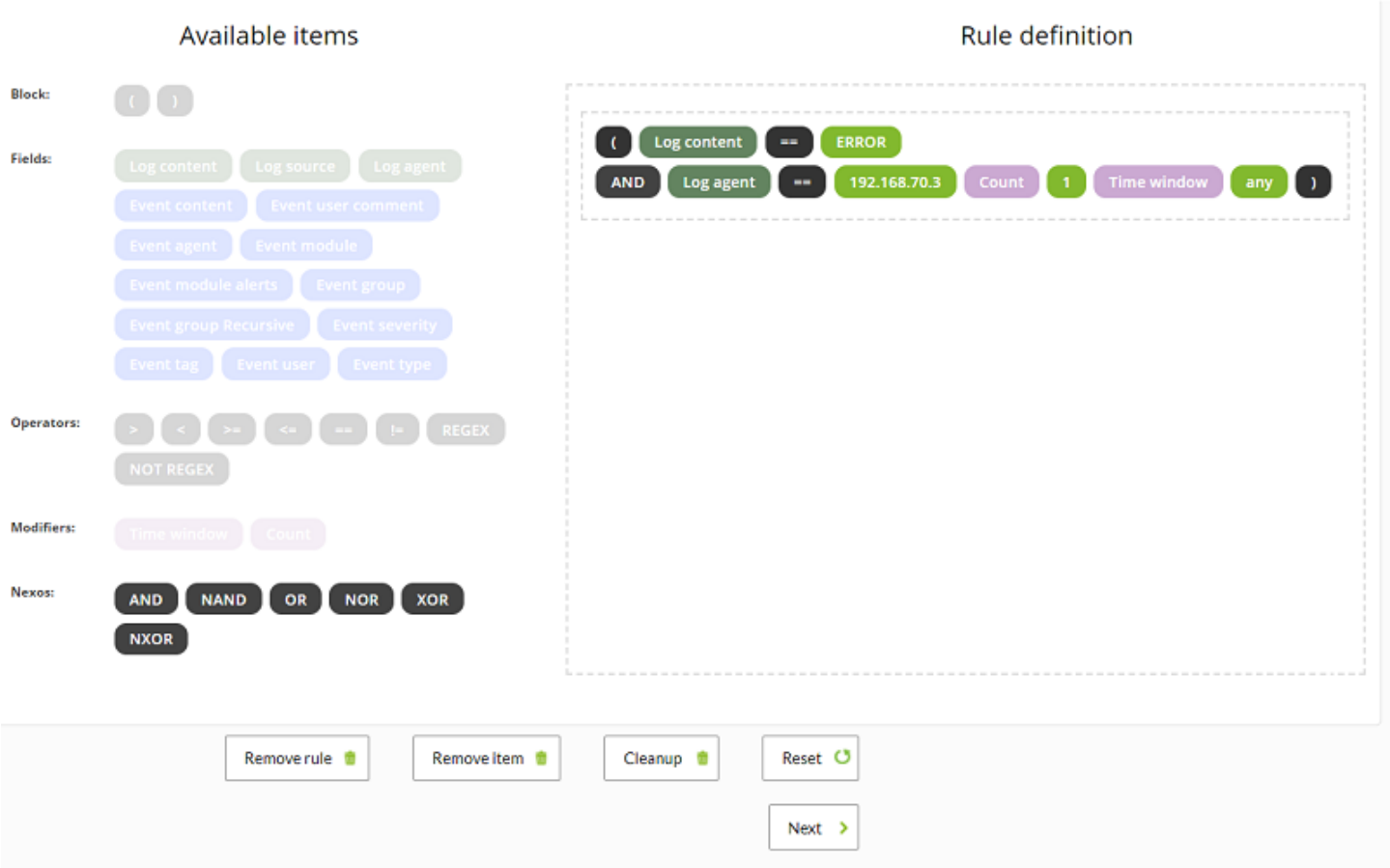
```
S -> R | R + NEXO +R
R -> ПОЛЕ + ОПЕРАТОР + C | ПОЛЕ + ОПЕРАТОР + C + МОДИФИКАТОР
C -> ПЕРЕМЕННАЯ
```

Где S - это набор правил, определенных для коррелирующего предупреждения.

Необходимо перетащить элемент в область определения правила:



Чтобы изображение выглядело, например, так:



В операторах сравнения == и != текстовые строки сравниваются буквально. Для большей гибкости вы можете использовать оператор REGEX, который применяет регулярные выражения.

Для очистки и отмены всех изменений доступны две кнопки: Cleanup и Reset.

Изменения сохранятся только после нажатия кнопки следующий (Next).

Помните:: Блоки работают одновременно при выполнении условия. Обратите внимание на следующие теоретические примеры.

```
(A and B)
```

Это заставляет анализируемый элемент (будь то событие или журнал) одновременно выполнять требования A и B.

```
A and B
```

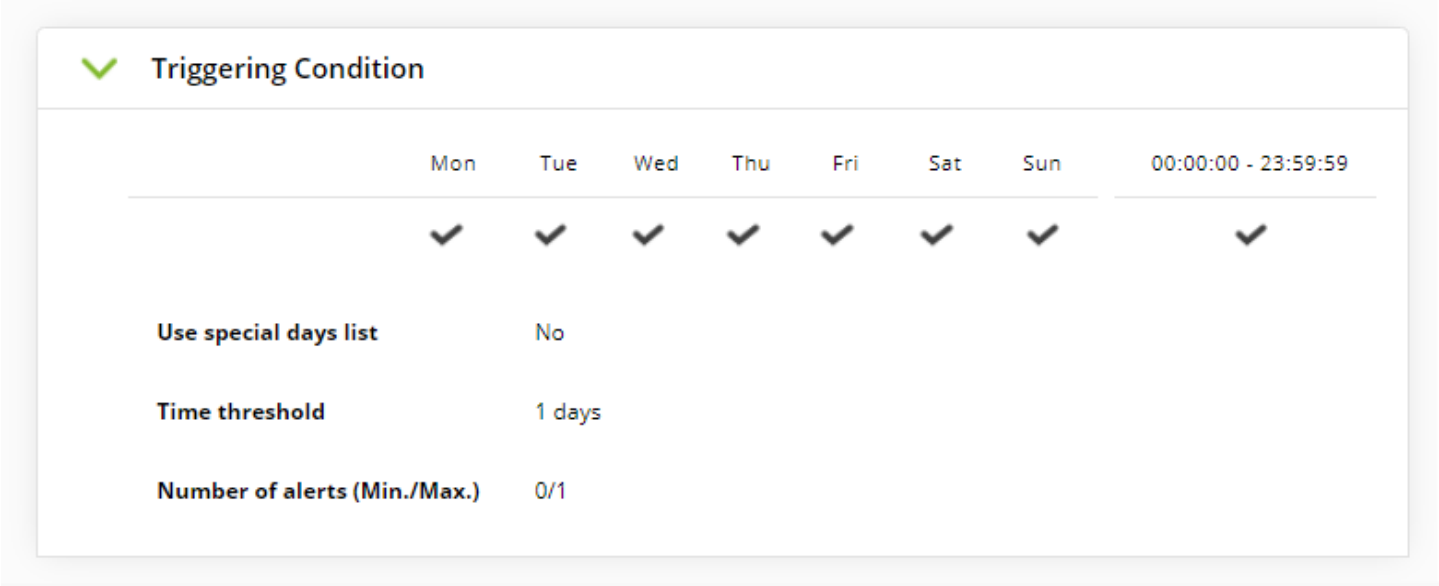
Это заставляет оба правила (A) и (B) быть выполненными в окне оценки. Это означает, что в последние секунды (определяемые параметрами `log_window` и `event_window`) должны быть записи, удовлетворяющие обоим правилам.

Поля внутри корреляционного предупреждения

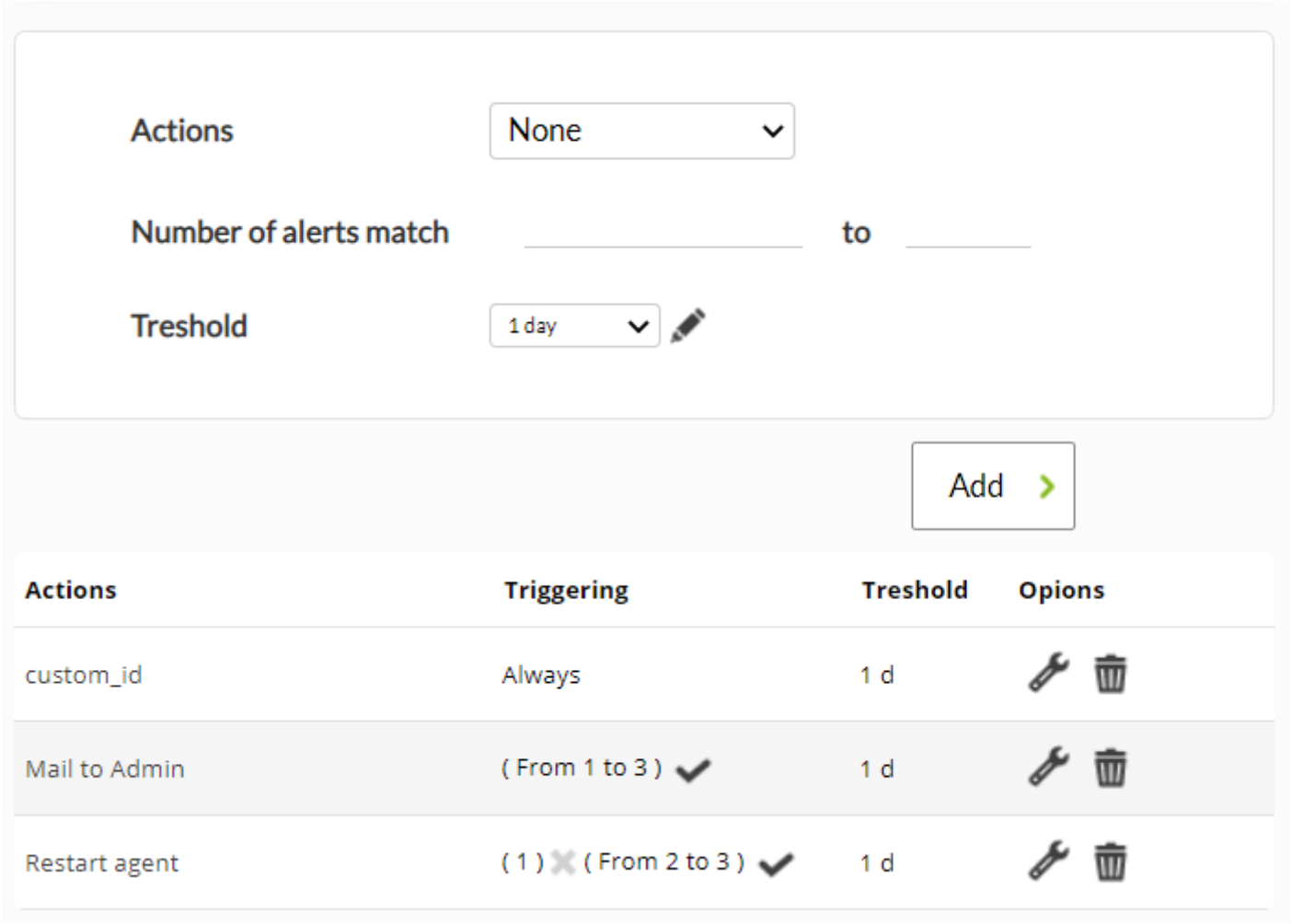
В предыдущем разделе "Система предупреждений" функционирование полей в предупреждениях объяснено более подробно.

Срабатывание в рамках корреляционного предупреждения

В этом разделе вы должны настроить действия, которые будут выполняться при срабатывании предупреждения, и указать, через какие промежутки времени и как часто будут выполняться эти действия.



В этом разделе мы видим предварительный просмотр конфигурации, которая была сделана в разделе Conditions, чтобы учесть ее при настройке выполнения действия.



Настройте действия с помощью полей:

Actions

Действия, которые вам необходимо выполнить.

Number of alerts match

Количество интервалов, которые должны пройти с момента срабатывания предупреждения до выполнения действия. Если вы хотите установить «всегда» в качестве интервала, оставьте эти поля пустыми.

Treshold

Интервал, который должен пройти для повторного выполнения действия после срабатывания сигнала тревоги.

Затем отобразите список настроенных действий. В этом списке поле triggering показывает, в каких интервалах предупреждения будет выполняться действие, как настроено в number of alerts match. Кроме того, в колонке Options можно удалить или изменить настроенные действия.

Множественные корреляционные предупреждения

Если доступно несколько предупреждений, они имеют определенный порядок оценки. Они всегда оцениваются по порядку, начиная с первого в списке.

Если мы настроим режим оценки правил PASS, то при выполнении корреляционного предупреждения будут оцениваться и следующие оповещения. Это режим *normal*.

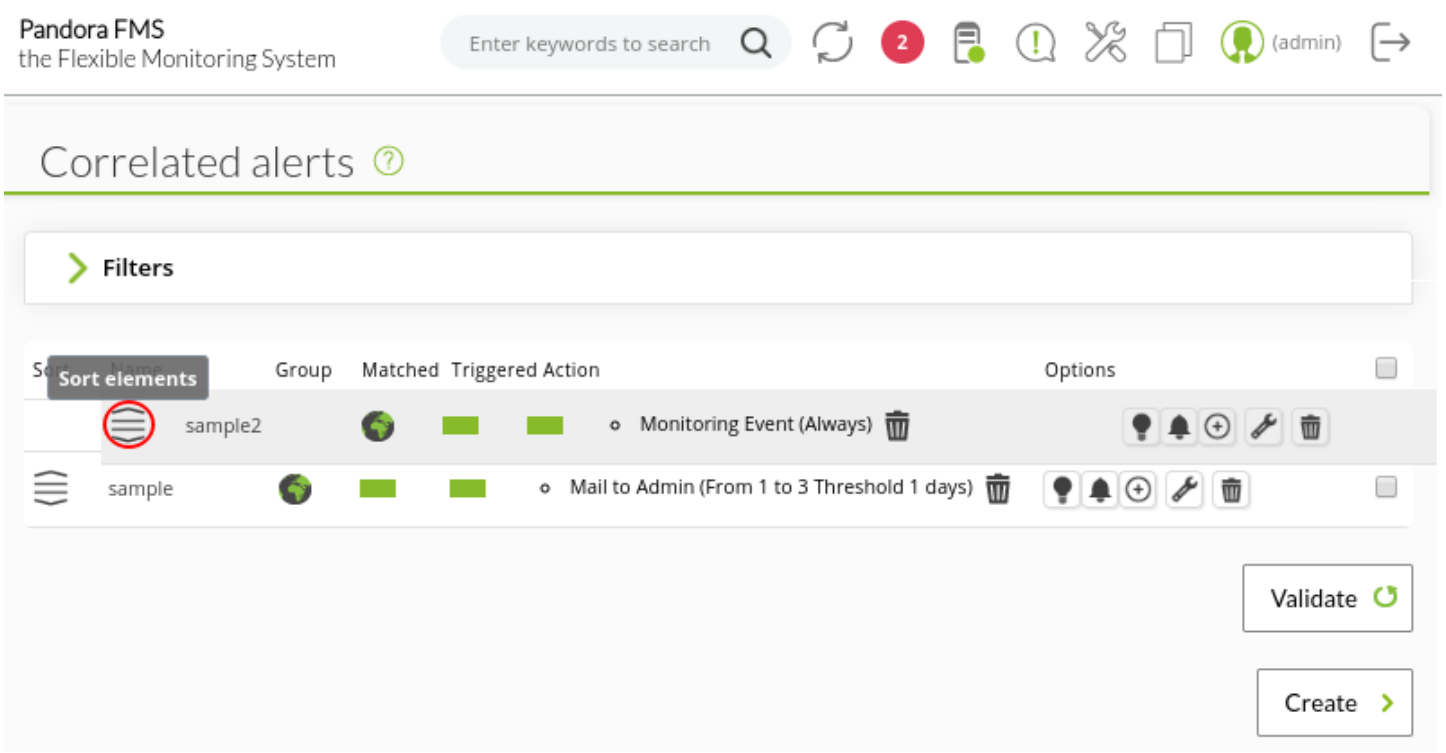
Если мы настроим режим оценки правил DROP, то при выполнении корреляционного предупреждения, настроенного с этим режимом, оценка правил, расположенных ниже него, будет остановлена. Эта функция обеспечивает возможность каскадной защиты предупреждений.

Например:

- Общее предупреждение.
- Специальное предупреждение.

Если общее предупреждение не сработало, нет необходимости оценивать специальное предупреждение. Установите оба предупреждения на DROP.

Нажмите на значок сортировки и перетащите его, чтобы изменить порядок, в котором оцениваются правила.



Остальные правила корреляции (поля действий и применение действий) работают аналогично остальным оповещениям Pandora FMS и не требуют дополнительных пояснений.

Макросы предупреждения о событии

Макросы, которые можно использовать в конфигурации предупреждений о событиях, перечислены в списке макросов в конце этой главы.

Список макросов

Макросы команд, Макросы действий и Макросы предупреждений о событиях являются общими друг для друга, но со следующими исключениями `_modulelaststatuschange_` , `_rca_` и `_secondarygroups_`

`_address_`

Адрес агента, вызвавшего предупреждение.

`_addressn_n_`

Адрес агента, соответствующий позиции, указанной в n. Пример: `addressn_1_` , `addressn_2_`

`_agent_`

Алиас агента, вызвавшего предупреждение. Если псевдоним не назначен, используется имя агента.

`_agentalias_`

Алиас агента, вызвавшего предупреждение.

`_agentcustomfield_n_`

Номер пользовательского поля n агента (например, `_agentcustomfield_9_`).

`_agentcustomid_`

Персональный идентификатор агента.

`_agentdescription_`

Описание агента, вызвавшего предупреждение.

`_agentgroup_`

Имя группы агента.

`_agentname_`

Имя агента, вызвавшего предупреждение.

agentos

Оперативная система агента.

agentstatus

Текущий статус агента.

_alert_critical_instructions_

Инструкции, содержащиеся в модуле для статуса critical.

_alert_description_

Описание предупреждения.

_alert_name_

Имя предупреждения.

_alert_priority_

Числовой приоритет предупреждения.

_alert_text_severity_

Приоритет в тексте предупреждения (Maintenance, Informational, Normal, Minor, Warning, Major, Critical).

_alert_threshold_

Порог предупреждения.

_alert_times_fired_

Количество раз срабатывания предупреждения.

_alert_unknown_instructions_

Инструкции, содержащиеся в модуле для статуса unknown.

_alert_warning_instructions_

Инструкции, содержащиеся в модуле для статуса warning.

_all_address_

Все адреса агента, вызвавшего предупреждение.

_critical_threshold_max_

Максимальный критический порог.

_critical_threshold_min_

Минимальный критический порог.

data

Данные, вызвавшие срабатывание предупреждения.

_email_tag_

Почтовые ящики, связанные с *тегами* модулей.

_event_cfX_

(Только предупреждения о событиях). Ключ пользовательского поля события, вызвавшего предупреждение. Например, если есть пользовательское поле, ключ которого IPAM, его значение можно получить с помощью макроса _event_cfIPAM_.

_event_description_

(Только предупреждения о событиях) Текстовое описание события Pandora FMS.

_event_extra_id_

(Только предупреждения о событиях) Дополнительный идентификатор.

_event_id_

(Только предупреждения о событиях) Идентификатор события, вызвавшего предупреждение.

_event_text_severity_

(Только предупреждения о событиях) Приоритет в тексте события, вызвавшего предупреждение (Maintenance, Informational, Normal Minor, Warning, Major, Critical).

eventTimestamp

Timestamp, в котором было создано событие.

fieldX

Поле X, определенное пользователем.

_group_contact_

Контактная информация группы. Настраивается при создании группы.

groupcustomid

Персональный идентификатор группы.

groupother

Другая информация о группе. Настраивается при создании группы.

homeurl

Это общедоступная ссылка URL, которая должна быть настроена в общих настройках конфигурации.

_id_agent_

Идентификатор агента, полезный для построения URL-адресов для доступа к консоли Pandora FMS.

_id_alert_

Идентификатор предупреждения, полезный для корреляции предупреждения в сторонних инструментах.

_id_group_

Идентификатор группы агента.

_id_module_

Идентификатор модуля.

interval

Интервал выполнения модуля.

module

Имя модуля.

modulecustomid

Индивидуальный идентификатор модуля.

_moduledata_X_

С помощью этого макроса («X» - имя рассматриваемого модуля) мы собираем последние данные этого модуля и, если они числовые, возвращаем их в формате с десятичными знаками, указанными в конфигурации консоли, и с единицей измерения (если она есть). Он может служить, например, для отправки электронного письма при срабатывании предупреждения модуля, а также для отправки дополнительной (и, возможно, очень актуальной) информации из других модулей того же Агента.

Если “X” (имя рассматриваемого модуля) содержит пробелы, они должны быть помещены как HTML-сущность:

Вы сможете найти список HTML-сущностей в Wikipedia.

moduledescription

Описание модуля.

_modulegraph_nh_

(Только для предупреждений, использующих команду eMail) Возвращает закодированное в base64 изображение графика модуля с периодом n часов (например, _modulegraph_24h_). Для этого необходимо правильно настроить подключение сервера к консоли через API, что делается в файле конфигурации сервера.

_modulegraphth_nh_

(Только для предупреждений, использующих команду _email_tag_) Та же операция, что и в вышеприведенном макросе, но только с критическими и предупреждающими порогами модуля, если они определены.

modulegroup

Имя группы модуля.

modulestatus

Статус модуля.

modulelaststatuschange

(Только для командных макросов)*timestamp*, в которую произошло последнее изменение состояния модуля.

`_moduletags_`

URL, связанные с *тегами* модулей.

`_name_tag_`

Имя *тегов*, связанных с модулем.

`_phone_tag_`

Телефоны, связанные с *тегами* модулей.

`_plugin_parameters_`

Параметры *плагина* модуля.

`_policy_`

Имя политики, к которой принадлежит модуль (если применимо).

`_prevdata_`

Предварительные данные до срабатывания предупреждения.

`_rca_`

Цепочка анализа первопричин (только для служб).

`_secondarygroups_`

Отображает подгруппы агента (только для макросов команд и макросов действий).

`_server_ip_`

IP-адрес сервера, на который назначен агент.

`_server_name_`

Имя сервера, на который назначен агент.

`_target_ip_`

IP-адрес цели модуля.

`_target_port_`

Порт цели модуля.

_time_down_human_

Время в длинном формате, например, «1day 10h 35m 40s» (этот макрос работает только для оповещений о восстановлении).

_time_down_seconds_

Время в секундах (этот макрос работает только для оповещений о восстановлении).

`_timestamp_`

Время и дата срабатывания предупреждения.

`_timezone_`

Часовой пояс, представленный в `_timestamp_`.

_warning_threshold_max_

Максимальный порог предупреждения.

_warning_threshold_min_

Минимальный порог предупреждения.

Вернуться в оглавление Документации Pandora FMS