



Мониторинг и сбор журналов



From:

<https://pandorafms.com/manual/!current/>

Permanent link:

https://pandorafms.com/manual/!current/ru/documentation/03_monitoring/09_log_monitoring

2024/06/10 14:36



Мониторинг и сбор журналов

[Вернуться в оглавление Документации Pandora FMS](#)

Сбор журналов

Введение

E Версия 5.0 и выше.

Мониторинг *журналов* в Pandora FMS настраивается двумя различными способами:

1. На основе модулей: Представляет *журналы* в Pandora FMS как асинхронные мониторы, способные связывать предупреждения с обнаруженными записями, которые выполняют ряд условий, предварительно настроенных пользователем. Модульное представление *журналов* позволяет:
 1. Создать модули, подсчитывающие количество происшествий регулярного выражения в *журнале*.
 2. Получение строк и контекста сообщений *журнала*.
2. На основе Комбинированной визуализации: Позволяет пользователю визуализировать в единой консоли всю информацию *журналов* из нескольких захватываемых источников, организуя информацию в последовательном порядке, используя метку времени, в которой были обработаны *журналы*.

Начиная с версии 7.0 NG 712, Pandora FMS включает **ElasticSearch** для хранения информации *журналов*, что подразумевает существенное улучшение производительности.

Как это работает



- *Журналы* проанализированные **Программными Агентами** (eventlog или текстовыми файлами), передаются на сервер Pandora FMS в «буквальном» виде (RAW) в **XML** отчета агента
- Сервер данных Pandora FMS получает XML от агента, который содержит информацию о мониторинге и *журналах*.

- Когда сервер данных обрабатывает XML-данные, он идентифицирует информацию из *журналов*, сохраняя в основной базе данных ссылки агента отчетности и источник *журнала*, а затем автоматически отправляет информацию в ElasticSearch.
- Pandora FMS хранит данные в индексах ElasticSearch, ежедневно генерируя уникальный индекс для каждого экземпляра Pandora FMS.
- Сервер Pandora FMS имеет задачу обслуживания, которая удаляет индексы через интервал, заданный системным администратором (по умолчанию 90 дней).

Конфигурация

Конфигурация сервера

Система хранения *журналов*, основанная на ElasticSearch, требует конфигурации и настройки своих компонентов.

Требования для сервера

Можно распространять Pandora FMS Server и ElasticSearch на независимых серверах.

- CentOS 7 или выше.
- Не менее 4 гигабайт оперативной памяти, хотя рекомендуется 6 ГБ оперативной памяти на каждый экземпляр ElasticSearch.
- Не менее 2 процессорных ядер.
- 20 ГБ дискового пространства для системы.
- 50 ГБ дискового пространства для данных ElasticSearch (количество может варьироваться в зависимости от объема данных, которые вы хотите хранить).
- Подключение сервера и консоли Pandora FMS к ElasticSearch API (порт по умолчанию 9200/TCP).

Установка и настройка ElasticSearch

Прежде чем приступить к установке этих компонентов, необходимо установить Java на дистрибутиве CentOS:

```
yum install java
```

После установки Java установите ElasticSearch [следуя официальной документации](#); для [сред Debian есть свои инструкции](#).

Настройка службы:

Параметры сети и, опционально, местоположение данных (и собственных журналов ElasticSearch) должны быть настроены в файле конфигурации, расположенном в `/etc/elasticsearch/elasticsearch.yml`.

```
# ----- Network -----  
-  
# Set a custom port for HTTP:  
http.port: 9200  
# ----- Paths -----  
-  
# Path to directory where to store the data (separate multiple locations by  
comma):  
path.data: /var/lib/elastic  
# Path to log files:  
path.logs: /var/log/elastic
```

Следующие строки также должны быть *декомментированы* и определены:

```
cluster.name: elkpandora  
node.name: ${HOSTNAME}  
bootstrap.memory_lock: true  
network.host: ["127.0.0.1", "IP"]
```

cluster.name

Это будет имя, присвоенное группе или *кластеру*.

node.name

Чтобы назвать узел с помощью системной переменной `${HOSTNAME}`, он автоматически принимает имя хоста.

bootstrap.memory_lock

Это всегда должно быть правдой «true».

network.host

IP-адрес сервера.

- В случае работы с одним узлом необходимо также добавить следующую строку:

```
discovery.type: single-node
```

- В случае работы с *кластером* нам потребуется заполнить параметр `discovery.seed_hosts`.

```
discover.seed_hosts : [{"ip:port"},|"ip", "ip"]]
```

Или же:

```
discovery.seed_hosts:  
- 192.168.1.10:9300  
- 192.168.1.11
```

```
- seeds.mydomain.com
```

Определите параметры ресурсов, назначенных ElasticSearch, путем настройки параметров, доступных в конфигурационном файле, расположенном по адресу `/etc/elasticsearch/jvm.options`. Рекомендуется использовать не менее 2 ГБ пространства на XMS.

```
# Xms represents the initial size of total heap space
# Xmx represents the maximum size of total heap space
-Xms2g
-Xmx2g
```

Распределение ресурсов будет зависеть от предполагаемого использования ElasticSearch, мы рекомендуем следовать [официальной документации](#).

Также необходимо изменить параметр `memlock unlimited` в конфигурационном файле ElasticSearch, расположенном в файле `/usr/lib/systemd/system/elasticsearch.service`, чтобы добавить следующий параметр:

```
MAX_LOCKED_MEMORY = unlimited
```

После завершения необходимо будет выполнить:

```
systemctl daemon-reload && systemctl restart elasticsearch
```

Команда для запуска службы следующая:

```
systemctl start elasticsearch
```

Если служба не запускается, проверьте журналы, расположенные в `/var/log/elasticsearch/`

Чтобы проверить установку ElasticSearch, выполните следующую команду в окне терминала:

```
curl -q http://{IP}:9200/
```

Вы получите ответ, аналогичный следующему:

```
{
  "name" : "3743885b95f9",
  "cluster_name" : "docker-cluster",
  "cluster_uuid" : "7oJV9hXqRw0IZVPBRbWIYw",
```

```
"version" : {
  "number" : "7.6.2",
  "build_flavor" : "default",
  "build_type" : "docker",
  "build_hash" : "ef48eb35cf30adf4db14086e8aabd07ef6fb113f",
  "build_date" : "2020-03-26T06:34:37.794943Z",
  "build_snapshot" : false,
  "lucene_version" : "8.4.0",
  "minimum_wire_compatibility_version" : "6.8.0",
  "minimum_index_compatibility_version" : "6.0.0-beta1"
},
"tagline" : "You Know, for Search"
}
```

Рекомендуется посетить ссылку на best practices Elasticsearch для производственных сред:

<https://www.elastic.co/guide/en/elasticsearch/reference/current/system-config.html#dev-vs-prod>

Pandora FMS Syslog Server

E Версия NG 717 или выше.

Этот компонент позволяет Pandora FMS анализировать **syslog** машины, на которой он расположен, анализируя его содержимое и сохраняя ссылки в соответствующем сервере Elasticsearch.

Основным преимуществом сервера Syslog является то, что он дополняет унификацию журналов.. Поддерживая функции экспорта Syslog Server в среды Linux® и Unix®, Syslog Server позволяет выполнять запросы журналов независимо от источника, осуществляя поиск в одной общей точке (средство просмотра журналов консоли Pandora FMS).

Установка Syslog Server должна быть выполнена как на клиенте, так и на сервере, а для ее выполнения необходимо запустить следующую команду:

```
yum install rsyslog
```

После установки syslog на используемое оборудование, нужно зайти в конфигурационный файл `/etc/rsyslog.conf`, чтобы включить *input* TCP и UDP.

(...)

```
# Provides UDP syslog reception
$ModLoad imudp
$UDPServerRun 514
```

```
# Provides TCP syslog reception
$ModLoad imtcp
$InputTCPServerRun 514

(...)
```

После выполнения этой настройки необходимо будет остановить и перезапустить службу rsyslog. Как только служба станет доступной, проверьте, что порт 514 доступен с помощью:

```
netstat -ltnp
```

Для получения дополнительной информации о настройке rsyslog, [посетите официальный сайт](#).

Настройте Клиента так, чтобы он мог отправлять журналы на сервер Syslog Server. Для этого еще раз зайдите в файл конфигурации rsyslog /etc/rsyslog.conf в клиенте . Найдите и включите строку, которая позволяет настроить удаленный хост.

```
.* @@remote-host:514
```

При отправке журналов создается агент-контейнер с именем клиента, поэтому рекомендуется создавать агентов с "alias as name", чтобы он совпадал с hostname клиента, что позволит избежать дублирования агентов.

Чтобы активировать эту функцию в Pandora FMS Server, включите в файл pandora_server.conf следующее содержание:

```
# Enable (1) or disable (0) the Pandora FMS Syslog Server
# (PANDORA FMS ENTERPRISE ONLY).
syslogserver 1

# Full path to syslog's output file (PANDORA FMS ENTERPRISE ONLY).
syslog_file /var/log/messages

# Number of threads for the Syslog Server
# (PANDORA FMS ENTERPRISE ONLY).
syslog_threads 2

# Maximum number of lines queued by the Syslog Server's
# producer on each run (PANDORA FMS ENTERPRISE ONLY).
syslog_max 65535
```

syslogserver

Булево, включает (1) или выключает (0) локальный механизм разбора SYSLOG.

syslog_file

Расположение файла, в который доставляются записи SYSLOG.

syslog_threads

Максимальное количество потоков, которые будут использоваться в системе производитель/потребитель Syslog Server.

syslog_max

Это максимальное окно обработки для сервера Syslog; будет максимальным количеством записей SYSLOG, которые будут обрабатываться в каждой итерации.

Вам понадобится включенный и настроенный сервер ElasticSearch; ознакомьтесь с предыдущими пунктами, чтобы узнать, как это сделать.

Помните, что вам необходимо изменить конфигурацию вашего устройства таким образом, чтобы журналы отправлялись на сервер Pandora FMS.

Рекомендации

Вращение журнала для ElasticSearch

Важно: Чтобы предотвратить неконтрольный рост журналов ElasticSearch, необходимо создать новую запись для демона или *daemon* вращения журналов в `/etc/logrotate.d`

```
cat> /etc/logrotate.d/elastic <<EOF
/var/log/elastic/elasticsearch.log {
    weekly
    missingok
    size 300000
    rotate 3
    maxage 90
    compress
    notifempty
    copytruncate
}
EOF
```

Очистка индексов

Список индексов и занимаемый ими размер можно посмотреть в любое время, запустив cURL запрос к серверу ElasticSearch:

```
curl -q http://<elastic>9200/_cat/indices?
```

Где `elastic` означает IP-адрес сервера.

Чтобы удалить любой из этих индексов, вы можете выполнить команду `DELETE`:

```
curl -q -XDELETE http://<elastic>9200/{index-name}
```

Где `{index-name}` - выходной файл вышеуказанной команды. Эта операция освобождает место, используемое удаленным индексом.

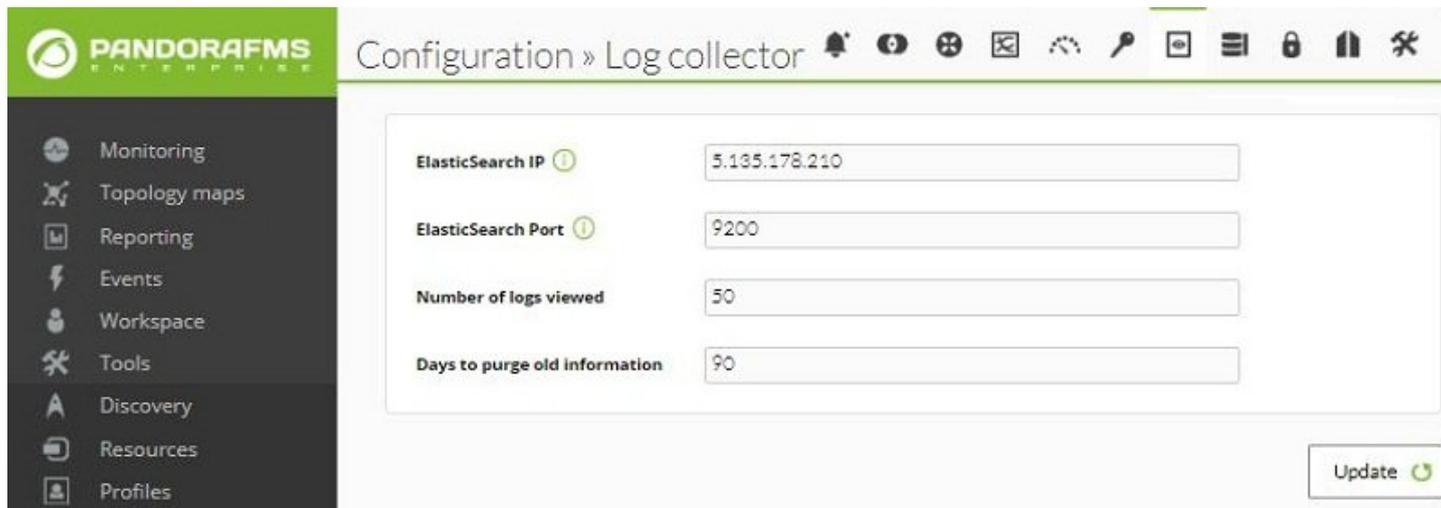
Конфигурация консоли

Чтобы активировать систему отображения журналов, необходимо активировать следующую конфигурацию:

The screenshot shows the PandoraFMS Enterprise configuration interface. The left sidebar contains the following menu items: Monitoring, Topology maps, Reporting, Events, Workspace, Tools, Discovery, Resources, Profiles, Configuration, Alerts, Events, Servers, **Setup**, Admin tools, Links, and Update manager. The main configuration panel includes the following settings:

- Use Enterprise ACL System:
- Collection size: 1000000 Bytes
- Event replication:
- Metaconsole DB engine: MySQL
- Metaconsole DB host: [Empty field]
- Metaconsole DB name: [Empty field]
- Metaconsole DB user: [Empty field]
- Metaconsole DB password: [Empty field]
- Metaconsole DB port: [Empty field]
- Inventory change blacklist:
- Inventory change blacklist items:
 - Out of black list: CDROM (Linux), CDROM (Windows), Cisco Configuration (Cisco), Cisco Interface Remote Inventory S, Cisco Interface Remote Inventory S, Cisco Interface Remote Inventory (Cisco Inventory (Cisco)), File system (Linux), File system (Windows), HD (Linux)
 - Into black list: CPU (Linux), CPU (Windows), Process (Linux), Process (Windows)
- Activate Log Collector: (highlighted in a red box)
- Enable update manager:
- Critical threshold for occupied addresses: 90
- Warning threshold for occupied addresses: 80

Затем вы можете настроить поведение средства просмотра журнала в Configuration > Log Collector:



The screenshot displays the Pandora FMS Configuration > Log collector interface. The left sidebar contains navigation options: Monitoring, Topology maps, Reporting, Events, Workspace, Tools, Discovery, Resources, and Profiles. The main content area shows the following configuration fields:

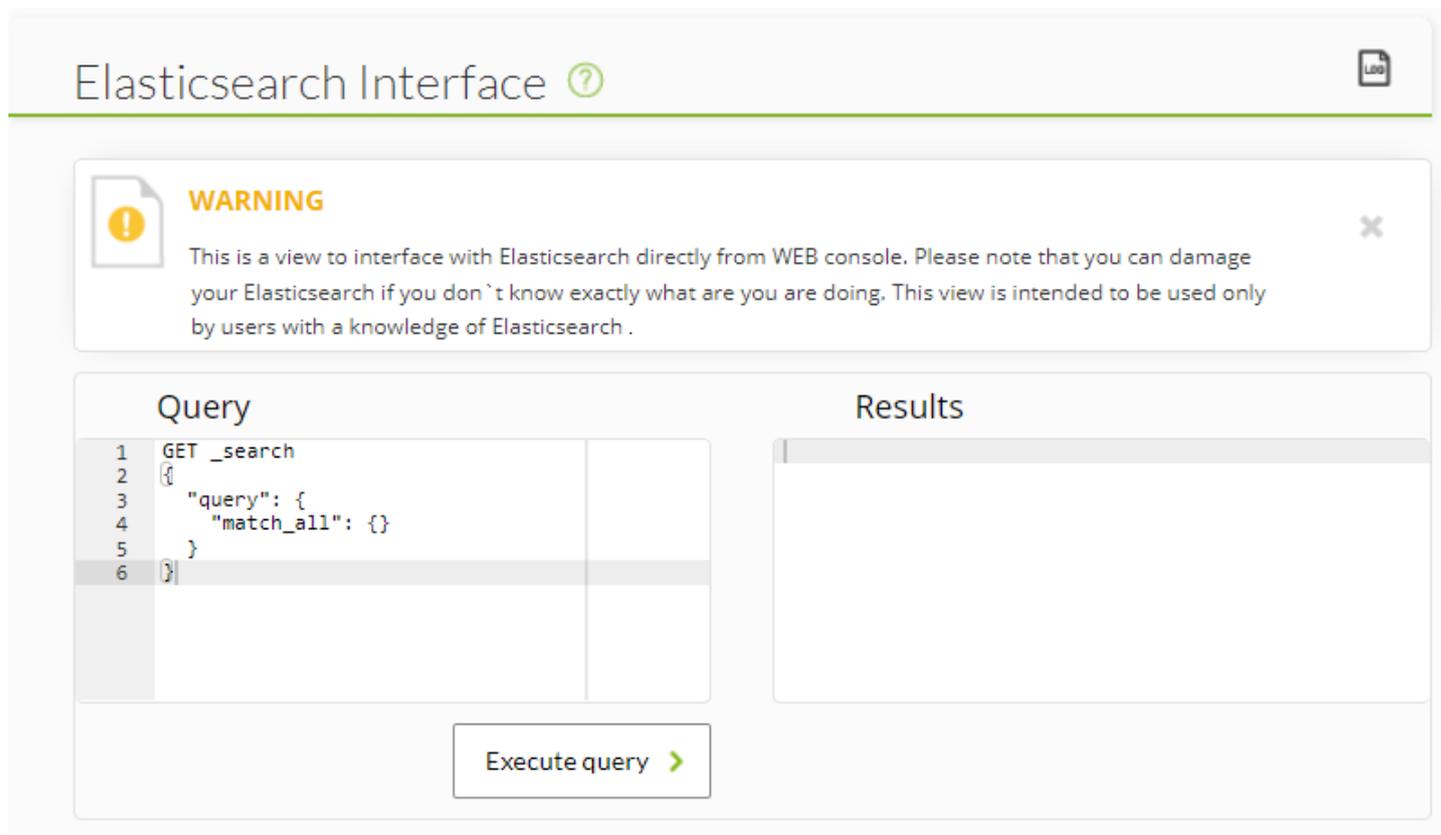
| Field | Value |
|-------------------------------|---------------|
| ElasticSearch IP | 5.135.178.210 |
| ElasticSearch Port | 9200 |
| Number of logs viewed | 50 |
| Days to purge old information | 90 |

An 'Update' button with a refresh icon is located at the bottom right of the configuration area.

- IP-адрес или FQDN и порт сервера, на котором размещена служба ElasticSearch
- Number of logs viewed: Для ускорения отклика консоли была добавлена динамическая загрузка записей. Пользователь должен прокрутить страницу до самого низа, что заставит загрузить следующий доступный набор записей, сгруппированных в определенном количестве;
- Days to purge old information: Чтобы избежать перегрузки размера системы, вы можете определить максимальное количество дней, в течение которых будет храниться информация журналов; начиная с этой даты, она будет автоматически удаляться в процессе очистки Pandora FMS.

ElasticSearch Interface

E Версия NG 747 или выше.



Elasticsearch Interface ?

WARNING

This is a view to interface with Elasticsearch directly from WEB console. Please note that you can damage your Elasticsearch if you don't know exactly what are you are doing. This view is intended to be used only by users with a knowledge of Elasticsearch .

Query

```
1 GET _search
2 {
3   "query": {
4     "match_all": {}
5   }
6 }
```

Results

Execute query >

В конфигурации по умолчанию, Pandora FMS генерирует один индекс в день, который ElasticSearch должен фрагментировать и распределить для будущего поиска.

Чтобы эти поиски были оптимальными, по умолчанию ElasticSearch генерирует индекс для каждого из них, поэтому мы должны настроить в нашей среде столько же поисков, сколько узлов ElasticSearch установлено.

Эти search и реплики настраиваются при создании индекса, который Pandora FMS генерирует автоматически, поэтому для изменения этой конфигурации мы должны использовать шаблоны или *templates*.

Шаблоны Elasticsearch

Шаблоны или *templates* - это конфигурации, которые применяются только во время создания индекса.

Изменение *template* не повлияет на уже существующие индексы.

Для создания базового *template* достаточно определить следующие поля:

```
{
  "index_patterns": ["pandorafms*"],
  "settings": {
    "number_of_shards": 1,
```

```
"auto_expand_replicas" : "0-1",
"number_of_replicas" : "0"
},
"mappings" : {
  "properties" : {
    "agent_id" : {
      "type" : "long",
      "fields" : {
        "keyword" : {
          "type" : "keyword",
          "ignore_above" : 256
        }
      }
    },
    "group_id" : {
      "type" : "long",
      "fields" : {
        "keyword" : {
          "type" : "keyword",
          "ignore_above" : 256
        }
      }
    },
    "group_name" : {
      "type" : "text",
      "fields" : {
        "keyword" : {
          "type" : "keyword",
          "ignore_above" : 256
        }
      }
    },
    "logcontent" : {
      "type" : "text",
      "fields" : {
        "keyword" : {
          "type" : "keyword",
          "ignore_above" : 256
        }
      }
    },
    "source_id" : {
      "type" : "text",
      "fields" : {
        "keyword" : {
          "type" : "keyword",
          "ignore_above" : 256
        }
      }
    },
    "suid" : {
      "type" : "text",
```

```
    "fields" : {
      "keyword" : {
        "type" : "keyword",
        "ignore_above" : 256
      }
    },
    "type" : {
      "type" : "text",
      "fields" : {
        "keyword" : {
          "type" : "keyword",
          "ignore_above" : 256
        }
      }
    },
    "utimestamp" : {
      "type" : "long"
    }
  }
}
```

Если вам нужно определить многоузловой *template*, вам следует учесть следующую информацию:

При настройке *шаблона* (формат JSON), вам нужно настроить столько *search*, сколько узлов у вас есть, однако для правильной настройки реплик вы должны вычесть 1 из количества узлов среды.

Например, в среде Pandora FMS с Elasticsearch с 3 настроенными узлами, когда вы изменяете поля `number_of_search` и `number_of_replicas`, это должно выглядеть следующим образом:

```
{
  "index_patterns": ["pandorafms*"],
  "settings": {
    "number_of_shards": 3,
    "auto_expand_replicas" : "0-1",
    "number_of_replicas" : "2"
  },
}
```

Вы можете выполнять эти операции через интерфейс Elasticsearch в Pandora FMS, используя собственные команды Elasticsearch.

- `PUT _template/<nombredeltemplate>`: позволяет ввести данные нашего *шаблона*.
- `GET _template/><nombredeltemplate>`: позволяет отобразить *template*.

Elasticsearch Interface **WARNING**

This is a view to interface with Elasticsearch directly from WEB console. Please note that you can damage your Elasticsearch if you don't know exactly what are you are doing. This view is intended to be used only by users with a knowledge of Elasticsearch .



Query

1 GET _template/pandorafms|

Results

```
{
  "pandorafms": {
    "order": 0,
    "index_patterns": [
      "pandorafms*"
    ],
    "settings": {
      "index": {
        "number_of_shards": "1",
        "auto_expand_replicas": "0-1",
        "number_of_replicas": "0"
      }
    },
    "mappings": {
      "properties": {
        "agent_id": {
          "type": "long",
          "fields": {
            "keyword": {
              "ignore_above": 256,
              "type": "keyword"
            }
          }
        },
        "group_id": {
          "type": "long",
          "fields": {
            "keyword": {
              "ignore_above": 256,
              "type": "keyword"
            }
          }
        },
        "group_name": {
          "type": "text",
          "fields": {
            "keyword": {
              "ignore_above": 256,
              "type": "keyword"
            }
          }
        },
        "utimestamp": {
          "type": "long"
        },
        "source_id": {
          "type": "text",
          "fields": {
            "keyword": {
              "ignore_above": 256,
              "type": "keyword"
            }
          }
        },
        "suid": {
          "type": "text",
          "fields": {
            "keyword": {
              "ignore_above": 256,
              "type": "keyword"
            }
          }
        }
      }
    }
  }
}
```

Execute query 

Миграция в систему Elasticsearch

После настройки новой системы хранения журналов вы можете перенести все данные, ранее хранившиеся в Pandora FMS, распределенным образом в каталогах в новую систему.

Для этого необходимо выполнить следующий скрипт, который находится в `/usr/share/pandora_server/util/`

```
# Migrate Log Data <7.0NG 712 to>= 7.0NG 712  
/usr/share/pandora_server/util/pandora_migrate_logs.pl  
/etc/pandora/pandora_server.conf
```

Визуализация и поиск

В инструменте сбора журналов интерес представляют две основные характеристики: возможность поиска информации - фильтрация по дате, источникам данных и/или ключевым словам и т.д. - и возможность визуализации этой информации в виде графиков происшествий за единицу времени. В этом примере мы ищем все сообщения журнала из всех источников за последний час; обратите внимание на Search, Start date и End date:

PANDORAFMS ENTERPRISE Pandora FMS the Flexible Monitoring System

Enter keywords to search

Log viewer

Search mode: Order:

Search: Source:

Agent: Group:

Start date: 13:50:25 End date: 14:50:25

[Advanced options](#)

Search Export to CSV [>](#)

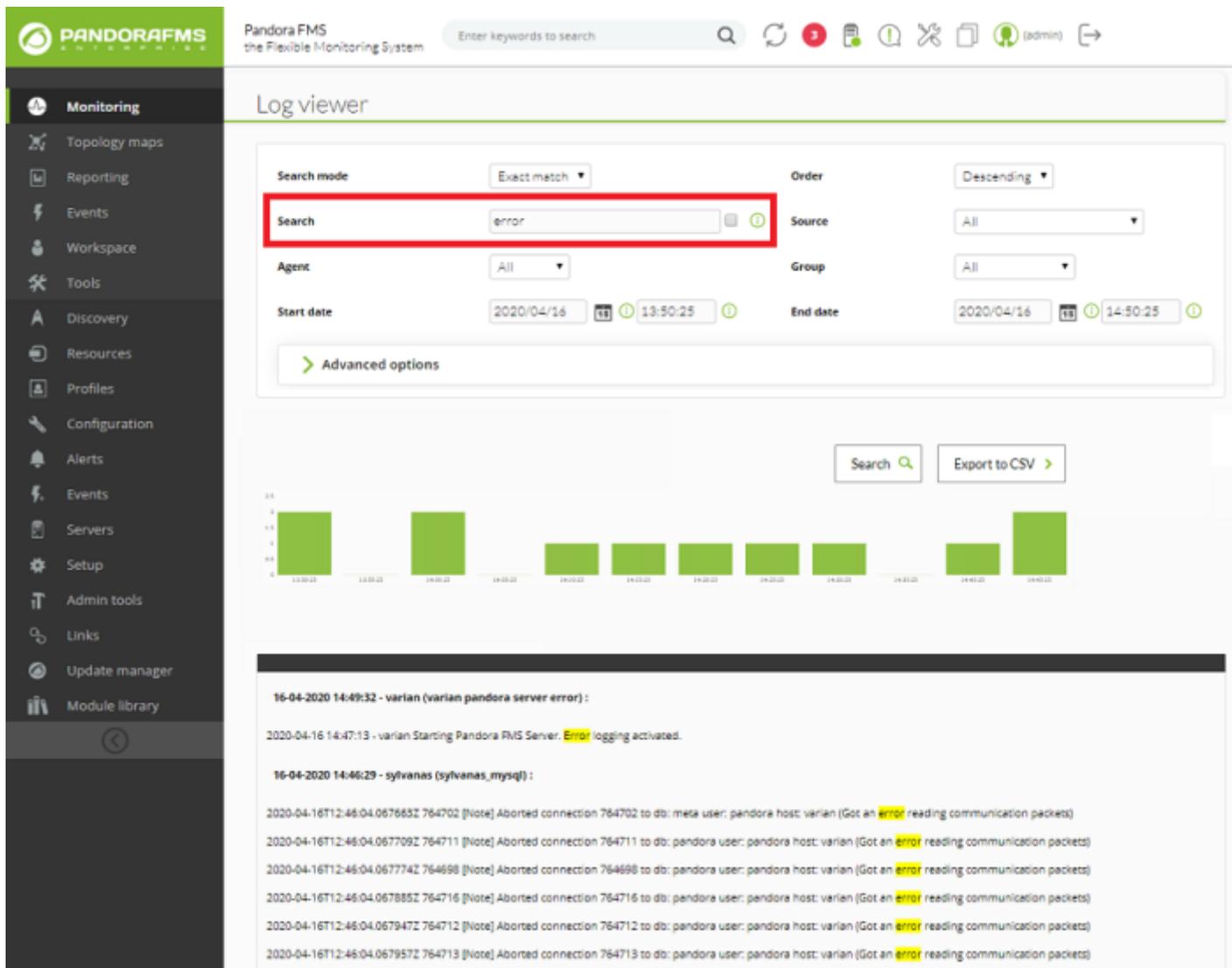
16-04-2020 14:50:01 - varian (Syslog):
 Apr 16 14:50:01 varian systemd: Started Session 5649 of user root.
 16-04-2020 14:50:01 - varian (Syslog):
 Apr 16 14:50:01 varian systemd: Started Session 5647 of user root.
 16-04-2020 14:50:01 - varian (Syslog):
 Apr 16 14:50:01 varian systemd: Started Session 5648 of user root.
 16-04-2020 14:49:32 - varian (varian pandora console log):
 CRON running [20336]
 CRON running [20336]
 Apr 16 14:45:01 ConsoleSupervisor: running.
 CRON running [30531]
 CRON running [30531]
 Apr 16 14:46:02 ConsoleSupervisor: running.
 CRON running [27826]
 CRON running [27826]

Просмотр происшествий во времени

Самым важным - и полезным - полем будет строка поиска, которую нужно ввести в текстовое поле Search в сочетании с тремя доступными типами поиска (Search mode).

Exact match

Буквальный строковый поиск, log содержит точное совпадение.



The screenshot shows the Pandora FMS Log viewer interface. The search mode is set to "Exact match" and the search term is "error". The search results are displayed as a bar chart and a list of log entries.

Search mode: Exact match

Search: error

Order: Descending

Agent: All

Start date: 2020/04/16 13:50:25

End date: 2020/04/16 14:50:25

Advanced options: >

Search results:

- 16-04-2020 14:49:32 - varian (varian pandora server error) :
- 2020-04-16 14:47:13 - varian Starting Pandora FMS Server. **Error** logging activated.
- 16-04-2020 14:46:29 - sylvanas (sylvanas_mysql) :
- 2020-04-16T12:46:04.067663Z 764702 [Note] Aborted connection 764702 to db: meta user: pandora host: varian (Got an **error** reading communication packets)
- 2020-04-16T12:46:04.067709Z 764711 [Note] Aborted connection 764711 to db: pandora user: pandora host: varian (Got an **error** reading communication packets)
- 2020-04-16T12:46:04.067774Z 764698 [Note] Aborted connection 764698 to db: pandora user: pandora host: varian (Got an **error** reading communication packets)
- 2020-04-16T12:46:04.067885Z 764716 [Note] Aborted connection 764716 to db: pandora user: pandora host: varian (Got an **error** reading communication packets)
- 2020-04-16T12:46:04.067947Z 764712 [Note] Aborted connection 764712 to db: pandora user: pandora host: varian (Got an **error** reading communication packets)
- 2020-04-16T12:46:04.067957Z 764713 [Note] Aborted connection 764713 to db: pandora user: pandora host: varian (Got an **error** reading communication packets)

All words

Поиск, содержащий все указанные слова, независимо от порядка в одной и той же строке лога (обратите внимание, что каждое слово разделено пробелами).



Log viewer

Search mode Order Search Source Agent Group Start date End date [Advanced options](#)

Search

Export to CSV [>](#)**16-04-2020 14:50:01 - varian (Syslog) :**

Apr 16 14:50:01 varian systemd: Started Session 5649 of user root.

16-04-2020 14:50:01 - varian (Syslog) :

Apr 16 14:50:01 varian systemd: Started Session 5647 of user root.

16-04-2020 14:50:01 - varian (Syslog) :

Apr 16 14:50:01 varian systemd: Started Session 5648 of user root.

16-04-2020 14:49:01 - varian (Syslog) :

Apr 16 14:49:01 varian systemd: Started Session 5645 of user root.

16-04-2020 14:49:01 - varian (Syslog) :

Any word

Поиск содержащий *любое* из указанных слов, независимо от порядка.

Pandora FMS
the Flexible Monitoring System

Enter keywords to search

Refresh 5 Alerts Settings Help Logout (admin)

Log viewer

Search mode: Any word

Search: System Error

Agent: All

Start date: 2020/04/16 13:50:25

Order: Descending

Source: All

Group: All

End date: 2020/04/16 14:50:25

> Advanced options

Search Export to CSV



```
16-04-2020 14:50:01 - varian (Syslog) :
Apr 16 14:50:01 varian systemd: Started Session 5649 of user root.

16-04-2020 14:50:01 - varian (Syslog) :
Apr 16 14:50:01 varian systemd: Started Session 5647 of user root.

16-04-2020 14:50:01 - varian (Syslog) :
Apr 16 14:50:01 varian systemd: Started Session 5648 of user root.

16-04-2020 14:49:32 - varian (varian pandora server error) :
2020-04-16 14:47:13 - varian Starting Pandora FMS Server. Error logging activated.

16-04-2020 14:49:01 - varian (Syslog) :
```

Если мы отметим опцию просмотра контекста отфильтрованного содержимого, мы получим обзор ситуации с информацией из других строк журналов, связанных с нашим поиском:

16-04-2020 14:49:32 - varian (varian pandora server error):

```
Use of uninitialized value $local_alert_status in numeric ne (!=) at /usr/lib/perl5/PandoraFMS/Enterprise.pm line 1606, <_AMONIO_> line 1.
Use of uninitialized value $status in numeric eq (==) at /usr/lib/perl5/PandoraFMS/Enterprise.pm line 1610, <_AMONIO_> line 1.
2020-04-16 14:47:13 - varian Starting Pandora FMS Server. Error logging activated.
```

16-04-2020 14:46:29 - sylvanas (sylvanas_mysql):

```
2020-04-16T12:46:04.067663Z 764702 [Note] Aborted connection 764702 to db: meta user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.067709Z 764711 [Note] Aborted connection 764711 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.067774Z 764698 [Note] Aborted connection 764698 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.067885Z 764716 [Note] Aborted connection 764716 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.067947Z 764712 [Note] Aborted connection 764712 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.067957Z 764713 [Note] Aborted connection 764713 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.067968Z 764735 [Note] Aborted connection 764735 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.068078Z 764710 [Note] Aborted connection 764710 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.068083Z 764719 [Note] Aborted connection 764719 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.068110Z 764700 [Note] Aborted connection 764700 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.068120Z 764724 [Note] Aborted connection 764724 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.068157Z 764699 [Note] Aborted connection 764699 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.068195Z 764723 [Note] Aborted connection 764723 to db: pandora user: pandora host: varian (Got an error reading communication packets)
2020-04-16T12:46:04.068244Z 764714 [Note] Aborted connection 764714 to db: pandora user: pandora host: varian (Got an error reading communication packets)
```

Расширенная визуализация и поиск:

E Версия NG 727 или выше.

С помощью этой функции вы можете графически отображать записи журнала, сортируя информацию на основе моделей захвата данных.

Эти модели захвата данных в основном представляют собой регулярные выражения и идентификаторы, которые позволяют разобрать источник данных и отобразить его в виде графика.

Для доступа к расширенным опциям нажмите на Advanced options. Появится форма, в которой можно выбрать тип просмотра результатов:

- Показать записи журнала (простой текст).
- Показать график журнала.

The screenshot shows the search configuration interface for Pandora FMS. It includes the following fields and options:

- Search mode:** Exact match
- Search:** GET /pandora_console/operation/agentes
- Source:** httpd_access
- Agent:** All
- Group:** All
- Start date:** 2018/08/01 00:00:00
- End date:** 2018/09/24 11:10:17
- Advanced options:**
 - Display mode:** Graph log results
 - Use capture model:** Apache log model. Next to it are a pencil icon for editing and a plus icon for creating a new model.
 - Graph type:** Vertical bars

В опции *показать график журнала* мы можем выбрать модель захвата.

Модель по умолчанию, Apache log model, предлагает возможность обработки или разбора журналов Apache в стандартном формате (`access_log`), позволяя извлекать сравнительные графики времени отклика, сгруппированные по посещенным страницам и коду ответа:

This screenshot is identical to the one above, but with a red rectangular box highlighting the 'Create new model' button (the plus icon) in the 'Use capture model' section of the advanced options.

Вы можете либо нажать кнопку редактирования , либо кнопку создания , чтобы создать новую модель захвата.

Edit capture model [X]

Title: Apache log model

Capture regexp: ^.*?\s+.*.*?\s(\V.*?)\?.*1.1"\s+(.*?)\s-

Fields: pagina, html_err_code, _tiempo_ [✓] ★

[Delete] [Update]

Capture regexp

Регулярное выражение для захвата данных, каждое извлекаемое поле идентифицируется подвыражением в скобках (*выражение для захвата*).

Fields

Поля в том порядке, в котором мы зафиксировали их с помощью регулярного выражения. Результаты будут сгруппированы по конкатенации ключевых полей, то есть тех, названия которых не заключены в символы подчеркивания:

key, _value_

key1, key2, _value_

key1, _value_, key2

Примечание: Если мы не укажем поле значений, будет автоматически подсчитываться количество вхождений, соответствующих регулярному выражению.

Примечание 2: Если мы указываем столбец *value*, мы можем выбрать между представлением кумулятивного значения (поведение по умолчанию) или установлением флажка для представления среднего значения.

Пример

Извлечение записей из *журнала* со следующим форматом:

```
Sep 19 12:05:01 nova systemd: Starting Session 6132 of user root.
Sep 19 12:05:01 nova systemd: Starting Session 6131 of user root.
```

Подсчет количества раз, когда они входили в систему, сгруппированных по пользователям:

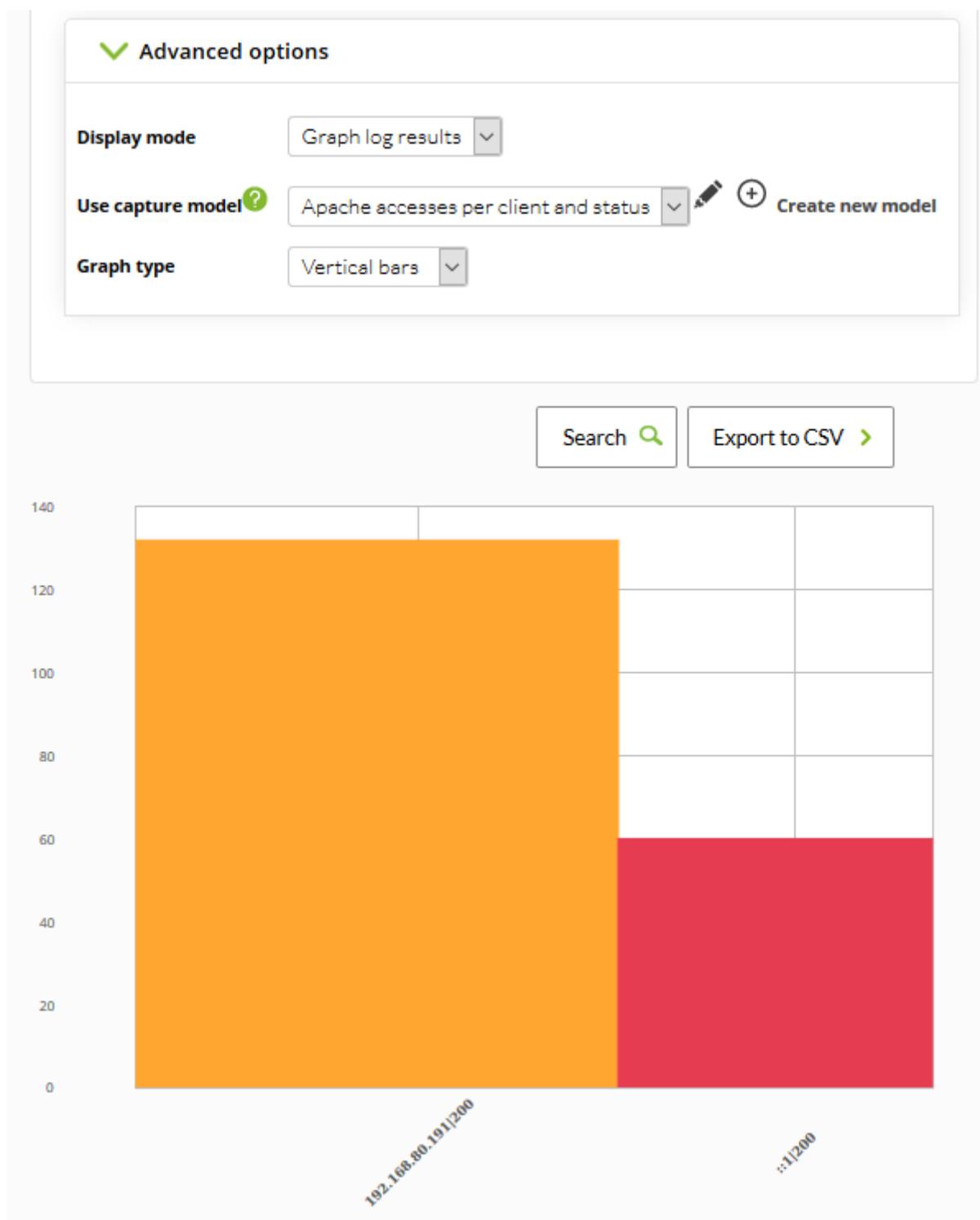
Регулярное выражение

```
Starting Session \d+ of user (.*)\.
```

Поля:

```
username
```

Эта модель захвата возвращает количество входов в систему для каждого пользователя за выбранный нами промежуток времени.



Конфигурация Агентов

Сбор журналов осуществляется с помощью агентов, как в агенте для Microsoft Windows®, так и в агентах Unix® (Linux®, MacOSX®, Solaris®, HPUX®, AIX®, BSD® и т.д.). В случае агентов Windows информацию также можно получить из средства просмотра событий операционной системы, используя те же фильтры, что и в модуле мониторинга средства просмотра событий.

Давайте рассмотрим два примера захвата информации журналов, на Windows и Unix:

Windows

Начиная с версии 750, это действие можно выполнить через **плагины агента**, активировав опцию *Advanced*.

Могут выполняться выполнения типа, показанного ниже:

Модуль logchannel

```
module_begin
module_name MyEvent
module_type log
module_logchannel
module_source <logChannel>
module_eventtype <event_type/level>
module_eventcode <event_id>
module_pattern <text substring to match>
module_description <description>
module_end
```

Модуль logevent

```
module_begin
module_name Eventlog_System
module_type log
module_logevent
module_source System
module_end
```

Модуль regexp

```
module_begin
module_name PandoraAgent_log
module_type log
module_regexp <%PROGRAMFILES%>\pandora_agent\pandora_agent.log
module_description This module will return all lines from the specified logfile
```

```
module_pattern .*  
module_end
```

Дополнительную информацию об описании модулей типа журнала можно найти в следующем разделе, касающемся [Специфических директив](#).

```
module_type log
```

Определяя этот тип тега, `module_type log`, вы указываете, что он не сохраняется в базе данных, а отправляется в коллектор `log`. Любой модуль с данными этого типа должен быть отправлен в коллектор, если он включен: в противном случае информация будет отброшена.

Примечание: Этот новый синтаксис действителен для агента версии 5.0 или выше, *не забудьте обновить* версию вашего Enterprise.

Системы Unix

В агенте версии 5.0 или выше можно использовать следующий синтаксис.

```
module_plugin grep_log_module /var/log/messages Syslog \. \*
```

Подобно плагину *разбора журналов* (`grep_log`), плагин `grep_log_module` отправляет обработанную информацию журнала в Log Collector с именем «Syslog» в качестве источника. Использует регулярное выражение `\. *` (в этом случае «все») в качестве шаблона при выборе того, какие строки отправлять, а какие нет.

Log Source в Виде Агентов

Начиная с версии 749 Pandora FMS, в Виде Агента добавлено поле `Log sources status`, в котором отображается дата последнего обновления журналов этим агентом. Нажатие на значок лупы `Review` перенаправляет к просмотру `Log Viewer`, отфильтрованному по данному журналу.

PANDORAFMS Pandora FMS the Flexible Monitoring System

Enter keywords to search

Monitoring / View / Main pandorafms

pandorafms

81.3%

Linux
192.168.207.135
7.0NG.748(Build 200804)
Created by Nodo1
Remote configuration enabled

Agent contact

Interval: 5 minutes
Last contact / Remote: 2 minutes 04 seconds / August 19, 2020, 10:43 am
Next contact: 107 s
Group: Unknown
Secondary groups: N/A
Parent: N/A
Last status change: 2 minutes 08 seconds

Agent info

Agent access rate (Last 24h)

Events (Last 24h)

List of modules ⓘ 2 1 13

Full list of alerts

✓ Log sources status

| Source | Review | Last contact |
|-------------|--------|----------------------|
| Httpdaccess | 🔍 | 2 minutes 08 seconds |

[Вернуться в оглавление Документации Pandora FMS](#)