

## Состав выходных данных и документов

v.3.10.84 - 14.07.2022



**Оглавление**

1	Перечень выходных документов .....	2
1.1	Экспорт данных .....	3
1.2	Экспорт свойств.....	4
1.3	Экспорт графиков .....	5
1.4	Экспорт отчётов по инцидентам .....	6
1.5	Экспорт виджетов типа "График" .....	7
1.6	Экспорт журнала пользовательских сессий .....	8
2	Перечень выходных данных.....	9
2.1	Данные проверки "Процесс по имени" .....	10
2.2	Данные проверки "Запрос в базу данных" .....	12
2.3	Данные проверки "SNMP Get-сенсор" .....	13
2.4	Данные проверки "SNMP Trap-сенсор" .....	14
2.5	Данные проверки "Выполнение программы/скрипта" .....	15
2.6	Данные проверки "Пинг-сенсор" .....	16
2.7	Данные проверки "Локальный порт" .....	17
2.8	Данные проверки "Удалённый порт" .....	18
2.9	Данные проверки "HTTP-запрос" .....	19
2.10	Данные проверки "JMX-сенсор" .....	21
2.11	Данные проверки "MQTT-сенсор" .....	22
2.12	Данные проверки "FTP-сенсор" .....	23
2.13	Данные проверки "Бинарный протокол" .....	24
2.14	Данные проверки "WMI-сенсор" .....	25
2.15	Данные проверки "Конфигурационный файл/директория" .....	26
3	Перечень выходных сигналов .....	27

### 1 Перечень выходных документов

АС "Центральный Пульт" включает в себя перечень форматов электронной документации для экспорта данных в удобный для пользователя вид: Excel, CSV.

Для экспорта доступна следующая информация:

- данные,
- свойства,
- графики,
- отчеты по инцидентам,
- виджеты типа "График".

### 1.1 Экспорт данных

В виде подробной информации или окне информации об объекте или связи находится секция "Данные". Эта секция содержит таблицу с результатами выполняемой проверки.

Для экспорта полученных результатов мониторинга нужно нажать кнопку



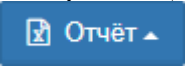
- Экспорт в CSV - в заголовке секции.

Файл содержит аналогичное таблице данных наполнение. Количество и содержание столбцов зависит от выбранного типа проверки.

### 1.2 Экспорт свойств

В качестве объекта мониторинга может выступать физическое устройство (сервер, процессор, маршрутизатор), программный модуль (база данных, web-сервер), объект бизнес-процесса (услуга, платформа). Любой объект может иметь свойства, при помощи которых возможно добавлять описание, адреса, ссылки и другую полезную для администрирования информацию.

Свойство - текстовая информация в формате "имя - значение".

Экспорт свойств осуществляется через окно поиска и групповых операций. Для этого необходимо отметить нужные объекты, нажать кнопку  и выбрать "Объекты и свойства". Информация выгружается в Excel-файл, который содержит:

- имена объектов,
- дату и время создания объектов,
- имена свойств,
- значения свойств,
- информацию о прикреплённой документации.

### 1.3 Экспорт графиков

Графики строятся автоматически на основании числовых значений из таблицы данных. Данные, отображённые на графике, можно экспортировать в CSV-файл. Для



этого необходимо нажать кнопку - Экспорт в CSV - в заголовке графика.

CSV-файл содержит:




- дату и время поступления данных,
- значения параметров.

### 1.4 Экспорт отчётов по инцидентам

Инцидент (IT Incident) - это любое явление, выходящее за рамки штатной работы IT-структуры, прямо, косвенно или потенциально ведущее к остановке процессов системы или негативно отражающееся на качестве её функционирования.

В АС "Центральный Пульт" инцидент генерируется, если:


- объект переходит в одно из состояний, для которого задан уровень критичности аварии,
- выполняются условия генерации аварий.

Системой предусмотрено сохранение отчёта по инцидентам. Отчёт возможно получить как для активных (кнопка  - Экспорт в Excel), так и для исторических (кнопка  - Экспорт в CSV) инцидентов на странице с инцидентами (кнопка  на панели режимов отображения).

### 1.5 Экспорт виджетов типа "График"

Стандартный вид - это отображение, которое предоставляет наиболее подробную информацию об объектах и связях между ними с точки зрения иерархии объектов.



Кнопкой  - Экспорт в Excel - на панели "хлебных крошек" в стандартном виде возможно выгрузить данные по всем виджетам типа "График" дочерних объектов.



### 1.6 Экспорт журнала пользовательских сессий

На странице журнала сессий (Конфигурация – Журнал сессий) доступна информация о пользовательских сессиях – время входа в систему, время выхода из системы, срок действия текущих сессий пользователей.



Кнопка  в правом верхнем углу экрана сохраняет журнал сессий за выбранный временной интервал в PDF-файл.

### 2 Перечень выходных данных

Поток выходной информации формируется из средств измерений. При помощи различных способов проверки возможно получить дополнительный набор выходных данных.

### 2.1 Данные проверки "Процесс по имени"

Этот тип проверки позволяет получить данные по процессу с указанным именем и/или их аргументами, запущенным в операционной системе.

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 1):

processId	parentId	name	state	tty	nice	arguments.0	arguments.1	bytesVirtual	bytesResident
564	1	nodejs	S	0	0	/usr/bin/nodejs	/opt/metric-server/index.js	888 M	33.4 M

Количество строк: 1

bytesShared	lastTime	startTime	userCpu	systemCpu	totalCpu	percentCpu	uptime
6.98 M	02.11.2020, 10:11:42	27.05.2020, 15:52:23	832 K	170 K	1 M	0.07%	2 undefined

Количество строк: 1

Рис. 1. Результат проверки "Процесс по имени"

Описание полей результата проверки "Процесс по имени" (часть 1 из 2):

Поле	Описание
arguments.xxx	Аргументы, с которыми был запущен данный процесс.
bytesResident	Показывает, сколько физической памяти использует процесс. Соответствует колонке "%MEM" утилит "ps" и "top" - процент использования оперативной памяти данным процессом.
bytesShared	Количество разделяемой памяти, которое используется процессом. Отображает количество памяти, которая потенциально может быть разделена с другими процессами.
bytesVirtual	Используемая виртуальная память или "виртуальный размер процесса". Показывает общее количество памяти, которое способна адресовать программа в данный момент времени.
lastTime	Время, когда последний раз процесс выполнялся на CPU.
name	Имя найденного процесса.
nice	Значение приоритета "nice" - приоритет, который пользователь хотел бы назначить процессу (от -20 до 19).
parentId	ID родительского процесса (PPID).
percentCpu	Количество CPU, используемое данным процессом.
processId	ID найденного процесса (PID).
startTime	Время, когда был запущен процесс.

Описание полей результата проверки "Процесс по имени" (часть 2 из 2):

Поле	Описание
state	<p>Код состояния процесса:</p> <ul style="list-style-type: none"><li>• D - uninterruptible sleep (usually IO) – процесс ожидает ввода-вывода (или другого недолгого события), непрерываемый;</li><li>• I - is multi-threaded (using CLONE_THREAD, like NPTL pthreads do) - многопоточный процесс;</li><li>• L – has pages locked into memory (for real-time and custom IO) – процесс использует страничную память;</li><li>• N - low-priority (nice to other users) - процесс с низким приоритетом, получает ресурсы позже прочих;</li><li>• R – running or runnable (on run queue) - процесс выполняется в данный момент или готов к выполнению (состояние готовности);</li><li>• s - is the session leader - процесс является лидером сессии;</li><li>• S – interruptible sleep (waiting for an event to complete) – процесс в состоянии ожидания (т.е. "спит" не менее 20 секунд);</li><li>• T - stopped, either by a job control signal or because it is being traced – процесс остановлен (stopped) или трассируется отладчиком;</li><li>• W - paging (not valid since the 2.6.xx kernel) – процесс в стадии "paging", не актуально для ОС с kernel старше 2.6;</li><li>• X – dead (should never be seen) – процесс в состоянии завершения;</li><li>• Z – defunct ("zombie") process, terminated but not reaped by its parent - закрывшийся процесс, код возврата которого пока не считан родителем;</li><li>• &lt; - high-priority (not nice to other users) - процесс с высоким приоритетом, получает ресурсы раньше прочих;</li><li>• + - is in the foreground process group - процесс запущен в foreground-режиме.</li></ul>
systemCpu	Время CPU, занятое системой.
totalCpu	Общее процессорное время, занятое процессом (сумма userCpu и systemCpu).
tty	Терминал, с которым связан данный процесс.
uptime	Время, в течение которого процесс находится в работе.
userCpu	Время CPU, которое занял пользователь.

### 2.2 Данные проверки "Запрос в базу данных"

Этот тип проверки осуществляет выборку из баз данных:

- MySQL (4.1 - 5.7),
- MS SQL (Microsoft SQL Server 2005/2008/2008 R2/2012/2014),
- PostgreSQL (9.x),
- Oracle (9.0 - 11.2),
- HP Vertica,

по параметрам, указанным при настройке мониторинга в поле "SQL-запрос".

2.3 Данные проверки "SNMP Get-сенсор"

Этот тип проверки позволяет получить значение переменной с соответствующим ей описанием.

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 2):



Рис. 2. Результат проверки "SNMP GET-сенсор"

Описание полей результата проверки "SNMP GET-сенсор":

Поле	Описание
Номер запрошенного OID	Значение запрошенного SNMP-объекта.

### 2.4 Данные проверки "SNMP Trap-сенсор"

Этот тип проверки позволяет получить информацию о произошедшем на объекте событии.

После настройки условий мониторинга в случае успешного выполнения проверки принимаемые данные будут отображаться в Журнале событий (Рис. 3):

STAGING Журнал Событий									
		SNMP		Фильтр		Вкл		Количество сообщений: 100	
Количество	Время	Критичность	Объект на схеме	Адрес отправителя	OID трапа	Текст	Данные	Ответственный	
100	03.11.2020, 13:40:53	Major	IT'S A TRAP	127.0.0.1	1.3.6.1.4.1.5089.2.0.99	0	1.3.6.1.4.1.5089.2.0.99 "0"	admin	
	03.11.2020, 13:39:53	Major	IT'S A TRAP	127.0.0.1	1.3.6.1.4.1.5089.2.0.99	0	1.3.6.1.4.1.5089.2.0.99 "0"		
	03.11.2020, 13:37:53	Major	IT'S A TRAP	127.0.0.1	1.3.6.1.4.1.5089.2.0.99	0	1.3.6.1.4.1.5089.2.0.99 "0"		

Рис. 3. Журнал событий

### 2.5 Данные проверки "Выполнение программы/скрипта"

Этот тип проверки осуществляет вызов исполняемого файла и возвращает его вывод из потоков `stdout`, `stderr`.

Данные возвращаются в следующих форматах:





- текстовый;
- числовой;
- JSON.



2.6 Данные проверки "Пинг-сенсор"

Этот тип проверки осуществляет проверку объекта или связи командой "Ping" по указанному IP-адресу или имени хоста.

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 4):

 Данные				:			
packetsTransmitted	packetsReceived	packetLossPercentile	numberOfErrors				
4	4	0	0				





 Данные					:			
numberOfDuplicat es	roundTripMinimal	roundTripAverage	roundTripMaximum	exitCode				
0	4.408	4.5440000000000005	4.826	0				

Рис. 4. Результат проверки "Пинг-сенсор"

Описание полей результата проверки "Пинг-сенсор":

Поле	Описание
packetsTransmitted	Количество переданных пакетов.
packetsReceived	Количество полученных пакетов.
packetLossPercentile	Процентиль потерь пакетов.
numberOfErrors	Количество ошибок.
numberOfDuplicat es	Количество дубликатов.
roundTripMinimal	Минимальное время приёма-передачи (round-trip time).
roundTripAverage	Среднее время приёма-передачи (round-trip time).
roundTripMaximum	Максимальное время приёма-передачи (round-trip time).
exitCode	Код завершения выполнения проверки (0 - без ошибок).

### 2.7 Данные проверки "Локальный порт"

Этот тип проверки проверяет доступность указанного локального порта.

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 5):



success	listenAddress	processId
true	127.0.0.1	5563

*Рис. 5. Результат проверки "Локальный порт"*

Описание полей результата проверки "Локальный порт":

Поле	Описание
success	Результат проверки: <ul style="list-style-type: none"><li>• true - порт доступен;</li><li>• false - порт недоступен.</li></ul>
listenAddress	Адрес, на котором используется проверяемый порт.
processId	ID процесса, который использует проверяемый порт.

### 2.8 Данные проверки "Удалённый порт"

Этот тип проверки проверяет доступность указанного удалённого порта.

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 6):



*Рис. 6. Результат проверки "Удалённый порт"*

Описание полей результата проверки "Удалённый порт":

Поле	Описание
success	Результат проверки: <ul style="list-style-type: none"><li>• true - порт доступен;</li><li>• false - порт недоступен.</li></ul>
errorMessage	Сообщения об ошибках выполнения проверки или о причинах недоступности проверяемого порта.

2.9 Данные проверки "HTTP-запрос"




Этот тип проверки позволяет выполнять следующие виды HTTP-запросов: GET, POST, HEAD, PUT, PATCH и DELETE.

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 7):

Данные

Таблица по полю: -- Не выбрано --

Точные значения: НЕТ






statusCode	statusText	headers.Transfer-Encoding	headers.Server	headers.Connection	headers.Set-Cookie
200	OK	chunked	nginx	keep-alive	pll_language=ru; expires=Tue, 28-Mar-2023 13:28:41 GMT; path=/

Данные

Таблица по полю: -- Не выбрано --

Точные значения: НЕТ






headers.Date	headers.Link	headers.Content-Type	headers.X-Powered-By	headers.X-Pingback
Mon, 28 Mar 2022 13:30:48 GMT	<https://wp.me/P4R7Dd-1HB>; rel=shortlink	text/html; charset=UTF-8	PHP/5.4.45-4+deprecated+dontuse+deb.sury.org~precise+1	https://saymon.info/xmlrpc.php

Данные

Таблица по полю: -- Не выбрано --

Точные значения: НЕТ



body	responseTimeMs
<!DOCTYPE html> <html lang="ru-RU" prefix="og: http://ogp.me/ns# article: http://ogp.me/ns/article#"> <head> <meta property="og:image" content="Array" /> <meta name="yandex-verification" content="55aa78545469d7be" /> <meta name="google-site-verification" content="kPNfIBxF40d-xxlbCDgceSeHREpREj3AbWIFdZGHol4" />  <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, initial-scale=1"> <link rel="profile" href="http://gmpg.org/xfn/11"> <link rel="pingback" href="https://saymon.info/xmlrpc.php">	1.04 K

Рис. 7. Результат проверки "HTTP-запрос"

Описание полей результата проверки "HTTP-запрос":

Поле	Описание
statusCode	Код состояния HTTP.
statusText	Текстовая интерпретация кода состояния HTTP.
headers.Xxx	Заголовки ответа.
body	Тело ответа.
body.Yyy	Тело ответа, разбитое на отдельные поля, если в ответе вернулись данные в форматах JSON или XML.
responseTimeMs	Время отклика ресурса в миллисекундах.

### 2.10 Данные проверки "JMX-сенсор"

Этот тип проверки позволяет получить данные о работе Java-приложений, поддерживающих JMX – Java Management Extensions:

- просмотр конфигурации приложения;
- сбор и публикация статистических данных о работе приложения;
- оповещение о смене состояний и ошибках в работе приложений.

Набор метрик индивидуален и зависит от проверяемого Java-приложения.

2.11 Данные проверки "MQTT-сенсор"

Этот тип проверки позволяет подписаться на топик MQTT-брокера и получать данные от устройств, поддерживающих работу по протоколу MQTT.

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 8):

Данные			
topic	message.L1.line	message.L1.I	message.L1.U
Saymon_Virtual	L1	12.47	219.42

Рис. 8. Результат проверки "MQTT-сенсор"

Описание полей результата проверки "MQTT-сенсор":

Поле	Описание
topic	MQTT-topic, указанный в настройках сенсора.
message.X.Y	Сообщение, полученное от MQTT-брокера.

### 2.12 Данные проверки "FTP-сенсор"

Этот тип проверки позволяет подключаться к FTP-директориям и получать данные о размещённых в них файлах и папках.

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 9):



count	totalSize	maxSize	minSize	firstModified	lastModified	content.names.0
4	9.09 M	2.33 M	2.2 M	1.49 T	1.49 T	1_149011621125.mp4

Рис. 9. Результат проверки "FTP-сенсор"

Описание полей результата проверки "FTP-сенсор":

Поле	Описание
count	Количество файлов в указанной директории.
totalSize	Размер указанной директории или суммарный размер всех вложенных директорий с файлами, если режим "Рассчитывать размер директорий" включен.
maxSize	Максимальный размер файла в директории.
minSize	Минимальный размер файла в директории.
firstModified	Дата первого изменения директории.
lastModified	Дата последнего изменения директории.
content.names.X	Имена файлов, вложенных в директории, если включен режим "Отображать имена файлов".



2.13 Данные проверки "Бинарный протокол"

Этот тип проверки позволяет отправлять бинарные данные на указанный при настройке мониторинга хост/порт, получать ответ в бинарном виде и трансформировать их в удобный для пользователя формат по заданным правилам.

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 10):

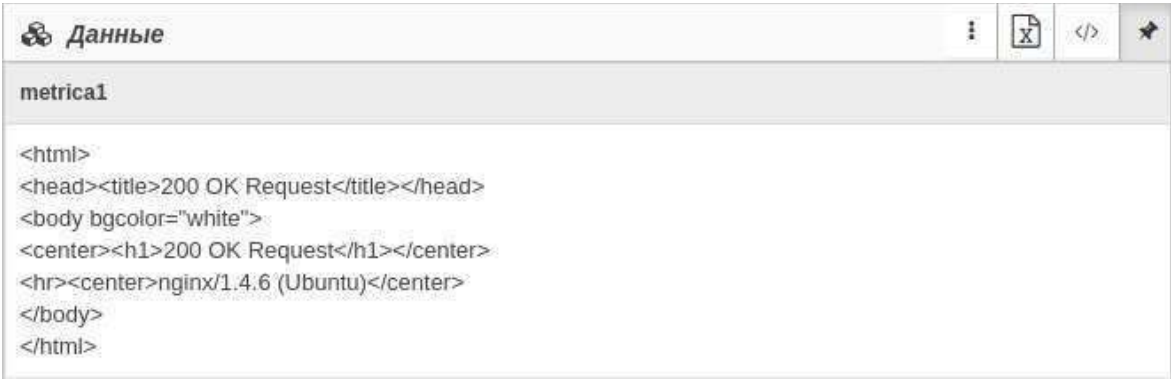


Рис. 10. Результат проверки "Бинарный протокол"

Описание полей результата проверки "Бинарный протокол":

Поле	Описание
metr1calX	Имя метрики, указанное в "Параметрах разбора".

2.14 Данные проверки "WMI-сенсор"

Этот тип проверки позволяет собирать информацию на операционных системах семейства Windows о классах WMI из указанного пространства имён с технологии "Windows Management Instrumentation".

После настройки условий мониторинга в случае успешного выполнения проверки в таблице данных отобразится следующая информация (Рис. 11):

Данные					
Status	FreePhysicalMemory	FreeSpaceInPagingFiles	FreeVirtualMemory	BootDevice	BuildNumber
OK	580596	2187052	2054088	\Device\HarddiskVolume1	2600

Рис. 11. Результат проверки "WMI-сенсор"

Описание полей результата проверки "WMI-сенсор":

Поле	Описание
Поля с названиями свойств запрошенного объекта	Имена свойств запрошенного WMI-объекта и их значения.

### 2.15 Данные проверки "Конфигурационный файл/директория"

Этот тип проверки позволяет наблюдать за изменением файлов и папок.

После успешного выполнения проверки в секции "Изменения конфигурации" появятся дата, время, история изменений, и содержимое файла/директории.

### 3 Перечень выходных сигналов

При переходе объектов в определенные состояния система может:

- отправлять email -уведомления;
- автоматически запускать программу или скрипт с параметрами;
- отправлять сообщения в Telegram;
- отправлять SMS;
- совершать голосовые вызовы;
- показывать визуальное уведомление в браузере, сопровождающееся звуком.

При одновременной или частой смене состояний система может отправлять сгруппированное уведомление о всех событиях, произошедших за определённый период времени, который настраивается администратором системы.

Формирование уведомлений доступно в разделе конфигурации "Шаблоны уведомлений" при помощи базовых переменных:

- `entityName` - имя элемента,
- `entityId` - ID элемента,
- `entityType` - тип элемента (объект/связь),
- `entityUrl` - URL элемента,
- `stateName` - имя состояния,
- `stateData` - информация о состоянии,
- `changedStateText` - текст о переходе в состояние:
  - "перешёл в состояние" - для объектов;
  - "перешла в состояние" для связей;
- `hasRootCause` - указывает на смену состояния, вызванную дочерним объектом:
  - возвращает `true`, если новое состояние унаследовано от дочернего элемента;
  - возвращает `false`, если состояние изменилось по другой причине;
- `rootCauseEntityName` - имя объекта-первопричины,
- `rootCauseEntityUrl` - URL объекта-первопричины,
- `rootCauseEntityId` - ID объекта-первопричины,
- `condition` - информация о сработавшем условии,
- `conditionDescription` - описание условия, вызвавшего переход,
- `eventTime` - время наступления события,
- `breadcrumbs` - полный путь в иерархии к элементу, по которому поступает уведомление.

Внутри переменной "`breadcrumbs`" также можно использовать переменные:

- `entityName`,
- `entityId`,
- `entityUrl`.

Параметры переменной "`breadcrumbs`" (по умолчанию значения параметров равны 0):

- `multi-break` - остановка на мультиродителе (0 - нет, 1 - да),
- `depth` - количество отображаемых уровней (0 - нет ограничения),
- `length` - максимальное суммарное количество символов (0 - нет ограничения).

Переменные группового уведомления:

- eventsCount - количество событий,
- uniqueCount - количество уникальных событий,
- fromTime - время наступления первого события из списка,
- toTime - время наступления последнего события из списка.

Для email-уведомлений предусмотрены следующие дополнительные переменные:

- stateLabel - цветная метка состояния,
- entityLink - имя-ссылка на элемент,
- rootCauseEntityLink - имя-ссылка на дочерний элемент-первопричину,
- goToObjectButton - кнопка перехода к элементу.

[www.cpult.ru](http://www.cpult.ru)

2022

