

COPM 2

Системы COPM 2 (lawful interception) предназначены для постановки на контроль абонентов мобильных сетей связи GPRS, LTE и абонентов сетей широкополосного доступа.

Компоненты

Системы СОРМ2 могут включать в себя следующие компоненты:

- съёмники,
- агрегаторы-балансировщики и фильтры,
- кольцевой буфер,
- «пульт»,
- рабочие места операторов.

Съёмник

Съёмник — центральный компонент систем СОРМ 2, предназначенный для отбора трафика по заданным критериям в режиме реального времени без потерь.

Агрегатор- балансировщик

Агрегатор-балансировщик — вспомогательное оборудование для коммутации, фильтрации и балансировки нагрузки на съёмники.

Сетевой фильтр

Сетевой фильтр предназначен для снижения нагрузки на съёмники за счет фильтрации нежелательного трафика.

Кольцевой буфер

В соответствии с изменениями в законодательстве системы СОПМ 2 должны сохранять копию всего трафика за период от 12 до 24 часов.

Для решения этой задачи используется кольцевой буфер — устройство с достаточным объёмом дискового пространства и обеспечивающее запись трафика на скорости канала связи.

«Пульт»

АПК для постановки на контроль и отображения результатов перехвата, включает в себя веб-сервер, сервер базы данных, дисковое хранилище, модули экспорта, авторизации, мониторинга и логирования, web-интерфейс управления.

Рабочее место оператора

В качестве рабочего места оператора может быть использован любой персональный компьютер с установленным на нём браузером и набором офисного ПО, необходимым для просмотра перехваченных документов, в том числе и на базе ОС linux.

Критерии отбора

- IP-адрес сервера, абонента
- Логин, IMSI, IMEI, MAC-адрес абонента
- Адрес сайта – URL
- Логин FTP-пользователя
- Адрес электронной почты
- Местоположение абонента
- Ник в мессенджере и т. д.
- Поиск по неточным критериям (?, *)

COPM2 → *nat-geo* url and all other types

Название сеанса	*nat-geo* url and all other types	■ Остановить
Интервал времени	От 11 марта 16:53	✎ Редактировать
Критерии поиска		📄 Экспорт
URL сайта	*nat-geo*	📁 Отправить в архив
Логин FTP	*	
Электронная почта	* ↔ *	
IM номер или никнейм	* ↔ *	
VoIP номер или никнейм	* ↔ *	
Типы трафика	☒ HTTP ☒ FTP ☒ Электронная почта ☒ IM ☒ VoIP ☒ Потоки	
Дата создания	11 марта 16:51	
Найдено записей	490	
Пользователь	👤 admin	

🔍 [Фильтры](#)

Удалить На перевод Важное Прочитано Не прочитано Экспорт

HTTP 270 FTP 19 Email 4 IM 196 VoIP 1						⌵ Без группировки	
☐	Дата	URL	Метод	Код ответа	Отправлено		
☐	11 марта 18:25:28	www.nat-geo.ru/6837b853e2539b78c7350402a6d3f95/	GET	200	1,4 кБ		
☐	11 марта 18:25:28	www.tns-counter.ru/V13a***R%3Ehttp://www.nat-geo.ru/page/6/*lmedia_ru/ru/UTF-8/tmsec=natgeo_total/807025..	GET	200	727 Б		
☐	11 марта 18:25:28	connect.ok.ru/dk	GET	200	723 Б		

COPM 2



Название сеанса	Найдено записей	Дата соз:
■ all	862	16 марта
■ test http + volp	4789	16 марта
🕒 fcenter.ru	175	15 марта
🕒 All types	564183	11 марта
🕒 test	286	11 марта
🕒 *nat-geo* url and all other types	490	11 марта

Всего: 6

Критерии отбора объединятся в сеансы наблюдения.

Данные

Результаты автоматически разделяются по типу HTTP, FTP, VoIP и т. д.

Таблица результатов может быть отсортирована по любому полю. Умный фильтр показывает только то, что нужно пользователю.

HTTP 494006 (493957)		FTP 19 (15)	Email 4 (1)	IM 199 (190)	VoIP 1	Потоки 83703 (83663)
HTTP → тынуженлюдям.рф						
☐	Дата	URL				
☐	16 марта 14:24:36	 тынуженлюдям.рф/sites/default/files/styles/project_news420w/public/project_news/ANoAR				
☐	16 марта 14:24:36	 тынуженлюдям.рф/sites/default/files/styles/project_news420w/public/project_news/RRoo2'				
☐	16 марта 14:24:36	 тынуженлюдям.рф/sites/default/files/styles/project_news70x44/public/project_news/ANoAI				
☐	16 марта 14:24:36	 тынуженлюдям.рф/sites/default/files/styles/project_news70x44/public/project_news/RRoo2				
☐	16 марта 14:24:36	 тынуженлюдям.рф/ru/content/Shadows+Into+Light				
☐	16 марта 14:24:36	 тынуженлюдям.рф/ru/content/%D1%84%D0%B8%D0%BD%D0%B8%D1%88%D0%BD%D0%F				
☐	16 марта 14:24:25	 тынуженлюдям.рф/sites/all/modules/jquery_update/replace/ui/themes/base/images/ui-icon				
☐	16 марта 14:24:25	 тынуженлюдям.рф/sites/all/modules/jquery_update/replace/ui/themes/base/images/ui-bg_с				

Основные параметры по каждому типу протоколов представлены в табличном виде.

Дата	URL	Метод	Код ответа	Отправлено	Получено
16 марта 14:24:25	тынуженлюдям.рф/misc/menu-collapsed.png	GET	200	666 Б	377 Б
16 марта 14:24:25	тынуженлюдям.рф/sites/default/files/styles/thumbnail/public/default_images/anonymous_1.jpg	GET	200	818 Б	5,5 кБ
— URL: тынуженлюдям.рф/sites/default/files/styles/thumbnail/public/default_images/anonymous_1.jpg — Хост: тынуженлюдям.рф — Параметры запроса: itok=Oi10THxd — Код ответа: 200 (OK) — Content-Type: image/jpeg — Метод: GET — Версия протокола HTTP: 1.1 — Cookie: _ym_uid=1458127350477274741; _ym_isad=1; has_js=1 — Set Cookie: — — Referer: http://тынуженлюдям.рф/ru/content/%D0%BA%D0%B0%D1%80%D1%82%D0%B0-%D0%BF%D1%80%D0%BE%D1%84%D0%B5%D1%81%D1%81%D0%B8%D0%B9 — User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.93 Safari/537.36 — PCap: 4/101/222/122469.pcap					
Протокол L4: TCP Протокол L7: HTTP Принято: 5,5 кБ Отправлено: 818 Б		Источник: 192.168.0.149:44625 Получатель: 83.69.230.86:80 Идентификатор NAS: — NAS: —		Логин пользователя: — IMSI: — IMEI/MAC: — CELL: — ID сессии: —	
16 марта 14:24:25	тынуженлюдям.рф/ru/content/Shadows+Into+Light	GET	404	955 Б	8,2 кБ
16 марта 14:24:25	тынуженлюдям.рф/sites/default/files/js/js_p2WQ00tU-5RGLUM-IlpkRR6FTUQmUETKQHwkHzzHk4.js	GET	200	1,4 кБ	35,9 кБ
16 марта 14:24:25	тынуженлюдям.рф/sites/default/files/js/js_d0L_yBL2LMHlgCptLGcBdefc35gMwt70CTVNfM_QC_Lr4.js	GET	200	1,4 кБ	40,4 кБ
16 марта 14:24:25	тынуженлюдям.рф/sites/default/files/css/css_cg0lksdvYJC6SqsFra9IWp_e6gtz7hCUZQaLrM_DJC0.css	GET	200	729 Б	756 Б
16 марта 14:24:25	тынуженлюдям.рф/sites/default/files/css/css_ChwB0FBFLph-siCso_IKRYb3IALxXyuQ_r3OZOnQSU.css	GET	200	795 Б	3,3 кБ
16 марта 14:24:25	тынуженлюдям.рф/ru/content/%D0%BA%D0%B0%D1%80%D1%82%D0%B0-%D0%BF%D1%80%D0%BE%D1%84...	GET	200	1,1 кБ	12,4 кБ
16 марта 14:23:22	тынуженлюдям.рф/sites/default/files/logo-min.png	GET	200	718 Б	8,2 кБ
16 марта 14:23:22	тынуженлюдям.рф/sites/all/themes/Porto_sub/img/logo-minobr-trans.png	GET	200	1,3 кБ	35,0 кБ

Для каждого типа протоколов доступен полный список полей.

Выбрано: 6 • Снять выделение

Экспорт

all_11_3_2016_csv_1.zip	http	707,4 МБ	11 марта 19:15
all_11_3_2016_html_2.zip	http	811,5 МБ	11 марта 19:24
all_11_3_2016_odt_3.zip	http	1,1 ГБ	11 марта 19:33
all_11_3_2016_odt_4.zip	http	88,5 кБ	11 марта 19:39
all_11_3_2016_csv_5.zip	ftp	3,5 МБ	11 марта 19:40
all_11_3_2016_html_8.zip	mail	2,9 МБ	11 марта 19:40
all_11_3_2016_csv_9.zip	mail	1,1 кБ	11 марта 19:40
all_11_3_2016_odt_10.zip	mail	19,6 кБ	11 марта 19:40
all_11_3_2016_html_11.zip	im	2,9 МБ	11 марта 19:40
all_11_3_2016_html_14.zip	voip	2,9 МБ	11 марта 19:41
all_11_3_2016_csv_15.zip	voip	939 Б	11 марта 19:41
all_11_3_2016_odt_16.zip	voip	16,9 кБ	11 марта 19:41
all_11_3_2016_html_17.zip	flow	3,0 МБ	11 марта 19:41
all_11_3_2016_csv_18.zip	flow	3,0 кБ	11 марта 19:41
all_11_3_2016_odt_19.zip	flow	88,5 кБ	11 марта 19:41
all_15_3_2016_html_20.zip	im	3,0 МБ	15 марта 12:44
all_15_3_2016_odt_21.zip	im	79,3 кБ	15 марта 12:45
all_15_3_2016_html_22.zip	http	3,0 МБ	15 марта 12:45
all_15_3_2016_odt_23.zip	http	88,5 кБ	15 марта 12:46

CSV [Настроить поля](#)

Имя файла

☐ Включить в экспорт собранные материалы

☒ Включить в экспорт рсар-файлы

Экспортировать

Статус	Пользователь FTP	IP источника
Файл успешно загружен на сервер	ildarka	192.168.0.186:56102
Файл успешно загружен на сервер	ildarka	192.168.0.186:56102
Ошибка скачивания файла	ildarka	192.168.0.186:56102
Файл успешно скачан	ildarka	192.168.0.186:56102
Файл успешно скачан	ildarka	192.168.0.186:56102
Файл успешно загружен на сервер	ildarka	192.168.0.186:56102
Файл успешно скачан	ildarka	192.168.0.186:56102
Файл успешно скачан	ildarka	192.168.0.186:56102
Файл успешно скачан	ildarka	192.168.0.186:56102
Файл успешно скачан	anonymous	192.168.0.155:39025
Ошибка скачивания файла	anonymous	216.240.21.42:21
Файл успешно скачан	anonymous	192.168.0.160:48322
Файл успешно загружен на сервер	anonymous	192.168.0.160:48320
Файл успешно скачан		192.168.0.149:48510
Файл успешно скачан		192.168.0.149:48497
Файл успешно скачан		192.168.0.149:48495
Файл успешно скачан		192.168.0.149:48493
Файл успешно скачан		192.168.0.149:48491
Файл успешно скачан		192.168.0.149:48460

Экспорт в различных форматах

Справочники

Справочники абонентов и базовых станций выгружаются оператором и позволяют определить принадлежность номера физическому или юридическому лицу, показать события на карте.



Базовые станции

красносельская



Обновлено: 11.03.2016

ID БС

Адрес

106300003 Москва г, Красносельская Н. ул, 35, кор. 48

- Имя базовой станции: 163
- Страна: Россия
- Оператор: SkyLink
- LAC, CELL: 0, 163
- Широта, долгота: 55.775, 37.673
- Азимут: 270
- Стандарт: CDMA
- Статус: Подключена
- Мощность: 26 Вт * 3 канала
- Высота подвеса: 40.5 м

Данные из справочника автоматически привязываются к результатам.

Справочник операторов

рос  Обновлено: 18.02.2014

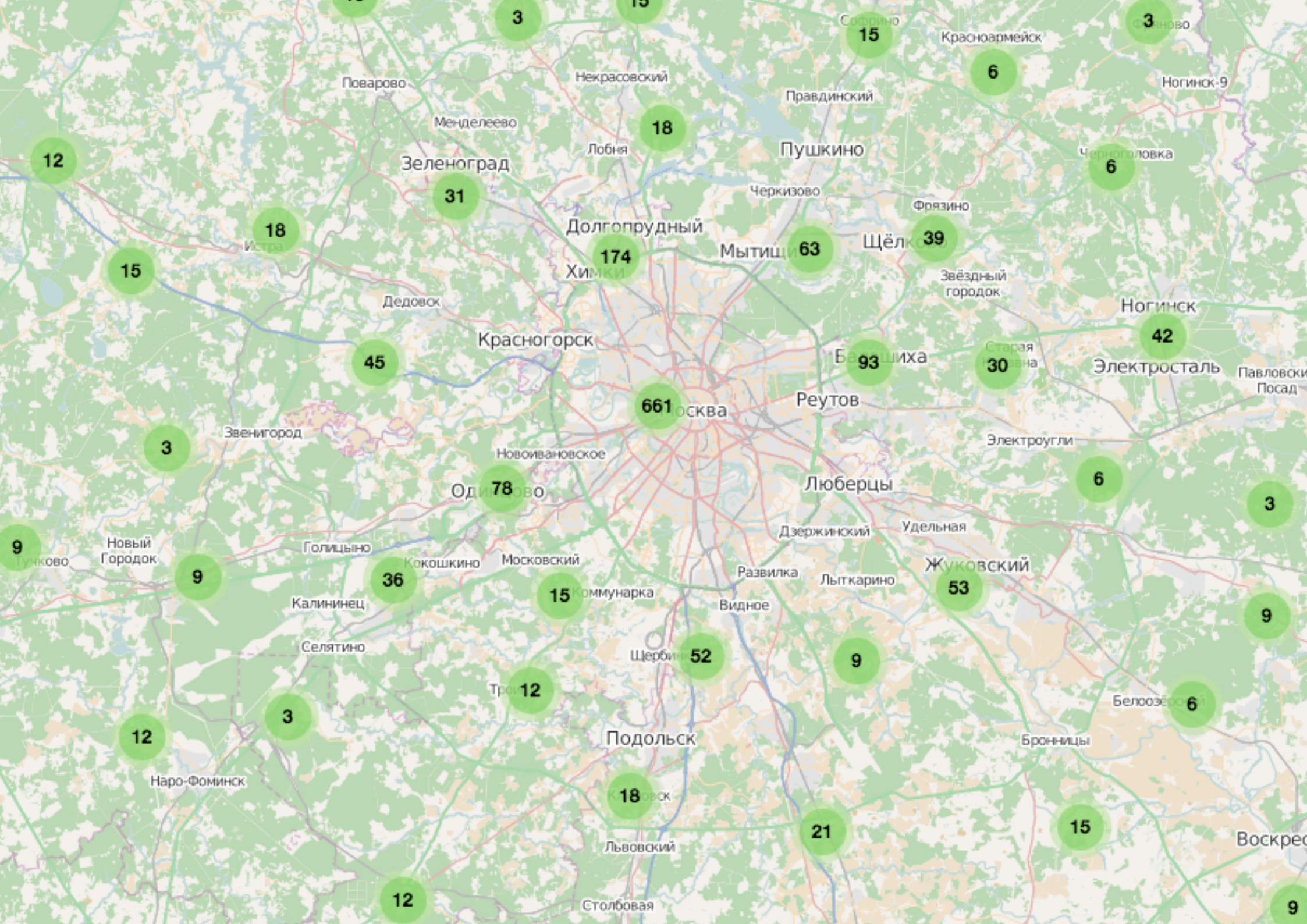
Код	Диапазон номеров	Оператор	Регион
+7 902	6405046	ОАО "Ростелеком"	Пермский край
+7 902	6324476	ОАО "Ростелеком"	Пермский край
+7 902	6324474	ОАО "Ростелеком"	Пермский край
+7 902	6324177	ОАО "Ростелеком"	Пермский край
+7 902	6321609	ОАО "Ростелеком"	Пермский край
+7 902	6320623	ОАО "Ростелеком"	Пермский край
+7 902	6320567	ОАО "Ростелеком"	Пермский край
+7 902	6320258	ОАО "Ростелеком"	Пермский край
+7 902	6319812	ОАО "Ростелеком"	Пермский край
+7 902	6319580	ОАО "Ростелеком"	Пермский край

[← Назад](#) [1](#) [2](#) [3](#) [4](#) [5](#) [...](#) [31](#) [Вперёд →](#) Показывать по: Всего: 307

Поиск по данным из справочников.

Местоположение

Информация о местоположении абонента визуализируется на карте.



4

Москва г, Щорса ул, 11

CellID: 4

Азимут: 75

★ [Добавить в избранное](#)

На карте можно посмотреть
местоположение абонентов.

Пользователи и система прав

Многоступенчатая система прав обеспечивает гибкие настройки разграничения зоны ответственности пользователей.

Пользователи



 admin

 spayk

 wintser

 Red Hot

 bae

Логин

admin

Фамилия И. О.

Administrator

Группа

Пользователи

Права пользователя

- Сеансы: полный доступ
- Данные: экспорт
- AAA: просмотр
- Устройства: управление
- Пользователи: управление
- Журналы: просмотр

Действителен

От 11.03.2016

Журналы

Все действия пользователей в системе логируются и сохраняются в журнал, это позволяет проводить проверки в случае возникновения утечек данных и прочих неправомерных действий.

Действия пользователей

Запросы

Дата	Событие	Полн
15.03.2016 13:02	Пользователь admin запросил данные по запросу «ildarka.ru»	a
15.03.2016 13:02	Пользователь admin просматривал очередь запросов	a
15.03.2016 12:57	Пользователь admin запросил данные по запросу «ildarka.ru» с фильтром «*css»	a
15.03.2016 12:57	Пользователь admin запросил данные по запросу «ildarka.ru» с фильтром «css»	a
15.03.2016 12:56	Пользователь admin запросил данные по запросу «ildarka.ru» с фильтром «kik»	a
15.03.2016 12:56	Запрос CORM-2 «ildarka.ru» изменен	a
15.03.2016 12:46	Экспорт данных по запросу «All»	a
15.03.2016 12:45	Экспорт данных по запросу «All»	a
15.03.2016 12:45	Экспорт данных по запросу «All»	a
15.03.2016 12:44	Экспорт данных по запросу «All»	a
15.03.2016 12:37	Пользователь admin запросил данные по запросу «All»	a
15.03.2016 12:37	Запрос CORM-2 «ildarka.ru» изменен — IP-адрес пользователя: 188.92.105.210 Все параметры Различающиеся Было: — Имя: ildarka.ru — ID: 5 — URL сайта: ildarka.ru — От 15 марта 12:36 — Типы трафика: ✓ HTTP — Статус выполнения: ACTIVE Стало: — Имя: ildarka.ru — ID: 5 — URL сайта: *ildarka.ru* — От 15 марта 12:36 — Типы трафика: ✓ HTTP — Статус выполнения: ACTIVE	a
15.03.2016 12:36	Новый запрос CORM-2 «ildarka.ru»	a

Мониторинг

В режиме онлайн производится мониторинг параметров серверов и прочего оборудования, входящего в состав комплекса это позволяет своевременно реагировать на возможные отказы аппаратуры.

Мониторинг

Название	IP-адрес	Загрузка CPU	Память	HDD
OLAP	192.168.0.26	8%	4%	1%
COPM2 съёмник	192.168.0.27:18888	100%	62%	30%
GUI	192.168.0.28	4%	13%	4%

OLAP. Данные мониторинга

CPU

8 %

45 °C

Занято памяти

580,0 МБ из 15,0 ГБ

4 %

Занято HDD

30,9 ГБ из 3 634,7 ГБ →

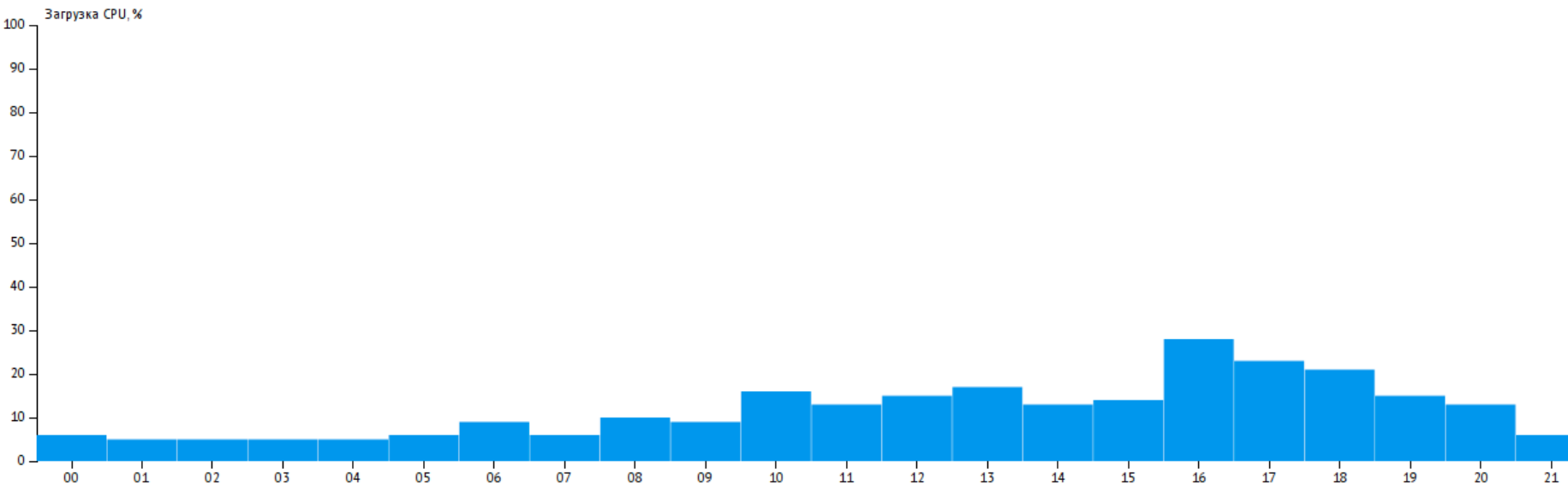
1 %

Сеть

1,2 Мбит/с

← 0 бит/с

- Загрузка CPU
- Температура CPU
- Память
- HDD



- По часам
- По дням
- По неделям
- По месяцам
- ← 15 марта
- 16 марта
- 17 марта →
- Средние
- Макс.

Сервис	Размер	Строк в логе
✔ mezzo_manager	3,7 МБ	54983
✔ postgresql	2,6 МБ	59070
✔ apache2	5,6 кБ	16
✔ gui_agent	6,5 МБ	30096

 Поиск

Сортировка по дате: Показыва

```

30081 2016-03-17 14:50:28,911 - root - DEBUG - [system.get_util_log] $ cat -n /var/log/mezzo/gui_agent.log | tac | sed -n 1,31p
30080 2016-03-17 14:50:28,902 - py_mezzo/library/database.Function - DEBUG - SELECT * FROM system.get_util_log('2ec1b92ebd04f6f4ebf11a68f44adc33', 'gui_agent')
30079 2016-03-17 14:50:28,902 - py_mezzo/proxy/gui_agent.Request - INFO - Request: {u'params': {u'direction': u'desc', u'end': 31, u'name': u'gui_agent', u'start': 1, u'token': u'2ec1b92ebd04f6f4ebf11a68f44adc33', u'grep': None}, u'jsonrpc': u'2.0', u'method': u'system.get_util_log', u'id': 401}
30078 2016-03-17 14:50:28,901 - py_mezzo/proxy/gui_agent.GuiAgent - INFO - Request string: {"jsonrpc": "2.0", "method": "system.get_util_log", "params": {"name": "gui_agent", "direction": "desc", "grep": null, "start": 1, "end": 31, "token": "2ec1b92ebd04f6f4ebf11a68f44adc33"}, "id": 401}
30077 2016-03-17 14:50:27,774 - py_mezzo/proxy/gui_agent.GuiAgent - DEBUG - Data: {"result": {"utils": [{"status": "running, process 15351", "name": "mezzo_manager", "log_ex": "log_path": "/var/log/mezzo/mezzo_manager.log", "lines": "54980", "processing": false, "readable": true, "size": 3848600}, {"status": "9.3/main (port 5432): online\n9.4/main online",
30076 2016-03-17 14:50:27,774 - py_mezzo/proxy/gui_agent.GuiAgent - DEBUG - Headers: [('Content-type', 'application/json'), ('Content-Length', '1090')]
30075 2016-03-17 14:50:27,628 - py_mezzo/proxy/gui_agent.GuiAgent - INFO - Request string: {"jsonrpc": "2.0", "method": "system.get_utils", "params": {"token": "2ec1b92ebd04f6f4ebf11a68f44adc33"}, "id": 400}
30074 2016-03-17 14:50:25,445 - py_mezzo/proxy/gui_agent.GuiAgent - DEBUG - Data: {"result": {"name": "sorm2_exporter", "log": "
59155 2016-03-11 19:25:55,559 15412 DEBUG [2016-03-11 19:24:34.558490 - 0] Archive: duplicate file [u'/opt/ta/store/pcap/4/143/009/2447.pcap',
30073 2016-03-17 14:50:25,445 - py_mezzo/proxy/gui_agent.GuiAgent - DEBUG - Headers: [('Content-type', 'application/json'), ('Content-Length', '8523')]
30072 2016-03-17 14:50:25,411 - root - DEBUG - [system.get_util_log] $ cat -n /var/log/mezzo/sorm2_exporter.log | tac | sed -n 1,31p
30071 2016-03-17 14:50:25,406 - py_mezzo/library/database.Function - DEBUG - SELECT * FROM system.get_util_log('2ec1b92ebd04f6f4ebf11a68f44adc33', 'sorm2_exporter')
30070 2016-03-17 14:50:25,405 - py_mezzo/proxy/gui_agent.Request - INFO - Request: {u'params': {u'direction': u'desc', u'end': 31, u'name': u'sorm2_exporter', u'start': 1, u'token': u'2ec1b92ebd04f6f4ebf11a68f44adc33', u'grep': None}, u'jsonrpc': u'2.0', u'method': u'system.get_util_log', u'id': 399}
30069 2016-03-17 14:50:25,404 - py_mezzo/proxy/gui_agent.GuiAgent - INFO - Request string: {"jsonrpc": "2.0", "method": "system.get_util_log", "params": {"name": "sorm2_exporter", "direction": "desc", "grep": null, "start": 1, "end": 31, "token": "2ec1b92ebd04f6f4ebf11a68f44adc33"}, "id": 399}
30068 2016-03-17 14:50:24,778 - py_mezzo/proxy/gui_agent.GuiAgent - DEBUG - Data: {"result": {"utils": [{"status": "running, process 15351", "name": "mezzo_manager", "log_ex": "log_path": "/var/log/mezzo/mezzo_manager.log", "lines": "54979", "processing": false, "readable": true, "size": 3848530}, {"status": "9.3/main (port 5432): online\n9.4/main online",

```

Особенности

Решение построено на базе компонентов с открытым исходным кодом, что снижает стоимость владения и поддержки.

Возможность работы со сторонними пультами по протоколу 83-го приказа.

Встроенный картографический сервер.

Поисковые поля с поддержкой ввода списков значений, загрузку значений из файла. Поиск по E-mail, IM, VoIP может содержать пары идентификаторов, например, можно искать только исходящую переписку с one@qip.ru на two@gmail.com.

Фильтры, полнотекстовый поиск и группировка облегчают обработку результатов перехвата.

Система прав пользователей позволяет гибко организовать работу с системой.