

# IQM Manager - руководство пользователя

---

## Оглавление

Оглавление.....	1
Общие принципы .....	5
Вход в систему .....	5
Элементы интерфейса .....	6
Меню .....	6
Формы конфигурации .....	6
Меню управления .....	7
Использование масок в формах.....	8
Дополнительные условия .....	9
Просмотр настроек.....	9
Фильтры.....	10
Режим массовой конфигурации.....	12
Задачи администрирования.....	16
Конфигурация доступа .....	16
Конфигурация apache.....	17
Управление пользователями IQMM.....	17
Ролевые профили .....	17
Пользователи IQMM.....	19
Контроль пользовательских сессий .....	21
Авторизация LDAP, Active Directory.....	22
Создание пользователя личного кабинета .....	23
Ограничение количества ошибок авторизации.....	25
Распределенный мониторинг .....	26
Подключение региональных СУ IQMM к центральной.....	27
Задачи конфигурирования.....	28
Требования к листам доступа (ACL) для работы системы IQM .....	28
Первичная конфигурация агента .....	29
Заведение агента в системе .....	30

Форма конфигурации агентов .....	30
Подключение агента, доступного в сети .....	33
Подключение группы агентов по списку .....	35
Размещение IQM-агента за NAT .....	36
Отключение Passive FTP в sender.pl .....	38
Передача CDR через проху .....	38
Обновление списка интерфейсов агента .....	39
Создание тестов.....	41
UQR: Universal Quality Responder .....	52
CXR: Cisco X Responder.....	53
Типы тестов .....	54
U0 .....	54
Ю, U7 .....	55
Ю, J1 .....	56
C0, C1, C2, C3 .....	59
TW, T1 .....	61
URL .....	61
BW .....	64
GSS.....	65
LOCAL .....	65
CMD, конфигурация пакетного теста .....	66
CMD, взаимодействие агента с пакетным тестом .....	70
CMD, пример пакетного теста .....	73
CMD, предустановленные пакетные тесты .....	76
MCAST_VIDEO, мониторинг IPTV .....	77
DNS.....	79
PPPOE.....	81
Измеряемые характеристики .....	81
Управление признаками.....	84
Управление списком сервисов.....	84
Управление списком провайдеров.....	85
Управление именами классов сервиса .....	86
Управление зонами.....	87
Архитектурные уровни.....	89

Контроль параметров .....	89
Управление пороговыми .....	90
Механизмы уведомления.....	93
Приемники syslog .....	93
Syslog-сервер.....	96
Ловушки SNMP-trap.....	97
SNMP-trapd сервер .....	98
Адресаты eMail .....	100
SMS-уведомления .....	102
Конфигурация сервера SMS.....	102
Конфигурация шаблона SMS .....	103
Конфигурация адресатов SMS .....	105
Профиль действий.....	106
Вызов внешней процедуры .....	108
Управление SLA-политиками.....	109
Конфигурация срочного аларма (LIVEMON).....	114
Передача аларма через e-Mail .....	121
Конфигурация SNMP-коллектора.....	124
Программное обеспечение .....	124
Конфигурирование коллектора CollectdV .....	126
CollectdV .....	126
CollectdV mongodb.....	126
CollectdV network.....	127
CollectdV snmp .....	127
MongoDB.....	128
Конфигурирование SNMP-тестов .....	128
Types.db. Управление именами наборов данных. ....	128
Types.db DS. Управление источниками данных.....	130
SNMP-plugin. Конфигурация Datablocks.....	133
SNMP-plugin. Конфигурация Hosts. ....	135
Datablock instances. Экземпляры блоков данных.....	137
Tests. Формирование трестов.....	139
Отчеты по SNMP-тестам .....	142
Диагностирование неисправностей в работе SNMP-плагина .....	144

Блокировки mongodb .....	146
Логи mongodb .....	146
Логи collectdV .....	146
Включение дебага в iqmm-collectd .....	146
Работа с отчетами .....	147
Доступ к отчетам .....	147
Графические отчеты .....	147
Комбинированные графические отчеты .....	148
Отчеты с группировкой .....	151
Мониторинг на ГИС .....	155
Звуковая сигнализация на ГИС .....	157
Операционные состояния агентов .....	158
QoS отчеты .....	159
Отчет с TopX .....	159
Табло сигналов о нарушениях .....	160
Создание пользовательских отчетов .....	163
Определение списка значений для select-поля .....	166
Привязка к фильтру и времени .....	166
Пример пользовательского отчета .....	167
Просмотр пользовательских отчетов .....	168
Предустановленные пользовательские отчеты .....	169
alarms db (alarms dashboard) .....	170
point db (point dashboard) .....	170
SLA Lost (SLA lost packets report) .....	171
Params report #1 (Граничные значения параметров для транспортных тестов #1) .....	171
Пользовательское табло мониторинга .....	172
Список документов .....	172



## Общие принципы

### Вход в систему

Для получения доступа к системе управления IQMM необходимо в интернет-браузере задать адрес `http://<host>/iqm/`. Возможно, что URL будет отличаться, от приведенного здесь шаблона, в этом случае необходимо выяснить адрес системы у ее администратора. Предполагается, что система будет работоспособна в следующих популярных браузерах: Chrome, Firefox, IE (с 11 версии до Edge), Safari, Opera. В IE до 11 версии может не работать.

Система запросит имя пользователя и пароль для проведения аутентификации пользователя. После успешной аутентификации пользователь получит доступ директории, в которой размещена система управления IQM.

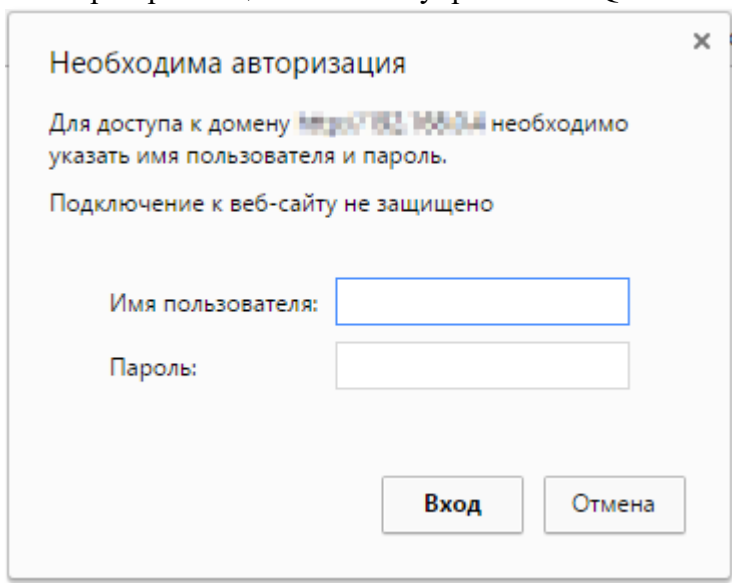


Рисунок 1 Диалог базовой аутентификации

Для работы в системе потребуется в ней авторизоваться. После успешной авторизации будет зарегистрирована сессия с правами доступа, соответствующими пользовательскому профилю. Длительность сессии ограничена.

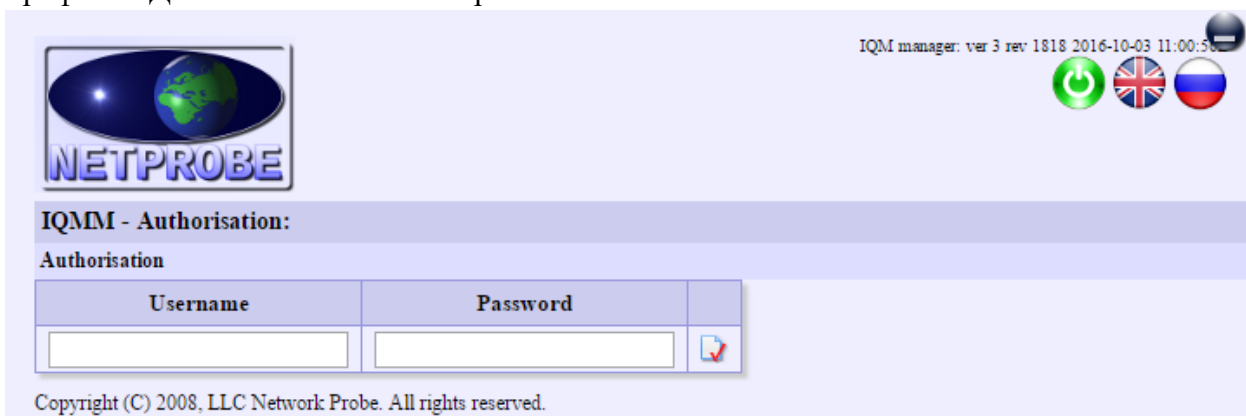


Рисунок 2 Форма авторизации в IQMM

## Элементы интерфейса

### Меню

Состав меню - настраиваемый и может отличаться от приведенного в примерах ниже.

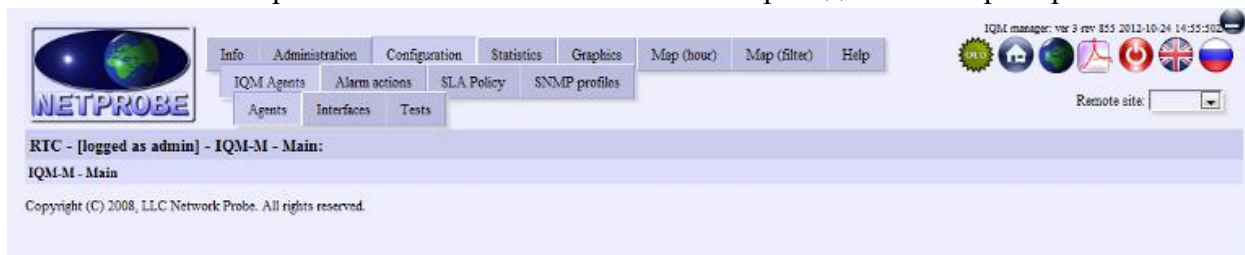


Рисунок 3 Многоуровневое меню

На следующем изображении базовые элементы интерфейса маркированы:

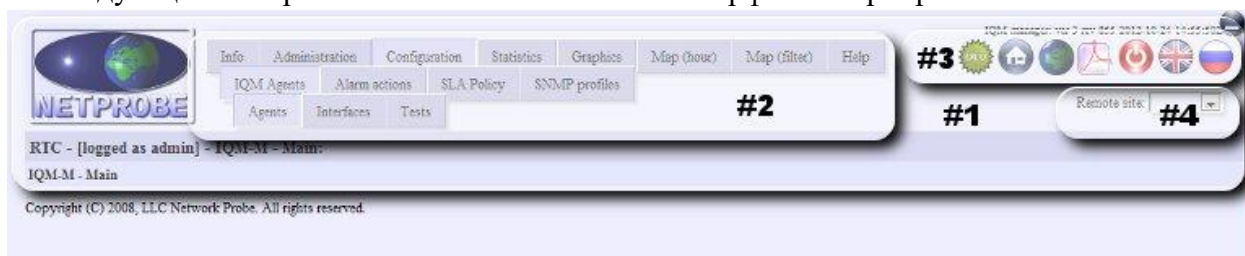


Рисунок 4 Элементы многоуровневого меню

- #1 – основной блок меню, содержащий динамические элементы: меню навигации, кнопочного меню, элемент выбора домена мониторинга, а так же статические элементы: логотип, строка с версией системы управления, кнопки для сворачивания всего блока. Основной блок меню можно сворачивать, освобождая, таким образом, рабочее пространство. Блок является элементом с фиксированным положением и остается на экране при горизонтальной прокрутке. При прокрутке он автоматически становится полупрозрачным, но остается доступным для работы с его элементами при наведении курсора. Таким образом, предоставляется максимум возможности для визуального анализа предоставленной информации.
- #2 – Блок многоуровневого меню навигации. На всех уровнях вложенности остаются доступными элементы, смежные, по отношению к текущему открытому пункту меню. Таким образом, сокращено число шагов, необходимых оператору для переключения между связанными задачами. Меню всегда развернуто к текущей задаче, предоставляя оператору доступ к логически связанным инструментам. Меню может быть персонализировано для каждого оператора.
- #3 – Блок кнопочного меню. Настраиваемые, персонализируемые ссылки для быстрого доступа к функциональным элементам системы.
- #4 – список доменов мониторинга для быстрого переключения между ними.

### Формы конфигурации

В системе реализованы единообразные формы для проведения конфигураций объектов. При открытии любой конфигурационной формы появляется таблица с параметрами, относящимися к конфигурации заданного объекта (Рисунок 5, блок #1), а так же кнопочное меню управления (Рисунок 5, блок #2). Меню управления имеет фиксированное положение, сворачивается при горизонтальной прокрутке, но при этом остается доступным оператору при наведении курсора мыши.

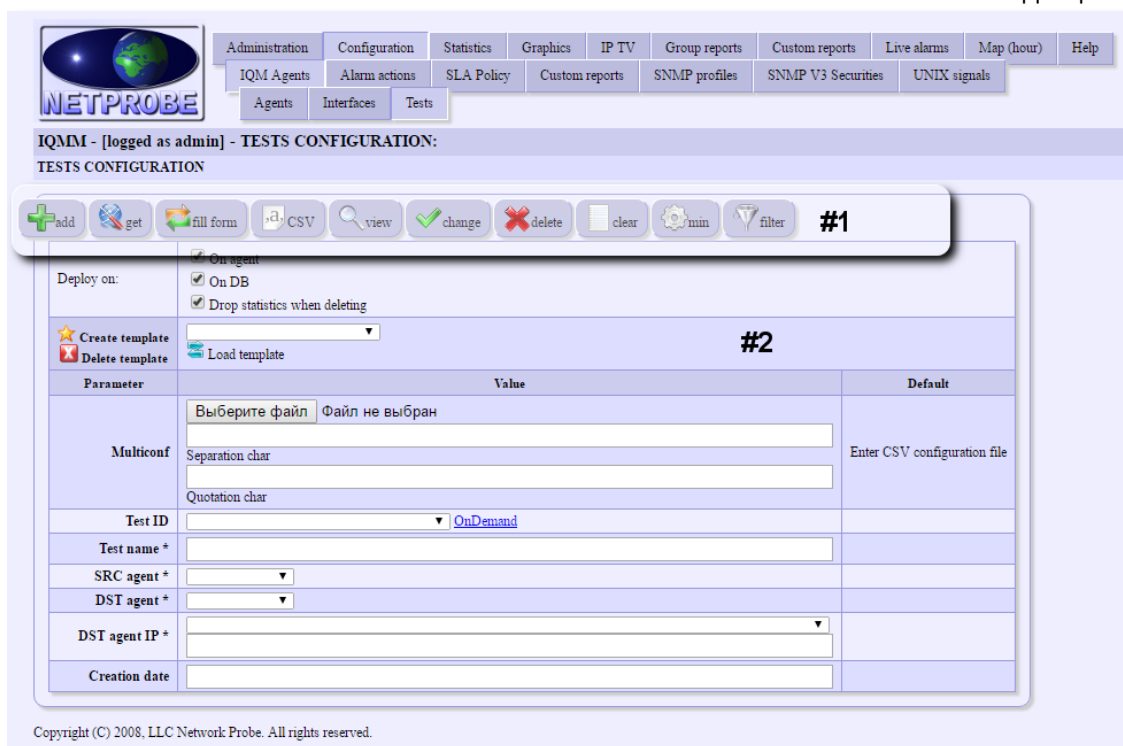


Рисунок 5 Форма конфигурации

При конфигурации объектов в системе часть полей является не обязательной для заполнения, часть – система может задать самостоятельно, часть – должны быть определены оператором. В связи с этим, таблицы конфигурации могут быть представлены в четырех режимах сложности от экспертного режима до минимального. Режим сложности определяет состав и сложность отображаемой оператору информации. Рисунок 5 приводит пример экранной формы конфигурации тестов в минимальном режиме. Как видно, создать базовый тест - просто, для этого потребуется задать всего 3 значения: имя теста (опционально), агент-инициатор, сопряженный агент (Creation date – заполняется автоматически и не доступно для редактирования).




### Меню управления








Меню управление приведено на рисунке:



Рисунок 6 Кнопочное меню управления

#### Кнопка Действие

- 
Добавить объект в базу. Для добавления требуется заполнить необходимые поля. Полям будут присвоены значения по-умолчанию (указаны в столбце Default), если не указано иное.
- 
Только для agents, tests. Подключиться к IQM-агенту, считать его конфигурацию, занести конфигурации в базу. Для получения конфигурации агента и тестов потребуется в форме agents указать Agent IP, Agent password, Agent type=IQM, [SNMP profile]. SNMP profile указывается для получения перечня интерфейсов по SNMP.
- 
Заполнить форму значениями для заданного <object> id или <object> name.

Кнопка	Действие
 CSV	Загрузить конфигурацию в формате CSV. В итоговую таблицу попадут записи, значения параметров которых соответствуют значениям/маскам, заданным в форме.
 View	Вывести настройки на страницу в табличной форме. В итоговую таблицу попадут записи, значения параметров которых соответствуют значениям/маскам, заданным в форме.
 Change	Изменить конфигурацию объекта для заданного <object> id или <object> name. Поля, заполненные в форме будут изменены на заданные значения для заданного <object> id или <object> name. Если поле содержит значение NULL, то система сформирует обращение к базе данных, подобное следующему: UPDATE objects SET object_param = NULL WHERE object_id = <id> Итоговое значение object_param зависит от его типа и определения, если поле допускает значение NULL, то оно будет сброшено в NULL. Операция сброса параметра теста на агенте не предусмотрена, для этого придется удалить тест, и соднать его заново без нежелательного параметра в конфигурации.
 Clear	Очистить форму.
 Delete	Удалить тест для заданного <object> id или <object> name.
 Expert	Выбор режима подробности представления параметров в конфигурационной таблице.
Noop	Expert - отображены все параметры, доступные для конфигурации
Nodef	Noop - скрыты опциональные параметры
Min	Nodef - скрыты параметры, имеющие заготовленные дефолтные значения
 Filter	Min - минимальный набор параметров, скрыты опциональные и дефолтные Отфильтровать содержимое списка <object> id. В список попадут тесты, значения параметров которых соответствуют значениям/маскам, заданным в форме.

*При добавлении объектов, поля, имеющие значение default, могут быть не заполнены, в этом случае, система использует значением по умолчанию.*

### Использование масок в формах

При выполнении действий, связанных с запросом списка объектов (CSV, View, Filter) допускается использование масок в полях параметров. При задании требований к значениям нескольких параметров, в запросе будет использовано логическое "И", т.е. в список попадут объекты, параметры которых одновременно удовлетворяют всем заданным требованиям. При задании масок, возможно использование специальных символов ? (один произвольный символ) и \* (любое количество любых символов).

#### маска            интерпретация

foo                Значение точно совпадает с foo

f??                Значение, начинающаяся с x и имеющее два произвольных символа в конце.  
Например: foo, fox

x\*                 Любое значение, имеющее в начале x. Например: f, fo, foo, foobar

Рисунок 1 содержит пример использования масок: в итоговый запрос попадут все объекты у которых name начинается с A и состоит из трех символов, IP представляет собой любой адрес из подсети 192.168.0.0/24, тип соответствует значению IQM.

Agent name *	A??	
Agent IP *	192.168.0.*	
Agent password *		xyz
Agent type	IQM	IQM

Рисунок 7 Использование масок в форме

### Дополнительные условия

В режиме конфигурации рабочих характеристик агента, а так же в режиме конфигурации теста возможно задать условия, которые должны быть учтены при выполнении запроса:

- On agent - провести изменения в агенте
- On DB - провести изменения в базе данных IQMM
- Drop statistics when deleting - при удалении удалить всю накопленную статистику, связанную с удаляемым объектом (агентом или тестом)

**AGENTS CONFIGURATION**

+ add
get
fill form
CSV
view
change
delete
clear
expert
filter

Deploy on:
 

- On agent
- On DB
- Drop statistics when deleting

Parameter	Value	Default
Multiconf	<div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-right: 5px;">Выберите файл</div> <div style="border: 1px solid #ccc; padding: 2px 5px;">Файл не выбран</div> </div>	Enter CSV configuration file
	Separation char	
	Quotation char	
Agent ID	<input type="text"/>	

Рисунок 8 Дополнительные условия запроса

### Просмотр настроек

При работе с запрошенными данными в режиме конфигурации объектов IQM, так же доступно контекстное меню, которое позволяет выполнить ряд операции экспорта предоставленных данных (без дополнительного запроса к БД), переключать режимы сложности, работать с фильтром отображаемых полей.

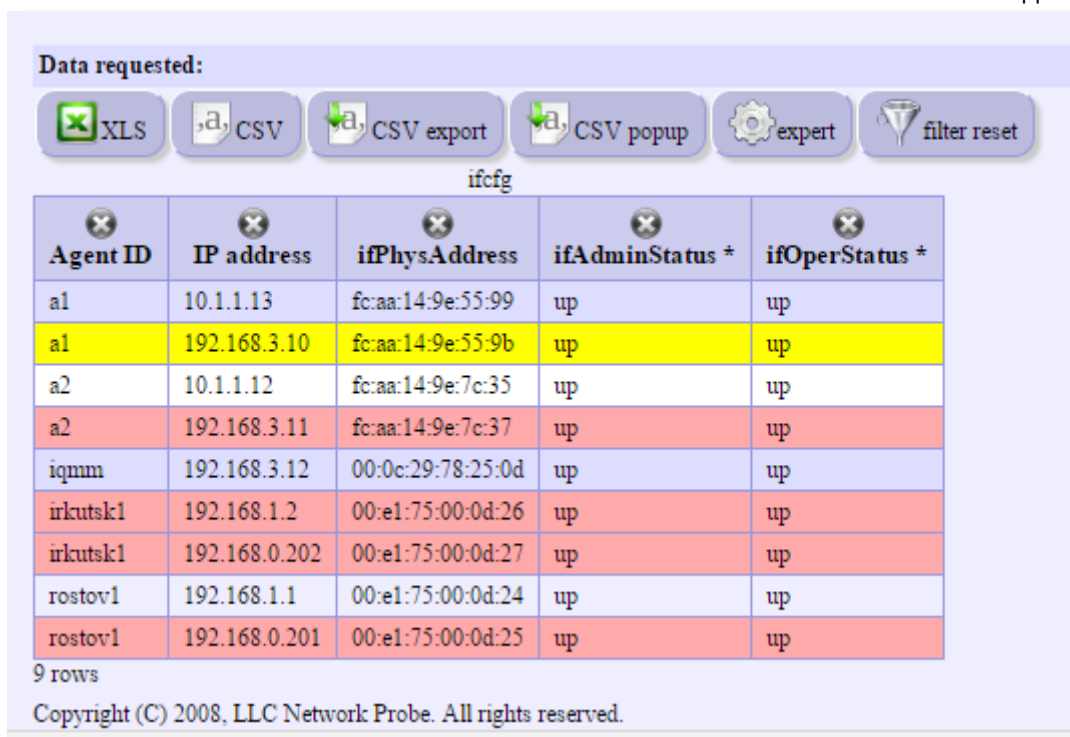





Рисунок 9 Просмотр таблицы, контекстное меню, однократное и многократное выделение строк

Для удобства работы с таблицами реализованы следующие функции:

- нажатие на кнопку  позволяет переключаться между режимами просмотра, изменяя, таким образом, состав отображаемых полей,
- Нажатие на кнопку  в заголовке каждого столбца таблицы позволяет скрыть столбец, для включения отображения всех скрытых столбцов следует нажать на  filter reset.
- однократное нажатие левой клавишей мыши над строкой подсветит ее желтым,
- для выделения множества строк следует нажать левую клавишу удерживая клавишу Ctrl, множественное выделение будет выделено розовым,
- двойной клик над выделенными строками с клавишей Ctrl позволяет скрыть все, что не выделено, повторный двойной клик с Ctrl отразит все скрытые строки,
- двойной клик (без дополнительных клавиш) снимет как однократное (желтое) так и множественное (розовое) выделения

## Фильтры

При работе с любыми отчетами в системе предусмотрена возможность фильтрации запрашиваемых данных по различным признакам: клиентам, провайдерам, сервисам, архитектурным уровням, зональным признакам, агентам тестирования, производимым тестам, классам сервиса, измеряемым параметрам. В зависимости от типов отчетов возможно дополнение этого списка условиями фильтрации, специфическими для получаемого отчета.



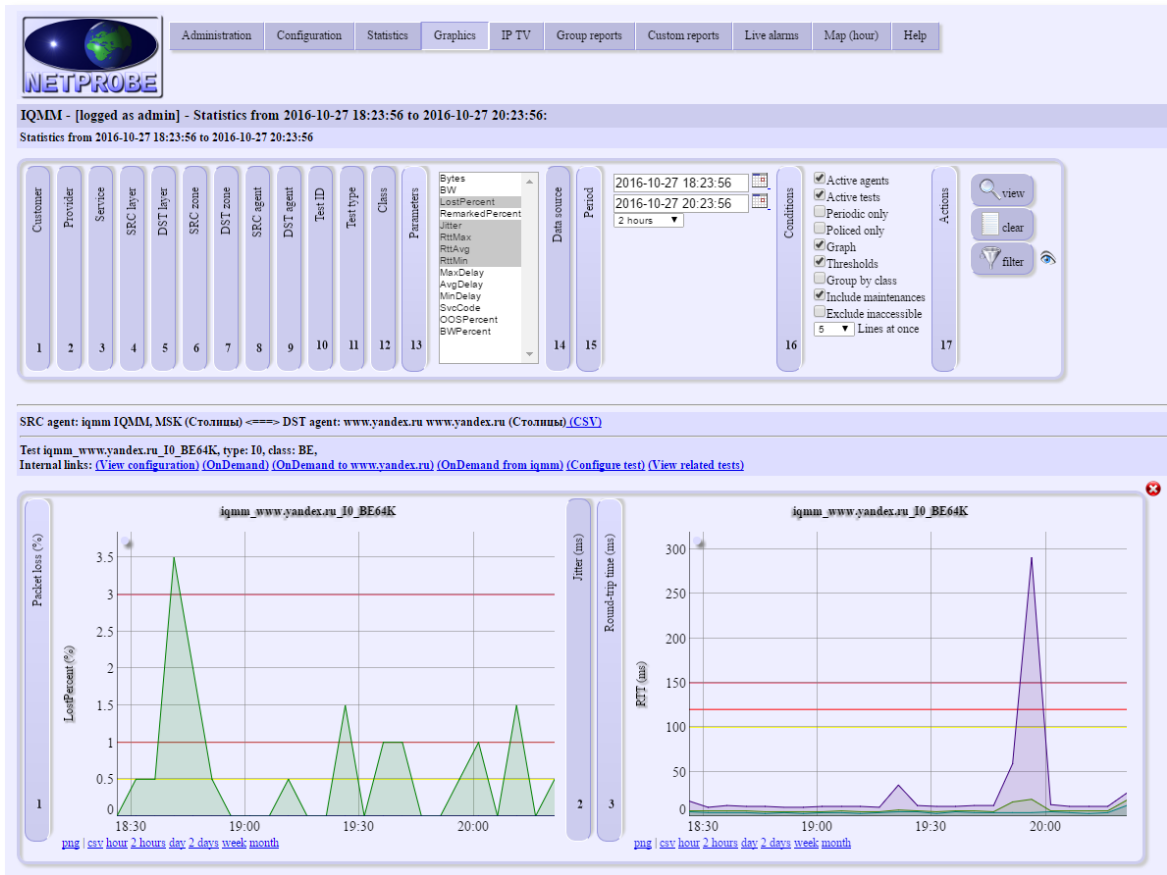


Рисунок 10 Графический отчет с фильтром по параметрам

Для осуществления фильтрации запрашиваемых данных предусмотрена возможность, как непосредственного выбора множества объектов из списка, так и возможность использования регулярных выражений, для автоматического выбора группы объектов.

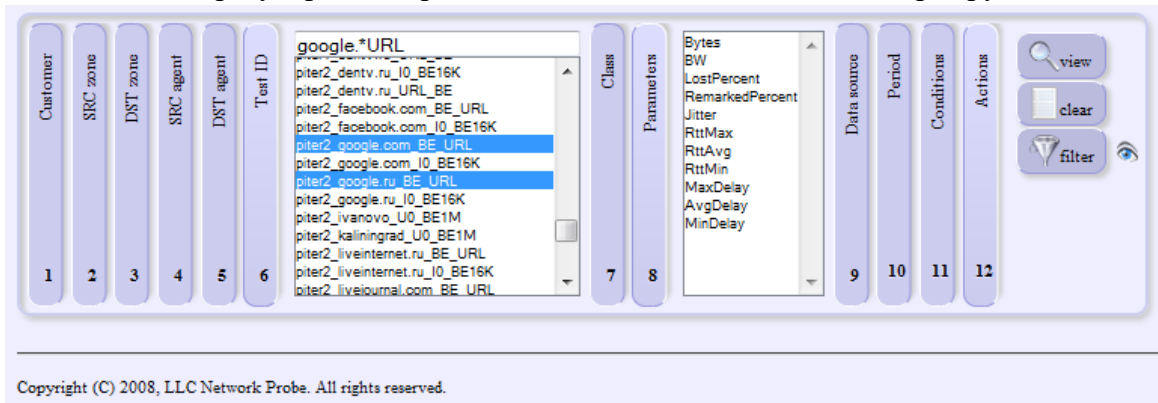


Рисунок 11 Выбор признаков фильтрации с помощью регулярного выражения

Фильтр реализован в виде аккордеона, элементы которого могут быть раскрыты или свернуты по необходимости. Фильтр, так же как и меню, является элементом с фиксированным положением, поэтому он доступен оператору после вертикальной прокрутки экрана. В процессе вертикальной прокрутки блок с фильтром смещается на край экрана, не мешая, таким образом, обзору запрошенной информации. Ниже на экранной форме видны элементы меню, ставшие полупрозрачными и смещенный в крайнее левое положение блок фильтра.

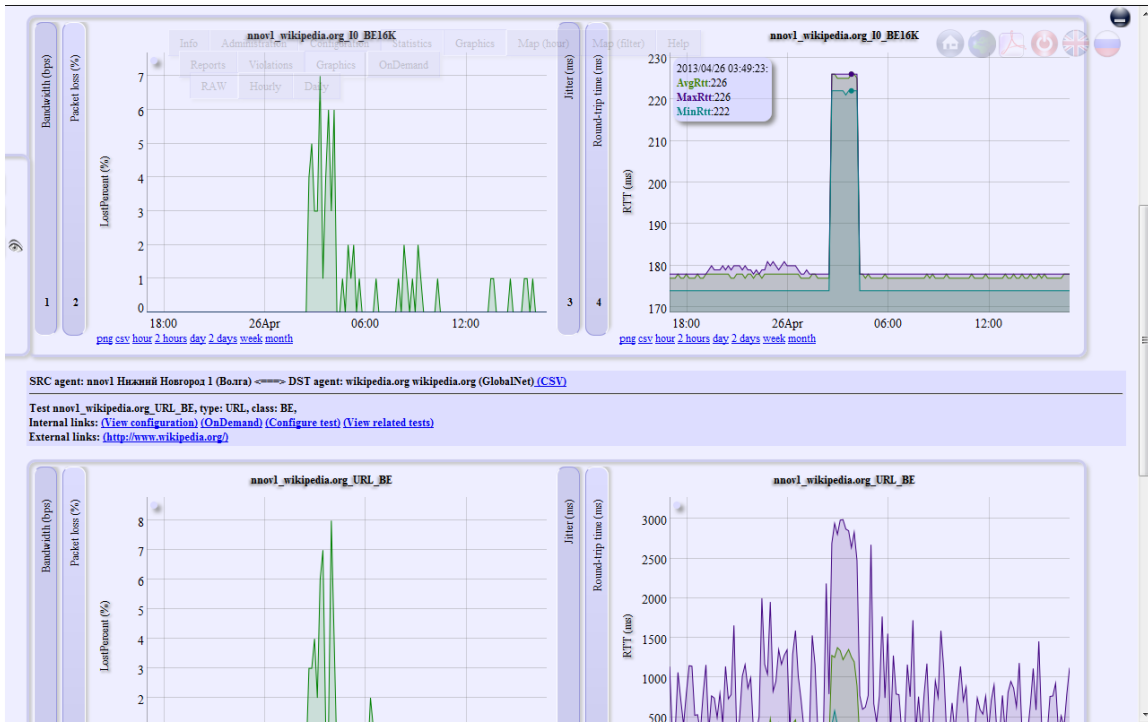


Рисунок 12 При прокрутке фильтр убирается за левый край экрана, меню становится полупрозрачным


При наведении курсора над иконкой , фильтр выдвигается, предоставляя оператору возможность работы с ним «на месте».








Рисунок 13 Фильтр в выдвинутом состоянии

## Режим массовой конфигурации

В IQMM предоставлена возможность проведения массовой конфигурации ряда объектов, управляемых системой: агенты, тесты, интерфейсы. Конфигурацию проворачивает система в



автоматическом режиме на основании параметров заранее определенных и сохраненных в CSV-таблице (мультиконфиг или шаблон конфигурации). Для проведения массовой конфигурации необходимо в поле Multiconf задать путь к заранее созданному CSV-файлу конфигурации, определить символ-разделитель и символ цитирования если они отличаются от заданных по умолчанию и выполнить действие. Допускаются действия:

-  Add - добавление множества объектов ,
-  Get - получение конфигурации с нескольких агентов,
-  Get via SNMP - получение конфигурации с нескольких агентов по SNMP,
-  Change - изменение множества объектов,
-  Delete - удаление множества объектов.

Символ-разделитель и символ цитирования, используемые по-умолчанию определены в файле конфигурации /home/iqm/iqmm/iqmm-cfg.pl:

```
$gCSVSepChar = ',';
$gCSVQuoteChar = '';
```

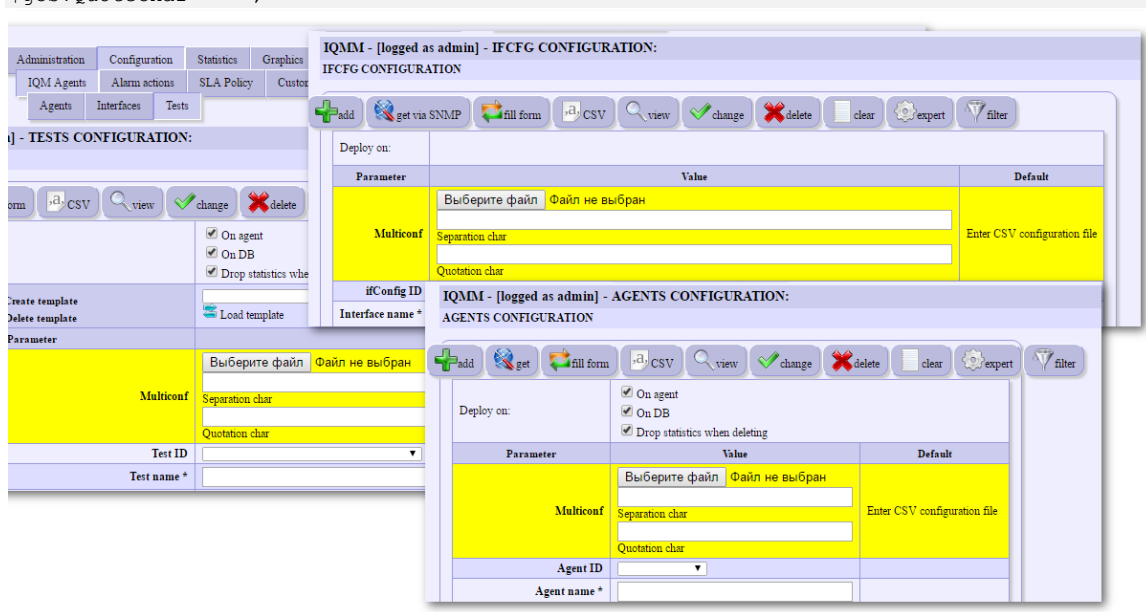


Рисунок 14 Поля Multiconf в формах конфигурации агентов, тестов, интерфейсов

Файл CSV обязательно должен иметь заголовок с именами полей. Имена полей соответствуют именам полей таблиц БД, предназначенных для хранения конфигурации объектов (agents, tests, ifcfg). Подробнее о структуре таблиц БД iqm и значениях полей см. [sql-base-structure-guide.pdf](#) (IP Quality Monitor: Структура базы данных. Руководство администратора.), см. так же /home/iqm/iqmm/sql/create\_cfg\_tables.sql.

Наиболее удобный и быстрый способ получения заготовки для таблицы


мультиконфигурации - это загрузка готовых конфигураций из базы  CSV в качестве образцов. При загрузке в CSV допускается использование масок для ограничения количества экземпляров.



Рисунок 15 Загрузка образца CSV-файла мультikonфигурации

Все поля файла мультikonфигурации, заголовки которых система не смогла определить, как известные ей, будут игнорированы. Это означает, что вы можете использовать любые вспомогательные поля, при подготовке файла. Последнее поле в файле мультikonфигурации система игнорирует, используйте его для комментирования. При заведении новых объектов система автоматически определяет идентификатор и время создания (Creation Date), не используйте эти поля. Используйте кодировку UTF-8. В случае, если значения полей содержат символы соответствующие символам разделения и/или цитирования полей - переопределите символы разделения и/или цитирования. Такая ситуация часто встречается при создании/модификации тестов, выполняемых по временному шаблону, т.к. шаблоны используют символы запятой `,` и точка с запятой `;`. В таком случае в качестве разделителя воспользуйтесь другим символом, например, знаком pipe `|`.

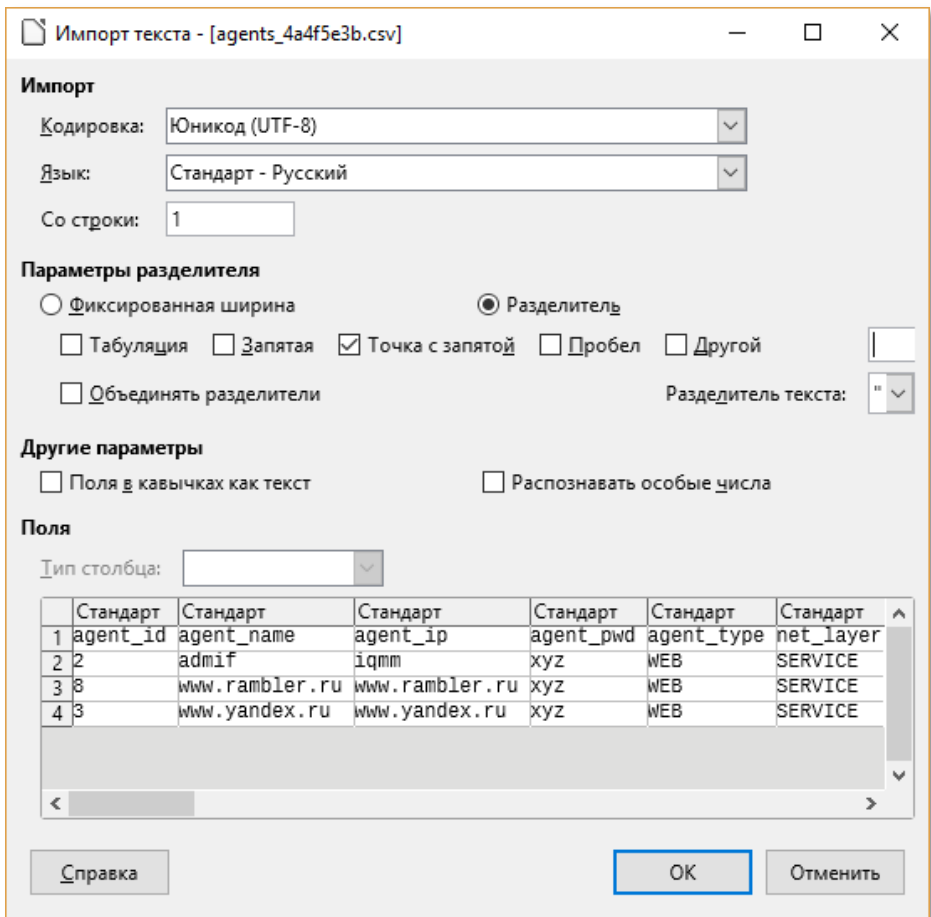


Рисунок 16 Диалог открытия CSV-файла в LibreOffice

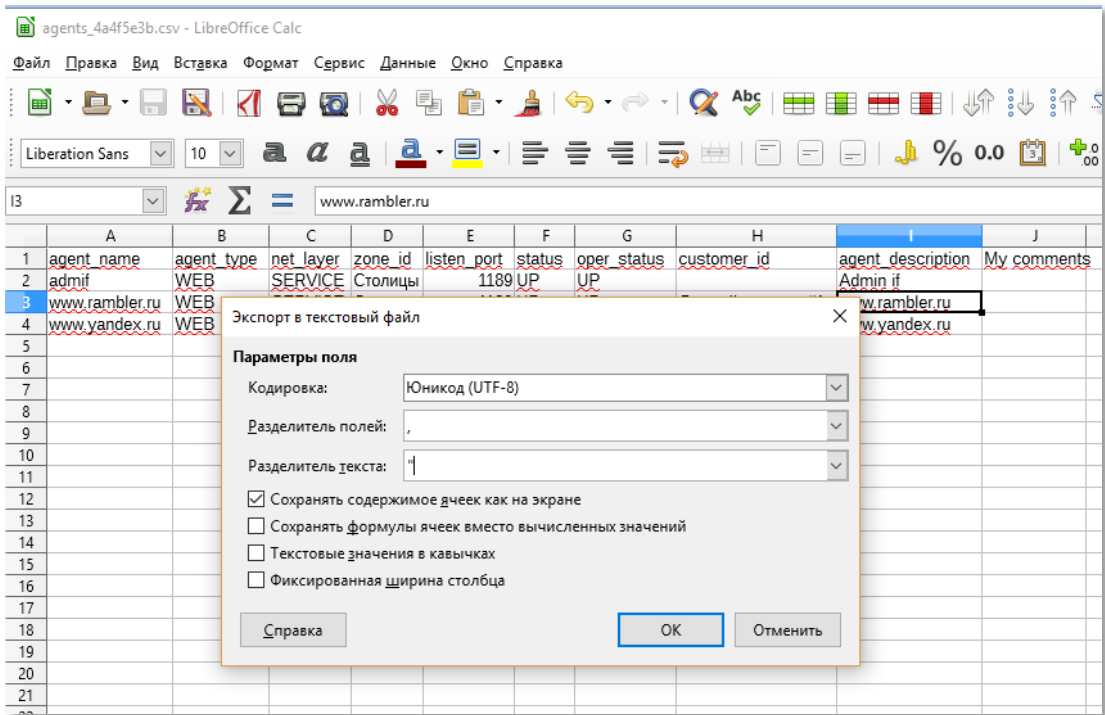


Рисунок 17 Диалог сохранения CSV-файла в LibreOffice

Пример файла мультikonфигурации:

```
agent_name;agent_type;net_layer;zone_id;listen_port;status;oper_status;customer_id;agent_description;My comments
```

```
adminif;WEB;SERVICE;Столицы;1189;UP;UP;;Admin if;
```

```
www.rambler.ru;WEB;SERVICE;Столицы;1189;UP;UP;Личный кабинет #1;www.rambler.ru;
```

```
www.yandex.ru;WEB;SERVICE;Столицы;1189;UP;UP;Личный кабинет #1;www.yandex.ru;
```

Для команд Add, Change, Delete в файле должны определяться объекты, над которыми должно быть произведено действие. Объект может быть определен его идентификатором или уникальным именем, в приведенном примере используется имя agent\_name.

Допускается определение значений параметров как в файле мультиконфигурации так и в форме. Приоритет имеет файл. Если в файле параметр определен (даже если ему не присвоено значение, но поле существует), в этом случае будет использовано значение из файла, если в файле параметр не определяется, а в форме задан, то для всех объектов, определяемых файлом будет использоваться единое значение параметра из формы.

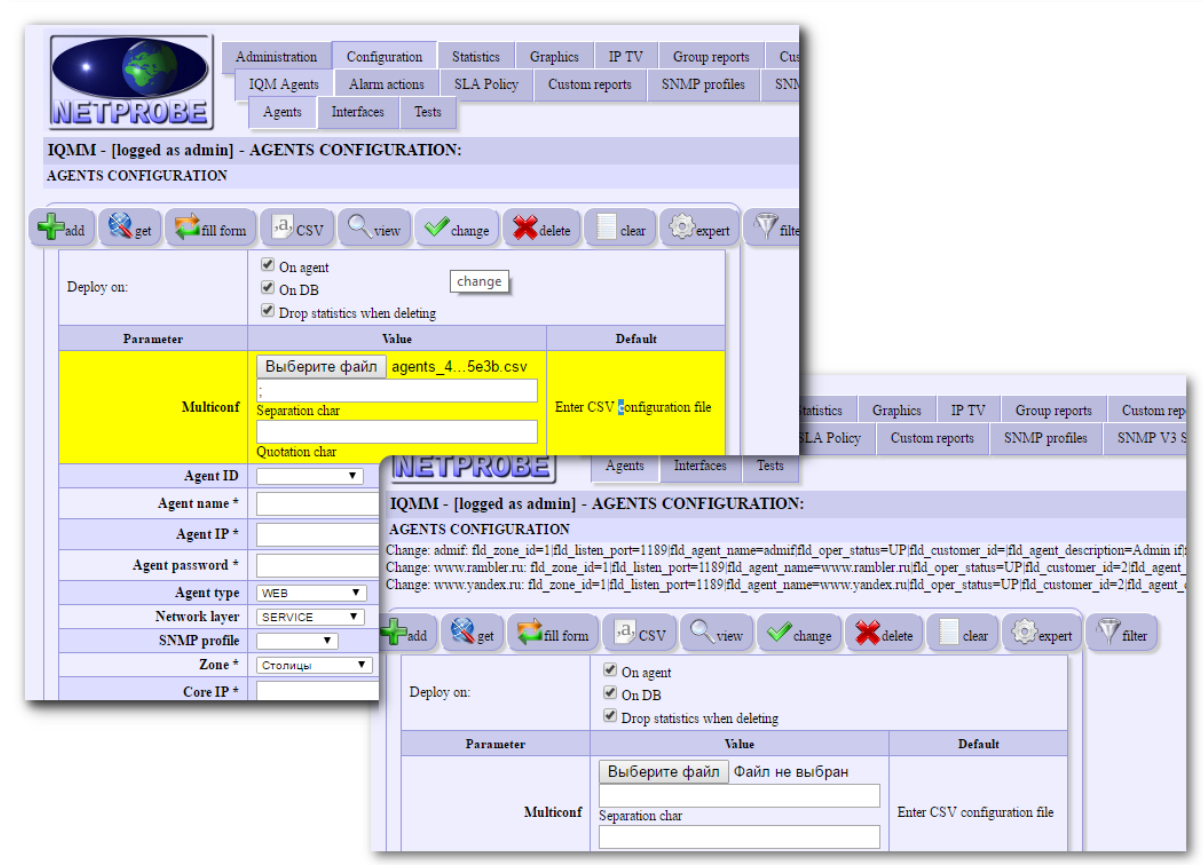


Рисунок 18 Применение мультиконфигурации в команде Change

## Задачи администрирования

### Конфигурация доступа

Ограничение доступа к системе осуществляется средствами аутентификации доступа к http-директории и авторизацией пользовательской сессии в системе с выдачей прав доступа к объектам в системе.

Информация о регистрационной записи на http директорию, содержится в файле /home/iqm/iqmm/doc/INSTALL.txt, пользователи системы приведены в файле SQL ~iqm/iqmm/sql/iqm\_users.sql. Описанные в этих файлах пары логин-пароль заводятся в системе сразу после ее инсталляции, настоятельно рекомендуем завести собственные логины, либо сменить пароли.

## Конфигурация apache

По умолчанию, рабочая директория http, находится в /home/iqm/iqmm/www/. Здесь размещены средства работы с системой, графическое оформление, сценарии JavaScript, директории с пользовательскими формами, документация.

Конфигурация директории находится в файле /etc/httpd/conf.d/99\_iqmm.conf, файл /home/iqm/iqmm/www/.htaccess задает правила аутентификации при доступе к директории, пользователи заводятся в файле /home/iqm/iqmm/.htpasswdIQM средствами утилиты htaccess. Рекомендуется сменить пароль администратора, при необходимости можно завести дополнительных пользователей.

## Управление пользователями IQMM

### Ролевые профили

Для заведения пользователя в системе IQM требуется определить его права доступа к объектом системы, для этого можно воспользоваться существующим профилем доступа, либо создать новый. Форма конфигурации ролевого профиля доступна в меню:

*Administration --> IQMM Roles*

---

Форма позволяет определить права доступа к каждому из объектов в системе (таблицам), к основным отчетам. Возможны три уровня доступа к объектам: write, read, none и два уровня доступа к отчетам: yes, none. Если не указано специально, предполагается, что доступа нет (none). В системе заведено несколько типовых ролей по-умолчанию:

- Supervisor - полный доступ
- Operator - только просмотр отчетов
- Configurator - конфигурация тестов, агентов, политик
- ReadOnly - только чтение на все объекты
- Rightless - без доступа, нужен для форсированной передачи алармов со стороны агентов

Role name *	Supervisor	Operator	Configurator	ReadOnly	Rightless
agents	write	none	write	read	none
alarm_actions	write	none	write	read	none
alarm_mail_rel	write	none	write	read	none
alarms	write	none	write	read	none
alarm_syslog_rel	write	none	write	read	none
alarm_trap_rel	write	none	write	read	none
alogs	none	none	none	none	none
classes	write	none	write	read	none
customers	write	none	write	read	none
custom_livemon_allow	none	none	none	none	none
data_aggr1	write	none	read	read	none
data_aggr2	write	none	read	read	none
data_raw	write	none	read	read	none
ifcfg	write	none	write	read	none
lm_alarms	none	none	none	none	none
login_alarms	none	none	none	none	none
login_alarms_log	none	none	none	none	none

Role name *	Supervisor	Operator	Configurator	ReadOnly	Rightless
login_invalid	none	none	none	none	none
mails	write	none	write	read	none
mcast_data_raw	none	none	none	none	none
mnt_rel	write	none	write	read	none
mnts	write	none	write	read	none
pa_roles	write	none	write	read	none
pa_sessions	write	none	write	read	none
pa_users	write	none	write	read	none
policy	write	none	write	read	none
policy_rel	write	none	write	read	none
providers	none	none	none	none	none
remotes	write	none	write	read	none
reports	none	none	none	none	none
roles	write	none	none	read	none
services	none	none	none	none	none
sessions	write	none	none	read	none
signals	none	none	none	none	none
snmp_profiles	write	none	write	read	none
snmp_v3_secs	none	none	none	none	none
syslogs	write	none	write	none	none
tests	write	read	write	read	none
test_templates	write	read	write	read	none
thresholds	write	none	write	read	none
thresholds_xaxe	none	none	none	none	none
thresholds_yaxe	none	none	none	none	none
total_quality	none	none	none	none	none
traps	write	none	write	read	none
users	write	none	none	read	none
zones	write	none	write	read	none
Alarms access	yes	yes	yes	yes	none
Reports access	yes	yes	yes	yes	none
Statistics access	yes	yes	yes	yes	none
Software management	yes	yes	yes	none	none
OnDemand tests	yes	yes	yes	yes	none

При создании нового профиля удобно воспользоваться существующим, внести свои изменения и сохранить под новым именем.

Parameter	Value	Default
Role ID	<input type="text"/>	
Role name *	<input type="text"/>	
agents	<input type="text"/>	none
alarm_actions	<input type="text"/>	none
alarm_mail_rel	<input type="text"/>	none
alarms	<input type="text"/>	none
alarm_syslog_rel	<input type="text"/>	none
alarm_trap_rel	<input type="text"/>	none
alogs	<input type="text"/>	none
classes	<input type="text"/>	none
customers	<input type="text"/>	none
custom_livemon_allow	<input type="text"/>	none

Рисунок 19 Форма конфигурации профиля доступа

### Пользователи IQMM

Форма управления пользователями доступна в меню:

*Administration --> IQMM Users*

Форма позволяет определить учетные данные для пользователя IQMM и механизмы ограничения доступа к системе. В системе по-умолчанию заведено несколько пользователей, каждый из которых соответствует одному из заранее определенных ролевых профилей:

User name *	admin	cfg	livemon	oper	recvstat	ro
Role ID	Supervisor	Configurator	Rightless	Operator	Rightless	ReadOnly
User description	Administrator's account	Configuration account	Livemon system account	Operator's account	RecvCDR system account	Read-Only access
Authentication method	sql	sql	nosql	sql	nosql	sql
Allowed domains	*	*	*	*	*	*
Allowed networks	*	*	*	*	*	*

Рисунок 20 Форма конфигурации пользователей

Поле	Значение
User ID	Идентификатор пользователя, конвертированный в уникальное имя пользователя
User name *	Уникальное имя пользователя. Допускается использование алфавитно-цифровых символов, пробелы.
User pass *	Пароль
Authentication method	Метод аутентификации (проверки пароля). Допускаются значения: sql - пароль в БД IQMM ldap - пароль в LDAP или AD posql - нужен для механизмов автоматизации, например, функционал livemon и. т.п. Не является пользователем системы.
User description	Текст с описанием
Allowed domains	Не используется
Allowed networks	IP-адреса, с которых разрешена авторизация. Список, разделенный пробелами или запятыми. Допускается ООО «НетПроб»



Поле	Значение
	использование масок типа: 1.2.3.4 1.*.3.* 1.2.3.0/24
Expiration	Дата завершения действия записи YYYY-MM-DD [hh:mm:ss]
Role ID	Ролевой профиль
Customer ID	Пользователь для личного кабинета
Map source URL	Сервер карт. Если пользователь находится в локальной сети, из которой нет доступа к сети Интернет, то ему следует предоставить доступ к локальному серверу карт. Например: http://172.16.1.125/tiles/
Для проведения аутентификации на LDAP (подробнее см. Авторизация LDAP, Active Directory) или AD потребуется определение параметров в файле конфигурации /home/iqm/iqmm/iqmm-cfg.pl:	
<pre># For LDAP \$gLDAPHost           = "10.71.30.51"; %gLDAPOptions        = (port=&gt;389,scheme =&gt; 'ldap',timeout=&gt;120); # See perldoc Net::LDAP \$gLDAPsearchbase     = "CN=nameOU=iqm,DC=okr,DC=local"; \$gLDAPproleattr      = "memberOf";</pre>	

### Контроль пользовательских сессий

*[Administration --> IQMM Sessions --> Table from \(List form\)](#)*

---

Для просмотра сессии необходимо нажать на View, для ее сброса - на delete. Аналогично можно воспользоваться формой в виде списка.

**IQMM - [logged as admin] - SESSIONS CONFIGURATION:**  
SESSIONS CONFIGURATION

Deploy on:

Parameter	Value	Default
Session	<input type="text"/>	
User ID	<input type="text"/>	
Role ID	<input type="text"/>	
Session timestamp	<input type="text"/>	
Session host	<input type="text"/>	
Session IP	<input type="text"/>	
Session forwarded	<input type="text"/>	

Data requested:

Session	User ID	Role ID	Session timestamp	Session host	Session IP	Session forwarded
kPH3OuveUUpSt3t3l736l1AHTOJgy1wX48	admin	Supervisor	1477657645	NULL	192.168.0.2	NULL

1 rows  
Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 21 Контроль пользовательских сессий

## Авторизация LDAP, Active Directory

Для проведения авторизации пользователей на сервере LDAP или Active Directory необходимо его описание в конфигурационном файле `~iqm/iqmm/iqmm-cfg.pl` системы IQMM.

- `$gLDAPHost` – адрес сервера,
- `%gLDAPOptions` – опции подключения, подробнее см. описание `Net::LDAP`,
- `$gLDAPpostfix` – постфикс, который будет добавлен к имени при авторизации на LDAP,
- `$gLDAPprefix` – префикс, который будет добавлен к имени при авторизации на LDAP,
- `$gLDAProle` – если не определено, ролевой профиль будет получен из SQL-конфигурации пользователя, если определено, имя ролевого профиля будет запрошено в LDAP,
- `$gLDAPsearchbase` – условия поиска соответствующей пользовательской записи,
- `$gLDAProleattr` – атрибут, содержащий имя ролевого профиля, в виде: `CN=IQM_<Role_name>`. Префикс `IQM_` будет удален системой. Ролевой профиль `<Role_name>` должен быть заведен в базе IQMM (См. Конфигурация ролевых профилей пользователей IQMM).

Пример конфигурации:

```
2207 # For LDAP
2208 $gLDAPHost      = "127.0.0.1";
2209 %gLDAPOptions   = (port=>389,scheme => 'ldap',timeout=>10); # See perldoc Net::LDAP
2210 $gLDAPpostfix    = ",ou=Users,dc=np,dc=com";
2211 $gLDAPprefix     = "userid=";
2212 $gLDAProle       = undef;
2213 $gLDAPsearchbase= "OU=asus,DC=okr,DC=local";
2214 $gLDAProleattr   = "memberOf";
```

## Создание пользователя личного кабинета

IQM предоставляет возможность ограниченного доступа к отчетам и данным для его предоставления региональным эксплуатационным службам и конечным пользователям услуг связи. Пользователь личного кабинета в зависимости от ролевого профиля может получить ограниченный доступ к различным отчетам системы, информации о рабочих параметрах.

Для привязки данных к конкретным заказчикам, для фильтрации объектов, отображаемых системой, используются клиентские идентификаторы. Изменить существующие или создать новые записи о клиентах можно при помощи формы CUSTOMERS CONFIGURATION. Форма вызывается через пункт меню:

*Administration -> Customers*



The screenshot shows the 'CUSTOMERS CONFIGURATION' page in the IQM Manager. At the top, there is a navigation menu with the following items: Administration, Configuration, Statistics, Graphics, IP TV, and Group reports. Below this, there is a sub-menu with Remote sites, IQMM Roles, IQMM Users, IQMM Sessions, and Customers. The main content area is titled 'IQMM - [logged as admin] - CUSTOMERS CONFIGURATION: CUSTOMERS CONFIGURATION'. Below the title, there is a toolbar with icons for add, fill form, CSV, view, change, delete, clear, and expert. The main form area contains a table with the following structure:

Parameter	Value	Default
Customer ID	<input type="text"/>	
Customer name *	<input type="text"/>	
Description	<input type="text"/>	

At the bottom of the page, there is a copyright notice: Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 22 Клиентские идентификаторы

Привязка к клиентским идентификаторам осуществляется в формах конфигурации объектов системы: агентов, тестов, пользовательских отчетов и пр. Для привязки используется поле Customer ID.

Специальный клиентский идентификатор с именем shared используется для привязки к объектам, которые должны отображаться для всех пользователей в разных личных кабинетах.

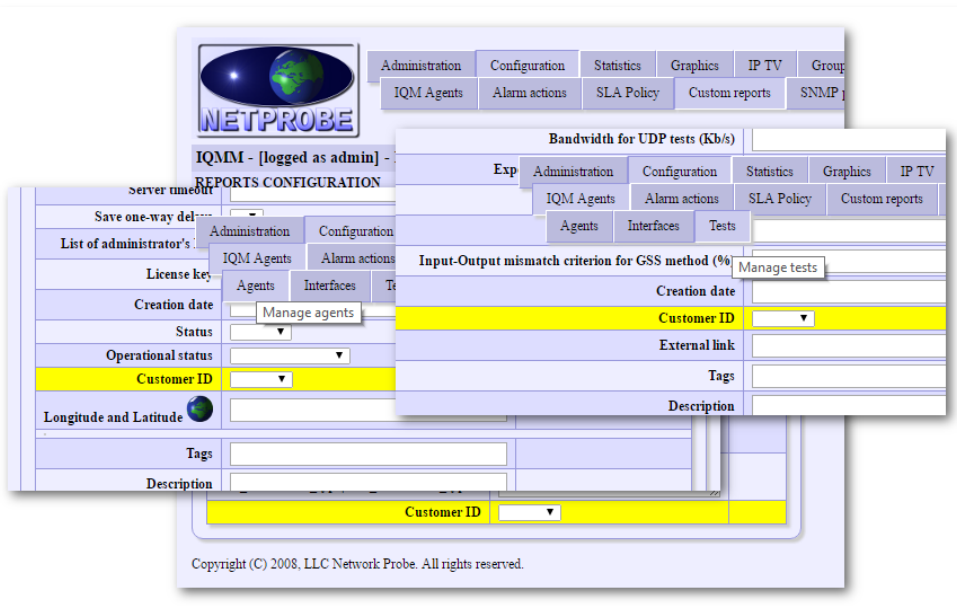


Рисунок 23 Поля Customer ID для привязки к клиентам

После создания клиентского идентификатора и привязки его к необходимым объектам, необходимо создать учетные записи пользователей, осуществить привязку пользователя к клиентскому идентификатору, назначить пользователю минимально-необходимые права доступа. Это делается через форму управления пользователями. См. Управление пользователями IQMM.

*Administration --> IQMM Users*

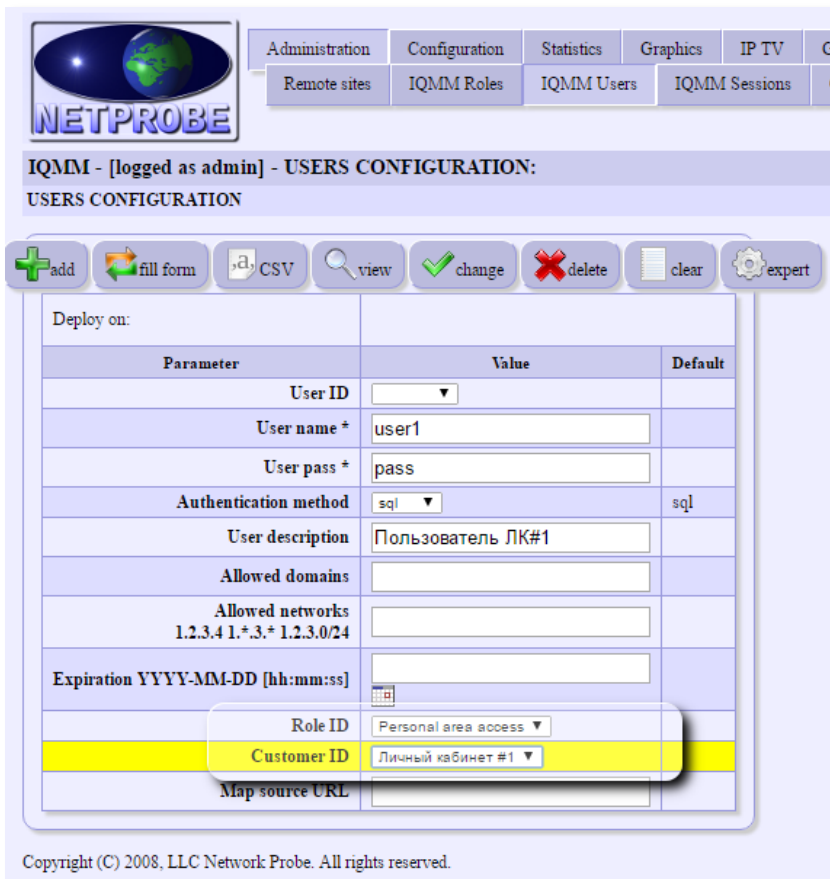


Рисунок 24 Создание пользователя личного кабинета

## Ограничение количества ошибок авторизации

Для создания препятствия в подборе пароля к системе управления IQMM - следует ограничить количество попыток авторизации в заданном временном промежутке. Для этого, проведите конфигурацию структуры gLoginCheckPolicy в конфигурационном файле /home/iqm/iqmm/iqmm-cfg.pl

```
%gLoginCheckPolicy = (
    "check_horizon_minutes" => 60,
    "invalid_login_seconds" => 60,
    "up_count"              => 3,
    "down_count"           => 0,
    "user_can_locked"      => 1,
    "user_locked_seconds"  => 60,
    "crimson_action"       => "login_invalid_action",
    "red_action"           => "login_invalid_action",
    "yellow_action"        => "login_invalid_action",
    "green_action"         => "login_invalid_action",
) ;
```

Параметр	Значение
check_horizon_minutes	Временной горизонт в минутах, на котором будет проводиться анализ попыток авторизаций.
invalid_login_seconds	Максимальный временной интервал между последовательными авторизациями, которые будут учтены как ошибочные
up_count	Количество ошибочных попыток авторизации, при превышении которого возникнет тревога уровня crimson. Тревоги уровня yellow и red равномерно распределены на интервале up_count: $1 * up\_count / 3$ - yellow $2 * up\_count / 3$ - red $3 * up\_count / 3$ - crimson
down_count	Дозволенное количество авторизаций во временном горизонте
user_can_locked	Разрешение блокировки пользователя
user_locked_seconds	Количество секунд, на которое пользователь будет заблокирован после превышения заданного количества авторизаций
crimson_action	Имя профиля crimson сигнала. Список уведомлений, который должен быть выполнен при возникновении тревоги уровня crimson. При разрешенной блокировке, пользователь будет заблокирован на user_locked_seconds секунд.
red_action	Имя профиля red сигнала. Список уведомлений, который должен быть выполнен при возникновении тревоги уровня red.
yellow_action	Имя профиля yellow сигнала. Список уведомлений, который должен быть

green\_action

выполнен при возникновении тревоги уровня yellow.  
Имя профиля green сигнала. Список уведомлений, который должен быть выполнен при возврате из состояния тревоги.

*Правила действуют одинаково для всех регистрационных записей в системе.*

## Распределенный мониторинг

Система IQM позволяет реализовать распределенный (многодоменный) мониторинг качественных параметров IP сети.

Контролируемая сеть может иметь ярко выраженную территориально распределенную структуру, с несколькими центрами концентрации трафика, региональными сетями. В этом случае разумным решением будет разбить сеть на домены мониторинга. В каждом домене будут присутствовать агенты, проводящие тесты между собой и локальная СУ IQMM куда будет отдаваться статистика внутримоментного мониторинга. Часть тестов будет проводиться на между доменном уровне, статистика таких тестов будет отдаваться в центральную СУ IQMM. Для реализации подобной архитектуры мониторинга используется несколько региональных (локальных) СУ IQMM, центральная СУ может получить доступ на управление/просмотр статистики посредством взаимодействия с локальными СУ и агентами.

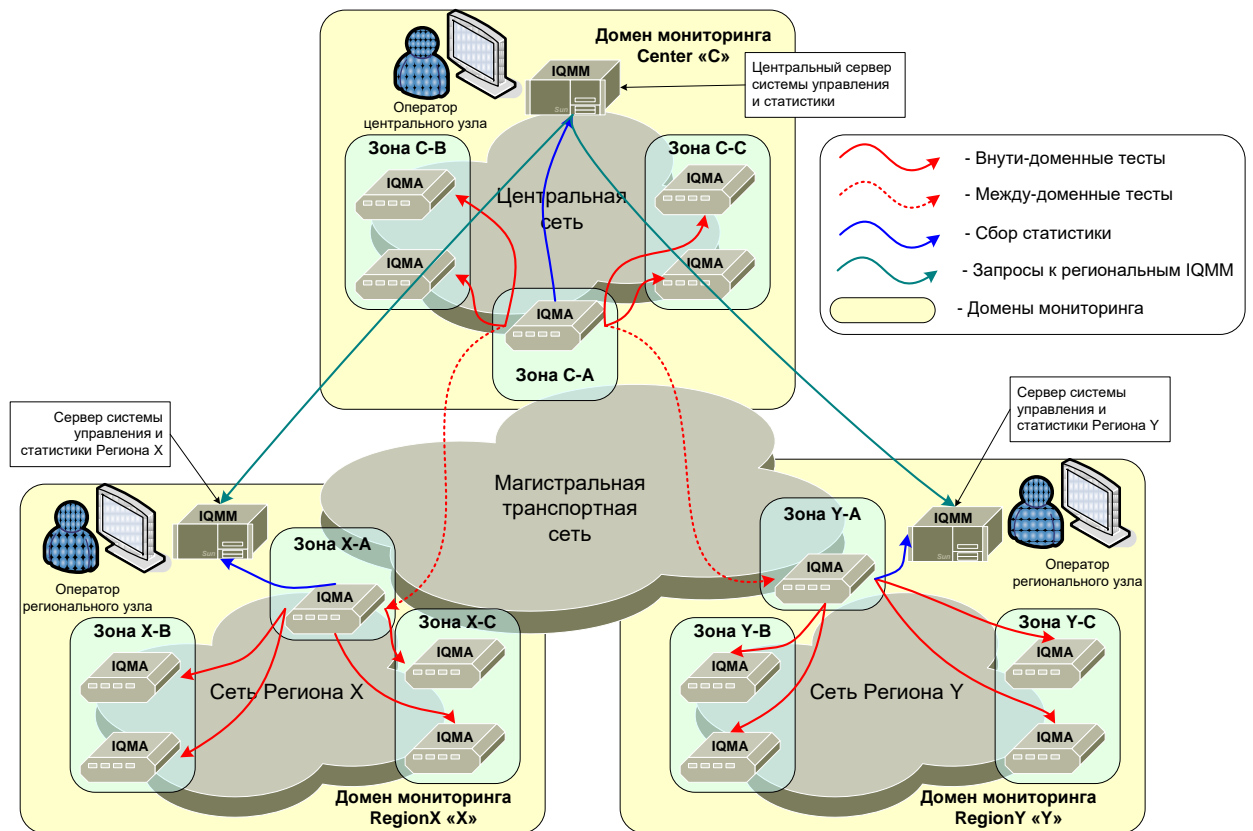


Рисунок 25 Распределенный мониторинг: центральный и региональные домены

На рисунке изображен пример построения распределенной системы мониторинга. Региональные операторы используют собственные региональные СУ IQMM для контроля и управления своими агентами. При необходимости, права управления можно перенести в центр, оставив региональным операторам права на просмотр статистики/аварий. В этой схеме, информация о проведенных тестах не уходит дальше домена мониторинга. Центральная СУ имеет доступ к статистике всех доменов через региональные СУ.

### Подключение региональных СУ IQMM к центральной

Для подключения региональных СУ IQMM к центральной необходимо наличие связанности на уровне IP центральной СУ с региональными агентами и СУ.

Взаимодействие с региональной СУ происходит на уровне базы данных, с региональными агентами – по собственному протоколу. На региональных СУ IQMM необходимо выдать права на доступ к СУБД со стороны центральной. Например, в MySQL

```
mysql> show grants for 'iqmuser'@'%domain.ru';
```

```
-----+
-----+
| Grants for iqmuser@%domain.ru |
-----+
-----+
| GRANT USAGE ON *.* TO 'iqmuser'@'%domain.ru' IDENTIFIED BY PASSWORD 'XXXXXXXXXXXX' |
| GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP ON `iqm`.* TO 'iqmuser'@'%domain.ru' |
-----+
-----+
2 rows in set (0.00 sec)
```

Либо

```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP
ON iqm.*
TO iqmuser@%domain.ru
IDENTIFIED BY 'secret';
```

В приведенных примерах любая станция СУ из домена имен «domain.ru», например iqmm1.domain.ru, iqmm2.domain.ru, сможет получить доступ к региональной СУ. Для работы интерфейса права на CREATE,DROP излишни, однако могут быть полезными при создании новых структур в БД. При отсутствии подобной необходимости, права на CREATE,DROP можно убрать.

*Примечание: наиболее удобно организовывать доступ к удаленным доменам мониторинга используя SSH-тоннели.*

---

После того, как права доступа к региональным СУ выданы – их можно подключить к центральной СУ. Для этого воспользуйтесь формой REMOTES CONFIGURATION. Форма вызывается через пункт меню:

*Configuration -> Remote sites*

---

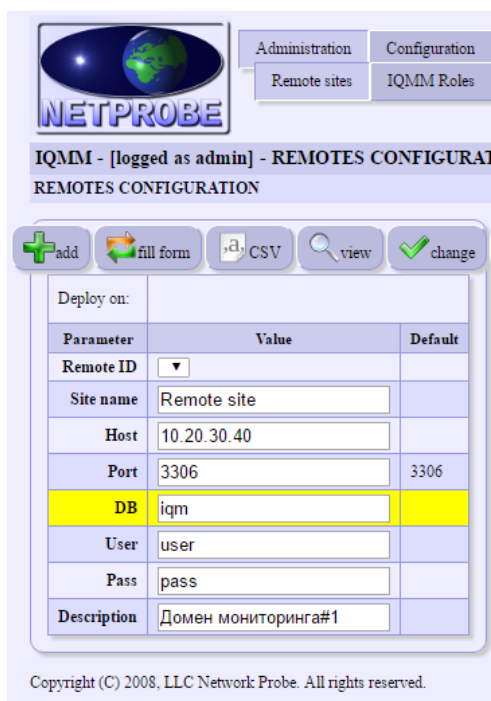


Рисунок 26 Распределенный мониторинг: центральный и региональные домены

Поле	Значение
Remote ID	Идентификатор домена, конвертированный в уникальное имя домена
Site name	Обязательное для заполнения поле. Уникальное имя домена, символическое обозначение удаленного сайта IQMM. Допускается использование алфавитно-цифровых символов, пробелы.
Host	Доменное имя или IP-адрес удаленного сайта.
DB	Имя базы данных.
User	Имя пользователя, которое будет использовано для авторизации доступа к БД.
Pass	Пароль, который будет использован для авторизации доступа к БД.
Description	Краткое описание удаленного сайта

## Задачи конфигурирования

### Требования к листам доступа (ACL) для работы системы IQM

Для работы системы необходимо обеспечить прохождение трафика:

- В рамках тестового домена:
- ICMP: лучше все, минимально Echo request, Echo reply, Time exceeded, Destination Unreachable
- UDP123 (NTP) (Для синхронизации агентов и СУ по времени)
- Между агентами (IQMA):
- TCP1189 (канал управления тестами)
- UDP1024-65535 - user-space диапазон (для проведения тестов)
- С системы управления (IQMM) на агенты (IQMA):

ООО «НетПроб»



- TCP1189 (канал управления тестами)
- TCP22 (SSH) (администрирование агентов)
- UDP161 (SNMP) (опрос агентов по SNMP)
- С системы управления (IQMM) к сети Интернет:
- желателен доступ к сети Интернет для установки ПО из публичных репозиториев.
- С агентов (IQMA) на систему управления (IQMM):
- TCP21(FTP) + FTP\_DATA (FTP от агентов на СУ - агенты инициируют передачу статистики по FTP (passive mode))
- С рабочей станции к системе управления (IQMM)
- TCP80 (доступ к интерфейсу, опционально)
- TCP22 (SSH) (администрирование агентов)
- С рабочей станции к серверу карт
- Если рабочая станция имеет доступ к сети Интернет, то карты могут загружаться с публичного карт-сервера <http://tile.openstreetmap.org>, в противном случае необходима установка сервера карт и организация доступа к нему со стороны рабочих станций.

## Первичная конфигурация агента

Агенты IQM могут поставляться в виде готового аппаратно-программного комплекса, либо, в виде программного обеспечения.

В случае поставки ПО агента, оно устанавливается на аппаратную платформу под управлением ОС Linux (дистрибутив и версия уточняются при заказе). Платформа должна удовлетворять требованиям, приведенным в документе " IQM: часто задаваемые вопросы" (IQM-FAQ-v<версия>.pdf или IQM-FAQ-v<версия>.doc), либо на сайте производителя. Вопросы управления такими платформами обговариваются с заказчиком отдельно.

В случае поставки агента в виде готового аппаратно-программного комплекса, для его корректной работы в сети потребуется проведение первичной конфигурации. В ее задачи входит:

- установка (при необходимости) ОС с требуемым функциональным набором,
- установка (при необходимости) ПО агента,
- установка сопутствующего ПО:
- SMNPD,
- NTPD,
- VLAN (при необходимости), для поддержки VLAN потребуется поддержка со стороны ОС,
- BRIDGE (при необходимости) , для поддержки BRIDGE потребуется поддержка со стороны ОС,
- настройка интерфейсов, IP, маршрутизации, NS,
- настройка сопутствующего ПО: локальный резолвер, синхронизация времени, SNMP
- первичная настройка агента: SID
- активация агента (выполняется производителем по запросу)

Рекомендуется провести все работы по первичной настройке агента до его отправки для установки площадке. При недостатке информации для проведения полного перечня работ по первичной конфигурации, минимально необходимым является настройка интерфейсов, IP и маршрутизации, для обеспечения связанности агента на уровне IP с системой управления.

*Работы должны проводиться квалифицированными специалистами, подробное описание действий по конфигурации устройства IQMA-P100 находится в документе " IP Quality Monitor. Настройка ip-адресов устройства ipplug. Руководство пользователя ". Настоятельно рекомендуется руководствоваться этим описанием при первичной настройке.*

---

## Заведение агента в системе

В общем случае, агентом в системе называется любое сетевое устройство, участвующее в измерениях, либо, являющееся источником данных о замерах, проведенных каким-либо способом. Агент-инициатор - это агент у которого хранится конфигурация теста, либо агент, инициирующий тестовую сессию. Сопряженный агент - второй, пассивный участник измерений, связанных с пропуском трафика. Например, PE-маршрутизатор, с которого проводится vrf-ping, является инициирующим агентом, SE-маршрутизатор, отвечающий на ICMP-запросы, является сопряженным агентом.

Обычно, в качестве инициатора выступает IQM-агент, однако, это может быть и TWAMP-устройство или любое другое устройство, проводящее измерения и передающее статистику в систему.

Для проведения измерений между любой парой сетевых устройств требуется их регистрация в системе.

## Форма конфигурации агентов

Для конфигурации агентов воспользуйтесь формой AGENTS CONFIGURATION (вид формы см. на Рисунок 27 ):

*Configuration --> IQM Agents --> Agents*

---

Поле Имя поля формы	Значение
Multiconf	Поле используется для осуществления массовой конфигурации агентов. Введите путь к CSV файлу, содержащий конфигурацию. Подробнее о формате файла см. а разделе Режим массовой конфигурации.
Agent ID fld_agent_id	Идентификатор, транслированный в Agent name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Agent name * fld_agent_name	Уникальное символическое обозначение агента. Допускается использование алфавитно-цифровых символов. Соответствует параметру SID в конфигурации рабочих параметров агента.
Agent IP * fld_agent_ip	IP-адрес агента, который будет использоваться СУ для взаимодействия с ним.
Agent password * fld_agent_pwd	Пароль, используемый при авторизации управляющей сессии с агентом. Соответствует параметру Password в конфигурации рабочих параметров агента.
Agent type fld_agent_type	Тип агента. Возможные значения: <ul style="list-style-type: none"> <li>• IQM,</li> <li>• UDP,</li> </ul>

Поле Имя поля формы	Значение
	<ul style="list-style-type: none"> <li>• ICMP,</li> <li>• WEB,</li> <li>• MCAST_VIDEO,</li> <li>• PPPOE,</li> <li>• CISCO_SNMP,</li> <li>• SAA,</li> <li>• STUB,</li> <li>• REMOTE_IQM.</li> </ul>
Network layer fld_net_layer	Архитектурный сетевой уровень, на котором размещен агент. По умолчанию, предусмотрены значения: CORE, DISTRIBUTION, ACCESS, SERVICE. При необходимости возможно расширение данного списка.
SNMP profile fld_snmp_profile_id	Профиль SNMP, который будет использован для получения дополнительной конфигурации агента, например, списка интерфейсов. Если профиль будет указан при получении конфигурации с агента, интерфейсы будут получены немедленно (при условии доступности службы SNMP на агенте), что исключит необходимость их определения в дальнейшем.
Zone * fld_zone_id	Список, из которого можно выбрать номер зоны, к которой относится данный агент. Соответствует параметру ZID в конфигурации рабочих параметров агента, принимает цифровое значение от 0 до 255. Для удобства в интерфейсе транслируется в уникальное имя, которое может быть определено оператором.
Core IP * fld_core_ip	IP адрес СУ IQMM куда агент будет высылать файлы с результатами тестов. Соответствует параметру CoreIP в конфигурации рабочих параметров агента.
CDR filesize (NoR) fld_res_file_nor	Количество строк в файле результатов тестов, по достижении которого он будет закрыт и поставлен в очередь на отправку в СУ. Для следующих записей будет открыт новый файл. Соответствует параметру ResFileNOR в конфигурации рабочих параметров агента.
CDR file timeout (min) fld_res_file_timeout	Количество минут, по истечении которых файл результатов тестов будет закрыт и поставлен в очередь на отправку в СУ. Для следующих записей будет открыт новый файл. Соответствует параметру ResFileTimeOut в конфигурации рабочих параметров агента. См. документ <b>Ошибка! Источник ссылки не найден.</b>
CDR send timeout (min) fld_res_send_timeout	Периодичность (в минутах), с которой файлы с записями о результатах тестов будут передаваться в СУ IQMM. Соответствует параметру SendTimeOut в конфигурации рабочих параметров агента.
Spool dir fld_spool_dir	Директория, в которой будут создана структура директорий IQMA (tmp/ cur/ new/) для обработки файлов с результатами тестов. Необходимо наличие прав на чтение, запись и выполнение. tmp/ - текущий файл, в который осуществляется запись cur/ - история new/ - временная директория используемая при ротации

Поле Имя поля формы	Значение
	Соответствует параметру SpoolDir в конфигурации рабочих параметров агента.
CDR transport script fld_send_cmd	Программа, которая будет выполняться по истечении <SendTimeOut> для передачи накопленных файлов с результатами тестов в СУ IQMM. В качестве параметра при запуске программы будет передан путь к конфигурационному файлу IQMA. Соответствует параметру SendCmd в конфигурации рабочих параметров агента.
FTP user fld_ftp_user	Имя пользователя, необходимое для авторизации при открытии транспортной сессии для передачи накопленных файлов с результатами тестов в СУ IQMM. Используется программой <SendCmd>. Соответствует параметру FtpUser в конфигурации рабочих параметров агента.
FTP password fld_ftp_pwd	Пароль, необходимый для авторизации при открытии транспортной сессии для передачи накопленных файлов с результатами тестов в СУ IQMM. Используется программой <SendCmd>. Соответствует параметру FtpPassword в конфигурации рабочих параметров агента.
Config source fld_config_src	<p>Место размещения конфигурационного файла для агента, размещенного за NAT и недоступного для конфигурации со стороны СУ IQMM. Возможно указание значений:</p> <ul style="list-style-type: none"> <li>• ftp, агент будет забирать конфиг по адресу: ftp://\${FtpUser}:\${FtpPassword}@\${CoreIP}/cfg/\${SID}_iqm_agent.conf</li> <li>• http, агент будет забирать конфиг по адресу: http://\${CoreIP}/cfg/\${SID}_iqm_agent.conf</li> <li>• либо в форме URL, понятной для программы wget</li> </ul> <p>На агенте для обновления файла конфигурации используется shell-программа /usr/local/iqm_agent/update_cfg.sh. Для включения режима самостоятельного обновления конфигурации агентом необходимо:</p> <ul style="list-style-type: none"> <li>• агенту назначить тип REMOTE_IQM,</li> <li>• указать URL файла-конфигурации в параметре Config Source,</li> <li>• первый раз перенести файл конфигурации на агента в ручную,</li> <li>• включить на агенте регулярное обновление конфигурации через cron при помощи скрипта /usr/local/iqm_agent/update_cfg.sh или другого средства</li> </ul>
Listen port fld_listen_port	Порт TCP, который будет использоваться агентами для открытия управляющего канала. Управляющий канал используется в взаимодействиях между агентами при проведении тестов, при конфигурации агента со стороны СУ IQMM. Соответствует параметру ListenPort в конфигурации рабочих параметров агента.
Server timeout fld_server_timeout	Таймаут взаимодействия с агентами в секундах. Время, в течение которого ожидается ответ от агента, по истечении этого промежутка времени считается, что ответа нет.

Поле Имя поля формы	Значение
Save one-way delays fld_one_way_delays	Директива агенту о необходимости сохранения значений односторонних задержек. Параметр был введен для совместимости со старыми версиями СУ IQMM. В нормальных условиях должен быть равен 1.
List of administrator's IPs fld_remote_admin_ip	Параметр позволяет предоставить административные функции только администраторам, чьи IP адреса содержатся в заданном параметром списке. Оператору, не входящему в этот список будет не только запрещено делать изменения в конфигурации агента, ему так же будет запрещено выполнять shutdown (остановка агента), showrun (просмотр конфигурации), showconf (зарезервировано), showtest (просмотр конфигурации отдельного теста) Список разделяется символом «;»
License key fld_lkey	Ключ, активирующий определенную функциональность агента. Предоставляется поставщиком решения IQM.
Creation date fld_creation_date	Дата подключения агента к IQMM. Поле заполняется автоматически.
Status fld_status	Административное состояние агента. UP – агент в работе, возможно поступление статистики. TEST = CFG – агент не доступен, тестовая конфигурация только в рамках БД. IQMM не будет подключаться к агенту при внесении изменений. DOWN – агент не доступен, статистика с него не поступает.
Operational status fld_oper_status	Операционное состояние агента. При заведении нового агента присваивается состояние UNKNOWN. В дальнейшем состояние определяется агент-монитором.
Customer ID fld_customer_id	Идентификатор клиента.
Longitude and Latitude fld_geo_lonlat	Географические долгота и широта, разделенные запятой (37.627487253967,55.766706073267). Для удобства предусмотрена ссылка на карту, при нажатии на нее открывается карта, на которой можно кликом левой кнопки мыши выбрать положение агента (см. рис.).
Tags fld_tags	Произвольные тэги, могут быть использованы для облегчения поиска, группировки в отчетах. До 512 символов.
Description fld_agent_description	Текстовое описание. До 512 символов.
Contract fld_contract	Номер контракта. До 512 символов.
Postal address fld_postal_address	Почтовый адрес. До 512 символов.

### Подключение агента, доступного в сети

После проведения первичной конфигурации в полном объеме, включения агента в сеть и достижения связности с ним на уровне IP, агент должен быть подключен к системе управления IQMM. После этого, все задачи по конфигурации ПО агента и тестов будут

выполняться, через интерфейс системы управления. Для заведения агента необходимо перейти в форму управления агентами AGENTS CONFIGURATION:

*Configuration --> IQM Agents --> Agents*

Parameter	Value	Default
Multiconf	Выберите файл   Файл не выбран Separation char Quotation char	Enter CSV configuration file
Agent ID	▼	
Agent name *		
Agent IP *	192.168.0.248	
Agent password *	xyz	xyz
Agent type	IQM ▼	IQM
Network layer	ACCESS ▼	CORE
SNMP profile	public ▼	
Zone *	▼	1
Core IP *		127.0.0.1

Рисунок 27 Подключение агента

Заполнить следующие поля:

- Agent IP \* - IP адрес подключаемого агента,
- Agent password \* - пароль для авторизации управляющего соединения с агентом,
- Agent type = IQM, необходимо указать, тип агента - IQM,
- Network layer - сетевой архитектурный уровень,
- SNMP profile - имя профиля SNMP, для получения списка интерфейсов.

Нажать на кнопку Get. Система подключится к агенту с указанным адресом, после успешной handshake-авторизации система считает текущую конфигурацию агента и тестов. В случае, если указан SNMP-профиль, система дополнительно попытается считать информацию об интерфейсах для подключаемого агента по SNMP. Полученную

конфигурацию система попытается занести в базу (таблицы agents, tests, ifcfg). В случае успеха, в интерфейсе будет выведен отчет о добавленных объектах.


```
1 row added to agents (iqmm)
```


```
1 row(s) added to ifcfg
```

При возникновении ошибок о них будет выдано соответствующее тревожное сообщение.

**Error: Couldn't connect to 192.168.0.2:1189: IO::Socket::INET: connect: No route to host 2277: error getting config from agent 192.168.0.2:1189**

*После подключения агента к СУ IQMM необходимо проверить его текущую конфигурацию, внести изменения при необходимости. Для изменения конфигурации агента удобно выбрать его Agent ID или Agent*

*name \*, нажать на  Fill form, форма будет заполнена текущей конфигурацией выбранного агента. После изменения значений требуемых*

*параметров в форме следует нажать на  Change. Все поля, с заданными значениями будут изменены.*

*Изменения в конфигурации агентов могут быть проведены массово, методом мультиконфигурации (см. Режим массовой конфигурации).*

## Подключение группы агентов по списку

Система позволяет проводить массовое включение агентов в автоматическом режиме с использованием метода мультиконфигурации. Подробно о режиме см. в разделе Режим массовой конфигурации. При заведении агентов по списку следует помнить о некоторых ограничениях:

- Подключение списка агентов методом get со считыванием конфигурации с агента
- допускается только для агентов типа IQM,
- для всех агентов из подключаемого списка должны быть проведены работы по первичной конфигурации,
- в процессе первичной конфигурации всем агентам из списка должны быть выданы уникальные имена.
- Заведение агентов методом add
- все обязательные конфигурационные поля, не имеющие default-значений, должны быть определены либо в файле мультиконфигурации индивидуально для каждого агента, либо в форме для всей группы
- в качестве agent\_name должны использоваться уникальные имена

Ниже приведен пример файла мультиконфигурации для подключения двух IQM агентов к системе. Наличие заключающего поля с комментариями - обязательно, его заполнение - не обязательно. Так как все параметры в конфигурации повторяются, в приведенном примере можно было бы оставить только поле agent\_ip и поле my\_comments, остальные поля заполнить в форме.

agent_ip	agent_pwd	agent_type	net_layer	snmp_profile_id	one_way_delays	status	oper_status	customer_id	my_comments
192.168.0.188	xyz	IQM	ACCESS	public	1	UP	UP	shared	
192.168.0.178	xyz	IQM	ACCESS	public	1	UP	UP	shared	

Файл мультиконфигурации сохраняется в формате CSV. Пример содержимого:

```
agent ip;agent pwd;agent type;net layer;snmp profile id;one way delays;status;oper status;customer id;my comments
192.168.0.188;xyz;IQM;ACCESS;public;1;UP;UP;shared;
192.168.0.178;xyz;IQM;ACCESS;public;1;UP;UP;shared;
```



Символ-разделитель и символ цитирования, используемые по-умолчанию определены в файле конфигурации /home/iqm/iqmm/iqmm-cfg.pl:

```
$gCSVSepChar = ',';  
$gCSVQuoteChar = '';
```

Символ-разделитель и символ цитирования не должны пересекаться со значениями в полях. В случае пересечения, следует воспользоваться нестандартными символами, их выбор - на усмотрение оператора. После создания файла мультиконфигурации его следует передать в СУ IQMM через форму управления агентами, поле Multiconf, после чего нажатием кнопки Get инициировать процесс автоматического подключения агентов.



Рисунок 28 Подключение списка агентов через Multiconf

По окончании работы система выдаст отчет по каждому добавленному объекту.

```
IQMM - [logged as admin] - AGENTS CONFIGURATION:  
AGENTS CONFIGURATION  
GetAgent: :  
fld_agent_pwd=xyz|fld_snmp_profile_id=1|fld_oper_status=UP|fld_customer_id=1|fld_agent_ip=192.168  
.0.188|fld_agent_type=IQM|fld_net_layer=ACCESS|fld_one_way_delays=1|fld_status=UP|  
GetAgent: :  
fld agent ip=192.168.0.178|fld customer id=1|fld agent type=IQM|fld snmp profile id=1|fld net lay  
er=ACCESS|fld oper status=UP|fld one way delays=1|fld status=UP|fld agent pwd=xyz|  
.....  
Processed 2 records:  
-----  
1 row added to agents (iqmm)  
1 row(s) added to ifcfg  
1 row added to agents (saratov1)  
2 row(s) added to ifcfg
```

*После подключения агентов к СУ IQMM необходимо проверить их текущую конфигурацию, внести изменения при необходимости. Изменения в конфигурации агентов так же могут быть проведены массово, методом мультиконфигурации.*

## Размещение IQM-агента за NAT

Часто возникает необходимость организовать мониторинг сервисов или качества участка сети для сетевого сегмента, размещенного за межсетевым устройством с трансляцией адресов (NAT) по отношению к СУ IQMM. Прямым решением поставленной задачи является настройка листов доступа (см. раздел Требования к листам доступа (ACL) для работы системы IQM) и статической трансляции (либо port-forwarding), для обеспечения прохождения трафика, необходимого для мониторинга. Однако, в ряде случаев,



проведение дополнительной настройки межсетевое устройства может оказаться затруднительным с организационной или с технической точки зрения. В таких случаях целесообразно воспользоваться REMOTE\_IQM режимом работы агента. Тип REMOTE\_IQM говорит СУ IQMM, что агент находится за NAT и не доступен для конфигурации. В этом случае СУ IQMM должна сохранить полный конфигурационный файл для агента в своей локальной директории, для того, чтобы агент его самостоятельно забрал с использованием механизма, который должен быть указан в параметре Config source. В качестве механизма допускается использовать:

- ftp, агент будет забирать конфиг по адресу:  
ftp://\${FtpUser}:\${FtpPassword}@\${CoreIP}/cfg/\${SID}\_iqm\_agent.conf
- http, агент будет забирать конфиг по адресу: http://\${CoreIP}/cfg/\${SID}\_iqm\_agent.conf
- URL, понятной для программы wget форме

На агенте для обновления файла конфигурации используется shell-программа /usr/local/iqm\_agent/update\_cfg.sh.

Локальная директория, в которой СУ IQMM будет сохранять подготовленные для REMOTE\_IQM конфигурационные файлы указывается в переменной gRemoteIqmCfgDir файла /home/iqm/iqmm/iqmm-cfg.pl

```
$gSLAHome = "/home/iqm";
$gSLARoot = "/home/iqm/iqmm";
$gHTML2PDF = "$gSLARoot/scripts/wkhtmltopdf-i386";
$gCDRDir = "$gSLAHome/stat";
$gRemoteIqmCfgDir= "$gSLAHome/cfg";
$gOldCDRDir = "$gCDRDir/old";
$gErrorCDRDir = "$gCDRDir/err";
$gCDRFileMask = "\\d{10}\\\.results\$";
```

По умолчанию, используется размещение /home/iqm/cfg/

```
[maxim@CO6 iqmm]$ ls -ld /home/iqm/cfg/
drwxrwxr-x. 2 iqm iqm 4096 Ноя  8 18:04 /home/iqm/cfg/
```


Файл конфигурации для REMOTE\_IQM сохраняется под именем <agent name>\_iqm\_agent.conf

Пример подготовки cfg -директории на СУ IQMM:

```
sudo chown iqm.iqm cfg/
sudo chmod 775 cfg/
sudo ln -s /home/iqm/cfg /var/ftp/stat/cfg
sudo chcon -t httpd_sys_content_rw_t /home/iqm/cfg/
```

Для включения режима самостоятельного обновления конфигурации агентом необходимо через интерфейс управления агентами:

### [Configuration --> IQM Agents --> Agents](#)

- выбрать нужный агент в списке Agent ID,
- выбранному агенту назначить тип REMOTE\_IQM в параметре Agent type,
- указать URL файла-конфигурации в параметре Config Source, для приведенного примера достаточно указать ftp,
-  Change

В директории /home/iqm/cfg/ будет создан файл <agent name>\_iqm\_agent.conf

```
1 row updated (saratov1)
```

```
on_agent=false for agent_type=REMOTE_IQM (!=IQM)
Updating config for agent_name=saratov1 (10) agent_type=REMOTE_IQM
Putting new config in /home/iqm/cfg/saratov1_iqm_agent.conf
```

- первый раз перенести файл конфигурации на агента в ручную,

- включить на агенте регулярное обновление конфигурации через cron при помощи скрипта `/usr/local/iqm_agent/update_cfg.sh` или другого средства

```

root@wtplug:~# /usr/local/iqm_agent/update_cfg.sh
Usage: /usr/local/iqm_agent/update_cfg.sh <path-to-iqm-config-file>

root@wtplug:/usr/local/iqm_agent# crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow   command
*/5 * * * * /usr/local/iqm_agent/update_cfg.sh /usr/local/iqm_agent/iqm_agent.conf > /dev/null
2>&1

```

В приведенном примере конфигурация агента будет раз в 5 минут проверяться на наличие обновлений. В случае, если контрольная сумма конфигурации изменится, обновленная конфигурация будет активирована.

### Отключение Passive FTP в sender.pl

Штатно, для передачи файлов с измерениями на сервер СУ IQMM агент использует скрипт `/usr/local/iqm_agent/sender.pl`. Для включения/отключения `passive-ftp` режима, отредактируйте следующую строчку:

```
my $ftp = Net::FTP->new($hostname, Debug => 0, Passive => 1)
```

Passive FTP по умолчанию - включен.

### Передача CDR через проху

Если из внутренней сети, где размещен агент, доступ к СУ IQMM разрешен только через прокси-сервер, установите утилиту `wput` и воспользуйтесь скриптом `send_cdr_wthproxy.sh` вместо `sender`

```

#!/bin/bash
http_proxy=87.255.9.22:57849
export http_proxy
ftp_proxy=87.255.9.22:57849
export ftp_proxy

if [ -z "$1" ] ; then
    echo "Usage: $0 <path-to-iqm-config-file>"
    exit 1
fi

CFG=$1

if [ ! -f $CFG ] ; then
    echo "Error accessing $CFG"
    exit 2
fi

eval `awk '{if($1 == "set"){printf("%s=%s\n",$2,$3);}}' $CFG`

CUR="${SpoolDir}/cur/"

```

```
URL="ftp://${FtpUser}:${FtpPassword}@${CoreIP}/stat/"

cd $CUR
/usr/bin/wput --proxy=http ${SID}* ${URL}
if [ $? != 0 ] ; then
    echo "Error loading file $URL to /tmp/$FILE"
    exit 5
fi

rm -f ${SID>*
```

## Обновление списка интерфейсов агента

Агент может иметь множество интерфейсов: физических, логических, вторичные адреса. Это может использоваться для проведения одновременных измерений на разных каналах, разных маршрутах, для отделения управляющего канала, канала сигнализации от тестовых. Для управления со стороны СУ IQMM используется интерфейс, указанный в ходе конфигурации агента в поле Agent IP. Интерфейсы и IP-адреса, которые будут использоваться в тестах определяются в процессе конфигурации теста в полях Source IP, DST agent IP \*. Для удобства работы с большим количеством IP-интерфейсов к каждому объекту агента в системе привязывается таблица с интерфейсами. Таблица автоматически заполняется при заведении нового агента методом get. Список интерфейсов система запрашивает агента по SNMP. Для того, чтобы система могла получить по SNMP список интерфейсов агента, в конфигурации агента следует указать SNMP-профиль. SNMP-профиль описывает параметры протокола SNMP, которые будут использованы при опросе агента. Если в процессе эксплуатации, настройка интерфейсов на агенте изменится, ее можно запросить заново, либо занести в ручную. Для этого служит форма IFCFG CONFIGURATION. Она вызывается в меню по пути:

*[Configuration --> IQM Agents --> Interfaces](#)*

---

Для обновления списка интерфейсов выберите в поле Agent ID имя агента, которого надо

опросить, нажать на  Get via SNMP.

Если в конфигурации агента не указан SNMP profile, система выдаст ошибку:

```
IQM::Util:1664: Error geting agent IP and snmp_profile, check agent's configuration
```

В этом случае следует сперва указать SNMP-профиль в форме AGENTS CONFIGURATION (см. Форма конфигурации агентов).

На агенте должен быть запущен и сконфигурирован сервис SNMP, для СУ IQMM предоставлен доступ к MIB-2.

**NETPROBE**

Administration Configuration Statistics Graphics IP TV  
 IQM Agents Alarm actions SLA Policy Custom reports SN  
 Agents Interfaces Tests

**IQMM - [logged as admin] - IFCFG CONFIGURATION:**  
**IFCFG CONFIGURATION**

+ add get via SNMP fill form CSV view change delete

Parameter	Value	Default
Multiconf	Выберите файл <input type="text" value="Файл не выбран"/> Separation char <input type="text"/> Quotation char <input type="text"/>	Enter CSV configuration file
ifConfig ID	iqmm:eth0:192.168.0.2	
Interface name *	iqmm:eth0:192.168.0.2	
Agent ID	iqmm	
IP address	192.168.0.2	
ifDescr *	eth0	
ifAlias		
ifType *	ethernetCsmacd	
ifMtu (Bytes) *	1500	
ifSpeed (bps) *	1000000000	
ifPhysAddress	00:0c:29:78:25:0d	
ifAdminStatus *	up	
ifOperStatus *	up	

**1 row(s) added to ifcfg**

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 29 Обновление списка интерфейсов

Значения полей формы приводятся в следующей таблице:

Поле	Значение
ifConfig ID	Идентификатор, транслированный в Interface name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Interface name	Обязательное для заполнения поле. Уникальное символическое обозначение интерфейса.

Поле	Значение
Agent ID	Идентификатор агента, которому принадлежит интерфейс. Транслирован в Agent name.
IP address	IP адрес, назначенный на интерфейс
ifDescr, ifAlias, ifType, ifMtu (Bytes), ifSpeed (bps), ifPhysAddress, ifAdminStatus, ifOperStatus	Поля – соответствующие значениям соответствующих OID из IF-MIB. При ручном заведении интерфейса допускается вольное определение этих полей. Поля в системе пока никак не используются. Их интерпретация возможна в будущем.

## Создание тестов

Под тестом понимается серия взаимодействий между сетевыми узлами с использованием объединяющей их сетевой инфраструктуры. В процессе взаимодействия фиксируются его временные, емкостные параметры, характеристики доставки, надежности. В более общем случае тестом является последовательность взаимодействий произвольной сложности с использованием ресурса ограниченной емкости с последующей фиксацией параметров доступности и производительности используемого ресурса. Состав и полнота измеряемых параметров зависит от агента-инициатора и от типа используемого теста. Тестирования и измерения могут проводиться на различных уровнях сетевой модели OSI от канального до прикладного, для этого предназначаются различные типы тестов. Инициировать проведение теста может только специализированный агент IQM, либо любой другой агент, встроенный в программное обеспечение сетевого оборудования других производителей.

После подключения IQM-агента к СУ IQMM, появляется возможность проведения конфигурации на нем тестов (для агентов типа IQM). Для конфигурации теста – воспользуйтесь формой TESTS CONFIGURATION. Форма вызывается через пункт меню:

*[Configuration --> IQM Agents --> Tests](#)*

В зависимости от выбора режима подробности представления параметров в форме конфигурации тестов может быть представлен разный состав настраиваемых параметров. В режиме Expert параметров довольно много, однако, не стоит пугаться, так как многие из них являются специфичными и значимы только для определенных типов тестов и не являются обязательными. Наличие default-значений а так же возможность использования шаблонов (templates) упрощает задачу конфигурации тестов. В простейшем случае, для создания базового теста потребуются определить только два параметра: агент инициатор (SRC agent \*) и сопряженный агент (DST agent \*). Рекомендуется самостоятельно определить правила именования тестов, однако, если имя теста не будет указано, система сформирует его автоматически, руководствуясь собственными правилами.

На рисунке приведен пример формы конфигурации тестов в режиме минимального необходимого количества настроек.

**Administration** | **Configuration** | Statistics | Graphics | IP TV | Gro  
 IQM Agents | Alarm actions | SLA Policy | Custom reports | SNM  
 Agents | Interfaces | Tests

**IQMM - [logged as admin] - TESTS CONFIGURATION:  
 TESTS CONFIGURATION**

+ add | get | fill form | CSV | view | change | delete | clear

Deploy on:  
 On agent  
 On DB  
 Drop statistics when deleting

★ Create template  
 ✖ Delete template

Load template

Parameter	Value	Default
Multiconf	Выберите файл   Файл не выбран Separation char Quotation char	Enter CSV configuration file
Test ID	OnDemand	
Test name *		
SRC agent *		
DST agent *		
DST agent IP *		
Creation date		

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 30 Форма конфигурации тестов с минимальным составом параметров

Специальные строки Deploy on, Template и Multiconf предоставляют вспомогательный функционал при работе с тестами.

**Deploy on:**

Форма конфигурации содержит строку Deploy on, которая определяет направление, в котором будут производиться изменения: агент и/или база СУ. В штатных ситуациях оба флага (On agent и On DB) должны быть возведены, что будет означать одновременное внесение изменений в конфигурации теста. Система сначала пытается произвести изменения на агенте, затем, в случае успеха – в базе данных. Если агент не доступен, система откажется делать изменения в базе. См. также раздел Дополнительные условия.

**Template:**

Строка для работы с шаблонами позволяет создавать, удалять и загружать предварительно заготовленные макеты тестовых конфигураций. Шаблоны представляют собой блок данных с произвольными параметрами теста, которые используются как предварительно определенная конфигурация теста. Для использования шаблонов оператор должен их предварительно определить – создать и сохранить в базе данных. Для создания шаблона воспользуйтесь той же формой TESTS CONFIGURATION.



Рисунок 31 Блок элементов для управления шаблонами.

Заполните поля, которые должны составлять шаблон в форме TESTS CONFIGURATION. При создании шаблона единственным обязательным полем является Test name, оно будет использовано в качестве уникального имени шаблона.

После заполнения Test name и необходимых вам полей, нажмите кнопку Create template. Шаблон будет добавлен в базу данных и появится в списке.

Для заполнения формы значениями из шаблона – выберите имя шаблона и нажмите кнопку Load template. Поля формы будут заполнены значениями из шаблона. После этого вам останется отредактировать нужные вам параметры и создать тест.

Для удаления шаблона выберите имя шаблона и нажмите кнопку Delete template. Шаблон будет удален.

#### Multiconf:

Форма допускает одновременную конфигурацию множества тестов по списку из файла мультиконфигурации. См. Режим массовой конфигурации.

Описание значения полей приведено ниже в таблице. Порядок полей может отличаться.

Поле Имя поля формы	Значение
Test ID (ID теста) fld_test_id	Идентификатор, транслированный в Test name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Test name (Название теста *) fld_test_name	Название теста. Уникальный символический идентификатор теста. Допускается использование алфавитно-цифровых символов. Формально поле является обязательным для заполнения, однако, если оператор не укажет значения Test name, система определит его самостоятельно по внутренним правилам. Соответствует параметру TID в конфигурации параметров теста на агенте
Class (IP Precedence or DSCP) fld_class_id	Класс сервиса. Значение, которое будет использовано при проведении теста. При значении меньше 8, будет маркироваться поле IP Precedence, значение большее либо равное 8 воспринимается как поле DSCP. Все значения классов сервиса заранее предустановлены в системе. В случае необходимости, их названия оператор может изменить (см. Управление именами классов сервиса). Соответствует параметру Class в конфигурации параметров теста на агенте.
SLA policy profile fld_policy_id	Профиль политики контроля. Позволяет назначить на тест политику контроля параметров, определенных в разделе



Поле Имя поля формы	Значение
	Управление SLA-политиками <b>Ошибка! Источник ссылки не найден..</b>
Live alarm expression fld_threshold_expression	Критерий для срочного уведомления, например: AvgRtt>10
URL for live alarm action fld_threshold_action	URL по которому будет передаваться срочное уведомление, например: <a href="http://usr:pass@ip/iqm/recvlivemon.cgi?USER=u1&amp;PASS=x1">http://usr:pass@ip/iqm/recvlivemon.cgi?USER=u1&amp;PASS=x1</a>
Service fld_service_id	Сервис, условный признак услуги, короткая предоставляется на измеряемом канале. Выбрать из списка: <ul style="list-style-type: none"> <li>• L2 VPN</li> <li>• L3 Access</li> <li>• L3 Core</li> <li>• L3 Distribution</li> <li>• L3 IP VPN</li> <li>• L4 Internet</li> <li>• L7 Internet</li> <li>• MCAST Video</li> </ul> <p>При необходимости можно изменить список сервисов в форме:</p> <p style="text-align: center;"><a href="#"><u>Configuration --&gt; SLA Policy --&gt; Services</u></a></p>
Provider fld_provider_id	Провайдер, условный признак провайдера телеком-услуги. Выбрать из списка: <ul style="list-style-type: none"> <li><input type="checkbox"/> Default</li> </ul> <p>При необходимости можно расширить список провайдеров в форме:</p> <p style="text-align: center;"><a href="#"><u>Configuration --&gt; SLA Policy --&gt; Providers</u></a></p>
SRC agent * fld_src_agent_id	Иницирующий агент. Агент, на котором конфигурируется тест. Соответствует параметру SID в конфигурации рабочих параметров агента.
DST agent * fld_dst_agent_id	Сопряженный агент. Идентификатор сопряженного (целевого) агента (его SID). Соответствует параметру DID в конфигурации параметров теста на агенте.
Source IP fld_src_ip	IP адрес инициатора. IP адрес, на который сопряженный агент будет высылать тестовый трафик. Специальное значение NAT, указывает сопряженному агенту использовать адрес, полученный из сокета управляющего соединения. Соответствует параметру SIP в конфигурации параметров



Поле Имя поля формы	Значение
	теста на агенте.
DST agent IP * fld_dst_agent_ip	IP адрес сопряженного агента. IP адрес, на который иницирующий агент будет высылать тестовый трафик. Соответствует параметру DIP в конфигурации параметров теста на агенте.
Local port fld_local_port	Указывает сопряженному агенту использовать заданный номер порта на иницирующем агенте во время передачи тестового трафика. Использование параметра необходимо при прохождении через листы доступа на межсетевом экране. Если параметр не задан, номер порта выделяется динамически. Соответствует параметру LocalPort в конфигурации параметров теста на агенте.
Remote port fld_remote_port	Указывает иницирующему агенту использовать заданный номер порта на сопряженном агенте во время передачи тестового трафика. Использование параметра необходимо при прохождении через листы доступа на межсетевом экране. Если параметр не задан, номер порта выделяется динамически.
Control port fld_ctl_port	TCP порт, который следует использовать для построения управляющей сессии с сопряженным агентом. Соответствует параметру StlPort в конфигурации параметров теста на агенте.
Test frequency (sec) fld_op_freq	Период в секундах между моментами запуска последовательных тестовых сессий. Если указанный период окажется меньше длительности тестовой сессии, то накладываемые тесты будут пропускаться. В регулярных тестах с заданным параметром Cron-like template не используется. Соответствует параметру OpFreq в конфигурации параметров теста на агенте.
Cron-like template fld_run_at	Определяет шаблон времени для запуска теста в определенные моменты. Имеет приоритет над параметром Test frequency. В качестве значения принимает шаблон, похожий на crontab для определения точных моментов времени запуска теста. <min>;<hour>;<day>;<month>;<wday> <min> - минута запуска теста (0-59) <hour> - час запуска теста (0-23) <day> - день запуска теста (1-31) <month> - месяц запуска теста (1-12) <wday> - день недели запуска теста (0-6, 0 - воскресенье) Если параметр пропущен - это означает любое допустимое значение. Список значений одного временного параметра разделяется запятыми. Список значений разных временных параметров разделяются точкой с запятой. Например, шаблон

Поле Имя поля формы	Значение
	<p>10,40;1;;;0 означает, что тест будет запускаться в 01:01 и 01:40 любого дня, любого месяца в воскресенье. При наличии корректно заданного параметра Cron-like template параметр Test frequency (sec) – игнорируется. Соответствует параметру RunAt в конфигурации параметров теста на агенте.</p>
Number of probes fld_num_probes	<p>Количество тестовых пакетов в серии. Для тестов прикладного уровня - количество последовательных загрузок. Например, для измерения 0.5% потерь необходимо выполнить не менее 200 посылок, для 0.1% - 1000 и.т.д. Соответствует параметру NumProbes в конфигурации параметров теста на агенте.</p>
Number of probes to ignore fld_ignore_first_delays	<p>Игнорировать результаты измерения задержек для заданного количества первых пакетов (загрузок на L7) в серии. На уровне сети требуется для тестирования каналов, устанавливаемых по требованию, DoD и т.п. На уровне приложений - для "разгона" TCP-сессии. Соответствует параметру IgnoreFirstDelays в конфигурации параметров теста на агенте.</p>
URL fld_url	<p>URL, с использованием которого следует проводить измерения типа URL или DNS. Структура URL стандартная, допускает задания логина-пароля, порта. &lt;схема&gt;://&lt;логин&gt;:&lt;пароль&gt;@&lt;хост&gt;:&lt;порт&gt;/&lt;URL-путь&gt;?&lt;параметры&gt;#&lt;якорь&gt;</p> <p>Поддерживается ssl. Наиболее полный список поддерживаемых схем находится в описании функциональных возможностей: IP Quality Monitor (IQM). Реализованные функции.</p> <p>Пример: <a href="https://ru.wikipedia.org/wiki/URL">https://ru.wikipedia.org/wiki/URL</a></p> <p>Соответствует параметру URL в конфигурации параметров теста на агенте.</p>
URL-test query interval (ms) fld_query_interval	<p>Интервал в миллисекундах. Пауза между последовательными запросами URL, при проведении измерений на уровне приложений. Если не задано, пауза не выдерживается.</p> <p>Соответствует параметру QueryInterval в конфигурации параметров теста на агенте.</p>
Cookie file fld_cookie_file	<p>Место расположения файла для хранения HTTP-cookie. Для всех HTTP-тестов, для которых не задан этот параметр, будет использоваться общий файл /tmp/iqma-cookie</p> <p>Соответствует параметру CookieFile в конфигурации параметров теста на агенте.</p>

Поле Имя поля формы	Значение
HTTP User-Agent fld_user_agent	<p>Тип браузера HTTP_USER_AGENT, который будет передаваться на HTTP-сервер при тестировании. Пример: Mozilla/5.0</p> <p>Если параметр не будет задан, то будет использовано значение по умолчанию: net-probe-iqma</p> <p>Соответствует параметру UserAgent в конфигурации параметров теста на агенте.</p>
Content download timeout fld_url_timeout	<p>Таймаут загрузки данных с ресурса в секундах. Соответствует параметру URLTimeOut в конфигурации параметров теста на агенте.</p>
DST agent type fld_dst_type	<p>Параметр устарел, не применяется. Используйте значение по-умолчанию (A).</p> <p>Тип сопряженного агента, допускаются значения: A – IQMA U – UDP-echo</p> <p>Соответствует параметру DType в конфигурации параметров теста на агенте.</p>
Test type fld_test_type	<p>Тип проводимого теста. Допускаются значения:</p> <ul style="list-style-type: none"> <li>• U0 - штатный двунаправленный Net-Probe UDP тест между IQM-агентами. U0 проводит максимально полный объем измерений на сетевом и транспортном уровнях. При наличии полноценных IQM-агентов на контролируемой сети, рекомендуется использовать именно этот тип теста для мониторинга транспортных характеристик.</li> <li>• I0 - ICMP-echo тест между IQM-агентом и стандартным ICMP-echo сервисом, осуществляет только круговые измерения. Используется при отсутствии IQM-агента на удаленном узле.</li> <li>• U7 - UDP-echo тест между IQM-агентом и стандартным UDP-echo сервисом, осуществляет только круговые измерения. Используется при отсутствии IQM-агента на удаленном узле.</li> <li>• J0 - NetProbe UDP тест между IQM-агентом и IQM-JX-респондером, аналог J1, но в отличие от J1 измеряет все параметры из состава U0. Контрольный протокол не используется. Не совместим с Juniper RPM.</li> <li>• J1 - Juniper RPM тест с контрольным протоколом. Проводится между IQM-агентом и Juniper RPM сервисом, встроенным в ПО JunOS сетевых устройств Juniper. Так же, в качестве сопряженного агента может использоваться IQM-JX-респондер. Используется при отсутствии IQM-агента на удаленном узле, и возможности использования в измерениях устройства Juniper.</li> <li>• C0 - расширение C1 для измерения всех параметров из списка U0. Измерения проводятся между IQM-агентом и</li> </ul>

Поле Имя поля формы	Значение
	<p>IQM-CX-респондером. Контрольный протокол не используется. Совместим с Cisco IP SLA, но при тестировании с IP SLA вместо IQM-CX-респондера, измерения будут аналогичны C1.</p> <ul style="list-style-type: none"> <li>• C1 - Cisco IP SLA тест с контрольным протоколом. Проводится между IQM-агентом и IP SLA сервисом, встроенным в ПО IOS сетевых устройств Cisco. Используется при отсутствии IQM-агента на удаленном узле, и возможности использования в измерениях устройства Cisco.</li> <li>• C2 - расширение C3 для измерения всех параметров из списка U0. Измерения проводятся между IQM-агентом и IQM-CX-респондером. Контрольный протокол не используется. Совместим с Cisco IP SLA, но при тестировании с IP SLA вместо IQM-CX-респондера, измерения будут аналогичны C3. Микросекундные измерения временных характеристик.</li> <li>• C3 - то же что и C1, но с микросекундными измерениями.</li> <li>• TW - измерения между IQM-агентом и любым устройством, поддерживающим RFC 5357 TWAMP-light без контрольного протокола. Используется при отсутствии IQM-агента на удаленном узле, и возможности использования в измерениях TWAMP устройств (Cisco, Juniper, RAD, Huawei, и т.д.).</li> <li>• T1 - расширение TW-теста, RFC 5357 TWAMP с реализацией контрольного протокола.</li> <li>• URL - тест уровня приложения (L7 OSI). Приложение определяется в структуре URL.</li> <li>• BW - тест между двумя агентами IQMA для измерения доступной полосы пропускания. Аналогичен U0, но при инициировании тестового потока не используется ограничение по скорости. Для проведения теста используется протокол UDP.</li> <li>• GSS - интеллектуальное измерений доступной полосы пропускания. Серия тестов U0 в ходе которой методом золотого сечения (Golden Section Search) осуществляется подбор скорости передачи тестового трафика, удовлетворяющей критериям, заданным параметрами: LossLimit – предельный уровень потерь, Precision – точность измерения скорости в процентах, InOutMismatch – рассогласование в процентах скорости инициализации тестового потока и скорости приема</li> <li>• LOCAL - аналог CMD-теста, который может выполняться локальным планировщиком СУ IQMM.</li> <li>• CMD - пакетный тест. Функциональность интерпретатора</li> </ul>

Поле Имя поля формы	Значение
	<p>тестов (пакетного теста) позволяет пользователю создавать любые тесты, реализовать произвольную логику тестирования любого сервиса, проводить любые измерения либо сбор рабочих параметров с сетевых устройств. представляет собой внешнюю программу, выполняющую измерения и возвращающую измеренные значения параметров в форматированном виде агенту. Агент может выступать в качестве инициатора пакетного теста, который будет проводиться между другими сетевыми устройствами. После завершения теста, агент может получать результаты проведенных измерений. Сам агент в тестировании не участвует. Этот подход позволяет проводить самые разнообразные нестандартные тестирования, например, не встраивая агента в адресное пространство контролируемой сети, или Cisco/Juniper-SNMP/CLI-PING, или измерение MTU, и т.п.. Пакетные тесты могут формироваться пользователем системы, имеющим достаточную для этого квалификацию. Для удобства система поставляется с несколькими готовыми пакетными тестами и шаблоном для создания новых.</p> <ul style="list-style-type: none"> <li>• MCAST_VIDEO - тест для измерения MDI в multicast IP TV.</li> <li>• DNS - тест DNS-приложения</li> <li>• PPPOE - измерение характеристик работы PPPoE - сессии.</li> </ul>
Time precision fld_time_precision	<p>Точность измерения времени:</p> <ul style="list-style-type: none"> <li>• Milli</li> <li>• Micro</li> <li>• Nano</li> </ul>
Test command (for LOCAL or CMD tests) fld_cmd	<p>Команда (для тестов LOCAL или CMD), путь к исполняемому файлу пакетного теста. Соответствует параметру CMD в конфигурации параметров теста на агенте.</p>
CMD options fld_cmd_options	<p>Опции запуска команды. Передаются в качестве опций командной строки при запуске Test command пакетного теста. Соответствует параметру CMDOptions в конфигурации параметров теста на агенте.</p>
CMD timeout kill signal fld_cmd_sig_kill	<p>UNIX-сигнал для завершения команды по таймауту. В системе определены следующие сигналы:</p> <ul style="list-style-type: none"> <li>• (1) SIGHUP Hang up—indicates that the terminal a process is using has closed</li> <li>• (10) SIGUSR1 User signal 1—Effect varies from one program to another</li> <li>• (11) SIGUSR2 User signal 2—Effect varies from one program to another</li> </ul>

Поле Имя поля формы	Значение
	<ul style="list-style-type: none"> <li>• (15) SIGTERM Terminate—end program operation gracefully (closing open files, etc.)</li> <li>• (2) SIGINT Interrupt—end program operation. The kernel sends this signal when you press Ctrl+C</li> <li>• (3) SIGQUIT Quit—terminate and leave a core file for debugging purposes. Normally initiated by a user action</li> <li>• (6) SIGABRT Abort—terminate and leave a core file for debugging purposes</li> <li>• (9) SIGKILL Kill—end program operation ungracefully; the program may not save open files, etc</li> </ul> <p>При необходимости можно изменить список UNIX-сигналов в форме:</p> <p style="text-align: center;"><a href="#"><u>Configuration --&gt; UNIX signals</u></a></p> <p>Соответствует параметру CMDKillSig в конфигурации параметров теста на агенте.</p>
Test timeout (sec) fld_test_timeout	<p>Таймаут выполнения теста (с). Если задано, по истечении заданного количества секунд тест будет принудительно завершен.</p> <p>Соответствует параметру TestTimeOut в конфигурации параметров теста на агенте.</p>
Test-specific parameters fld_specific_params	<p>Специфические для теста параметры. Будут переданы на стандартный ввод STDIN команды Test command в формате:</p> <pre style="background-color: #f0f0f0; padding: 5px;">par1=val1 par2=val2 ... parN=valN</pre> <p>При записи значения параметра на агенте и в базе данных СУ IQMM символы переводов строк[/возврата каретки] будут заменены на амперсанды '&amp;'. При конфигурации параметра в WEB-форме допускается использовать любые из этих символов в качестве разделителей пар var=val.</p> <p>Соответствует параметру SpecificParams в конфигурации параметров теста на агенте.</p>
Send config to CMD's STDIN fld_cmd_send_cfg	<p>Передать конфигурацию теста на STDIN команды. Если 1, то конфигурация теста будет передана на стандартный ввод команды Test command.</p> <p>Соответствует параметру CMDSendCFG в конфигурации параметров теста на агенте.</p>
Log CMD's STDOUT fld_cmd_out2log	<p>Журналировать STDOUT команды Test command в лог-файл IQM-агента с приоритетом INFO (7).</p> <p>Соответствует параметру CMDOut2Log в конфигурации параметров теста на агенте.</p>
Redirect CMD's STDERR to STDOUT fld_cmd_err2out	<p>Перенаправить STDERR команды Test command на STDOUT. Требуется для журналирования STDERR вместе с STDOUT в лог-файл IQM-агента с приоритетом INFO (7).</p> <p>Соответствует параметру CMDErr2Out в конфигурации</p>

Поле Имя поля формы	Значение
	параметров теста на агенте.
Enabled fld_enabled	Состояние теста: 1 – тест включён 0 – тест отключён Соответствует параметру Enabled в конфигурации параметров теста на агенте.
Packet size (B) fld_packet_size	Размер одного пакета без учета размера заголовка IP и UDP (payload). Соответствует параметру PacketSize в конфигурации параметров теста на агенте.
On demand test fld_on_demand	Признак теста по требованию: 1 – тест выполняется по требованию и отсутствует в расписании, параметры Cron-like template и Test frequency (sec) игнорируются. 0 – тест выполняется по расписанию, время повторения определяется параметрами Cron-like template или Test frequency (sec). Соответствует параметру OnDemand в конфигурации параметров теста на агенте.
Bandwidth for UDP tests (Kb/s) fld_bandwidth	Скорость в KBps = 1024 Kbps, на которой будет инициироваться поток тестовых пакетов. Игнорируется для Test Type=BW. Соответствует параметру Bandwidth в конфигурации параметров теста на агенте.
Reverse bandwidth for UDP tests (Kb/s) fld_bandwidth_reverse	Скорость в KBps = 1024 Kbps, на которой будет инициироваться поток тестовых пакетов в направлении от сопряженного агента к инициатору. Игнорируется для Test Type=BW. Если параметр не задан, будет считаться, что тест симметричен и будет использоваться Bandwidth for UDP tests (Kb/s)  Соответствует параметру BandwidthReverse в конфигурации параметров теста на агенте.
Expected bandwidth for UDP tests (Kb/s) fld_exp_bandwidth	Ожидаемая скорость для UDP тестов (Кб/с). Соответствует параметру ExpectedBandwidth в конфигурации параметров теста на агенте.
Expected reverse bandwidth for UDP tests (Kb/s) fld_exp_bandwidth_reverse	Ожидаемая скорость для UDP тестов (Кб/с) в направлении от сопряженного агента к инициатору. Соответствует параметру ExpectedBandwidthReverse в конфигурации параметров теста на агенте.
Loss Limit for GSS method (%) fld_loss_limit	Критерий для GSS-теста: количество потерь в процентах не должно превышать значение этого параметра. Если количество потерь превышает заданное параметром значение, следующее измерение будет проходить с пониженной скоростью. Значение по-умолчанию – 0%. Соответствует параметру LossLimit в конфигурации параметров теста на агенте.
Precision for GSS method	Критерий для GSS-теста: точность измерения скорости в

Поле Имя поля формы	Значение
(%) fld_bw_precision	процентах. Отношение модуля разницы между значениями верхней и нижней промежуточных точек золотого сечения к значению верхней промежуточной точки. $100\% *  S(\max) - S(\min)  / S(\max)$ S(max) – верхняя промежуточная точка золотого сечения S(min) – нижняя промежуточная точка золотого сечения По достижении заданной точности и заданного процента потерь, серия тестов GSS останавливается. Значение по-умолчанию – 10%. Соответствует параметру Precision в конфигурации параметров теста на агенте.
Input-Output mismatch criterion for GSS method (%) (InOutMismatch) fld_in_out_mismatch	Критерий для GSS-теста: рассогласование в процентах скорости инициализации тестового потока и скорости его приема. В случае, если рассогласование превышает значение, заданное параметром значение, следующее измерение будет проходить с пониженной скоростью. Значение по-умолчанию – 10%. Соответствует параметру InOutMismatch в конфигурации параметров теста на агенте.
Creation date fld_creation_date	Дата создания теста. Поле заполняется автоматически.
Customer ID fld_customer_id	Идентификатор клиента.
External link fld_ext_link	Внешние ссылки, будут отображаться вместе с графическими отчетами в блоке внешних ссылок. Допускается множество ссылок, разделенных пробелами. До 1000 символов. Формат ссылки Name URL либо URL. Пример: <code>www.rambler.ru YANDEX www.ya.ru</code>
Tags fld_tags	Произвольные тэги, могут быть использованы для облегчения поиска, группировки в отчетах. До 512 символов.
Description fld_test_description	Необязательное поле. Краткое описание теста. До 512 символов.
Contract fld_contract	Номер контракта. Текстовое поле. До 512 символов.

## UQR: Universal Quality Responder

UQR - программное обеспечение, разрабатываемое для широкого спектра аппаратных платформ и операционных систем. Работает как ответчик для разнообразных тестов, поддерживаемых IQM-агентами на уровне сети и транспорта (L3/L4 OSI), в том числе и для JX-тестов.

Список поддерживаемых тестов доступен по ключу -v.

```
root@wtplug:~# ./uqr -v
net-probe Universal Quality Responder v3-021001841
Proto supported are:J0,J1,U7
```

Запуск ответчика осуществляется с командной строки. Параметры запуска можно получить по ключу -h

```
root@wtplug:~# ./uqr -h
```



```

Usage: ./uqr [options]
Options are:
  --help                - print this text and exit
  -h                    - print this text and exit
  --version              - print version and exit
  -v                    - print version and exit
  --copyright            - print copyright and exit
  --pidfile[=filename]  - using this pidfile
  -P[filename]          - using this pidfile
  --nodaemon             - work in foreground
  --log[=filename]      - do logging to filename
  --syslog               - do logging to syslog
  --nostdout             - do not output to stdout/stderr if no daemon
  --notos                - dont send same TOS
  --notttl               - dont read TTL
  --nosamesend           - dont send using recv dst addr as src
  --ipv4-only            - using IPv4 family only
  -4                    - using IPv4 family only
  --ipv6-only            - using IPv6 family only
  -6                    - using IPv6 family only
  --without-u7           - disable U7 protocol processing
  --u7-port=N            - use this UDP port for U7 protocol
  --without-jx           - disable Jx protocol processing
  --jx-port=N            - use this UDP port for Jx protocol
  --jx-sessions=N        - maximum active sessions for J0 protocol
  --jx-timeout=milliseconds
                        - timeout for active sessions cache for J0 protocol

Defaults are:
  pidfile=uqr.pid
  daemon=1
  log=0
  filename=uqr.log
  syslog=0
  stdout=1
  tos=1
  ttl=1
  samesend=1
  ipv4-only=0
  ipv6-only=0
  u7-port=7
  jx-port=49160
  jx-sessions=5
  jx-timeout=15000
root@wtplug:~#

```

## CXR: Cisco X Responder

CXR - программное обеспечение, разрабатываемое для широкого спектра аппаратных платформ и операционных систем. Работает как ответчик для Cisco C0, C1, C2, C3 тестов, поддерживаемых IQM-агентами.

Запуск ответчика осуществляется с командной строки. Информация о версии и поддерживаемых тестах выводится по ключу -v. Ключ -h предоставляет информацию о параметрах командной строки.

```

root@wtplug:~# ./cxr -v
v1.0.0
Proto:C0,C1,C2,C3
root@wtplug:~# ./cxr -h
Usage: ./cxr [options]
Options are:
  --help                - print this text and exit
  -h                    - print this text and exit
  --version              - print version and exit
  -v                    - print version and exit
  --copyright            - print copyright and exit
  --pidfile=[filename]  - using this pidfile
  -P[filename]          - using this pidfile
  --port=port           - using this UDP port for ACP
  -pport                - using this UDP port for ACP
  --nodaemon             - work in foreground
  --notos                - dont send same TOS
  --nosamesend           - dont send using recv dst addr as src

```

```
--maxsessions=N - set limit for session cache entries
Defaults are:
  pidfile=cxr.pid
  port=1967
  maxsessions=50
```

## Типы тестов

### U0

U0 - штатный двунаправленный Net-Probe UDP тест между IQM-агентами. U0 проводит максимально полный объем измерений на сетевом и транспортном уровнях. При наличии полноценных IQM-агентов на контролируемой сети, рекомендуется использовать именно этот тип теста для мониторинга транспортных характеристик.

*Планируется разместить U0-респондер в ПО UQR: Universal Quality Responder. Для проверки наличия требуемого функционала выполните `uqr -h`.*

---

Для создания U0 теста необходимо определить агента-инициатора. В обычных условиях рекомендуется в качестве инициатора использовать агента, стоящего на более высоком архитектурном уровне в сети, такой агент сможет проводить тесты на множестве направлений. Например, один агент на уровне агрегации/дистрибуции сможет проводить тесты с множеством агентов уровня доступа. Основная причина такого выбора - минимизация потоков файлов с измеренными данными в сторону системы управления и, как следствие, минимизация затрат на обеспечение этих процессов. Кроме этого, контроль множества VPN может быть реализован с использованием минимального количества агентов на уровне ядра или PE.

*Таким образом, рекомендуемая топология измерений должна стремиться к типу звезда или созвездие, чтобы минимизировать потоки с данными об измерениях.*

---

Конфигурация теста на IQM агенте осуществляется через WEB-интерфейс. В качестве сопряженного агента указывается IQM агент. Тип теста U0. Пример конфигурации приведен в таблице.

Test name *	iqmm_saratov1_U0_BE64K
Class (IP Precedence or DSCP)	BE
Service	L4 Internet
Provider	Default
SRC agent *	iqmm
DST agent *	saratov1
Source IP	NAT
DST agent IP *	192.168.0.2
Test frequency (sec)	60
Number of probes	200
DST agent type	A
Test type	U0

<b>Test name *</b>	<b>iqmm_saratov1_U0_BE64K</b>
Enabled	1
Packet size (B)	60
On demand test	0
Bandwidth for UDP tests (Kb/s)	64
Expected bandwidth for UDP tests (Kb/s)	64

### **I0, U7**

I0/U0 - ICMP/UDP-echo тесты проводятся между IQM-агентом и стандартными ICMP/UDP-echo сервисами, доступными практически в любых операционных системах. Осуществляются только круговые измерения. Используется при отсутствии IQM-агента на удаленном узле. Для конфигурации теста ICMP/UDP-echo следует указать тип теста I0 (ICMP-echo) или U7 (UDP-echo). Примеры конфигурации приведены в таблице.

<b>Test name *</b>	<b>iqmm_saratov1_I0_BE64K</b>	<b>iqmm_saratov1_U7_BE64K</b>
Class (IP Precedence or DSCP)	BE	BE
Service	L4 Internet	L4 Internet
Provider	Default	Default
SRC agent *	iqmm	iqmm
DST agent *	saratov1	saratov1
Source IP	NAT	NAT
DST agent IP *	192.168.0.2	192.168.0.2
Test frequency (sec)	60	60
Number of probes	200	200
DST agent type	A	A
Test type	I0	U7
Enabled	1	1
Packet size (B)	60	60
On demand test	0	0
Bandwidth for UDP tests (Kb/s)	64	64
Expected bandwidth for UDP tests (Kb/s)	64	64

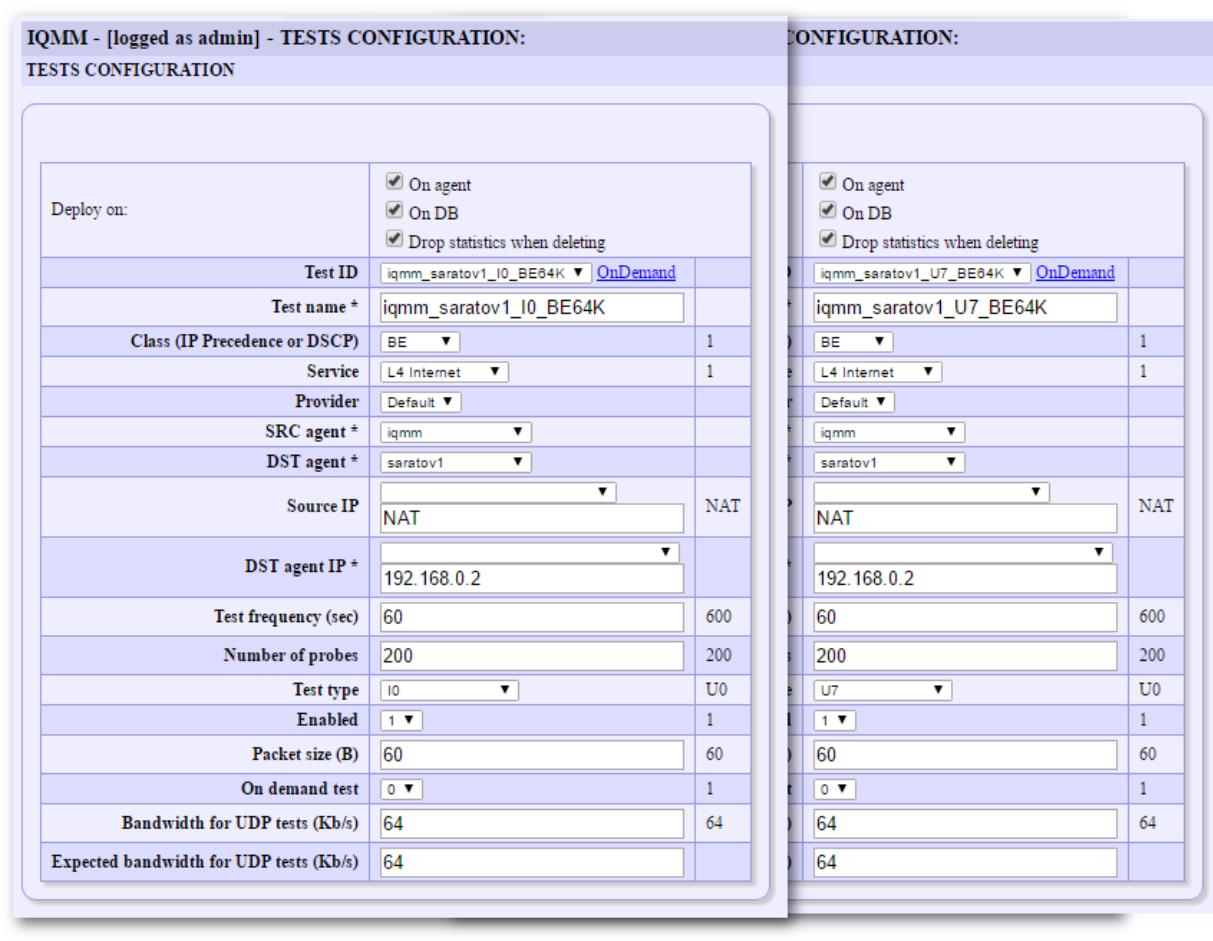


Рисунок 32 Формы конфигурации тестов J0 и J1

### J0, J1

J0 - NetProbe UDP тест между IQM-агентом и IQM-JX-респондером, аналог J1, но в отличие от J1 измеряет все параметры из состава U0. Контрольный протокол не используется. Не совместим с Juniper RPM.

J1 - Juniper RPM тест с контрольным протоколом. Проводится между IQM-агентом и Juniper RPM сервисом, встроенным в ПО JunOS сетевых устройств Juniper. Так же, в качестве сопряженного агента может использоваться IQM-JX-респондер. Используется при отсутствии IQM-агента на удаленном узле, и возможности использования в измерениях устройства Juniper.

Для проведения тестов JX потребуется конфигурация Juniper RPM (J1), либо запуск ПО UQR (см. UQR: Universal Quality Responder) на аппаратной платформе, которую планируется использовать в качестве сопряженного агента. При запуске UQR ответчика можно задать номера портов, на которых ответчик слушает запросы, ограничить количество одновременных JX-сессий. Это делается при помощи параметров командной строки:

```
--u7-port=N      - use this UDP port for U7 protocol
--jx-port=N      - use this UDP port for Jx protocol
--jx-sessions=N  - maximum active sessions for J0 protocol
```

Значения, используемые по умолчанию:

```
u7-port=7
jx-port=49160
```

Конфигурация теста на IQM агенте осуществляется через WEB-интерфейс. В качестве сопряженного агента указывается Juniper RPM агент либо IQM-JX-респондер. Тип теста J0 или J1. Следует указать номер порта для JX теста, в противном случае агент проведет U7 (UDP-echo) тест на порт UDP7. Примеры конфигурации приведены в таблице и на экранных формах (см. Рисунок 33 Формы конфигурации тестов J0 и J1).

*Ограничения по размеру пакета для J0 - не менее 76 байт. При размере пакета от 52 до 76 байт, тест J0 будет работать в режиме J1. Добавленные параметры измеряться не будут.*

*Ограничения по размеру пакета для J1 - не менее 52 байт. При размере пакета от 12 до 52 байт, состав измеряемых характеристик будет ограничен.*

*При получении пакета меньше 12 байт измерения проводится не будут для J0 и J1.*

---

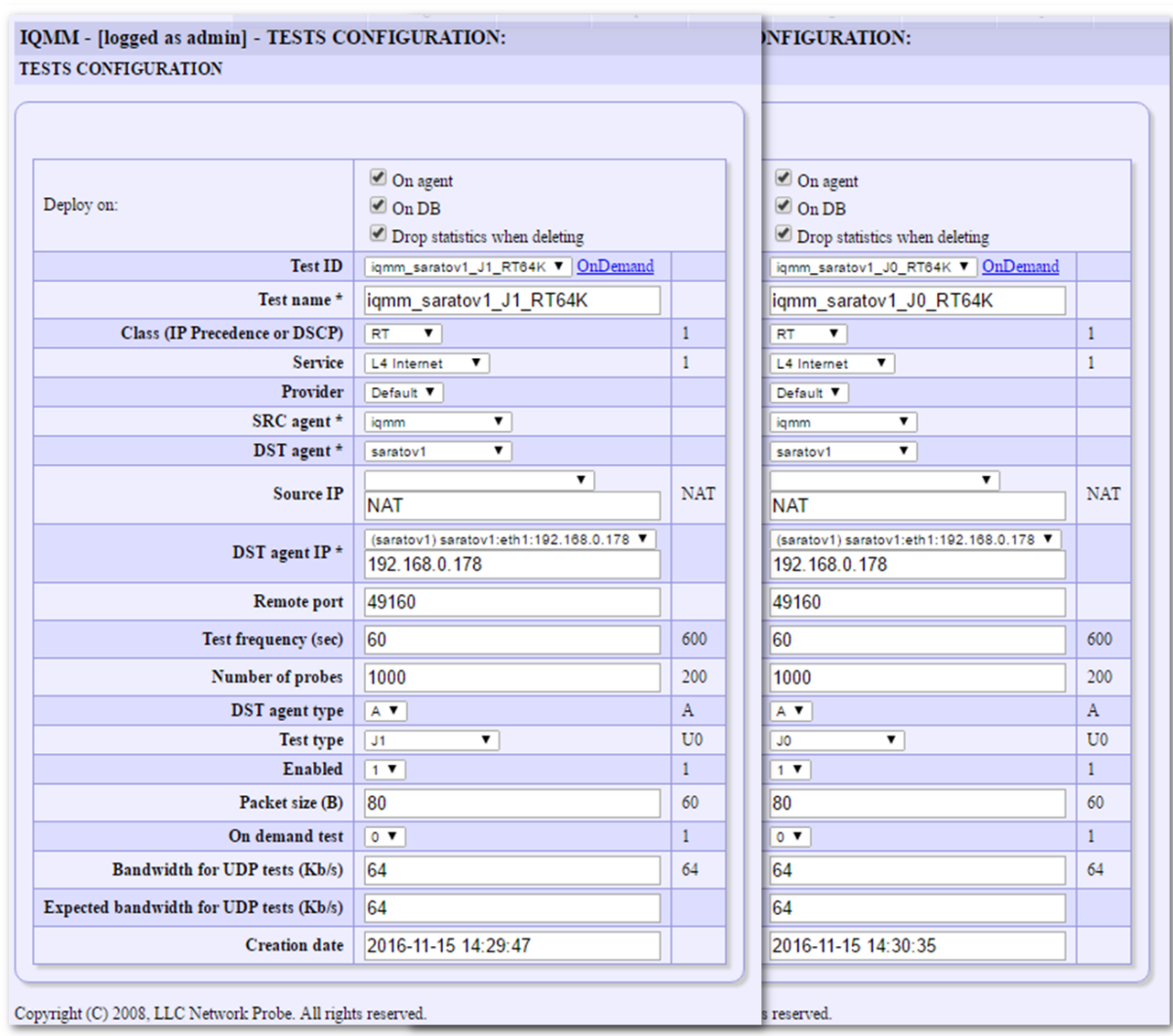


Рисунок 33 Формы конфигурации тестов J0 и J1

Test name *	iqmm_saratov1_J0_RT64K	iqmm_saratov1_J1_RT64K
Class (IP Precedence or DSCP)	RT	RT
SRC agent *	iqmm	iqmm
DST agent *	saratov1	saratov1
Source IP	NAT	NAT
DST agent IP *	192.168.0.178	192.168.0.178
Remote port	49160	49160
Test frequency (sec)	60	60
Number of probes	1000	1000
Test type	J0	J1
Enabled	1	1
Packet size (B)	80	80
On demand test	0	0
Bandwidth for UDP tests (Kb/s)	64	64
Expected bandwidth for UDP tests (Kb/s)	64	64

## C0, C1, C2, C3

C0 - расширение C1 для измерения всех параметров из списка U0. Измерения проводятся между IQM-агентом и IQM-CX-респондером. Контрольный протокол не используется. Совместим с Cisco IP SLA, но при тестировании с IP SLA вместо IQM-CX-респондера, измерения будут аналогичны C1.

C1 - Cisco IP SLA тест с контрольным протоколом. Проводится между IQM-агентом и IP SLA сервисом, встроенным в ПО IOS сетевых устройств Cisco. Используется при отсутствии IQM-агента на удаленном узле, и возможности использования в измерениях устройства Cisco.

C2 - расширение C3 для измерения всех параметров из списка U0. Измерения проводятся между IQM-агентом и IQM-CX-респондером. Контрольный протокол не используется. Совместим с Cisco IP SLA, при тестировании с IP SLA вместо IQM-CX-респондера, измерения будут аналогичны C3. Микросекундные измерения временных характеристик.

C3 - то же что и C1, но с микросекундными измерениями.

Для проведения тестов CX потребуется конфигурация Cisco IP SLA, либо запуск ПО CXR (см. CXR: Cisco X Responder) на аппаратной платформе, которую планируется использовать в качестве сопряженного агента. При запуске CXR ответчика можно задать номер порта, на котором ответчик слушает запросы, ограничить количество одновременных CX-сессий. Это делается при помощи параметров командной строки:

```
--port=port
-pport          - using this UDP port for ACP
--maxsessions=N - set limit for session cache entries
```

Значения, используемые по умолчанию.

```
port=1967
maxsessions=50
```

Конфигурация теста на IQM агенте осуществляется через WEB-интерфейс. В качестве сопряженного агента указывается Cisco IP SLA агент либо IQM-CX-респондер. Тип теста C0, C1, C2, C3. Следует указать номер порта для CX теста, в противном случае тест будет неуспешным. Примеры конфигурации приведены в таблице и на экранных формах (см. Рисунок 34).

<b>Test name *</b>	<b>iqmm_saratov1_C0_RT64K</b>
Class (IP Precedence or DSCP)	RT
Service	L4 Internet
Provider	Default
SRC agent *	iqmm
DST agent *	saratov1
Source IP	NAT
DST agent IP *	192.168.0.178
Remote port	1967
Test frequency (sec)	60
Number of probes	1000
Test type	C0
Enabled	1
Packet size (B)	80
On demand test	0
Bandwidth for UDP tests (Kb/s)	64
Expected bandwidth for UDP tests (Kb/s)	64

**IQMM - [logged as admin] - TESTS CONFIGURATION:**  
**TESTS CONFIGURATION**

Deploy on:	<input checked="" type="checkbox"/> On agent <input checked="" type="checkbox"/> On DB <input checked="" type="checkbox"/> Drop statistics when deleting	
Test ID	iqmm_saratov1_C0_RT64K ▼ <a href="#">OnDemand</a>	
Test name *	iqmm_saratov1_C0_RT64K	
Class (IP Precedence or DSCP)	RT ▼	1
Service	L4 Internet ▼	1
Provider	Default ▼	
SRC agent *	iqmm ▼	
DST agent *	saratov1 ▼	
Source IP	NAT	NAT
DST agent IP *	(saratov1) saratov1:eth1:192.168.0.178 ▼ 192.168.0.178	
Remote port	1967	
Test frequency (sec)	60	600
Number of probes	1000	200
Test type	C0 ▼	U0
Enabled	1 ▼	1
Packet size (B)	80	60
On demand test	0 ▼	1
Bandwidth for UDP tests (Kb/s)	64	64
Expected bandwidth for UDP tests (Kb/s)	64	

Рисунок 34 Формы конфигурации тестов СХ

*Ограничения по размеру пакета для*

*C0- не менее 32 байт*

*C1 - не менее 16 байт*

*C2 - не менее 72 байт*

*C3 - не менее 56 байт*



## TW, T1

TW - измерения между IQM-агентом и любым устройством, поддерживающим RFC 5357 TWAMP-light без контрольного протокола. Используется при отсутствии IQM-агента на удаленном узле, и возможности использования в измерениях TWAMP устройств (Cisco, Juniper, RAD, Huawei, и т.д.).

T1 - расширение TW-теста, RFC 5357 TWAMP с реализацией контрольного протокола. требует принудительного указания UDP порта.

### TWAMP на Cisco

На стороне IQMA настраивается тест T1 (twamp no auth no encryption with control protocol). Агент выступает инициатором.

На сетевом устройстве Cisco проводится конфигурация ответной стороны:

```
ip sla responder twamp
  timeout 301
ip sla responder
ip sla server twamp
  port 862
  timer inactivity 302
```

таймеры указывать не обязательно, приведены для примера.

## URL

URL - тест уровня приложения (L7 OSI). Приложение определяется в структуре URL. Для проведения тестирования на уровне приложения могут использоваться различные сетевые сервисы: FTP, HTTP, IMAP, RTSP, SMTP, TFTP. Актуальный список поддерживаемых схем находится в описании функциональных возможностей: "IP Quality Monitor (IQM). Реализованные функции." Для тестирования сервиса доменных имен реализован отдельный тест DNS.

При тестировании уровня приложений поддерживаются следующие возможности:

- использования протокола SSL (Secure Sockets Layer – уровень защищённых сокетов) на уровне представления модели OSI. Таким образом, поддерживаются защищенные протоколы HTTPS, FTPS и другие.
- Проведение серии взаимодействий в рамках одного транспортного соединения позволяет повлиять на механизм TCP-window и осуществить разгон TCP-сессии.
- Раскраска трафика в заданный класс сервиса,
- Авторизация доступа к сервису
- При тестировании HTTP сервиса поддерживаются: cookies, HTTP-redirects, режим HTTP persistent connection, также называемый HTTP keep-alive, или повторное использование соединений HTTP — использование одного TCP соединения для отправки и получения множественных HTTP запросов и ответов вместо открытия нового соединения для каждой пары запрос-ответ.

При конфигурации теста прикладного уровня следует корректно сформировать URL, который агент будет использовать для отправки запросов. Структура URL - стандартная:

```
<схема>:// [<логин>[:<пароль>]@]<хост>[:<порт>]/<URL-путь>[?<параметры>[#<якорь>]]
```

При тестировании HTTP-сервиса проще URL скопировать из адресной строки браузера. Для HTTP-протокола используется режим HTTP persistent connection. Постоянное HTTP-соединение, также называемые HTTP keep-alive или повторное использование соединений HTTP (англ. HTTP connection reuse) - использование одного TCP-соединения для отправки и получения многократных HTTP-запросов и ответов вместо открытия нового соединения для каждой пары запрос-ответ. Совместно с использованием HTTP keep-alive полезно воспользоваться параметром "Number of probes to ignore".

- "Number of probes to ignore" для "холостого прогона" нескольких запросов и, например, разгона TCP-соединения,
- "URL-test query interval (ms)" позволит делать паузу на заданное количество миллисекунд между последовательными запросами,
- "Cookie file" - позволит сохранить cookie в отдельном файле,
- "HTTP User-Agent" - определит тип пользовательского браузера,
- "Content download timeout" - задаст таймаут в секундах для загрузки данных по URL

Параметры Packet size (B) и Bandwidth for UDP tests (Kb/s) игнорируются. Пример конфигурации HTTP-теста приведен ниже в таблице и на экранной форме.

Test name *	iqmm_www.yandex.ru_URL_BE
Class (IP Precedence or DSCP)	BE
SLA policy profile	policy_basic_web
Service	L7 Internet
Provider	Default
SRC agent *	iqmm
DST agent *	www.yandex.ru
Source IP	NAT
DST agent IP *	www.yandex.ru
Test frequency (sec)	600
Number of probes	105
Number of probes to ignore	5
URL	https://www.yandex.ru/
URL-test query interval (ms)	100
Cookie file	/tmp/cookie-yandex.txt
HTTP User-Agent	Mozilla/5.0
Content download timeout	3
Test type	URL
Enabled	1
Packet size (B)	60
On demand test	0
Bandwidth for UDP tests (Kb/s)	64
Expected bandwidth for UDP tests (Kb/s)	64
External link	https://www.yandex.ru/

Пример взаимодействия с HTTP-сервером:

```
GET /R/A3cKIGNiM2Y1MDIzNWlYmJQ3YjE5ZGIyMGYxzWM0NWI3ZmVjEgQBIhEWGNwEIGH-
KgcIBBC_09NJKgcIAxDrmrhJMgoIBBC_09NJGIAKONaRiFhCIJxIgnQUrNtRixPv6itpYaAuh62t_OV1XO4WVOYpV-
eYSICDKA== HTTP/1.1
```

```
Host: su.ff.avast.com
Accept: */*
Content-Type: application/octet-stream
Pragma: no-cache
Connection: keep-alive

HTTP/1.1 200 OK
Content-Type: application/octet-stream
Pragma: no-cache
Cache-control: no-cache
Connection: keep-alive
Transfer-Encoding: chunked
```

**IQMM - [logged as admin] - TESTS CONFIGURATION:**  
**TESTS CONFIGURATION**

Deploy on:	<input checked="" type="checkbox"/> On agent	
	<input checked="" type="checkbox"/> On DB	
	<input checked="" type="checkbox"/> Drop statistics when deleting	
Test ID	iqmm_www.yandex.ru_URL_BE <a href="#">OnDemand</a>	
Test name *	iqmm_www.yandex.ru_URL_BE	
Class (IP Precedence or DSCP)	BE	1
SLA policy profile	policy_basic_web	
Service	L7 Internet	1
Provider	Default	
SRC agent *	iqmm	
DST agent *	www.yandex.ru	
Source IP	NAT	NAT
DST agent IP *	www.yandex.ru	
Test frequency (sec)	600	600
Number of probes	105	200
Number of probes to ignore	5	
URL	https://www.yandex.ru/	
URL-test query interval (ms)	100	
Cookie file	/tmp/cookie-yandex.txt	
HTTP User-Agent	Mozilla/5.0	
Content download timeout	3	
Test type	URL	U0
Enabled	1	1
Packet size (B)	60	60
On demand test	0	1
Bandwidth for UDP tests (Kb/s)	64	64
External link	https://www.yandex.ru/	

Рисунок 35 Форма конфигурации теста URL

### BW

BW - тест между двумя агентами IQMA для измерения доступной полосы пропускания. Аналогичен U0, но при инициировании тестового потока не используется ограничение по ООО «НетПроб»

скорости. Для проведения теста используется протокол UDP. Допустим для измерения скорости передачи физического канала.

*Не применим для каналов с механизмами обслуживания трафика, выделения полосы ниже физической скорости (policing, shaping, rate-limiting). Не рекомендуется запускать на регулярной основе. При необходимости регулярной проверки наличия емкости в контролируемом канале рекомендуется использовать тест U0.*

---

## GSS

GSS - интеллектуальное измерений доступной полосы пропускания. Серия тестов U0 в ходе которой методом золотого сечения (Golden Section Search) осуществляется подбор скорости передачи тестового трафика, удовлетворяющей критериям, заданным параметрами: LossLimit – предельный уровень потерь, Precision – точность измерения скорости в процентах, InOutMismatch – рассогласование в процентах скорости инициализации тестового потока и скорости приема

- LossLimit – количество потерь с заданной скоростью передачи не должно превышать этот параметр,
- Precision – точность измерения скорости в процентах. Рассчитывается как отношение разницы измеренной полосы в двух последних итерациях, к последнему измерению.
- InOutMismatch – рассогласование в процентах скорости инициализации тестового потока и скорости приема. Рассчитывается как отношение абсолютного значения разницы измеренной скорости на приеме и скорости отдачи к скорости отдачи.

Введено искусственное ограничение на длительность GSS-теста – 600 секунд. По истечении этого промежутка времени измерение останавливается вне зависимости от достижения заданных критериев.

Метод золотого сечения подробно описан в статье:

[http://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4\\_%D0%B7%D0%BE%D0%BB%D0%BE%D1%82%D0%BE%D0%B3%D0%BE\\_%D1%81%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D1%8F](http://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4_%D0%B7%D0%BE%D0%BB%D0%BE%D1%82%D0%BE%D0%B3%D0%BE_%D1%81%D0%B5%D1%87%D0%B5%D0%BD%D0%B8%D1%8F)

*Тест может не сходиться по объективным причинам, из-за неправильно подобранных параметров в конфигурации. Следует применять тест с осторожностью, в режиме on-demand, не рекомендуется запускать на регулярной основе. При необходимости регулярной проверки наличия емкости в контролируемом канале рекомендуется использовать тест U0.*

---

## LOCAL

LOCAL - аналог CMD-теста, который может выполняться локальным планировщиком СУ IQMM.

### CMD, конфигурация пакетного теста

CMD - пакетный тест. Функциональность интерпретатора тестов (пакетного теста) позволяет пользователю создавать любые тесты, реализовать произвольную логику тестирования любого сервиса, проводить любые измерения либо сбор рабочих параметров с сетевых устройств. Представляет собой внешнюю программу, выполняющую измерения и возвращающую измеренные значения параметров в форматированном виде агенту. Агент может выступать в качестве инициатора пакетного теста, который будет проводиться между другими сетевыми устройствами. После завершения теста, агент может получать результаты проведенных измерений. Сам агент в тестировании не участвует. Этот подход позволяет проводить самые разнообразные нестандартные тестирования, например, не встраивая агента в адресное пространство контролируемой сети, или Cisco/Juniper-SNMP/CLI-PING, или измерение MTU, и т.п.. Пакетные тесты могут формироваться пользователем системы, имеющим достаточную для этого квалификацию. Для удобства система поставляется с несколькими готовыми пакетными тестами и шаблоном для создания новых.

Простейший пакетный тест - это запуск любой unix утилиты, например, ping или traceroute. Для того, чтобы агент, воспринял проведенные измерения, необходима соответствующая обвязка с параметризацией вывода. Вывод утилиты ping агент может проанализировать самостоятельно, если его версия не превышает 3.11. Возможен запуск тестов без необходимой обвязки в режиме on-demand, в этом случае вывод внешней программы будет без изменений отображен в web-интерфейсе. Пример конфигурации пакетного теста с выполнением команды ping приведен в таблице ниже:

Test name *	CMD_PING
Class (IP Precedence or DSCP)	BE
Service	L4 Internet
Provider	Default
SRC agent *	iqmm
DST agent *	www.yandex.ru
Source IP	NAT
DST agent IP *	www.yandex.ru
Test frequency (sec)	600
Number of probes	200
DST agent type	A
Test type	CMD
Test command (for LOCAL or CMD tests)	/bin/ping
CMD options	-q&-c&10&-i&0.1&ya.ru
CMD timeout kill signal	(15) SIGTERM
Test timeout (sec)	3
Log CMD's STDOUT	1
Redirect CMD's STDERR to STDOUT	1
Enabled	1
On demand test	1

**IQMM - [logged as admin] - TESTS CONFIGURATION:**

**TESTS CONFIGURATION**

Deploy on:	<input checked="" type="checkbox"/> On agent <input checked="" type="checkbox"/> On DB <input checked="" type="checkbox"/> Drop statistics when deleting	
Test ID	CMD_PING ▾ <a href="#">OnDemand</a>	
Test name *	CMD_PING	
Class (IP Precedence or DSCP)	BE ▾	1
Service	L4 Internet ▾	1
Provider	Default ▾	
SRC agent *	iqmm ▾	
DST agent *	www.yandex.ru ▾	
Source IP	NAT	NAT
DST agent IP *	www.yandex.ru	
Test frequency (sec)	600	600
Number of probes	200	200
Test type	CMD ▾	U0
Test command (for LOCAL or CMD tests)	/bin/ping ▾ /bin/ping	
CMD options	-q&-c&10&-i&0.1&ya.ru	
CMD timeout kill signal	(15) SIGTERM ▾	
Test timeout (sec)	3	
Log CMD's STDOUT	1 ▾	
Redirect CMD's STDERR to STDOUT	1 ▾	
Enabled	1 ▾	
On demand test	1 ▾	

Рисунок 36 Форма конфигурации теста CMD

Опишем значения некоторых параметров:

- **Test type** = CMD, указывает агенту, что тест будет выполнять внешняя программа, определенная параметром Test command,
- **Test command** (for LOCAL or CMD tests) - путь к исполняемому файлу пакетного теста на агенте, который следует выполнить для проведения теста,
- **CMD options** - опции запуска программы, пробелы будут заменены на символы амперсанда '&' для корректного хранения в конфигурационном файле агента. При запуске программы, пробелы будут восстановлены. Передаются в качестве опций командной строки при запуске Test command пакетного теста. Обратите внимание, что опции

командной строки передаются «как есть», без дополнительной обработки. Если вы ожидаете от CMD-теста поведения системного интерпретатора командной строки unix (shell), например подстановку шаблонов файлов или перенаправление ввода и вывода, то вам следует создавать отдельный скрипт, реализующий эти возможности.

- **CMD timeout kill signal** -UNIX-сигнал для завершения команды по таймауту.
- **Test timeout (sec)** - Таймаут выполнения теста (с). Если задано, по истечении заданного количества секунд тест будет принудительно завершен.
- **Log CMD's STDOUT** - журналировать STDOUT программы Test command в лог-файл IQM-агента с приоритетом INFO (7).
- **Redirect CMD's STDERR to STDOUT** - перенаправить STDERR программы Test command на STDOUT. Требуется для журналирования STDERR вместе с STDOUT в лог-файл IQM-агента с приоритетом INFO (7).
- **Test-specific parameters** (в приведенном примере не используется) - специфические для теста параметры. Будут переданы на стандартный ввод STDIN команды Test command в формате:
  - par1=val1
  - par2=val2
  - ...
  - parN=valN
- **Send config to CMD's STDIN** (в приведенном примере не используется) - передать конфигурацию теста на STDIN команды. Если 1, то конфигурация теста будет передана на стандартный ввод команды Test command.

Параметры Log CMD's STDOUT и Redirect CMD's STDERR to STDOUT нужны для отладки пакетного теста. Они позволяют перенаправить все потоки вывода отлаживаемого теста в журнал с приоритетом INFO (7). В рабочем режиме, журналирование для пакетного теста должно быть выключено, приоритет журналирования для агента понижен до уровня WARN (5).

Пример журналирования вывода команды трассировки маршрута:

```
[Nov 23 20:54:23.033]: [140568321566464;Informational] Test CMD_TRACE_YA.RU started: NAT -
5.255.255.5 (www.yandex.ru)
[Nov 23 20:54:30.049]: [140568353036032;Informational] CMD OUT: traceroute to ya.ru
(213.180.193.3), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  103.261 ms  103.245 ms  104.932 ms
 2  10.134.0.1 (10.134.0.1)  107.168 ms  104.920 ms  107.172 ms
 3  10.254.244.17 (10.254.244.17)  107.146 ms  107.104 ms  108.963 ms
 4  mag9-cr01-be12.51.msk.stream-internet.net (212.188.1.5)  108.943 ms  108.892 ms  108.847 ms
 5  m9-cr04-be8.77.msk.stream-internet.net (212.188.54.213)  110.628 ms  110.633 ms  110.623 ms
 6  m9-cr03-ae13.77.msk.stream-internet.net (212.188.42.106)  106.848 ms  107.878 ms  107.862 ms
 7  yandex-m9.msk.stream-internet.net (195.34.36.30)  108.255 ms  106.778 ms  106.067 ms
 8  std-p2-be14.yndx.net (87.250.239.62)  108.192 ms  m9-p2-eth-trunk16.yndx.net (87.250.239.29)
114.604 ms  113.347 ms
 9  fol5-c2-ae4.yndx.net (87.250.239.109)  108.028 ms  107.444 ms  107.985 ms
10  * * *
11  www.yandex.ru (213.180.193.3)  110.241 ms  * *
12  www.yandex.ru (213.180.193.3)  112.150 ms  106.002 ms  107.169 ms

[Nov 23 20:54:30.050]: [140568321566464;Informational] Test CMD_TRACE_YA.RU finished
[Nov 23 20:54:30.050]: [140568321566464;Informational] Scheduler is unpaused
```

При отладке пакетных тестов рекомендуется выполнять их по требованию:

[Statistics --> OnDemand](#)





Для вывода неформатированных результатов предусмотрена кнопка **Stdout**.  
 Примеры выводов тестов по требованию для пакетных тестов приведены на рисунках ниже.

**IQMM - [logged as admin] - OnDemand tests:**

OnDemand tests

	<input type="button" value="Choose test"/>
	<input type="checkbox"/> OnDemand tests only
SRC agent	<input type="text"/>
DST agent	<input type="text" value="www.yandex.ru"/>
Tests	<input type="text" value="CMD_PING"/>
Pause scheduler (sec)	<input type="text"/>
Wait before run (sec)	<input type="text"/>
Num of iterations	<input type="text"/>
<input type="button" value="Run"/> <input type="button" value="Results"/> <input type="button" value="Stdout"/> <input type="button" value="Cancel"/>	

Details for test CMD_PING (Configure)	
Test name *	CMD_PING
Class (IP Precedence or DSCP)	BE
Service	L4 Internet
Provider	Default
SRC agent *	iqmm
DST agent *	www.yandex.ru
Source IP	NAT
DST agent IP *	www.yandex.ru
Test frequency (sec)	600
Number of probes	200
DST agent type	A
Test type	CMD
Test command (for LOCAL or CMD tests)	/bin/ping
CMD options	-q&-c&10&-i&0.1&ya.ru
CMD timeout kill signal	(15) SIGTERM
Test timeout (sec)	3
Log CMD's STDOUT	1
Redirect CMD's STDERR to STDOUT	1
Enabled	1
Packet size (B)	60
On demand test	1
Bandwidth for UDP tests (Kb/s)	64
Expected bandwidth for UDP tests (Kb/s)	64
Creation date	2016-11-23 17:50:14

1 rows

```

PING ya.ru (93.158.134.3) 56(84) bytes of data.

--- ya.ru ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 1145ms
rtt min/avg/max/mdev = 105.431/106.844/108.708/0.946 ms, pipe 2
                    
```

ID	DD	SZone	DZone	DType	TestType	TID	TStart	Class	NumProbes	SDLost	SDLostPercent	DSLost	DSLostPercent	MaxRtt	AvgRtt	MaxRtt	SDJitter	DSJitter	ServiceCode	SDBytes	DSBytes	SDBW	DSBW	
1	iqmm	www.yandex.ru	Слованы	Слованы	A	CMD	CMD_PING	2016-11-23 18:02:32	0	10	0	0	0	0	104	106	110	2	0	0	840	840	3957	3957

1 rows

Рисунок 37 Форматированный отчет и вывод STDOUT для пакетного теста с использованием утилиты Ping

ООО «НетПроб»

69

**IQMM - [logged as admin] - OnDemand tests:**

OnDemand tests

	Choose test
	<input type="checkbox"/> OnDemand tests only
<b>SRC agent</b>	<input type="text"/>
<b>DST agent</b>	<input type="text" value="www.yandex.ru"/>
<b>Tests</b>	<input type="text" value="CMD_TRACE_YA.RU"/>
<b>Pause scheduler (sec)</b>	<input type="text"/>
<b>Wait before run (sec)</b>	<input type="text"/>
<b>Num of iterations</b>	<input type="text"/>
<input type="button" value="Run"/> <input type="button" value="Results"/> <input type="button" value="Stdout"/> <input type="button" value="Cancel"/>	

Details for test CMD_TRACE_YA.RU (Configure)	
Test name *	CMD_TRACE_YA.RU
Class (IP Precedence or DSCP)	BE
Service	L4 Internet
Provider	Default
SRC agent *	iqmm
DST agent *	www.yandex.ru
Source IP	NAT
DST agent IP *	www.yandex.ru
Test frequency (sec)	600
Number of probes	200
DST agent type	A
Test type	CMD
Test command (for LOCAL or CMD tests)	/bin/traceroute
CMD options	ya.ru
CMD timeout kill signal	(15) SIGTERM
Test timeout (sec)	10
Log CMD's STDOUT	1
Redirect CMD's STDERR to STDOUT	1
Enabled	1
Packet size (B)	60
On demand test	1
Bandwidth for UDP tests (Kb/s)	64
Expected bandwidth for UDP tests (Kb/s)	64
Creation date	2016-11-23 20:53:55

1 rows

```

traceroute to ya.ru (213.180.193.3), 30 hops max, 60 byte packets
 1 192.168.0.1 (192.168.0.1) 103.261 ms 103.245 ms 104.932 ms
 2 10.134.0.1 (10.134.0.1) 107.168 ms 104.920 ms 107.172 ms
 3 10.254.244.17 (10.254.244.17) 107.146 ms 107.104 ms 108.963 ms
 4 mag9-cr01-be12.51.msk.stream-internet.net (212.188.1.5) 108.943 ms 108.892 ms 108.847 ms
 5 m9-cr04-be8.77.msk.stream-internet.net (212.188.54.213) 110.628 ms 110.633 ms 110.623 ms
 6 m9-cr03-ae13.77.msk.stream-internet.net (212.188.42.106) 106.848 ms 107.878 ms 107.862 ms
 7 yandex-m9.msk.stream-internet.net (195.34.36.30) 108.255 ms 106.778 ms 106.067 ms
 8 std-p2-be14.yndx.net (87.250.239.62) 108.192 ms m9-p2-eth-trunk16.yndx.net (87.250.239.29) 114.604 ms 113.347 ms
 9 fo15-c2-ae4.yndx.net (87.250.239.109) 108.028 ms 107.444 ms 107.985 ms
10 * * *
11 www.yandex.ru (213.180.193.3) 110.241 ms * *
12 www.yandex.ru (213.180.193.3) 112.150 ms 106.002 ms 107.169 ms
                    
```

Test CMD\_TRACE\_YA.RU complete

Рисунок 38 Варианты отчетов выполненного пакетного теста с использованием утилиты traceroute

### CMD, взаимодействие агента с пакетным тестом

При выполнении пакетного теста агент создает копию процесса вызовом `fork(2)`, при необходимости (определяется параметром "Redirect CMD's STDERR to STDOUT"), направляет поток ошибок в стандартный поток вывода (`STDERR>STDOUT`). В созданной копии процесса выполняется через `execve(2)` код программы, указанный в параметре `CMD`. В качестве опций командной строки при запуске `CMD` передаются значения "CMD options" (символы амперсанда `&` предварительно заменяются на пробелы). Дополнительной обработки, характерной для shell агентом не производится. После запуска `CMD` в поток стандартного ввода программы передаются значения параметра "Test-specific parameters", если он задан. Следом, на ввод программы передается полная конфигурация теста, если это требуется параметром "Send config to CMD's STDIN". В

процессе выполнения перехватывается стандартный вывод (STDOUT) программы вместе с потоком ошибок (STDERR), если это требуется.

### Анализ ping "на лету":

В случае если команда CMD - ping, а вывод содержит строку "ping statistics", характерный для ОС Linux, а версия агента не превышает 3.11, то вывод будет проинтерпретирован как вывод команды ping.

```
--- ya.ru ping statistics ---
10 packets transmitted, 9 received, 10% packet loss, time 1007ms
rtt min/avg/max/mdev = 5.384/5.948/6.539/0.323 ms
```

Будут заполнены параметры:

Параметр агента	Вывод ping
NumProbes	packets transmitted
SDLost	transmitted - received
SDLostPercent	lost * 100.0 / transmitted
DSLost	0
DSLostPercent	0.0
MinRtt	rtt min
AvgRtt	rtt avg
MaxRtt	rtt max
SDJitter	mdev

В остальных случаях, вывод программы будет проинтерпретирован по описанным далее правилам. Интерпретируются строки в формате 'variable=value' или 'variable value', интерпретируются только определенные параметры variable:

Параметр агента	Параметр value вывода программы	тип
NumProbes	total_count	uint
SDLost	total_count - success_count	uint
SDLostPercent	SDLost * 100.0 / total_count	double
DSBytes	min_bytes	u_int64
SDBytes	max_bytes	u_int64
DSBW	min_speed	u_int64
SDBW	max_speed	u_int64
MinRtt	min_delay	int
AvgRtt	avg_delay	int
MaxRtt	max_delay	int
SDJitter	jitter	uint

Агент так же воспринимает параметры, имена которых соответствуют стандартному внутреннему именованию:

Параметр агента	Параметр value вывода программы	тип
SID	SID	string
DID	DID	string
SZone	SZone	int
DZone	DZone	int
DType	DType	string
TStart	TStart	uint
Class	Class	uint

Параметр агента	Параметр value вывода программы	тип
NumProbes	NumProbes	uint
SDLost	SDLost	uint
SDLostPercent	SDLostPercent	double
DSLost	DSLost	uint
DSLostPercent	DSLostPercent	double
SDRemarked	SDRemarked	uint
SDRemarkedPercent	SDRemarkedPercent	double
DSRemarked	DSRemarked	uint
DSRemarkedPercent	DSRemarkedPercent	double
MinRtt	MinRtt	int
AvgRtt	AvgRtt	int
MaxRtt	MaxRtt	int
SDJitter	SDJitter	uint
DSJitter	DSJitter	uint
ServiceCode	ServiceCode	uint
SDBytes	SDBytes	u_int64
DSBytes	DSBytes	u_int64
SDBW	SDBW	u_int64
DSBW	DSBW	u_int64
SDMinDelay	SDMinDelay	int
SDAvgDelay	SDAvgDelay	int
SDMaxDelay	SDMaxDelay	int
DSMinDelay	DSMinDelay	int
DSAvgDelay	DSAvgDelay	int
DSMaxDelay	DSMaxDelay	int
SDOOS	SDOOS	uint
SDOOSPercent	SDOOSPercent	double
DSOOS	DSOOS	uint
DSOOSPercent	DSOOSPercent	double
SDDup	SDDup	uint
SDDupPercent	SDDupPercent	double
DSDup	DSDup	uint
DSDupPercent	DSDupPercent	double

Порядок, в котором агент запишет параметры о выполнении теста описан в параметре @gCDRColNames в конфигурационном файле системы управления IQMM /home/iqm/iqmm/iqmm-cfg.pl:

```
@gCDRColNames = qw[ SID DID SZone DZone DType TestType TID TStart Class NumProbes
SDLost SDLostPercent DSLost DSLostPercent
MinRtt AvgRtt MaxRtt SDJitter DSJitter
ServiceCode SDBytes DSBytes SDBW DSBW
SDRemarked SDRemarkedPercent DSRemarked DSRemarkedPercent
SDMinDelay SDAvgDelay SDMaxDelay DSMinDelay DSAvgDelay DSMaxDelay ];
```

Описание параметров приводится там же в описании структуры данных %gTFN\_IQM\_RAW:

```
'params' =>
{
  '_DEFAULT' => [qw/LostPercent Jitter RttAvg/],
  '_NAMES' => [qw/Bytes BW LostPercent RemarkedPercent Jitter RttMax RttAvg
RttMin MaxDelay AvgDelay MinDelay SvcCode OOSPercent BWPercent/],
  'DESCR' =>
  {
```

```

'BW'          => _("Bandwidth"). " (bps)",
'Bytes'       => _("Data transmitted"). " (Bytes)",
'LostPercent' => _("Packet loss"). " (%)",
'RemarkedPercent'=> _("Remarked packets"). " (%)",
'RttMax'      => _("Maximum round-trip time")." (ms)",
'RttAvg'      => _("Average round-trip time")." (ms)",
'RttMin'      => _("Minimum round-trip time")." (ms)",

'MaxDelay'    => _("Maximum delay time")." (ms)",
'AvgDelay'    => _("Average delay time")." (ms)",
'MinDelay'    => _("Minimum delay time")." (ms)",
'SvcCode'     => _("Service code"),
'OOSPercent'  => _("Out-of-sequence"). " (%)",
'BWPercent'   => _("Bandwidth load"). " (%)",

'Jitter'      => _("Jitter")." (ms)"
},
'BW'          => 'SDBW, -DSBW',
# 'BW'         => 'SDBW',
# 'Bytes'      => 'SDBytes, -DSBytes',
# 'Lost'       => 'SDLost, DSLost',
'LostPercent' => 'SDLostPercent, -DSLostPercent',
'RemarkedPercent'=> 'SDRemarkedPercent, -DSRemarkedPercent',
'RttMax'      => 'MaxRtt',
'RttAvg'      => 'AvgRtt',
'RttMin'      => 'MinRtt',
'SvcCode'     => 'ServiceCode',

'MaxDelay'    => 'SDMaxDelay, -DSMaxDelay',
'AvgDelay'    => 'SDAvgDelay, -DSAvgDelay',
'MinDelay'    => 'SDMinDelay, -DSMinDelay',
'BWPercent'   => 'SDBWPercent, -DSBWPercent',
'OOSPercent'  => 'SDOOSPercent, -DSOOSPercent',

'Jitter'      => 'SDJitter, -DSJitter'
},

```

Разумеется, передаваемые параметры могут иметь произвольный физический смысл, вплоть до фазы Луны. Описание говорит о том, как и в каких полях эти измерения будут представлены.

После того, как агент запишет полученные от программы результаты в файл, они будут переданы в систему управления IQMM и записаны в базу данных. Далее система управления будет оперировать с полученными цифрами, как если бы измерения были проведены самим агентом, а не внешней программой. Параметры могут быть представлены в различных отчетах, на графиках и таблицах, могут быть проанализированы политиками контроля и вызваны сигналы тревоги, при их неудовлетворительных значениях.

### CMD, пример пакетного теста

Рассмотрим учебный скрипт, который записывает свои рабочие параметры в файл а в качестве результатов выдает значения тригонометрических функций в зависимости от времени:

```

#!/bin/bash

LANG=C
lf=/tmp/cmd-tst.log
function sin(){ echo "scale=10; 50 + 50*s($1*a(1)/45);" | bc -l; }
function cos(){ echo "scale=10; 50 + 50*c($1*a(1)/45);" | bc -l; }

echo > $lf
date >> $lf
echo $0 - $@ >> $lf
echo Running $0 - $@ ...

echo >> $lf

```

```
while read -t 1 -r line
do
    echo $line >> $1f
done

ts=`date +%s`
s=`sin $ts`
c=`cos $ts`
echo NumProbes 100
echo SDLost `printf "%.0f" $s`
echo SDLostPercent `printf "%.0f" $s`
echo DSLost `printf "%.0f" $c`
echo DSLostPercent `printf "%.0f" $c`
echo SDJitter `printf "%.0f" $s`
echo DSJitter `printf "%.0f" $s`
echo MinRtt $(printf "%.0f" $s)
echo AvgRtt $((2 * $(printf "%.0f" $s) ))
echo MaxRtt $((4 * $(printf "%.0f" $s) ))
```

### Конфигурация теста в базе с

Test name *	CMD_TST
Service	L4 Internet
Provider	Default
SRC agent *	iqmm
DST agent *	www.yandex.ru
Source IP	NAT
DST agent IP *	www.yandex.ru
Test frequency (sec)	10
Number of probes	200
Test type	CMD
Test command (for LOCAL or CMD tests)	/root/tst.sh
CMD options	-q&-c&10&-i&0.1&ya.ru
CMD timeout kill signal	(15) SIGTERM
Test timeout (sec)	3
Test-specific parameters	par1=val1&par2=val2
Send config to CMD's STDIN	1
Log CMD's STDOUT	1
Redirect CMD's STDERR to STDOUT	1
Enabled	1
On demand test	0

В результате выполнения данного теста в файле /tmp/cmd-tst.log будет запись с опциями запуска и принятыми в потоке стандартного ввода дополнительными параметрами и конфигурацией теста:

```
Thu Nov 24 23:15:11 MSK 2016
/root/tst.sh -q -c 10 -i 0.1 ya.ru

par1=val1
par2=val2
# test CMD_TST
test CMD_TST set OpFreq 10
test CMD_TST set NumProbes 200
test CMD_TST set DID www.yandex.ru
test CMD_TST set DIP www.yandex.ru
test CMD_TST set DZone 1
test CMD_TST set DType A
test CMD_TST set TestType CMD
```



В лог-файле окажется вывод программы, как того требуют рабочие параметры теста:

```
[Nov 24 23:23:55.182]: [140186270803712;Informational] CMD OUT: Running /root/tst.sh -q -c 10 -i
0.1 ya.ru ...
NumProbes 100
SDLost 45
SDLostPercent 45
DSLost 100
DSLostPercent 100
SDJitter 45
DSJitter 45
MinRtt 45
AvgRtt 90
MaxRtt 180

[Nov 24 23:23:55.182]: [140186312763136;Informational] Test CMD_TST finished
```

### CMD, предустановленные пакетные тесты

Система управления поставляется с набором заранее приготовленных пакетных тестов. Для использования какого-нибудь из этих тестов необходимо его переместить на агента, на котором он будет запускаться. Проверить работоспособность теста запуском с командной строки. Тесты отлажены, однако, могут потребовать установки дополнительных библиотек или другого дополнительного ПО на агента. Тесты размещены в директории /home/iqm/iqmm/scripts/.

Файл	Функция
cmd_check_avail.sh	Тест проверки доступности заданной страницы. Подробности см. в коде.
cmd_cisco_snmp_ping.pl	Реализует функции Cisco SNMP ping. Проводит тестирование доступности CE-маршрутизатора с Cisco-PE в заданном VRF. Потребуется SNMP community с правами на запись. Подробности см. в коде.
cmd_cisco_telnet_ping.pl	Реализует функции Cisco CLI ping через telnet-сессию. Проводит тестирование доступности CE-маршрутизатора с Cisco-PE в заданном VRF. Потребуется login на Cisco-PE-маршрутизатор. Для получения расширенных результатов потребуется enable. Подробности см. в коде.
cmd_mtu_chk.pl	Измерение MTU. Тест проводит измерения максимального размера пакета, пропускаемого сетью. Подробности см. в коде.
cmd_mtu_chk.sh	Измерение MTU. Тест проводит измерения максимального размера пакета, пропускаемого сетью. Подробности см. в коде.
cmd_srv_info.sh	Простой тест для использования в режиме on-demand, выдает информацию об аппаратной платформе агента:

```
#!/bin/bash
echo -e "\n===== NTP"
ntpq -p
echo -e "\n===== DISK"
df -h
echo -e "\n===== RAM"
free
echo -e "\n===== NET"
```



Файл	Функция
cmd_test_template.pl	<pre>/sbin/ifconfig echo -e "\n===== ROUTE" netstat -rn echo -e "\n===== LISTEN PORTS" netstat -lntup echo -e "\n===== PCI" lspci echo -e "\n===== HARDWARE" dmidecode</pre> Шаблон пакетного теста, которым можно воспользоваться для написания собственного теста на языке perl.
cmd_tst.sh	Тест рассмотренный в данной документации

### **MCAST\_VIDEO, мониторинг IPTV**

MCAST\_VIDEO - тест для измерения MDI в multicast IP TV.

Система IQM предлагает решение для мониторинга качественных параметров услуги IPTV для операторов. Решение встраивается в единую систему управления IQMM. Решаются задачи контроля качества поставщиков IPTV и контроля работы Head End.

*Поставляется по отдельному заказу либо как дополнительный модуль к основной системе мониторинга, либо как самостоятельное решение. Подробная информация по настройке мониторинга IPTV находится в документе "IQM: запуск мониторинга IP TV".*

---

Под задачи мониторинга IP TV реализован дополнительный специализированный комплекс:

- высокопроизводительная аппаратная платформа агента,
- специальное программное обеспечение для агента,
- модуль системы управления IQMM для управления IPTV-агентами и обработки данных мониторинга.

IPTV-агент осуществляет подписку на мультикаст-видео, принимает и анализирует пакеты. Результаты измерений передаются в систему управления IQMM, где они могут быть проанализированы политиками контроля и представлены операторам наряду с другими измерениями. Мониторинг может осуществляться на уровне главного и регионального узлов.

Мониторинг IPTV осуществляется на транспортном уровне модели OSI. Измеряются следующие параметры:

- Наличие/отсутствие сигнала: Stream availability

- Определение битрейта потока (Mbps):
  - CBR. Constant bitrate. Скорость потока (Mbps). По RFC 4445 принимается постоянной.
  - VBR. Variable bitrate. Текущая скорость потока в (Mbps). В реальности (в отличие от RFC 4445) скорость меняется, параметр фиксирует текущую скорость.
- Измерение MDI согласно RFC 4445 для постоянного битрейта потока, для переменного битрейта потока, согласно методике Bridgetech
  - DF. Delay Factor (по RFC 4445). Фактор задержки в миллисекундах.
  - MLR. Media Loss Rate (по RFC 4445). Кол-во потерянных пакетов за секунду.
  - IAT. Inter-packet Arrival Time (в терминах Bridgetech) - наибольшее время прибытия пакета за время измерения. В миллисекундах.

Рисунок 40 и Рисунок 41 демонстрирует экранные формы некоторых отчетов и панели мониторинга IPTV.

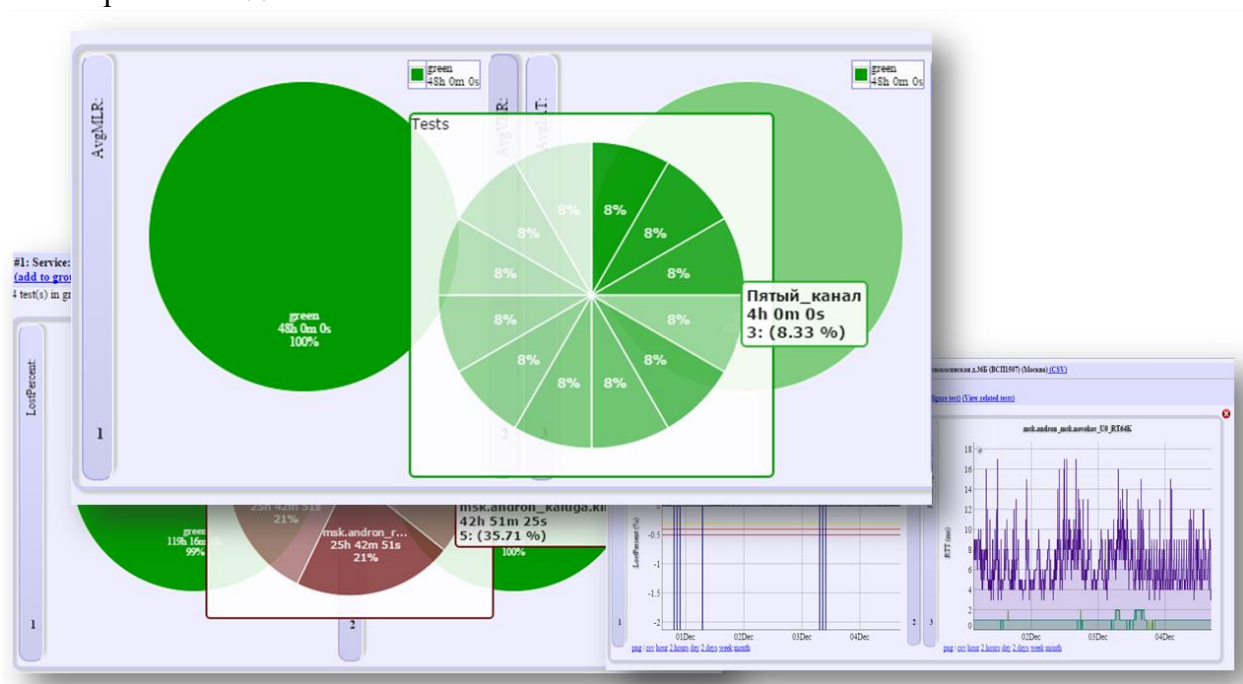


Рисунок 40 Некоторые отчеты по результатам мониторинга IPTV

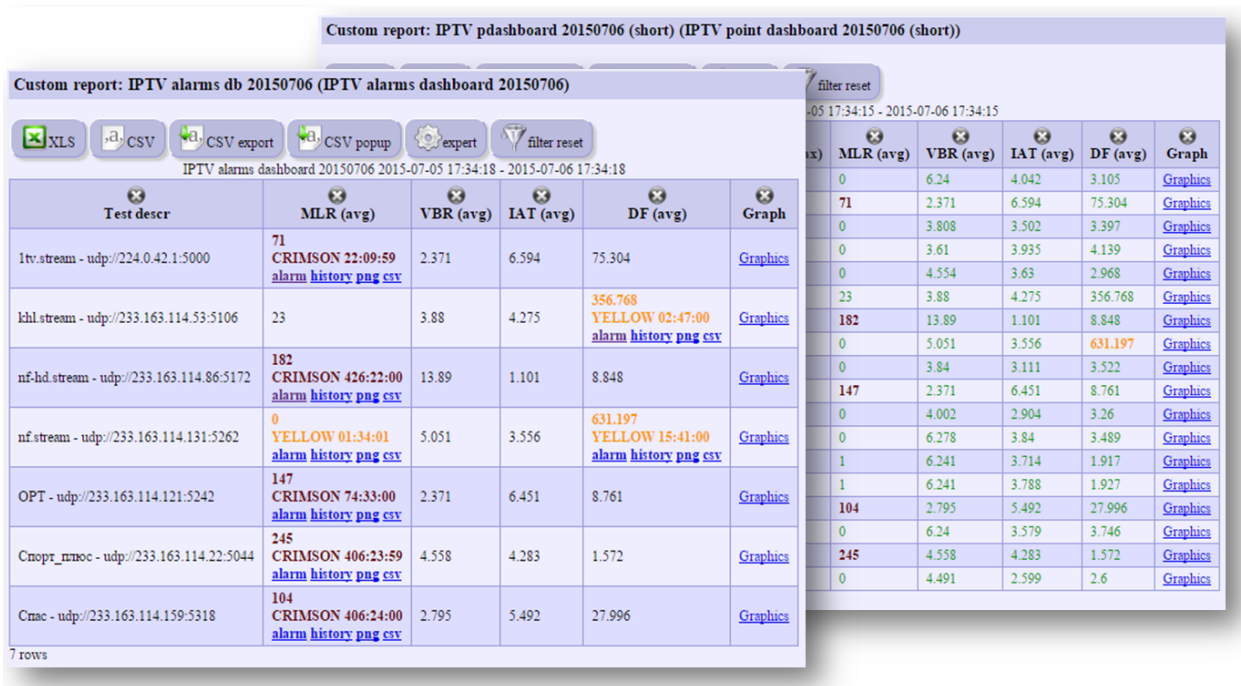


Рисунок 41 Панели мониторинга IPTV

## DNS

DNS - измерение характеристик сетевого сервиса доменных имен. Тест инициируется агентом IQM, проводится с заданным в конфигурации сервисом доменных имен. Для создания теста необходимо завести в списке агентов тестируемый сервис с типом WEB. Заведенному сервису можно определить несколько IP-адресов для основного и вторичного. В форме конфигурации тестов указать в DST agent \* - тестируемый сервис DNS, в DST agent IP \* - адрес тестируемого сервера DNS. Тип теста - DNS. Из имени, или IP-адреса, который необходимо запросить сервер DNS формируется URL, в качестве схемы указывается dns.

**dns://[type[:class]]@fqdn**  
**dns://ptr[:class]@ip**

- class - необязательное поле, класс ресурсной записи - IN (сети TCP/IP). Другие значения устарели и не используются.
- type - необязательное поле, тип запрашиваемой ресурсной записи. Наиболее важные типы DNS-записей:

type	Значение
A	(address record) или запись адреса связывает имя хоста с адресом протокола IPv4
NS	(name server) указывает на DNS-сервер для данного домена
CNAME	(canonical name record) или каноническая запись имени (псевдоним) используется для перенаправления на другое имя
SOA	(Start of Authority) или начальная запись зоны указывает, на каком сервере хранится эталонная информация о данном домене, содержит контактную информацию лица, ответственного за данную зону, тайминги (параметры

<b>type</b>	<b>Значение</b>
PTR	времени) кэширования зонной информации и взаимодействия DNS-серверов (pointer) или запись указателя связывает IP-адрес хоста с его каноническим именем. Запрос в домене in-addr.arpa на IP-адрес хоста в reverse-форме вернёт имя (FQDN) данного хоста
MX	(mail exchange) или почтовый обменник указывает сервер(ы) обмена почтой для данного домена
AAAA	(IPv6 address record) связывает имя хоста с адресом протокола IPv6
SRV	(server selection) указывает на серверы для сервисов

*Подробнее о типах ресурсных записей DNS см.*

*[https://ru.wikipedia.org/wiki/%D0%A2%D0%B8%D0%BF%D1%8B\\_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D0%BD%D1%8B%D1%85\\_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D0%B5%D0%B9\\_DNS](https://ru.wikipedia.org/wiki/%D0%A2%D0%B8%D0%BF%D1%8B_%D1%80%D0%B5%D1%81%D1%83%D1%80%D1%81%D0%BD%D1%8B%D1%85_%D0%B7%D0%B0%D0%BF%D0%B8%D1%81%D0%B5%D0%B9_DNS)*

Пример теста для измерение характеристик сетевого сервиса доменных имен приведен ниже:

Test name *	iqmm_google-public-dns_DNS_BE64K
Class (IP Precedence or DSCP)	BE
Service	L4 Internet
Provider	Default
SRC agent *	iqmm
DST agent *	google-public-dns
Source IP	NAT
DST agent IP *	8.8.8.8
Test frequency (sec)	60
Number of probes	100
URL	dns://a:in@www.net-probe.ru
DST agent type	A
Test type	DNS
Enabled	1
Packet size (B)	60
On demand test	0
Bandwidth for UDP tests (Kb/s)	64

**IQMM - [logged as admin] - TESTS CONFIGURATION:**  
**TESTS CONFIGURATION**

Deploy on:	<input checked="" type="checkbox"/> On agent <input checked="" type="checkbox"/> On DB <input checked="" type="checkbox"/> Drop statistics when deleting	
Test ID	iqmm_google-public-dns_DNS_BE64K <a href="#">OnDemand</a>	
Test name *	iqmm_google-public-dns_DNS_BE64K	
Class (IP Precedence or DSCP)	BE	1
Service	L4 Internet	1
Provider	Default	
SRC agent *	iqmm	
DST agent *	google-public-dns	
Source IP	NAT	NAT
DST agent IP *	(google-public-dns) google-public-dns-a.google.com 8.8.8.8	
Test frequency (sec)	60	600
Number of probes	100	200
URL	dns://a.in@www.net-probe.ru	
Test type	DNS	U0
Enabled	1	1
Packet size (B)	60	60
On demand test	0	1
Bandwidth for UDP tests (Kb/s)	64	64

Рисунок 42 Форма конфигурации теста сервиса доменных имен (DNS)

### PPPOE

PPPOE - измерение характеристик работы PPPoE - сессии.  
 Поддержка PPPOE тестирования реализуется по спец-запросу.

### Измеряемые характеристики

При проведении измерений тестом из состава тестов, доступных на стандартном агенте на уровне L2-L3 состав измеряемых параметров может быть разным, одинаковые параметры имеют одинаковое обозначение.

1. Bytes SD, Bytes DS. Объем данных переданных в направлении от инициатора к сопряженному агенту и в обратном направлении.
2. BW SD, BW DS. Скорость передачи в направлении от инициатора к сопряженному агенту и в обратном направлении. Рассчитывается как скорость, с которой был осуществлен прием тестовых пакетов.

3. **LostPercent SD, LostPercent DS.** Процент потерянных пакетов. Измерения производятся в каждом направлении.
4. **RttMax, RttAvg, RttMin.** Круговые задержки. Круговые задержки представляют собой сумму односторонних задержек. Фиксируются минимальные, средние и максимальные за сессию значения.
5. **MaxDelay SD, MaxDelay DS, AvgDelay SD, AvgDelay DS, MinDelay SD, MinDelay DS.** Односторонние задержки. Проводятся измерения в каждом направлении передачи, фиксируются минимальные, средние и максимальные за сессию значения.
6. **Jitter SD, Jitter DS.** Вариация задержки. Измерения производятся в каждом направлении.
7. **RemarkedPercent SD, RemarkedPercent DS.** Процент пакетов доставленных с измененным классом сервиса.
8. **OOSPercent SD, OOSPercent DS.** Процент пакетов доставленных с нарушением порядка (Out-of-order, Out-of-sequence).

На уровне L7 измеряемые параметры имеют те же обозначения, но иной смысл:

1. **Bytes SD, Bytes DS.** Bytes SD - объем данных (максимальный за тестовую сессию), полученных от сетевого приложения. Bytes DS - объем данных (минимальный за тестовую сессию), полученных от сетевого приложения.
2. **BW SD, BW DS.** Скорость получения данных с сетевого сервиса. BW SD максимальная скорость за тестовую сессию, BW DS - минимальная.
3. **LostPercent SD.** Процент отказов в обслуживании со стороны сетевого сервиса. Причина отказа может быть как на уровне транспортной сети, так и на уровне приложения (например 400 - ошибки HTTP). LostPercent DS - не используется.
4. **RttMax, RttAvg, RttMin.** Время получения данных от сетевого сервиса (минимальное, среднее, максимальное в серии измерений), которое состоит из:
  - 4.1. Время получения сетевого адреса из DNS,
  - 4.2. Время установления соединения с сервисом,
  - 4.3. Время получения запрошенных данных от сервиса,
5. **Jitter SD.** Вариация времени реакции сетевого сервиса на серии измерений, характеризующая стабильность отклика. Jitter DS- не используется.
6. **Service Code** - для некоторых приложений имеет индивидуальную интерпретацию, обозначающую статус завершения связи с приложением.
7. Другие обозначения не используются.

Параметры IPTV описаны отдельно (см. MCAST\_VIDEO, мониторинг IPTV).

Изменяемые параметры для тестов сетевого/транспортного уровня:

<b>Тест</b>	<b>U0</b>	<b>B</b>	<b>I0</b>	<b>J0</b>	<b>J1</b>	<b>C</b>	<b>C1</b>	<b>C2</b>	<b>C3</b>	<b>TW</b>	<b>T1</b>
	<b>GS</b>	<b>W</b>	<b>U7</b>			<b>0</b>					
	<b>S</b>										
<b>Сопряженный агент</b>	iqm	iq	any	uq	Juniper	cx	Cisc	cxr	Cisc	TWAM	TWAM
		m		r	r	r	o		o	P	P

Тест	U0 GS S	B W	I0 U7	J0	J1	C 0	C1	C2	C3	TW	T1
Параметр/ Время	мс	мс	мс	мс	мс	мс	мс	мс	мс	мс	мс
					uqr		sxr		sxr		
								мк с	мкс		
Bytes SD	Да	Да	Нет	Да	Нет	Да	Нет	Да	Нет	Нет	Нет
Bytes DS	Да	Да	Да	Да	Да	Да	Нет	Да	Нет	Нет	Нет
BW SD	Да	Да	Нет	Да	Нет	Да	Нет	Да	Нет	Нет	Нет
BW DS	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да
LostPercent SD	Да	Нет	Нет	Да	Нет	Да	Да	Да	Да	Нет	Нет
LostPercent DS	Да	Нет	Да	Да	Да	Да	Да	Да	Да	Да	Да
RemarkedPercent SD	Да	Да	Нет	Да	Нет	Да	Нет	Да	Нет	Нет	Нет
RemarkedPercent DS	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да	Да
Jitter SD	Да	Нет	Нет	Да	Да	Да	Да	Да	Да	Да	Да
Jitter DS	Да	Нет	Да	Да	Да	Да	Да	Да	Да	Да	Да
RttMax	Да	Нет	Да	Да	Да	Да	Да	Да	Да	Да	Да
RttAvg	Да	Нет	Да	Да	Да	Да	Да	Да	Да	Да	Да
RttMin	Да	Нет	Да	Да	Да	Да	Да	Да	Да	Да	Да
MaxDelay SD	Да	Нет	Нет	Да	Да	Да	Да	Да	Да	Нет	Нет
MaxDelay DS	Да	Нет	Нет	Да	Да	Да	Да	Да	Да	Нет	Нет
AvgDelay SD	Да	Нет	Нет	Да	Да	Да	Да	Да	Да	Нет	Нет
AvgDelay DS	Да	Нет	Нет	Да	Да	Да	Да	Да	Да	Нет	Нет
MinDelay SD	Да	Нет	Нет	Да	Да	Да	Да	Да	Да	Нет	Нет
MinDelay DS	Да	Нет	Нет	Да	Да	Да	Да	Да	Да	Нет	Нет
OOSPercent SD	Да	Нет	Нет	Да	Нет	Да	Нет	Да	Нет	Нет	Нет
OOSPercent DS	Да	Нет	Да	Да	Нет	Да	Да	Да	Да	Да	Да

## Управление признаками

Для удобства работы с большим объемом данных в системе предусмотрена возможность их классификации с использованием различных признаков. Оператор, формирующий запрос на получение отчета, может осуществить фильтрацию запрашиваемых данных с привязкой к различным признакам: клиентам, провайдерам, сервисам, архитектурным уровням, зональным признакам, агентам тестирования, производимым тестам, классам сервиса, измеряемым параметрам. В зависимости от типов отчетов возможно дополнение этого списка условиями фильтрации, специфическими для получаемого отчета. Перечень признаков фильтрации или группировки отчетов расширяется.

## Управление списком сервисов

Признак сервиса присутствует в параметрах теста. Под сервисом понимается телекоммуникационная услуга, для которой осуществляется измерение и контроль качественных характеристик. Это абстрактный признак, может использоваться в любых других подходах при классификации. По умолчанию, после установки в системе управления IQMM уже определен первичный набор сервисов.

service ID	service name	Description
7	L2 VPN	L2 VPN
6	L3 Access	L3 Access
4	L3 Core	L3 Core
5	L3 Distribution	L3 Distribution
3	L3 IP VPN	L3 IP VPN
1	L4 Internet	L4 Internet
2	L7 Internet	L7 Internet
8	MCAST Video	MCAST Video

Для изменения списка сервисов служит форма SERVICES CONFIGURATION. Форма вызывается через пункт меню:

*Configuration --> SLA Policy --> Services*

---



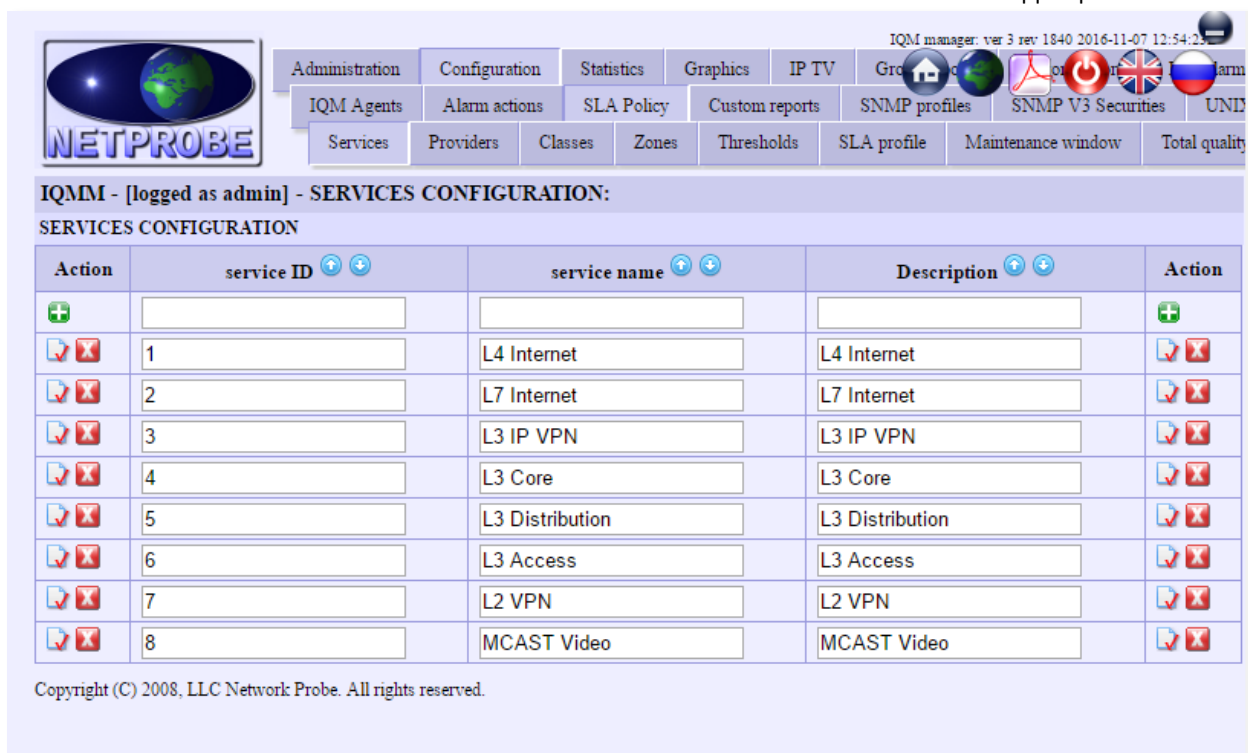





Рисунок 43 Форма конфигурации сервисов

Значения полей приведены в таблице ниже:

Поле	Значение
Service ID	Идентификатор, не редактируемое поле
Service Name	Короткое имя сервиса, под которым он будет отображаться в формах настройки тестов
Description	Описание
Action	Допустимые действия:  - добавить новую запись  - внести изменения в текущую запись  - удалить текущую запись

### Управление списком провайдеров

Признак провайдера присутствует в параметрах теста. Под провайдером понимается поставщик телекоммуникационных услуг и каналов связи, для которых осуществляется измерение и контроль качественных характеристик. Это абстрактный признак, может использоваться в любых других подходах при классификации. По умолчанию, после установки в системе управления IQMM уже определен один признак в таблице провайдеров: Default. Он будет назначаться всем тестам по умолчанию. Для изменения списка провайдеров служит форма PROVIDERS CONFIGURATION. Форма вызывается через пункт меню:

*Configuration --> SLA Policy --> Providers*



Рисунок 44 Форма конфигурации провайдеров

Значения полей приведены в таблице ниже:

Поле	Значение
Provider ID	Идентификатор, не редактируемое поле
Provider Name	Короткое имя провайдера, под которым он будет отображаться в формах настройки тестов
Description	Описание
Action	Допустимые действия: - добавить новую запись - внести изменения в текущую запись - удалить текущую запись

### Управление именами классов сервиса

В случае если названия классов сервиса отличаются от предварительно определенных, или предопределенные классы не загружались – их можно определить при помощи формы CLASSES CONFIGURATION. Форма вызывается через пункт меню:

*Configuration --> SLA Policy --> Classes*

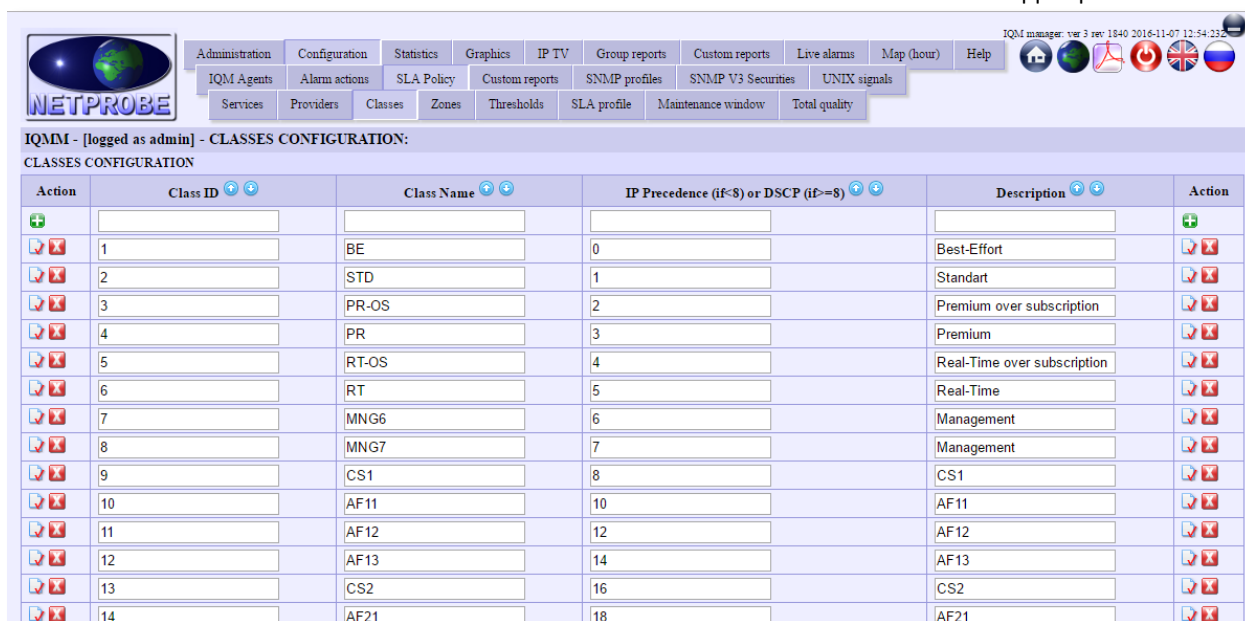





Рисунок 45 Форма управления именами классов сервиса.

Значения полей приведены в таблице ниже:

Поле	Значение
Class ID	Идентификатор, не редактируемое поле
Class Name	Короткое имя класса, под которым он будет отображаться в формах настройки тестов
IP Precedence (if<8) or DSCP (if=>8)	Значение, которое будет использовано при проведении теста. При значении меньше 8, будет маркироваться поле IP Precedence, значение большее либо равное 8 воспринимается как поле DSCP.
Description	Описание
Action	Допустимые действия:  - добавить новую запись  - внести изменения в текущую запись  - удалить текущую запись

### Управление зонами

Признак зоны относится к агенту. Под зоной понимается географический или административный признак размещения агента. Это абстрактный признак, может использоваться в любых других подходах при классификации. Кроме фильтрации зоны могут использоваться в групповом назначении политик контроля, при послойном отражении данных на ГИС.

По умолчанию, после установки в системе управления IQMM уже определен список зон.

Столбец1	Столбец2	Столбец3
Zone ID	Zone name	Description
0	Лондон	Лондон
1	Столицы	Москва, Санкт-Петербург
2	Север и центр	Север и Центр Европейской части РФ
3	Юг	Юг Европейской части РФ и Поволжье

4	Урал	Урал
5	Сибирь	Сибирь
6	Дальний Восток	Дальний Восток
7	Япония	Япония

При создании зональной структуры и распределении агентов по зонам рекомендуется сгруппировать агентов таким образом, чтобы можно было предъявить одни и те же требования к значениями контролируемых параметров для всех межзональных тестов с одинаковыми зонами-источниками тестов и целевыми зонами. Например, при мониторинге направления Москва-Екатеринбург, можно все агенты, размещенные на различных узлах в Москве сгруппировать в зону «Москва», агенты в Екатеринбурге – в зону «Екатеринбург».

Если в мониторинге на зональном уровне нет необходимости – можно отнести всех агентов к одной зоне.

Для определения зон – воспользуйтесь формой ZONES CONFIGURATION. Форма вызывается через пункт меню:




[Configuration --> SLA Policy --> Zones](#)



Рисунок 46 Форма управления зонами.

Значения полей приведены в таблице ниже:

Поле	Значение
Zone ID	Идентификатор, не редактируемое поле
Zone Name	Короткое имя зоны, под которым она будет отображаться в формах настройки агентов
Description	Описание
Action	Допустимые действия:

Поле	Значение
	 - добавить новую запись  - внести изменения в текущую запись  - удалить текущую запись

## Архитектурные уровни

Предоставлена возможность задания агенту признака принадлежности к архитектурному сетевому уровню. В системе определены стандартные сетевые архитектурные уровни. Названия уровней определяются в момент создания базы данных в скрипте, определяющем схему (/home/iqm/iqmm/sql/create\_cfg\_tables.sql):

```
CREATE TABLE IF NOT EXISTS agents (
...
net_layer          ENUM('CORE','DISTRIBUTION','ACCESS','SERVICE') DEFAULT "CORE",
...

```

и в конфигурационном файле (/home/iqm/iqmm/iqmm-cfg.pl):

```
%gTables = ('agents' =>      {'_NAMES'=> ['agent_id',
...
'net_layer'      =>      {'type' => 'enum', 'descr' => _('Network layer')},
'values'=>['CORE','DISTRIBUTION','ACCESS','SERVICE'], 'default'=>'CORE'}),

```

Таким образом, по умолчанию определены пять архитектурных сетевых уровней:

- CORE - агент размещен на уровне магистральных узлов сети (ядро или backbone),
- DISTRIBUTION - агент размещен на уровне узла распределения трафика,
- ACCESS - агент размещен на уровне узла доступа к услуге связи,
- SERVICE - агент размещен на площадке доступа к прикладным телекоммуникационным услугам

В большинстве случаев, приведенного списка признаков оказывается достаточно, в случае необходимости его дополнения или переопределения внесите соответствующие изменения в базу при помощи SQL-запроса:

```
ALTER TABLE agents CHANGE COLUMN net_layer net_layer
ENUM('CORE','DISTRIBUTION','ACCESS','SERVICE','REGIONAL_AGGREGATION') DEFAULT "CORE";

```

и приведите конфигурационный файл /home/iqm/iqmm/iqmm-cfg.pl в соответствие с базой данных:

```
%gTables = ('agents'      =>      {'_NAMES'=> ['agent_id',
...
'net_layer'      =>      {'type' => 'enum', 'descr' => ('Network layer')},
'values'=>['CORE','DISTRIBUTION','ACCESS','SERVICE','REGIONAL_AGGREGATION'], 'default'=>'CORE'},

```

Так как переопределение архитектурных уровней разовая задача, специальной web-формы для этого не создано.

## Контроль параметров

Задача контроля параметров включает в себя создание политик контроля, назначение их на контролируемые ресурсы и мониторинг с использованием активных элементов отображения и механизмов уведомления о состоянии. Политики контроля действуют как индивидуально, так и для произвольной группы измеряемых параметров, формируют несколько зон критичности и определяют способы реагирования на переходы значения параметров между зонами критичности. Предусмотрена возможность назначения каждому параметру нескольких пороговых значений: три пороговых значения, ограничивающих значение параметра сверху:

- Зеленый: предел нормального значения.

- Желтый: предел высокого значения.
- Красный: предел максимального значения.

и одно для ограничения снизу:

- Голубой: предел минимального значения.

Зона	Порог	Трактовка порога
красная		
	красный	предел максимального значения параметра
желтая		
	желтый	предел высокого значения параметра
зеленая		
	зеленый	предел нормального значения параметра
голубая		
	голубой	предел минимального значения параметра

При переходе параметра из одной зоны критичности в другую формируется событие, которое может быть связано с различными средствами оповещения:

- Уведомления средствами WEB-интерфейса
- e-Mail,
- SNMP-trap,
- syslog,
- SMS,
- механизм вызова внешних процедур позволяет реализовать любой желаемый способ уведомления: HTTP, SQL и пр...

Предусмотрена возможность реагирования как на единичные события, так и на события, возникающие чаще заданного порога. Для конфигурации частотного срабатывания уведомления определяется временной горизонт и количество нарушений в заданном горизонте, достаточное для срабатывания политики. Так же определяется количество нарушений, достаточное для выхода из зоны тревоги, т.е. прохождения зеленого аларма.

## Управление порогами

В случае если стоит задача получать сигналы о превышениях пороговых значений, необходимо для каждого из контролируемых параметров задать эти значения. Если пороги не будут определены, система, будет работать в режиме пассивного наблюдения: статистика для каждого теста будет собираться, ее можно будет просмотреть в отчетах, но сигналы тревоги генерироваться не будут. Так же не будут доступны отчеты с анализом нарушений.

В системе предусмотрена возможность определения нескольких пороговых уровней, превышение каждого из которых может быть связано с генерацией тревог различных критичностей: Maximum limit (максимальный уровень), High limit (высокий уровень), Normal limit (нормальный уровень), Minimum limit (минимальный уровень).

*Распределение пороговых значений и интерпретация зон критичности могут быть проведены произвольным способом в зависимости от имеющихся требований и используемых подходов к мониторингу. Следующий способ интерпретации приведен в качестве примера.*

В случае если значение параметра находится в пределах между нормальным и высоким значением – генерируется желтый сигнал. Критичность желтого сигнала соответствует предупреждению. Это означает, что значение контролируемого параметра пока не влияет на жизнеспособность сетевых сервисов, но приближается к критическому значению.

В случае если значение параметра находится в пределах между высоким и максимальным значением – генерируется красный сигнал. Критичность красного сигнала говорит о значительной деградации качества. Многие сетевые сервисы могут страдать, но продолжают работать.

В случае если значение параметра превышает максимальное значение – генерируется кровавый сигнал. Критичность кровавого сигнала говорит о наличии аварийной ситуации в контролируемом направлении. Сетевые сервисы, критичные к данному параметру качества перестают работать.

Минимальный уровень значения предназначен для контроля доступной полосы пропускания. Если значение оказывается ниже минимального значения, генерируется синий сигнал. Синий сигнал говорит о недостатке выделенного сетевого ресурса.

Для определения пороговых значений – воспользуйтесь формой THRESHOLDS CONFIGURATION. Форма вызывается через пункт меню:

*Configuration – SLA Policy – Thresholds*

Parameter	Value	Default
Threshold ID	AvgRTT-100-120-150	
Threshold name	AvgRTT-100-120-150	
Description		
Table name	data_raw	data_raw
Value name	AvgRtt	
Maximum limit	150.00	
High limit	120.00	
Normal limit	100.00	
Minimum limit		

Copyright (C) 2008, LLC Network Probe. All rights reserved.



Рисунок 47 Форма управления пороговыми значениями для контролируемых параметров

Поле	Значение
Threshold ID	Идентификатор, транслированный в Threshold name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Threshold name	Обязательное для заполнения поле. Уникальное символическое обозначение порога. Допускается использование алфавитно-цифровых символов, пробелы.
Description	Краткое описание
Table name	<p>Обязательное для заполнения поле. Имя таблицы, из которой будут извлекаться параметры для контроля пороговых значений.</p> <p>data_raw – таблица не усредненных значений,</p> <p>data_aggr1 – таблица значений с первым уровнем усреднения (по умолчанию – 1 час),</p> <p>data_aggr2 – таблица значений со вторым уровнем усреднения (по умолчанию – сутки),</p> <p>cisco_saa_data (устаревшая) - таблица данных мониторинга, полученных от агентов Cisco Service Assurance (Cisco IP SLA), сейчас данные размещаются в таблице data_raw и агрегируются в data_aggr1 и data_aggr2,</p> <p>mcast_data_raw - таблица данных мониторинга IPTV MDI,</p> <p>pppoe_data_raw - таблица с измеренными характеристиками работы PPPoE - сессии.</p> <p>В зависимости от применяемых средств мониторинга, список таблиц для контролируемых параметров может меняться.</p> <p>Значение, применяемое по умолчанию - data_raw</p>
Value name	Обязательное для заполнения поле. Имя поля, подвергающегося контролю, соответствует одному из контролируемых параметров. Описание стандартных параметров дано в разделе "Измеряемые характеристики".
Maximum limit	Предел максимального значения параметра. Включительно.
High limit	Предел высокого значения параметра. Включительно.



Поле	Значение
Normal limit	Предел нормального значения параметра. Включительно.
Minimum limit	Предел минимального значения параметра. Включительно.

## Механизмы уведомления

IQM предоставляет возможность использования разных средств уведомления в произвольной комбинации. Уведомления могут проводиться в ответ на смену состояний контролируемых параметров, при большом количестве попыток авторизации в системе (вероятном подборе пароля). Для конфигурации каждого механизма уведомления предназначена отдельная форма в группе меню

### *Configuration – Alarm actions*

---

Комбинирование механизмов уведомления осуществляется в профиле действий (Action profile).

## Приемники syslog

Уведомления через syslog – стандартный способ интеграции с внешними системами управления. Для этого, используется syslog-сервер, который собирает сообщения о событиях с разных устройств, в том числе и других систем мониторинга. Для передачи аварийных сообщений через syslog потребуется конфигурация одного или нескольких приемников syslog-сообщений. Для этого воспользуйтесь формой SYSLOGS CONFIGURATION. Форма вызывается через пункт меню:

### *Configuration – Alarm actions – Syslogs*

---

**IQMM - [logged as admin] - SYSLOGS CONFIGURATION:**  
**SYSLOGS CONFIGURATION**

add
 fill form
 CSV
 view
 change
 delete

Deploy on:		
Parameter	Value	Default
Syslog ID	<input type="text"/>	
Syslog name *	<input type="text"/>	
Socket type	<input type="text"/>	inet
Host	<input type="text"/>	
Facility	<input type="text"/>	LOG_LOCAL6
Priority	<input type="text"/>	LOG_INFO
Syslog ident	<input type="text"/>	iqm-manager
Syslog description	<input type="text"/>	

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 48 Форма конфигурации приемников syslog-сообщений

Значения полей:

Поле	Значение
Syslog ID	Идентификатор, транслированный в Syslog name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Syslog name *	Обязательное для заполнения поле. Уникальное символическое обозначение приемника syslog-сообщений. Допускается использование алфавитно-цифровых символов, пробелы.
Socket type	<p>Тип соединения для передачи сообщения приемнику:</p> <ul style="list-style-type: none"> <li>• native - локальная запись сообщения с использованием C-функции из библиотеки syslog(3)</li> <li>• eventlog - передача сообщения на Win32 event logger</li> <li>• tcp - передача сообщения через TCP сокет, с использованием "syslog/tcp" или "syslogng/tcp"</li> <li>• udp - передача сообщения через UDP сокет, с использованием "syslog/udp"</li> <li>• inet - передача сообщения через INET-сокет, TCP или UDP</li> </ul>

Поле	Значение
	<ul style="list-style-type: none"> <li>• unix - передача сообщения через UNIX-сокеты</li> </ul> <p>наиболее часто используемые типы: Unix - для локальной передачи сообщения, inet - для передачи через сеть.</p>
Host	Хост-приемник сообщений, при передаче через сеть
Facility	Категория сообщения. В выпадающем списке приведены наиболее часто используемые категории.
Priority	<p>Уровень важности передаваемого сообщения. В выпадающем списке приведены все уровни:</p> <ul style="list-style-type: none"> <li>• LOG_EMERG - паника</li> <li>• LOG_ALERT - серьезная ошибка</li> <li>• LOG_CRIT - критическая ошибка</li> <li>• LOG_ERR - ошибка</li> <li>• LOG_WARNING - предупреждения</li> <li>• LOG_NOTICE - замечание</li> <li>• LOG_INFO - общая информация</li> <li>• LOG_DEBUG - отладочное сообщение</li> </ul>
Syslog ident	Идентификатор отправителя сообщения
Syslog description	Текстовое описание приемника syslog-сообщений

В системе по умолчанию сконфигурирован локальный приемник syslog-сообщений:

<b>Syslog name *</b>	<b>syslog_local</b>
Socket type	unix
Host	
Facility	LOG_LOCAL6
Priority	LOG_INFO
Syslog ident	iqm-manager

Syslog description	
--------------------	--

## Syslog-сервер

Для корректной отработки поступающих сообщений со стороны syslog-приемника необходимо провести конфигурацию syslog-сервера. Далее приводится пример конфигурации на платформе CentOS 6.

- Сконфигурировать selinux для разрешения rsyslog трафика

```
semanage -a -t syslogd_port_t -p udp 514
```

- Сконфигурировать и перезапустить iptables для приема трафика на UDP/514. В файле /etc/sysconfig/iptables должно присутствовать правило:

```
-A INPUT -m state --state NEW -m udp -p udp --dport 514 -j ACCEPT
```

- В файле конфигурации демона rsyslogd /etc/rsyslog.conf разрешить прием по сети, раскомментировать нужные строки, сконфигурировать запись данных в файл:

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

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

local4.*                /var/log/iqmm-traps
local5.*                /var/log/iqmm
local6.*                /var/log/iqmm-alarms
...
```

- Обеспечить пропуск syslog-трафика на межсетевых экранах и прочих фильтрах в сторону syslog-сервера. Syslog использует порт 514/udp.

### Syslog-сообщения передаются в строго определенном формате:

```
[maxim@CO6 iqmm]$ sudo tail -f /var/log/iqmm-alarms
[sudo] password for maxim:
Nov 26 11:46:03 CO6 iqm-manager:
action_id=1;alarm_id=4;check_horizon=60;class=BE;count=1;param=SDLostPercent;policy_name=policy_b
asic_web;severity=crimson;status=UP;table=data_raw;test_id=14;test_name=iqmm_www.yandex.ru_URL_BE
;threshold=3.00;time_end=2016-11-26 11:46:02;time_start=2016-11-26
10:46:02;url=http://localhost/iqm/?action=alarms;alarm_id=4
Nov 26 16:44:02 CO6 iqm-manager:
action_id=1;alarm_id=5;check_horizon=60;class=BE;count=1;param=SDLostPercent;policy_name=policy_b
asic_web;severity=crimson;status=UP;table=data_raw;test_id=14;test_name=iqmm_www.yandex.ru_URL_BE
;threshold=3.00;time_end=2016-11-26 16:44:02;time_start=2016-11-26
15:44:02;url=http://localhost/iqm/?action=alarms;alarm_id=5
Nov 26 19:32:01 CO6 iqm-manager:
action_id=1;alarm_id=6;check_horizon=60;class=BE;count=1;param=SDLostPercent;policy_name=policy_b
asic_web;severity=crimson;status=UP;table=data_raw;test_id=14;test_name=iqmm_www.yandex.ru_URL_BE
;threshold=3.00;time_end=2016-11-26 19:32:01;time_start=2016-11-26
18:32:01;url=http://localhost/iqm/?action=alarms;alarm_id=6
Nov 27 18:29:02 CO6 iqm-manager:
action_id=1;alarm_id=7;check_horizon=60;class=BE;count=6;param=SDLostPercent;policy_name=policy_b
asic_web;severity=crimson;status=UP;table=data_raw;test_id=14;test_name=iqmm_www.yandex.ru_URL_BE
;threshold=3.00;time_end=2016-11-27 18:29:02;time_start=2016-11-27
17:29:02;url=http://localhost/iqm/?action=alarms;alarm_id=7
Nov 28 14:10:02 CO6 iqm-manager:
action_id=1;alarm_id=7;check_horizon=60;class=BE;count=0;param=SDLostPercent;policy_name=policy_b
```

```

asic_web;severity=green;status=UP;table=data_raw;test_id=14;test_name=iqmm_www.yandex.ru_URL_BE;t
hreshold=0;time_end=2016-11-28 14:10:02;time_start=2016-11-27
17:29:02;url=http://localhost/iqm/?action=alarms;alarm_id=7
Nov 29 17:23:02 CO6 iqm-manager:
action_id=1;alarm_id=8;check_horizon=60;class=BE;count=1;param=SDLostPercent;policy_name=policy_b
asic_web;severity=yellow;status=UP;table=data_raw;test_id=14;test_name=iqmm_www.yandex.ru_URL_BE;
threshold=0.50;time_end=2016-11-29 17:23:02;time_start=2016-11-29
16:23:02;url=http://localhost/iqm/?action=alarms;alarm_id=8
Nov 29 18:23:03 CO6 iqm-manager:
action_id=1;alarm_id=8;check_horizon=60;class=BE;count=0;param=SDLostPercent;policy_name=policy_b
asic_web;severity=green;status=UP;table=data_raw;test_id=14;test_name=iqmm_www.yandex.ru_URL_BE;t
hreshold=0;time_end=2016-11-29 18:23:02;time_start=2016-11-29
16:23:02;url=http://localhost/iqm/?action=alarms;alarm_id=8
Nov 29 23:13:03 CO6 iqm-manager:
action_id=1;alarm_id=9;check_horizon=60;class=BE;count=1;param=SDLostPercent;policy name=policy b
asic_web;severity=yellow;status=UP;table=data_raw;test_id=14;test_name=iqmm_www.yandex.ru_URL_BE;
threshold=0.50;time_end=2016-11-29 23:13:03;time_start=2016-11-29
22:13:03;url=http://localhost/iqm/?action=alarms;alarm_id=9
Nov 30 02:02:03 CO6 iqm-manager:
action_id=1;alarm_id=9;check_horizon=60;class=BE;count=1;param=SDLostPercent;policy name=policy
basic_web;severity=crimson;status=UP;table=data_raw;test_id=14;test_name=iqmm_www.yandex.ru_URL_B
E;threshold=3.00;time_end=2016-11-30 02:02:02;time_start=2016-11-30
01:02:02;url=http://localhost/iqm/?action=alarms;alarm_id=10
Nov 30 03:01:02 CO6 iqm-manager:
action_id=1;alarm_id=10;check_horizon=60;class=BE;count=0;param=SDLostPercent;policy name=policy
basic web;severity=green;status=UP;table=data raw;test id=14;test name=iqmm www.yandex.ru URL BE;
threshold=0;time_end=2016-11-30 03:01:02;time_start=2016-11-30
01:02:02;url=http://localhost/iqm/?action=alarms;alarm_id=10

```

## Ловушки SNMP-trap

Для передачи аварийных сообщений через SNMP-Trap потребуется конфигурация одного или нескольких приемников SNMP-trap. Для этого воспользуйтесь формой TRAPS CONFIGURATION. Форма вызывается через пункт меню:

*Configuration – Alarm actions – SNMP-traps*

**IQMM - [logged as admin] - TRAPS CONFIGURATION:**

**TRAPS CONFIGURATION**

add
 fill form
 CSV
 view
 change
 delete
 clear
 expert

Deploy on:		
Parameter	Value	Default
Trap host ID	<input type="text"/>	
Trap host name *	<input type="text"/>	
SNMP profile	<input type="text"/>	
Trap host domain name or IP	<input type="text"/>	localhost
Trap description	<input type="text"/>	

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 49 Форма конфигурации ловушек SNMP-trap

Значения полей:

Поле	Значение
Trap host ID	Идентификатор, транслированный в Trap host name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Trap host name *	Обязательное для заполнения поле. Уникальное символическое обозначение блока конфигурации ловушки SNMP-trap. Допускается использование алфавитно-цифровых символов, пробелы.
SNMP profile	<p>Профиль SNMP. Запись конфигурация параметров SNMP-взаимодействия. В системе, по умолчанию заведены записи:</p> <ul style="list-style-type: none"> <li>• netiqm: community public, SNMPv2, port 162, timeout 1s, retries 5</li> <li>• public: community public, SNMPv2, port 162, timeout 1s, retries 5</li> <li>• public-trap: community public, SNMPv2, port 162, timeout 1s, retries 5</li> </ul> <p>Воспользуйтесь записью public-trap, либо создайте собственную. Управление SNMP-профилями осуществляется через пункт меню:</p> <p style="text-align: center;"><a href="#"><u>Configuration --&gt; SNMP profiles</u></a></p>
Trap host domain name or IP	Хост-приемник, при передачи через сеть
Trap description	Текстовое описание ловушки SNMP-trap

В системе по умолчанию сконфигурирован локальный приемник SNMP-trap-сообщений:

<b>Trap host name *</b>	<b>trap_local</b>
SNMP profile	public-trap
Trap host domain name or IP	localhost
Trap description	

### SNMP-trapd сервер

Для получения возможности принимать SNMP-TRAP-ы во внешних системах управления необходимо подключить MIB NP-IQM3-NOTIFICATION-MIB.txt, который находится в /home/iqm/iqmm/doc/NP-IQM3-NOTIFICATION-MIB.txt.

При использовании Net-SNMP это можно сделать несколькими способами:

- использовать опцию -m +NP-IQM3-NOTIFICATION-MIB.txt при запуске snmptrapd. Опции запуска snmptrapd можно указать в /etc/sysconfig/snmptrapd, например, для логирования в syslog local4:

```
# snmptrapd command line options
OPTIONS="-Ls4 -p /var/run/snmptrapd.pid -m +/usr/share/snmp/mibs/NP-IQM-NOTIFICATION-MIB.txt "
```

- В одном из конфигурационных файлов \$HOME/.snmp/snmp.[local].conf, /usr/local/share/snmp.[local].conf или /etc/snmp/snmp.[local].conf поместить запись

```
mibs +NP-IQM-NOTIFICATION-MIB
```

- Так же можно использовать переменную окружения. При необходимости указания нескольких MIB-ов, они указываются через двоеточие.

```
MIBS+=NP-IQM-NOTIFICATION-MIB
export MIBS
```

*Так же см. man snmpcmd.*

- Для разрешения приема трапов в конфигурации snmptrapd /etc/snmp/snmptrapd.conf необходимо определить community:

```
# Example configuration file for snmptrapd
#
# No traps are handled by default, you must edit this file!
#
authCommunity log,execute,net public
```

- Сконфигурировать и перезапустить iptables для приема трафика на UDP/514. В файле /etc/sysconfig/iptables должно присутствовать правило:

```
-A INPUT -m state --state NEW -m udp -p udp --dport 161 -j ACCEPT
```

При конфигурировании записи SNMP-trap сообщений в syslog local4 (см. так же Syslog-сервер) в файле /var/log/iqmm-traps будут собираться сообщения, подобные следующим:

```
[maxim@CO6 iqmm]$ sudo tail -5 /var/log/iqmm-traps
Nov  3 13:22:03 CO6 snmptrapd[2383]: 2016-11-03 13:22:03 localhost [UDP: [127.0.0.1]:60569->[127.0.0.1]]:#012DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8057409)
22:22:54.09#011SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.40597.11.1.1.1#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.3.0 = INTEGER: 60#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.1.0 = STRING: "2016-11-03 11:14:02"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.6.0 = STRING: "data raw"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.2.0 = STRING: "2016-11-03 13:22:03"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.13.0 = STRING: "http://localhost/iqm/?action=alarms;alarm_id=140"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.10.0 = INTEGER: 0#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.9.0 = STRING: "0"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.7.0 = STRING: "SDLostPercent"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.5.0 = STRING: "BE"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.8.0 = STRING: "policy_basic"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.11.0 = STRING: "green"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.12.0 = STRING: "UP"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.4.0 = STRING: "iqmm_www.yandex.ru_I0_BE64K"
Nov  3 13:28:03 CO6 snmptrapd[2383]: 2016-11-03 13:28:03 localhost [UDP: [127.0.0.1]:54532->[127.0.0.1]]:#012DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8093376)
22:28:53.76#011SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.40597.11.1.1.1#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.3.0 = INTEGER: 60#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.1.0 = STRING: "2016-11-03 11:14:02"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.6.0 = STRING: "data raw"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.2.0 = STRING: "2016-11-03 13:28:03"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.13.0 = STRING: "http://localhost/iqm/?action=alarms;alarm_id=140"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.10.0 = INTEGER: 1#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.9.0 = STRING: "0.50"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.7.0 = STRING: "SDLostPercent"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.5.0 = STRING: "BE"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.8.0 = STRING: "policy_basic"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.11.0 = STRING: "yellow"#011SNMPv2-
```

```

SMI::enterprises.40597.11.1.2.1.1.12.0 = STRING: "UP"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.4.0 = STRING: "iqmm_www.yandex.ru_I0_BE64K"
Nov 3 14:29:04 CO6 snmptrapd[2383]: 2016-11-03 14:29:04 localhost [UDP: [127.0.0.1]:34106->
[127.0.0.1]]:#012DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (8458953)
23:29:49.53#011SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.40597.11.1.1.1#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.3.0 = INTEGER: 60#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.1.0 = STRING: "2016-11-03 13:29:03"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.6.0 = STRING: "data_raw"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.2.0 = STRING: "2016-11-03 14:29:03"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.13.0 = STRING:
"http://localhost/iqm/?action=alarms;startdate=2016-11-03%2013%3A29%3A03;enddate=2016-11-
03%2014%3A29%3A03"#011SNMPv2-SMI::enterprises.40597.11.1.2.1.1.10.0 = INTEGER: 30#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.9.0 = STRING: "3.00"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.7.0 = STRING: "SDLostPercent"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.5.0 = STRING: "BE"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.8.0 = STRING: "policy_basic"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.11.0 = STRING: "crimson"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.12.0 = STRING: "UP"#011SNMPv2-
SMI::enterprises.40597.11.1.2.1.1.4.0 = STRING: "iqmm_a2_U0_BE64K"
    
```

## Адресаты eMail

Для передачи аварийных сообщений через сервис почтовых сообщений eMail потребуется определение одного или нескольких eMail-адресатов. Для этого воспользуйтесь формой MAI LS CONFIGURATION. Форма вызывается через пункт меню:

*Configuration – Alarm actions – e-Mails*

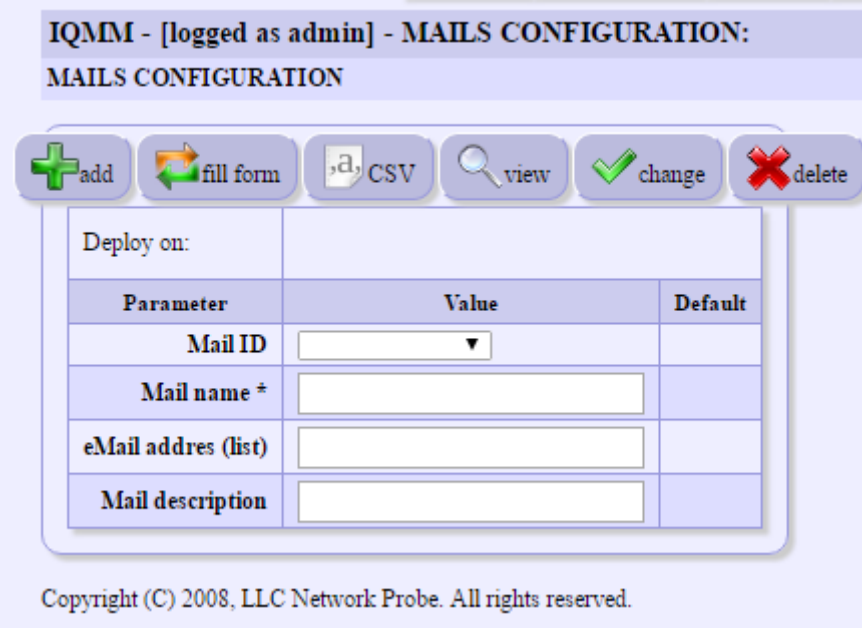


Рисунок 50 Форма конфигурации e-Mail адресатов

Значения полей:

Поле	Значение
Mail ID	Идентификатор, транслированный в Mail name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Mail name *	Обязательное для заполнения поле. Уникальное символическое обозначение eMail адресата. Допускается использование алфавитно-



Поле	Значение
	цифровых символов, пробелы.
eMail address (list)	eMail адрес, либо список адресов со стандартными разделителями
Mail description	Текстовое описание eMail адресата

Отправляемые почтовые уведомления о нарушениях политик контроля будут содержать описание тестовой конфигурации, таблицу со срезом измерений и график поведения параметра:

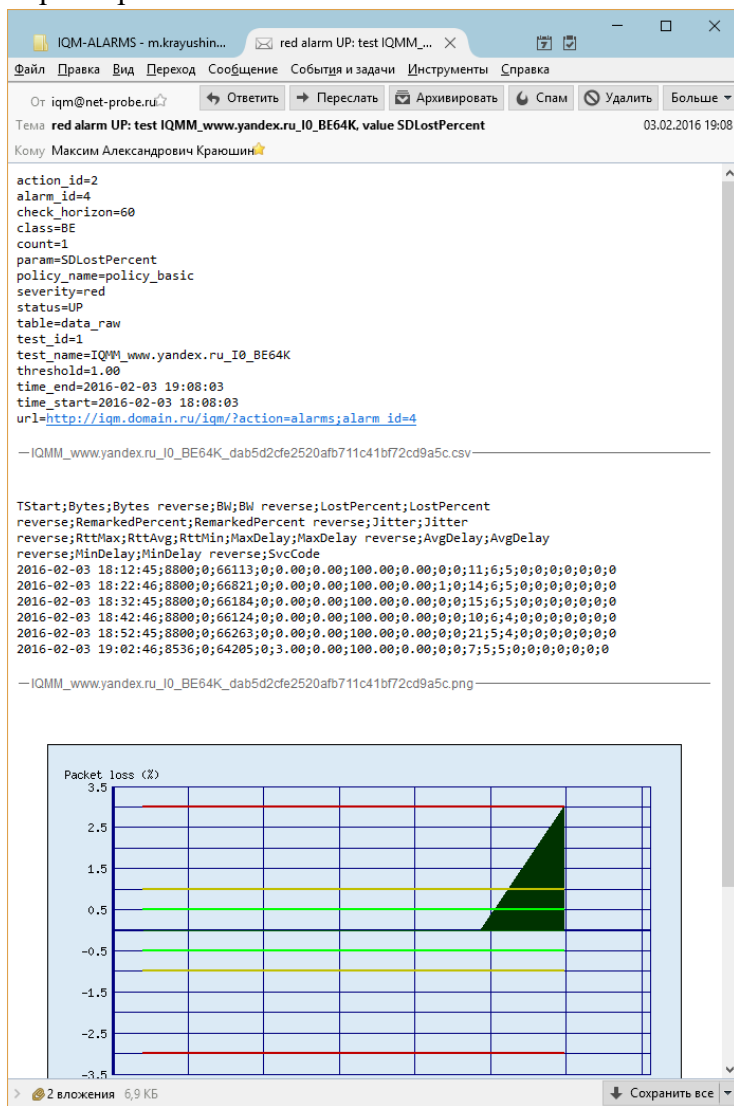


Рисунок 51 Пример eMail сообщения о тревоге уровня red

## SMS-уведомления

*Для работы SMS-уведомлений необходимо наличие дополнительного модуля IQM: iqmm-smpp.*

При отправке SMS-уведомлений используется протокол SMPP — (Short Message Peer-to-Peer) короткие сообщения одноранговой Сети. Протокол является открытым стандартом в телекоммуникационной отрасли, который разработан специально, чтобы обеспечить гибкий интерфейс для передачи коротких сообщений между внешними сущностями (устройства, приложения) коротких сообщений (ESME), маршрутизаторами и центров сообщений (SMSC).







Для корректной работы механизма SMS-уведомлений требуется конфигурация сервера сообщений SMSC, профиля сообщений и номера, на который сообщения будут отправляться.

### Конфигурация сервера SMS

SMS-сервер, SMSC - центр сообщений, SMS-шлюз. Отвечает за получение, хранение, конвертацию и передачу SMS-сообщений. Взаимодействует по разным протоколам (HTTP, SMTP, SMPP и т.д.) с источниками SMS-сообщений в IP-сети, с другой стороны взаимодействует (напрямую, либо опосредованно) с центрами SMS мобильных операторов для передачи сообщений адресатам. Параметры центра SMS необходимо получить у соответствующего оператора. Для конфигурации серверов SMS воспользуйтесь формой THRESHOLDS CONFIGURATION. Форма вызывается через пункт меню:

*Configuration – Alarm actions – SMPP servers*

**IQMM - [logged as admin] - SMPP\_SERVERS CONFIGURATION:**  
**SMPP\_SERVERS CONFIGURATION**

 add  fill form  CSV  view  change  delete

Deploy on:		
Parameter	Value	Default
ID	<input type="text"/>	
SMPP server name	<input type="text"/>	
Server IP address	<input type="text"/>	
Server TCP port	<input type="text"/>	2775
SMPP system ID (5.2.1)	<input type="text"/>	
SMPP password (5.2.2)	<input type="text"/>	
SMS source address	<input type="text"/>	
SMPP server description	<input type="text"/>	

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 52 Форма конфигурации SMS-серверов (SMSC)

Описание значения полей приведено ниже в таблице.

Поле	Значение
ID	Идентификатор, транслированный в SMPP server name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
SMPP server name	Обязательное для заполнения поле. Уникальное символическое имя сервера. Допускается использование алфавитно-цифровых символов, пробелы.
Server IP address	IP адрес SMS-шлюза
Server TCP port	TCP порт для взаимодействия по SMPP. По умолчанию 2775.
SMPP system ID (5.2.1)	Идентификатор пользователя, для авторизации доступа к шлюзу SMS
SMPP password (5.2.2)	Пароль пользователя, для авторизации доступа к шлюзу SMS
SMS source address	Идентификатор отправителя сообщения SMS
SMPP server description	Текстовое описание сервера

### Конфигурация шаблона SMS

SMS шаблон определяет формат передаваемого сообщения. Для конфигурации шаблона SMS воспользуйтесь формой SMS\_MESSAGE\_TEMPLATES CONFIGURATION. Форма вызывается через пункт меню:

*[Configuration – Alarm actions – SMPP templates](#)*

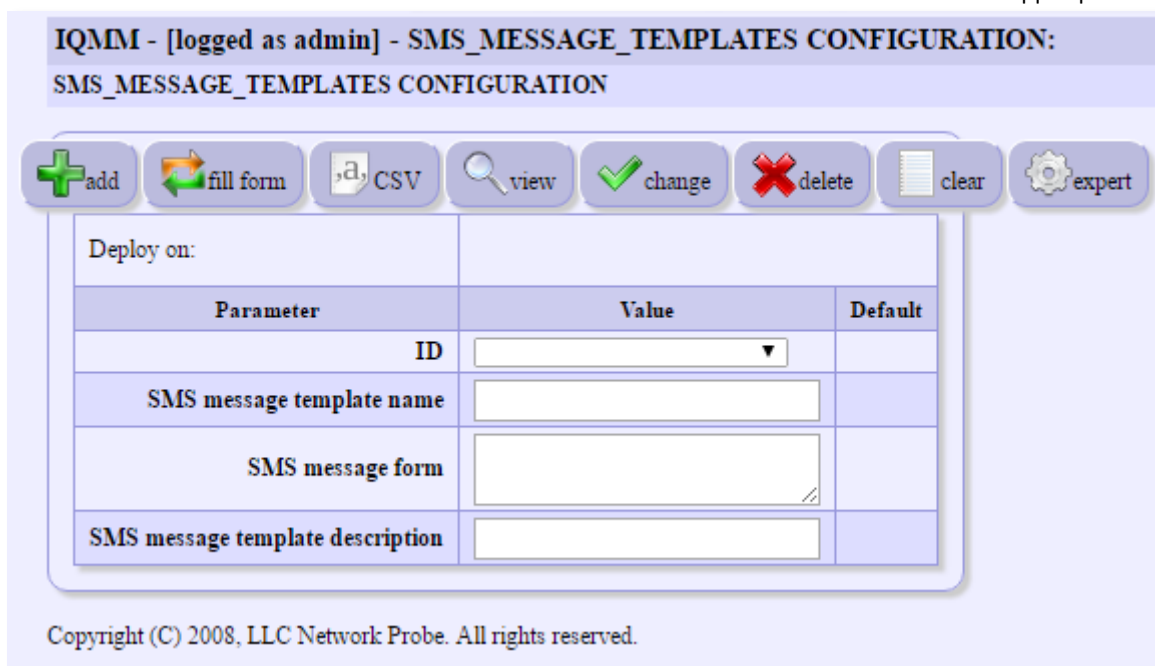


Рисунок 53 Форма конфигурации SMS-шаблона

Описание значения полей приведено ниже в таблице.

Поле	Значение
ID	Идентификатор, транслированный в SMS message template name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
SMS message template name	Обязательное для заполнения поле. Уникальное символическое имя шаблона SMS. Допускается использование алфавитно-цифровых символов, пробелы.
SMS message form	Шаблон SMS-сообщения
SMS message template description	Текстовое описание шаблона

В системе заведены готовые шаблоны.

SMS message template name	SMS message form	SMS message template description
alarm template	Alarm severity=%{severity} status=%{status} start=%{time_start} end=%{time_end} horizon=%{check_horizon} tid=%{test_id} test=%{test_name} class=%{class} table=%{table} param=%{param} policy=%{policy_name} thres=%{threshold} count=%{count} url=%{url}	Alarm default template
alarm template russian	Тревога уровень=%{severity} статус=%{status} начало=%{time_start} конец=%{time_end} горизонт=%{check_horizon} номер теста=%{test_id} тест=%{test_name} класс=%{class} данные=%{table} параметр=%{param} политика=%{policy_name} порог=%{threshold} разы=%{count} ссылка=%{url}	Шаблон для SMS про алармы на русском

SMS message template name	SMS message form	SMS message template description
login invalid template	Invalid login, username={user_name} severity={severity} time={time} ip={remote_ip} host={remote_host} forw={remote_forwarded} reason={reason}	Login invalid template
login invalid template russian	Плохой логин, логин={user_name} уровень={severity} время={time} ip={remote_ip} хост={remote_host} форв={remote_forwarded} причина={reason}	Шаблон для SMS на русском

### Конфигурация адресатов SMS

После конфигурации SMS-сервера и шаблона можно определить адресатов, которые будут получать SMS-уведомления. Для конфигурации адресатов SMS воспользуйтесь формой SMS\_NUMBERS CONFIGURATION. Форма вызывается через пункт меню:

*Configuration – Alarm actions – SMPP numbers*

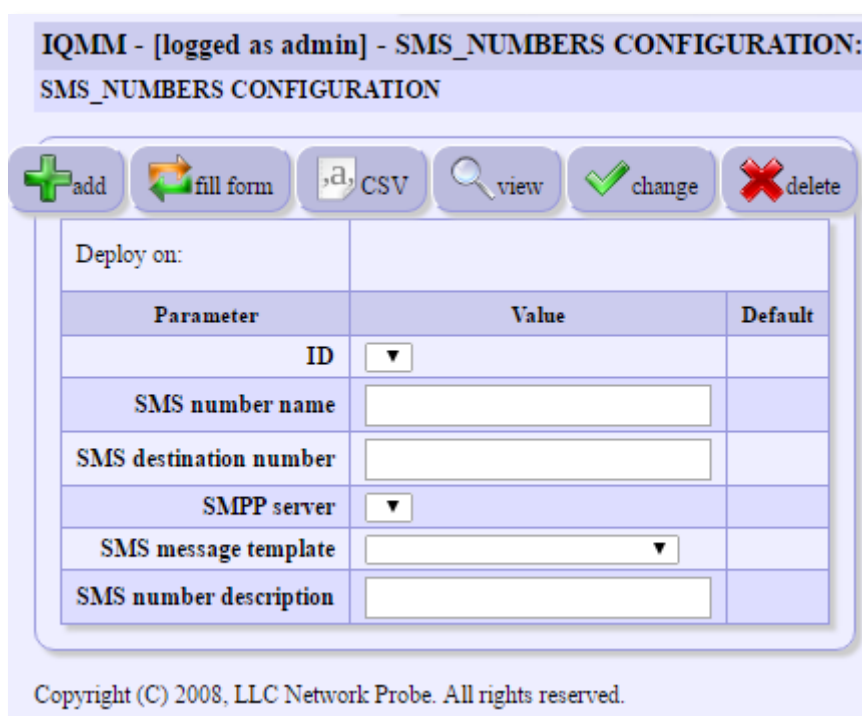


Рисунок 54 Форма конфигурации адресатов SMS сообщений

Описание значения полей приведено ниже в таблице.

Поле	Значение
ID	Идентификатор, транслированный в SMS number name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
SMS number name	Обязательное для заполнения поле. Уникальное символическое обозначение адресата SMS. Допускается использование алфавитно-цифровых символов, пробелы.

Поле	Значение
SMS destination number	Номер адресата
SMPP server	Выбор сервера SMS из выпадающего списка. См. Конфигурация сервера SMS.
SMS message template	Выбор шаблона SMS из выпадающего списка. См. Конфигурация шаблона SMS.
SMS number description	Текстовое описание адресата

### Профиль действий

В системе предусмотрены разнообразные способы реагирования на изменения состояния контролируемых параметров. Профили действий используются для произвольного комбинирования всевозможных средств реагирования и оповещения для дальнейшего их использования в политиках контроля. Например, благодаря профилям действий существует возможность отсылки syslog в качестве реакции на попадание параметра в желтую зону, SMS+syslog - для красной зоны, широковещательного уведомления на адреса e-Mail+SMS+syslog+вызов внешней процедуры для кровавой зоны.

Для создания профиля уведомлений необходимо определить механизмы уведомления. Затем воспользуйтесь формой ALARM\_ACTIONS CONFIGURATION. Форма вызывается через пункт меню:

*[Configuration – Alarm actions – Action profile](#)*

---

**IQMM - [logged as admin] - ALARM\_ACTIONS CONFIGURATION:**  
**ALARM\_ACTIONS CONFIGURATION**

Deploy on:		
Parameter	Value	Default
Alarm action ID	action_syslog ▼	
Alarm action name *	action_syslog	
Alarm action description	send local syslog	
IQMM URL	http://localhost/iqm/	http://localhost/iqm/
External program		
Trap hosts	trap_local ▲▼	
Syslog hosts	syslog_local ▲▼	
Email	mail_root@local ▲▼	
SMS number	223-322-232-332 ▲▼	

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 55 Форма конфигурации профиля действий

Поле	Значение
Alarm action ID	Идентификатор, транслированный в Alarm action name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Alarm action name *	Обязательное для заполнения поле. Уникальное символическое обозначение профиля действий. Допускается использование алфавитно-цифровых символов, пробелы.
Alarm action description	Текстовое описание профиля действий.
IQMM URL	URL, адрес, который будет использоваться при формировании ссылок на объекты в системе управления IQMM.

Поле	Значение
	Например: <a href="http://iqm-system.ru/iqm/">http://iqm-system.ru/iqm/</a>
External program	Путь к внешней программе, установленной в системе IQMM, которая должна быть выполнена. На стандартный ввод программы будет передана информация о событии.
Trap hosts	Приемник SNMP-trap. Возможен множественный выбор, в этом случае сообщения будут высланы поочередно на каждый из приемников. См. разделы Ловушки SNMP-trap, так же SNMP-trapd сервер.
Syslog hosts	Приемник syslog-сообщений. Возможен множественный выбор, в этом случае сообщения будут высланы поочередно на каждый из приемников. См. разделы Приемники syslog, так же Syslog-сервер.
Email	Адресаты e-Mail-сообщений. Возможен множественный выбор. См. раздел Адресаты eMail.
SMS number	Адресаты SMS-сообщений. Возможен множественный выбор. См. раздел SMS-уведомления.

В системе по умолчанию заведен профиль действий, позволяющий пересылать локальные syslog-сообщения в категории LOCAL6 и приоритетом INFO.

<b>Alarm action name *</b>	<b>action_syslog</b>
Alarm action description	send local syslog
IQMM URL	<a href="http://localhost/iqm/">http://localhost/iqm/</a>
External program	
Trap hosts	
Syslog hosts	syslog_local
Email	
SMS number	

### Вызов внешней процедуры

Программа, которая должна быть выполнена в ответ на изменение состояния контролируемого параметра, конфигурируется в профиле действий (см. Профиль действий). При конфигурации указывается полный путь к исполняемому файлу программы. В качестве программы может быть использован shell-скрипт, программа языкового интерпретатора (perl, python, ruby и т.п.), или бинарный исполняемый файл. Возможно указать только один исполняемый файл, для запуска множества программ - воспользуйтесь внешней shell-оболочкой. Возможность вызова внешней процедуры придает системе гибкости в выборе механизмов реагирования на события.

Для изучения поведения системы при запуске внешней процедуры создайте тестовый скрипт, который логирует передаваемую ему информацию. Сконфигурируйте путь к нему



в профиле действий, создайте политику контроля. Пример скрипта:  
`/home/iqm/iqmm/scripts/tst-alarm.sh`

```
[root@CO6 scripts]# cat /home/iqm/iqmm/scripts/tst-alarm.sh
#!/bin/bash

LANG=C
lf=/tmp/alarm-tst.log
echo >> $lf
date >> $lf
echo $0 $@ >> $lf
echo Running $0 $@ ...

echo >> $lf
while read -t 1 -r line
do
    echo $line >> $lf
done
```

После регистрации аварийного события в лог-файле сохранится запись:

```
Mon Dec 5 14:30:04 MSK 2016
/home/iqm/iqmm/scripts/tst-alarm.sh

check_horizon=60
count=1
policy name=policy basic
time_start=2016-12-05 13:30:04
cmd=/home/iqm/iqmm/scripts/tst-alarm.sh
threshold=150.00
test_id=7
status=UP
table=data raw
test_name=iqmm_google-public-dns_DNS_BE64K
alarm_id=22
time_end=2016-12-05 14:30:04
url=http://localhost/iqm/
class=BE
severity=crimson
param=AvgRtt
```

## Управление SLA-политиками

SLA-политика (политика контроля) выполняет задачу связывания событий, происходящих в системе с механизмами оповещения, которые могут быть специфическими и зависеть от критичности события. Выполняя задачи мониторинга, политики связывают факты нарушения требований, предъявляемых к параметрам через пороговые значения, с механизмами оповещения, определяемыми профилями действий. Политика так же определяет механизм срабатывания нарушения. Срабатывание нарушения, т.е. переход из нормального состояния в состояние тревоги и обратно, происходит в случае, если частота нарушений в заданном интервале, определяемом горизонтом контроля, превышает или равна заданной. Частота определяется в политике контроля. В разных политиках могут использоваться разные значения.

Политики действуют на результаты измерений, проведенных отдельными тестами или группой тестов.

После назначения политики контроля на тест система станет:

- Отображать пороговые значения в исторических отчетах
- Генерировать сигналы тревоги в случае превышения параметрами установленных значений
- Для тестов, контролируемых политиками, станут доступны отчеты с критическим анализом контролируемых направлений

Назначить политику контроля на тест можно двумя способами:

- Индивидуально, назначив политику непосредственно конкретному тесту. Назначение политики происходит в форме конфигурации тестов (см. Создание тестов).
- На группу, определив класс сервиса, зону инициатора теста и приемную зону. В этом случае, политика автоматически применится на все тесты, попадающие под эти критерии.

В случае, если для определенного теста назначены одновременно две политики, индивидуально и групповым способом, то для контроля будет выбрана индивидуальная политика. Политики, назначенные непосредственно на тест имеют приоритет. В случае, если на тест назначено несколько политик групповым способом, ни одна из политик действовать не будет. В связи с этим:

*Во избежание возникновения конфликтов рекомендуется назначать политики только индивидуально на тесты. При необходимости конфигурации большого количества тестов - воспользуйтесь режимом массовой конфигурации (см. Режим массовой конфигурации, так же Создание тестов).*

---

Для определения пороговых значений – воспользуйтесь формой POLICY CONFIGURATION. Форма вызывается через пункт меню:

*Configuration – SLA Policy – SLA Profile*

---

**IQMM - [logged as admin] - POLICY CONFIGURATION:**  
**POLICY CONFIGURATION**

add
 fill form
 CSV
 view
 change
 delete
 clear
 expert

Deploy on:		
Parameter	Value	Default
Policy ID	<input type="text"/>	
Policy name	<input type="text"/>	
Class (IP Precedence or DSCP)	<input type="text"/>	
Source zone	<input type="text"/>	
Destination zone	<input type="text"/>	
Number of violations enough to rise a problem	<input type="text"/>	1
Number of violations enough to down a problem	<input type="text"/>	0
Check horizon (min)	<input type="text"/>	60
Crimson action	<input type="text"/>	
Red action	<input type="text"/>	
Yellow action	<input type="text"/>	
Green action	<input type="text"/>	
Blue action	<input type="text"/>	
Description	<input type="text"/>	
Thresholds	<div style="border: 1px solid #ccc; padding: 2px;">                     AvgRTT-100-120-150 ▲                      AvgRtt-1000-2000-3000 ▲                      df_avg_500-700-900 ▲                      df_max_10-12-15 ▼                 </div>	

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 56 Форма конфигурации политик контроля

Значения полей описаны в таблице ниже:

Поле	Значение
Policy ID	Идентификатор, транслированный в Policy name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Policy name	Обязательное для заполнения поле. Уникальное символическое обозначение политики контроля. Допускается использование алфавитно-цифровых символов, пробелы.
Class (IP Precedence or DSCP)	<p>Класс сервиса, который будет использован в качестве критерия для автоматического назначения политики группе тестов. Если поле не заполнено – политику можно будет назначить только непосредственно на тест.</p> <p style="color: blue; font-style: italic;">Параметр необходим для группового назначения политики. Требуется одновременное определение трех</p>

Поле	Значение
	<p><i>параметров: Class, Source zone, Destination zone.</i></p> <p><i>Вместо зонального назначения политики, рекомендуется воспользоваться режимом массовой конфигурации для индивидуального.</i></p> <hr style="width: 50%; margin-left: auto; margin-right: 0;"/>
Source zone	<p>Зона инициатора теста, которая будет использована в качестве критерия для автоматического назначения политики группе тестов. Если поле не заполнено – политику можно будет назначить только непосредственно на тест.</p> <p><i>Параметр необходим для группового назначения политики. Требуется одновременное определение трех параметров: Class, Source zone, Destination zone.</i></p> <p><i>Вместо зонального назначения политики, рекомендуется воспользоваться режимом массовой конфигурации для индивидуального.</i></p> <hr style="width: 50%; margin-left: auto; margin-right: 0;"/>
Destination zone	<p>Зона инициатора теста, которая будет использована в качестве критерия для автоматического назначения политики группе тестов. Если поле не заполнено – политику можно будет назначить только непосредственно на тест.</p> <p><i>Параметр необходим для группового назначения политики. Требуется одновременное определение трех параметров: Class, Source zone, Destination zone.</i></p> <p><i>Вместо зонального назначения политики, рекомендуется воспользоваться режимом массовой конфигурации для индивидуального.</i></p> <hr style="width: 50%; margin-left: auto; margin-right: 0;"/>
Number of violations enough to rise a problem	<p>Количество нарушений, достаточное для срабатывание политики. В случае, если в заданном горизонте наблюдений, количество нарушений будет выше либо равно заданному, сработает политика, проводятся уведомления по профилю, соответствующему критичности нарушения.</p>
Number of violations enough to down a problem	<p>Количество нарушений, достаточное для перехода в зеленую зону. Возврат из состояния тревоги в нормальное состояние происходит в случае, если количество нарушений в заданном горизонте контроля ниже или равна заданной. Проводятся уведомления по зеленому профилю, если он назначен.</p>

Поле	Значение
Check horizon (min)	Горизонт контроля нарушений – плавающее временное окно в минутах, задаваемое текущим моментом и моментом в прошлом, на заданном интервале времени до этого момента. На этом промежутке осуществляется контроль нарушений.
Crimson action	Малиновый (красный) сигнал. Профиль действий, который будет выполнен, при срабатывании данного уровня тревоги.
Red action	Красный сигнал. Профиль действий, который будет выполнен, при срабатывании данного уровня тревоги.
Yellow action	Желтый сигнал. Профиль действий, который будет выполнен, при срабатывании данного уровня тревоги.
Green action	Зеленый сигнал. Профиль действий, который будет выполнен, при срабатывании данного уровня тревоги.
Blue action	Синий сигнал. Действие, которое будет выполнено, когда значение контролируемого параметра окажется ниже минимального значения.
Description	Краткое описание политики контроля.
Thresholds	<p>Группа пороговых значений, которые составят формируемую политику.</p> <p style="color: blue; text-align: center;"><i>Будьте внимательны! При назначении нескольких порогов на один и тот же параметр политика не будет работать.</i></p> <hr style="width: 50%; margin: auto;"/>

В системе по умолчанию заведены несколько политик контроля:

Policy name	policy_basic	policy_basic_ipvtv	policy_basic_web	stub
Class (IP Precedence or DSCP)				
Source zone				
Destination zone				
Number of violations enough to rise a problem	1	1	1	1
Number of violations enough to down a problem	0	0	0	0
Check horizon (min)	60	60	60	60

Policy name	policy_basic	policy_basic_iptv	policy_basic_web	stub
Crimson action	action_syslog	action_syslog	action_syslog	
Red action	action_syslog	action_syslog	action_syslog	
Yellow action	action_syslog	action_syslog	action_syslog	
Green action	action_syslog	action_syslog	action_syslog	
Blue action				
Description				Do not delete it
Thresholds	SDLoss-0.5-1-3 DSLloss-0.5-1-3 SDJitter-10-20-30 DSJitter-10-20-30 AvgRTT-100-120-150	mlr_avg_20_40_60 iat_avg_250_300_350 df_avg_500-700-900 vbr_avg_0.5	SDLoss-0.5-1-3 DSLloss-0.5-1-3 AvgRtt-1000-2000-3000	

Названия порогов содержат значения порогов yellow-red-crimson.

## Конфигурация срочного аларма (LIVEMON)

Время реакции системы мониторинга на аварию или ухудшение качественных характеристик зависит от нескольких факторов:

1. Периодичность измерения определяет максимальное время от возникновения устойчивой деградации до ее измерения.
2. Периодичность передачи информации о замерах в систему управления.
3. Периодичность вызова процедур обработки данных о замерах с последующим анализом выполнения требований политик контроля.

В стандартных настройках агент передает информацию о замерах раз в 5 минут, раз в 1 минуту происходит обработка и анализ данных в системе управления IQMM. При периодичности измерений раз в 5 минут, при наихудшем стечении обстоятельств, максимальное время обнаружения деградации будет 11 минут. В большинстве случаев этого вполне достаточно. В особенности, если учесть, что время устранения деградации может быть больше на 1-2-3 порядка. Однако, в редких ситуациях требуется получение информации о деградации непосредственно после ее обнаружения. Для этого разработан специальный режим работы агента LIVEMON, в котором первичный несложный анализ полученных измерений производит сам агент непосредственно после тестирования. Режим LIVEMON на агенте позволяет незамедлительно передавать сообщение о деградации измеренного параметра в систему управления.

Проверить, поддерживается ли режим LIVEMON можно запустив ПО агента с ключем -v:

```
# /usr/local/iqm_agent/iqm_agent -v
iqm agent
Version: 3-099001838
Tests available are: U0,U7,BW,GSS,I0,J0,J1,URL,CMD,C0,C1,C2,C3,TW,T1,DNS
Features available are: CDR,OOS,BWP,SSL,LIVEMON
```

Для конфигурации режима LIVEMON необходимо определить в тесте два параметра:

- **Live alarm expression** (ThresholdExpression): критерий срабатывания срочного уведомления, например: AvgRtt>10 (без пробелов!)

- **URL for live alarm action** (ThresholdAction): URL по которому будет передаваться срочное уведомление, например: `http://usr:pass@ip/iqm/recvlivemon.cgi?USER=u1&PASS=x1`

Возможно использовать только одно выражение в Live alarm expression. Поэтому необходимо задать требования к наиболее критичному параметру. В большинстве случаев этот параметр - потери. Более скрупулезный анализ измеренных значений на соответствие политикам контроля будет произведен в системе управления IQMM. Допустимые операции:

Операция	Значение	Пример	Комментарий
<	Меньше	SDBW < DSBW	Сигнализировать, если скорость от инициатора меньше скорости от сопряженного агента. (Возможно, бессмысленное условие, приводится для демонстрации)
<=	Меньше или равно	2.0<=MaxRtt	Сигнализировать, если максимальная круговая задержка больше либо равна 2 мс
>	Больше	AvgRtt>2.0	Сигнализировать, если средняя круговая задержка больше 2 мс
>=	Больше или равно	SDJitter>=50	Сигнализировать, если джиттер от инициатора выше 50 мс
=	Равно	ServiceCode=404	Сигнализировать, если ServiceCode равен 404
<>	Не равно	SDRemarkedPercent<>0	Сигнализировать, если процент перемаркированных пакетов не равен 0
!=	Не равно (аналог <>)	DSLostPercent!=0	Сигнализировать, если процент потерянных пакетов не равен 0

Параметры, которые допускается использовать в выражениях, приведены в таблице:

Параметр	тип
SDLost	uint
SDLostPercent	double
DSLost	uint
DSLostPercent	double
SDRemarked	uint
SDRemarkedPercent	double
DSRemarked	uint
DSRemarkedPercent	double
MinRtt	int
AvgRtt	int
MaxRtt	int
SDJitter	uint
DSJitter	uint
ServiceCode	uint
SDBytes	u_int64
DSBytes	u_int64
SDBW	u_int64
DSBW	u_int64
SDMinDelay	int

Параметр	тип
SDAvgDelay	int
SDMaxDelay	int
DSMinDelay	int
DSAvgDelay	int
DSMaxDelay	int

Для получения подробного описания значения параметров см. раздел "Измеряемые характеристики".

В системе управления IQMM предусмотрены специальные средства для поддержки Live-алармов, поступающих со стороны агента: HTTP-интерфейс в сторону агентов, модуль обработки сообщений, соответствующая структура в базе данных.

Значение URL для ThresholdAction имеет следующий вид:  
http://usr:pass@ip/iqm/recvlivemon.cgi? USER=u1&PASS=x1

- usr:pass - имя пользователя и пароль для авторизации на http - сервисе, задается при помощи утилиты htpasswd.
- USER=u1&PASS=x1 - пользователь и пароль для авторизации в системе регистрации срочных алармов (recvlivemon.cgi).

*Имя пользователя для аутентификации на http-сервисе а так же имя для авторизации на модуле IQM должны совпадать и иметь значение livemon.*

*Пример:*

*http://livemon:livemon@172.17.66.147/iqm/recvlivemon.cgi?USER=livemon&PASS=livemon*

---

Пользователь для авторизации запроса на регистрацию срочного аларма заводится через форму управления всеми пользователями системы (см. Пользователи IQMM).

*Administration --> IQMM Users*

---

Принципиально важно, чтобы у этого пользователя параметры были определены следующим образом:

- Authentication method = nosql
- Role ID = Rightless

Это специальный способ авторизации, который исключает возможность предоставления пользователю прав доступа к интерфейсу управления IQMM. В системе по умолчанию для проведения срочного информирования о нарушениях заведен пользователь livemon.

User name *	livemon
User pass *	Смените пароль
Authentication method	nosql
User description	Livemon system account
Allowed domains	*
Allowed networks1.2.3.4 1.*.3.* 1.2.3.0/24	*



Expiration YYYY-MM-DD [hh:mm:ss]	
<b>Role ID</b>	<b>Rightless</b>
Customer ID	
Map source URL	

**IQMM - [logged as admin] - USERS CONFIGURATION:**  
**USERS CONFIGURATION**

add
 fill form
 CSV
 view
 change
 delete
 clear
 expert

Deploy on:		
Parameter	Value	Default
User ID	livemon ▼	
User name *	livemon	
User pass *	c37fb8b77da93f15d0b025917a51	
Authentication method	nosql ▼	sql
User description	Livemon system account	
Allowed domains	*	
Allowed networks 1.2.3.4 1.*.3.* 1.2.3.0/24	*	
Expiration YYYY-MM-DD [hh:mm:ss]		
Role ID	Rightless ▼	
Customer ID	▼	
Map source URL		

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 57 Конфигурация пользователя для доставки срочных алармов

В целях дополнительной безопасности, идентификатор пользователя для срочных алармов должен быть занесен в таблицу custom\_livemon\_allow. Это делается в ручную при помощи SQL-запроса:

```
INSERT INTO custom_livemon_allow (user) SELECT user_id FROM users
WHERE user_name = 'livemon';
```

```
mysql> INSERT INTO custom_livemon_allow (user) SELECT user_id FROM users WHERE user_name =
'livemon';
Query OK, 1 row affected (0.06 sec)
Records: 1 Duplicates: 0 Warnings: 0

mysql> SELECT * FROM custom livemon allow;
+----+-----+
| id | user |
+----+-----+
| 1 | 5 |
+----+-----+
1 row in set (0.00 sec)
```

mysql>

В противном случае, запрос на регистрацию аларма авторизован не будет, даже при наличии корректно заведенного для этих целей пользователя. Об этом будет сделана запись в журнале агента:

```
[Dec 13 15:06:59.715]: [139681767343872;Error] lm-send-curl: Response
`http://192.168.0.188/iqm/recvlivemon.cgi?USER=u1&PASS=p1&TID=iqmm_www.yandex.ru_URL_BE&VAR=AvgRt
t&VAL=202&STATE=1': 403: ERR: You have no rights
```

Пример конфигурации теста со срочным алармом:

Test name *	iqmm_www.yandex.ru_URL_BE
Class (IP Precedence or DSCP)	BE
SLA policy profile	policy_basic_web
Live alarm expression (AvgRtt>10)	AvgRtt>100
URL for live alarm action(http://usr:pass@ip/iqm/recvlivemon.cgi?USER=u1&PASS=x1)	http://usr:pass@192.168.0.188/iqm/recvlivemon.cgi?USER=u1&PASS=p1
Service	L7 Internet
Provider	Default
SRC agent *	iqmm
DST agent *	www.yandex.ru
Test frequency (sec)	60
Number of probes	105
Number of probes to ignore	5
URL	https://www.yandex.ru/
URL-test query interval (ms)	100
Cookie file	/tmp/cookie-yandex.txt
HTTP User-Agent	Mozilla/5.0
Content download timeout	3
Test type	URL
Enabled	1
On demand test	0
External link	https://www.yandex.ru/

При конфигурации теста следует учесть, что на него должна быть назначена политика контроля (см. Управление SLA-политиками), в которой параметр из Live alarm expression ограничен crimson-порогом. Наличие политики необходимо для привязки live-аларма и последующего его наследования алармом системы управления.

**IQMM - [logged as admin] - TESTS CONFIGURATION:**  
**TESTS CONFIGURATION**

add
 get
 fill form
 CSV
 view
 change
 delete
 clear
 expert
 filter

Deploy on:	<input checked="" type="checkbox"/> On agent <input checked="" type="checkbox"/> On DB <input checked="" type="checkbox"/> Drop statistics when deleting	
Test ID	iqmm_www.yandex.ru_URL_BE	OnDemand
Test name *	iqmm_www.yandex.ru_URL_BE	
Class (IP Precedence or DSCP)	BE	1
SLA policy profile	policy_basic_web	
Live alarm expression (AvgRtt>10)	AvgRtt>100	
URL for live alarm action (http://usr:pass@ip/iqm/recvlivemon.cgi?USER=u1&PASS=x1)	http://[redacted]@192.168.0.18	
Service	L7 Internet	1
Provider	Default	
SRC agent *	iqmm	
DST agent *	www.yandex.ru	
Test frequency (sec)	60	600
Number of probes	105	200
Number of probes to ignore	5	
URL	https://www.yandex.ru/	
URL-test query interval (ms)	100	
Cookie file	/tmp/cookie-yandex.txt	
HTTP User-Agent	Mozilla/5.0	
Content download timeout	3	
Test type	URL	U0
Enabled	1	1
On demand test	0	1
External link	https://www.yandex.ru/	

Рисунок 58 Пример конфигурации теста со срочным алармом

В приведенном примере агент будет проверять параметр AvgRtt на превышение 100мс (AvgRtt>100). При выполнении заданного критерия будет выполнен HTTP-POST запрос по указанному URL (http://usr:pass@192.168.0.188/iqm/recvlivemon.cgi?USER=u1&PASS=p1). Дамп запроса-ответа будет подобен следующему:

```
POST /iqm/recvlivemon.cgi HTTP/1.1
Authorization: Basic XXXXXXXXXXXXXXXX=
Host: 192.168.0.188
Accept: */*
Content-Length: 104
Content-Type: application/x-www-form-urlencoded

USER=u1&PASS=p1&TID=iqmm_www.yandex.ru_URL_BE&VAR=AvgRtt&VAL=114&STATE=1
HTTP/1.1 200 OK
Date: Tue, 13 Dec 2016 16:29:57 GMT
Server: Apache/2.2.15 (CentOS)
```

```
Connection: close
Transfer-Encoding: chunked
Content-Type: text/plain; charset=utf-8

f
OK: insert data
HTTP/1.1 200 OK
Date: Tue, 13 Dec 2016 16:29:57 GMT
Server: Apache/2.2.15 (CentOS)
Connection: close
Transfer-Encoding: chunked
Content-Type: text/plain; charset=utf-8

f
OK: insert data
0
```

**После прохождения срочного аларма в журнале агента появится запись:**

```
[Dec 13 20:01:34.116]: [139680884438784;Informational] Test iqmm www.yandex.ru URL BE started:
NAT - 5.255.255.55 (www.yandex.ru)
[Dec 13 20:01:34.117]: [139681756854016;Informational] URL-test: url=https://www.yandex.ru/
cookie file=/tmp/cookie-yandex.txt user agent=Mozilla/5.0
[Dec 13 20:01:57.325]: [139680884438784;Informational] Test iqmm www.yandex.ru URL BE finished:
SDLost 0, SDLostPercent 0.000000, min 94 avg 119 max 233
[Dec 13 20:01:57.326]: [139680884438784;Informational] Test iqmm www.yandex.ru URL BE finished
[Dec 13 20:01:57.651]: [139681756854016;Informational] lm-send-curl: Response
`http://192.168.0.188/iqm/recvlivemon.cgi?USER=u1&PASS=p1&TID=iqmm_www.yandex.ru_URL_BE&VAR=AvgRt
t&VAL=119&STATE=1': 200: OK: insert data
```

Сообщение уровня Informational, для того, чтобы запись появилась в журнале iqm-агента требуется его запуск с соответствующим уровнем журналирования: --level=7.

**В таблице lm\_alarms появится запись:**

```
mysql> select * from lm_alarms limit 1;
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| id | lm_time_start | lm_time_end | lm_test_id | lm_policy_id | lm_value_table |
| lm_value_field | lm_class | lm_threshold | lm_status | lm_severity | lm_value |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | 2016-12-13 15:48:57 | 0000-00-00 00:00:00 | 14 | 3 | data_raw |
| AvgRtt | BE | 150.00 | UP | CRIMSON | 118.00 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql>
```

В случае, если на тест не назначена политика, аларм не будет зарегистрирован, а агент выдаст ошибку в журнале:

```
[Dec 13 20:16:54.781]: [139681756854016;Informational] Test iqmm www.yandex.ru URL BE finished
[Dec 13 20:16:55.097]: [139680884438784;Error] lm-send-curl: Response
`http://192.168.0.188/iqm/recvlivemon.cgi?USER=u1&PASS=p1&TID=iqmm_www.yandex.ru_URL_BE&VAR=AvgRt
t&VAL=225&STATE=1': 409: ERR: no test: no needs
```

В системе на базе функционала пользовательских отчетов (см. Создание пользовательских отчет) предустановлены два отчета по срочным и системным алармам, которые объединены в панель мониторинга. Панель доступна через пункт меню верхнего уровня:

*[Live alarms](#)*

---

Панель автоматически обновляется (при включенном autoupdate (min)) и позволяет наблюдать поступление срочного аларма и его последующий переход в системный.

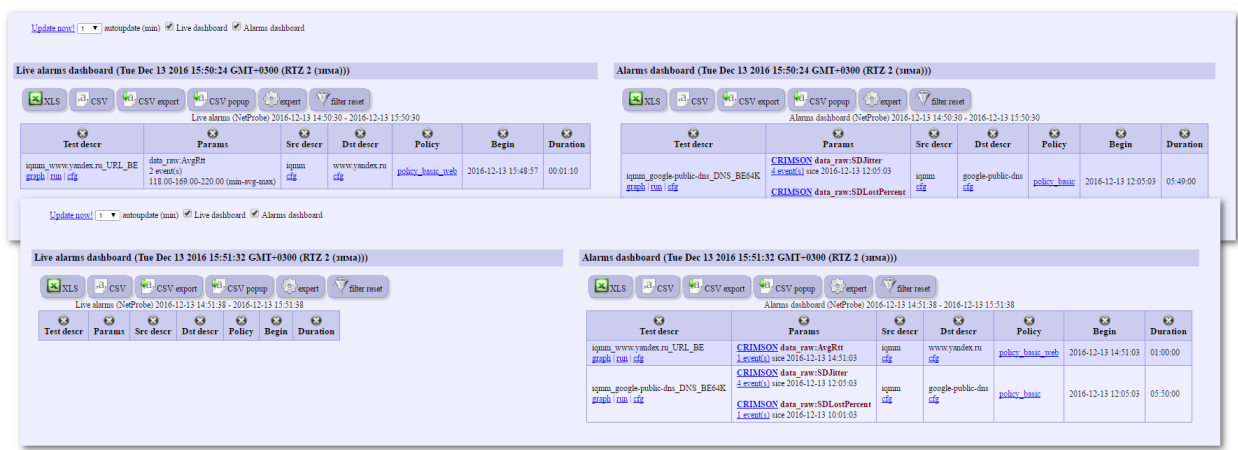


Рисунок 59 Прохождение срочного аларма на пользовательском табло мониторинга

*Можно создать собственный пользовательский отчет для отображения необходимых данных об алармах. (см. Создание пользовательских отчет)*

## Передача аларма через e-Mail

Чтобы получать по электронной почте сообщения о событиях, зафиксированных политиками контроля, для системы IQMM необходимо зарегистрировать учетную запись на почтовом сервере. Через нее система IQM будет отсылать почту. Информацию о порядке авторизации на почтовом сервере необходимо передать системе IQMM через конфигурационный файл /home/iqm/iqmm/iqmm-cfg.pl:

```
%gMail = (smtp=> 'mail.domain.ru',
  from    => 'iqm@domain.ru',
  auth    => LOGIN,
  authid  => 'iqm@domain.ru',
  authpwd => 'secret');
```

Для отправки сообщений используется модуль Mail::Sender, структура %gMail представляет собой хеш, передаваемый конструктору new Mail::Sender. В связи с этим допускается определение других параметров, принимаемых Mail::Sender. Для получения подробной информации - см. руководство по Mail::Sender.

Адресат для отправки сообщений заводится в форме MAILS CONFIGURATION (см. раздел Адресаты eMail) в меню:

*Configuration->Alarm Actions->e-Mails:*

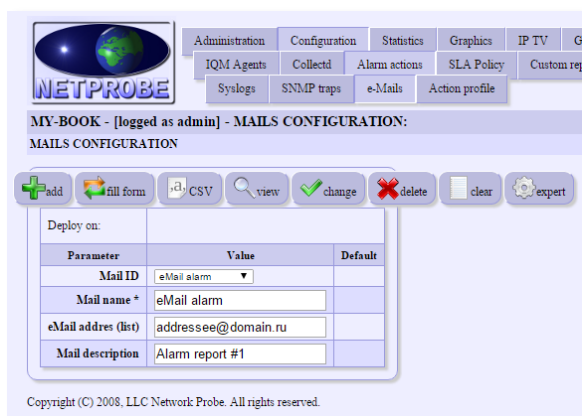


Рисунок 60 Конфигурация адресата

Допускается определение нескольких адресов в поле eMail address (list) через запятую. После этого необходимо обновить существующий профиль уведомления или создать новый в форме ALARM\_ACTIONS CONFIGURATION (см. раздел Профиль действий) в МЕНЮ:

*Configuration->Alarm Actions->Action Profile:*

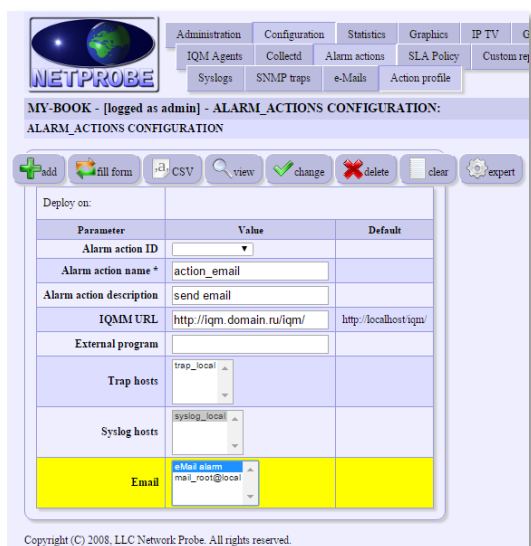


Рисунок 61 Конфигурация профиля уведомлений

Приведенный в примере профиль будет отсылать syslog и eMail сообщения. Созданный или обновленный профиль уведомления доступен для использования в политиках контроля (см. раздел Управление SLA-политиками) в меню:

*Configuration->SLA Policy->SLA Profile:*

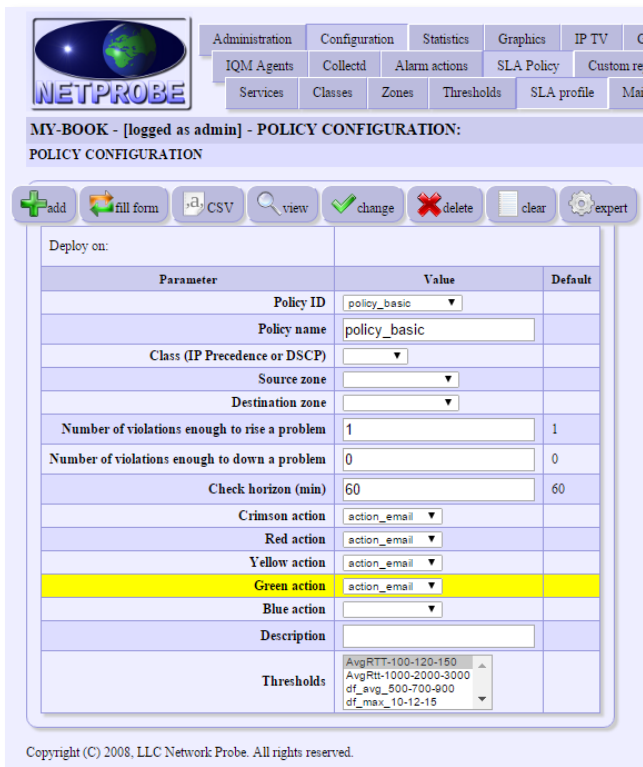


Рисунок 62 Конфигурация политики контроля

Определенную политику необходимо назначить тестам, результаты измерений которых она будет контролировать (см. раздел Создание тестов).

*Configuration->IQM Agents->Tests:*

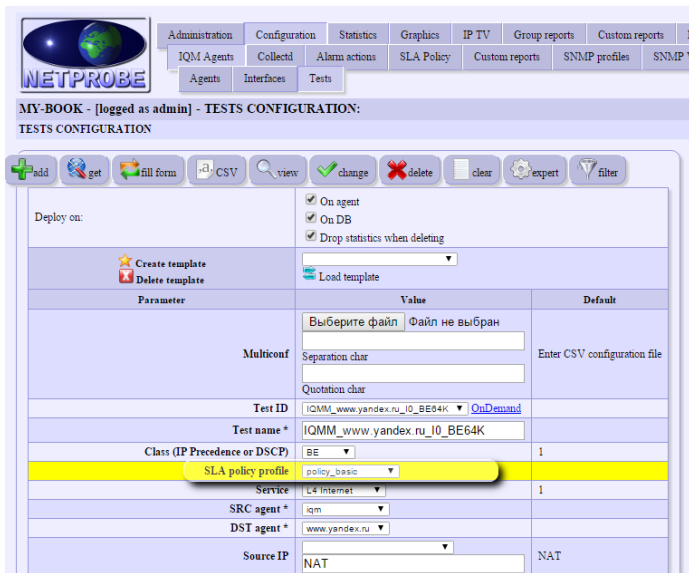


Рисунок 63 Назначение политики на тест

После назначения политики контроля на тест, система будет отсылать уведомления о зарегистрированных нарушениях на указанный почтовый адрес. Приходящие сообщения будут содержать:

- сводку по нарушению





- mongodb-org-tools-2.6.11-1.i686
- mongodb-org-shell-2.6.11-1.i686
- iqmm-perl-modules - комплект perl-модулей для IQM обвязки
- IQMM-обвязка:
  - iqmm-kernel - комплект perl-модулей,
  - iqmm-editor - комплект шаблонов, встраиваемых в административный интерфейс, для управления объектами,
  - iqmm-collectd - демон для обеспечения передачи данных из mongodb в MySQL

В силу особенностей функционирования collectdV в комплекте с SNMP-модулем возникла потребность в скоростной буферной базе данных для хранения промежуточных результатов, получаемых в результате опроса сетевых устройств по SNMP. В качестве такой буферной базы используется документ-ориентированная база MongoDB. Демон iqm-mongodb-mysqld (из пакета iqmm-collectd) осуществляет выборку данных из MongoDB в соответствии с тестовой конфигурацией и складывает данные в MySQL. Ниже приведена схема, иллюстрирующая взаимодействие между приложениями для обработки данных, получаемых коллектором через соответствующие адаптеры (в том числе и SNMP).

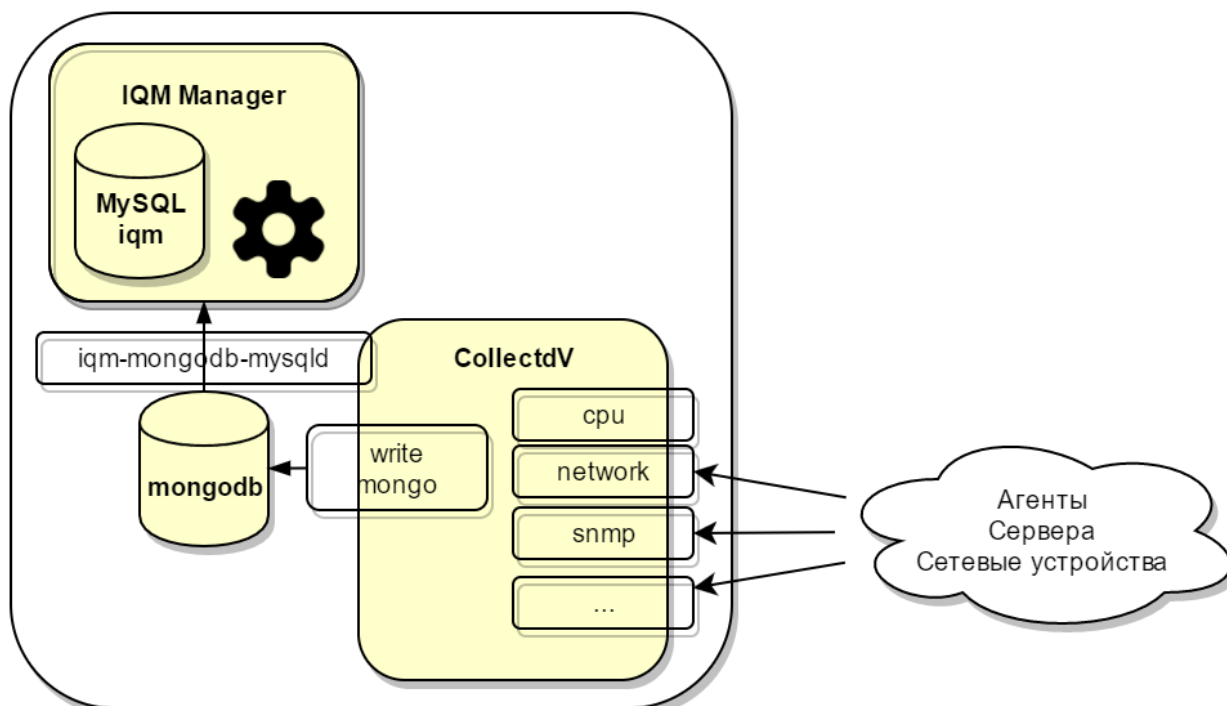


Рисунок 65 Информационные потоки между IQMM, MongoDB, CollectdV и сетевыми источниками

В базе mysql:iqm требуется наличие специальной структуры для конфигурации SNMP-объектов. Она должна быть создана на этапе установки SNMP-расширения для IQMM. Для манипуляций структурой данных в БД mysql:iqm в директории /home/iqm/iqmm/sql лежат SQL-скрипты с говорящими за себя названиями:

```
[maxim@CO6 iqmm]$ ls /home/iqm/iqmm/sql/collectd *  
/home/iqm/iqmm/sql/collectd_backup.sh  
/home/iqm/iqmm/sql/collectd_create.sql  
/home/iqm/iqmm/sql/collectd_drop.sql
```

Например, для создания структуры необходимо выполнить:

```
mysql -u root < collectd_create.sql
```

Crontab-планировщику назначается ряд задач:

```
[maxim@CO6 iqmm]$ sudo cat /etc/cron.d/iqmm-collectd
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=iqm
HOME=/
1,11,21,31,41,51 * * * * iqm /home/iqm/iqmm/scripts/iqm-collect-aggregator.pl -tables
iqm_collectd.aggr0
3 * * * * iqm /home/iqm/iqmm/scripts/iqm-collect-aggregator.pl -tables iqm_collectd.aggr1
33 1 * * * iqm /home/iqm/iqmm/scripts/iqm-collect-aggregator.pl -tables iqm_collectd.aggr2
```

Должны быть сконфигурированы init-скрипты:

```
[maxim@CO6 iqmm]$ chkconfig --list|grep -e iqm -e mongo -e collect
collectdV      0:выкл  1:выкл  2:вкл   3:вкл   4:вкл   5:вкл   6:выкл
iqma           0:выкл  1:выкл  2:вкл   3:вкл   4:вкл   5:вкл   6:выкл
iqmm           0:выкл  1:выкл  2:выкл  3:вкл   4:вкл   5:вкл   6:выкл
iqmm-collectd 0:выкл  1:выкл  2:выкл  3:вкл   4:вкл   5:вкл   6:выкл
iqmm-raw2sql  0:выкл  1:выкл  2:выкл  3:вкл   4:вкл   5:вкл   6:выкл
mongod         0:выкл  1:выкл  2:вкл   3:вкл   4:вкл   5:вкл   6:выкл
```

Запущенные процессы:

```
[maxim@CO6 iqmm]$ ps ax | grep -e iqm -e mongo -e collectdV
2307 ?        S          0:00 /bin/sh /etc/rc5.d/S55iqmm start
2405 ?        Ss         0:28 /usr/local/iqm agent/iqm agent --pid=/var/run/iqm agent.pid --
log=/usr/local/iqm agent/iqm agent.log --config=/etc/iqm agent.conf --level=7
2732 ?        Sl         1:13 /usr/bin/mongod -f /etc/mongod.conf
2766 ?        Ssl        0:03 /usr/sbin/collectdV -C /etc/collectdV.conf
2868 ?        Ss         0:00 iqm-mongodb-mysqld: listen
2869 ?        S          0:35 iqm-mongodb-mysqld: circle queue
2886 ?        S          0:04 iqm-raw2sql3d: sleep
```

## Конфигурирование коллектора CollectdV

*Подробное описание возможностей CollectdV выходит за рамки данного руководства, при необходимости, для получения более детальной информации необходимо обратиться к документации CollectdV. Документация на коллектор и плагины доступны через [man](http://man) либо на странице <https://collectd.org/>.*

### CollectdV

Конфигурация демона CollectdV находится в файле: `/etc/collectdV.conf`

```
#TypesDB      "/usr/share/collectdV/types.db" # путь к types-db
Hostname      "iqmm" # Имя хоста, на котором запущен CollectdV
FQDNLookup    false # Не использовать полные доменные имена
```

Файлы конфигурации плагинов находятся в директории: `/etc/collectdV.d/`

После изменения конфигурации CollectdV требуется произвести его перезапуск:

```
service collectdV start
```

### CollectdV mongodb

Для записи данных, собранных CollectdV в базу MongoDB необходим плагин `collectdV-mongodb`. Конфигурация CollectdV-плагины `mongodb` находится в файле:

```
/etc/collectdV.d/write_mongodb.conf
```

```
LoadPlugin write_mongodb
<Plugin write_mongodb>
  <Node "iqm">
    Host "localhost"
    Port "27017"
    Timeout 1000
    StoreRates true
  #
  # Database "auth_db"
  # User "auth user"
  # Password "auth passwd"
  </Node>
</Plugin>
```

### CollectdV network

Отправки и приема по сети данных, между коллекторами CollectdV, установленными на разных хост-машинах потребуется плагин collectdV-network. Конфигурация CollectdV-плагина network находится в файле:

/etc/collectdV.d/network.conf

Для отправки данных по сети следует настроить отсылку (Server), на ответной стороне - прием (Listen).

```
LoadPlugin network
<Plugin network>
#   # client setup:
#   Server "ff18::efc0:4a42" "25826"
#   <Server "239.192.74.66" "25826">
#       SecurityLevel Encrypt
#       Username "user"
#       Password "secret"
#       Interface "eth0"
#   </Server>
#   TimeToLive "128"
#
#   # server setup:
#   Listen "ff18::efc0:4a42" "25826"
#   <Listen "239.192.74.66" "25826">
#       SecurityLevel None
#       SecurityLevel Sign
#       AuthFile "/etc/collectd/passwd"
#       Interface "eth0"
#   </Listen>
#   MaxPacketSize 1024
#
#   # proxy setup (client and server as above):
#   Forward true
#
#   # statistics about the network plugin itself
#   ReportStats false
#
#   # "garbage collection"
#   CacheFlush 1800
</Plugin>
```

### CollectdV snmp

Для работы CollectdV по протоколу SNMP требуется плагин collectdV-snmp.

Конфигурация CollectdV плагина snmp находится в файле:

/etc/collectdV.d/snmp.conf

Плагин SNMP опрашивает сетевые устройства по SNMP, конвертирует полученные значения во внутренний формат CollectdV. Полученные данные передаются дальше с использованием плагинов записи. В системе управления IQMM используется collectdV-mongodb для записи значений в коллекции MongoDB.

Конфигурация содержит блоки:

- Блок Data содержит список значений, которые должны быть запрошены по SNMP

- Блок Host определяет сетевые узлы, которые должны быть опрошены по SNMP, определяет параметры SNMP протокола, содержит список блоков Data, для определения объектов, которые должны быть запрошены.

При конфигурации объектов Data block и Hosts в системе управления IQMM через WEB-интерфейс выводятся соответствующие блоки конфигурации плагина которые должны быть перенесены в файл конфигурации /etc/collectdV.d/snmp.conf, после чего потребуется перезагрузить коллектор.

## MongoDB

Файл конфигурации MongoDB находится в /etc/mongod.conf.

```
# Listen to local interface only. Comment out to listen on all interfaces.
bind ip=127.0.0.1

nohttpinterface = true
```

После изменения конфигурации MongoDB, потребуется перезапуск демона:

```
service mongod restart
```

## Конфигурирование SNMP-тестов


### Types.db. Управление именами наборов данных.

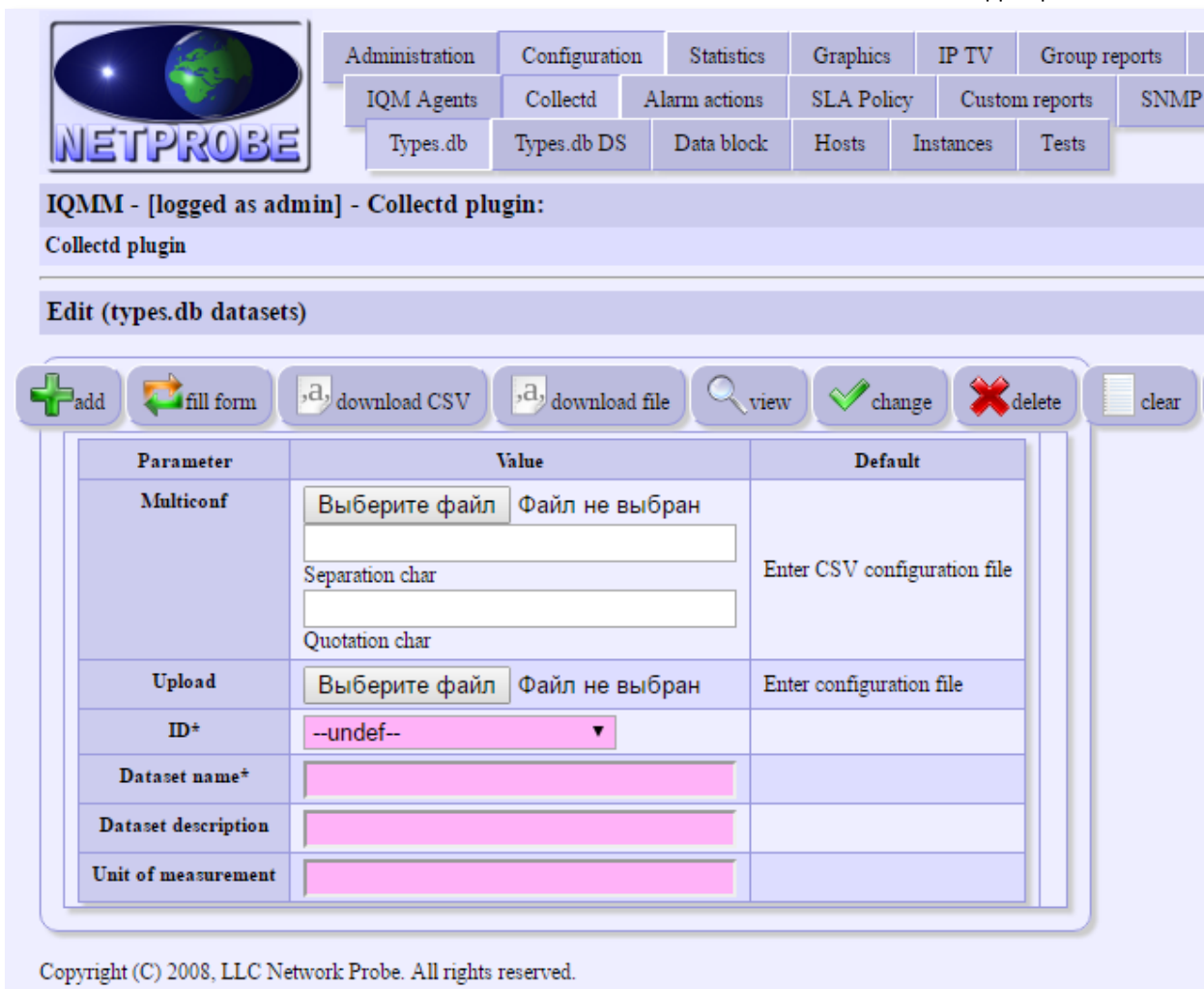
Пункт меню Types.db позволяет определить имена типов наборов данных (Dataset), дать им текстовые описания, задать единицы, в которых измерения будут представлены. Воспользуйтесь формой types.db datasets из плагина iqmm-collectd. Форма вызывается через пункт меню:

#### *Configuration – Collectd – Types.db*

---

Обычно, достаточно стандартного набора описанного в файле /usr/share/collectdV/types.db, файл принадлежит пакету collectdV. Перед началом конфигурирования SNMP-тестов рекомендуется занести описания типов данных из этого файла в базу IQMM. Для этого необходимо сохранить файл на локальном компьютере оператора. В форме Types.db

выбрать файл в строке Upload, и нажать на  Add. Система заберет имена датасетов из файла и занесет их в базу данных. Форма так же позволяет проводить импорт-экспорт данных через CSV-таблицу в режиме мультikonфигурации (см. раздел Режим массовой конфигурации) и вносить изменения в ручном режиме.



Administration Configuration Statistics Graphics IP TV Group reports  
 IQM Agents Collectd Alarm actions SLA Policy Custom reports SNMP  
 Types.db Types.db DS Data block Hosts Instances Tests

**IQMM - [logged as admin] - Collectd plugin:**  
 Collectd plugin

**Edit (types.db datasets)**


+ add ↻ fill form 📄 download CSV 📄 download file 🔍 view ✅ change ❌ delete 🗑 clear

Parameter	Value	Default
Multiconf	Выберите файл <input type="button" value="Файл не выбран"/> <input type="text"/> Separation char <input type="text"/> Quotation char <input type="text"/>	Enter CSV configuration file
Upload	Выберите файл <input type="button" value="Файл не выбран"/> <input type="text"/>	Enter configuration file
ID*	--undef-- ▼	
Dataset name*	<input type="text"/>	
Dataset description	<input type="text"/>	
Unit of measurement	<input type="text"/>	

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 66 Форма управления типами наборов данных

Поля формы имеют следующие значения:

Поле	Значение
Multiconf	Поле используется для осуществления массовой конфигурации имен наборов данных. Введите путь к CSV файлу, содержащий конфигурацию. Подробнее о формате файла см. в разделе Режим массовой конфигурации.
Upload	Поле специально выделено для загрузки данных из файла types.db. Сохраните файл на локальном компьютере оператора. Выберите путь к файлу types.db, нажмите  Add. Система заберет имена датасетов из файла и занесет их в базу данных.
ID	Идентификатор, транслированный в Dataset name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Dataset name	Обязательное для заполнения поле. Уникальное символическое имя типа набора данных.
Dataset description	Текстовое описание записи
Unit of measurement	Единица измерения, в которых следует отображать полученные данные. Текстовое поле.

### Types.db DS. Управление источниками данных.

Пункт меню Types.db DS позволяет определить источники данных для соответствующих наборов, задать параметры, осуществить привязку к таблицам базы данных.

Воспользуйтесь формой types.db datasources из плагина iqmm-collectd. Форма вызывается через пункт меню:

#### *Configuration – Collectd – Types.db DS*

---



Обычно, достаточно стандартного набора описанного в файле /usr/share/collectdV/types.db, файл принадлежит пакету collectdV. Перед началом конфигурирования SNMP-тестов рекомендуется занести конфигурацию источников данных из этого файла в базу IQMM сразу же после занесения имен наборов данных (см. раздел Types.db. Управление именами наборов данных.). Для этого необходимо сохранить файл на локальном компьютере оператора. В форме Types.db DS выбрать файл в строке Upload, и нажать на  Add. Система заберет конфигурацию источников для датасетов из файла и занесет их в базу данных. Форма так же позволяет проводить импорт-экспорт данных через CSV-таблицу в режиме мультikonфигурации (см. раздел Режим массовой конфигурации) и вносить изменения в ручном режиме.

Рисунок 67 Форма управления источниками данных (Datasource) для наборов (Datasets)

Поля формы имеют следующие значения:

Поле	Значение
Multiconf	Поле используется для осуществления массовой конфигурации источников для наборов данных. Введите путь к CSV файлу, содержащий конфигурацию. Подробнее о формате файла см. а разделе Режим массовой конфигурации.
Upload	Поле специально выделено для загрузки данных из файла types.db. Сохраните файл на локальном компьютере оператора. Выберите путь к файлу types.db, нажмите  Add. Система заберет конфигурацию для датасетов из файла и занесет их в базу данных.

Поле	Значение
ID	Идентификатор, транслированный в Datasource name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Datasource name	Обязательное для заполнения поле. Уникальное символическое имя для записи об источнике для набора данных.
Dataset	Идентификатор, транслированный в имя типа набора данных (Dataset name). Определяет к какому набору данных принадлежит источник.
DS value name	Имя источника.
SQL field name	Имя поля в MySQL базе, в которое будут записываться полученные значения
Data type	<p>Тип данных. Возможные типы аналогичны используемым в кольцевой БД RRD:</p> <ul style="list-style-type: none"> <li>• COUNTER - счетчик. Используется для постоянно возрастающих или убывающих величин, например, объем переданного трафика. Сохраняется разница текущего и предыдущего значений.</li> <li>• GAUGE - шкала. Используется для хранения величины параметра. Сохраняется само значение, без изменений, как есть.</li> <li>• DERIVE - модификация счетчика, позволяющая хранить значения величин, которые могут возрастать и убывать. Сохраняется разница текущего и предыдущего значений. Разница может быть отрицательной. Не производится проверка на переполнение. Для этого типа часто используют ограничения границ, например: MIN=0</li> <li>• ABSOLUTE - модификация счетчика, разница между значениями не вычисляется, а сохраняются сами значения счетчика и счетчик обнуляется при чтении. Этот тип удобно использовать для подсчета количества событий, произошедших с момента последнего считывания.</li> </ul> <p>В системе не предусмотрен тип COMPUTE - вычисляемый, который используется для записи вычисляемых значений на основании данных из других источников данных.</p>
Data minimum	Ограничение на минимальное значение величины параметра
Data maximum	Ограничение на максимальное значение величины параметра
Aggregated function	<p>Агрегирующая функция. Определяет способ вычисления значения на периоде агрегации. Возможны значения:</p> <ul style="list-style-type: none"> <li>• LAST - использовать последнее значение из периода</li> <li>• SUM - использовать сумму значений на периоде</li> <li>• AVG - арифметическое среднее всех значений на периоде</li> <li>• MAX - минимальное значение на периоде</li> <li>• MIN - максимальное значение на периоде</li> </ul> <p style="text-align: center;"><i>При загрузке данных из файла types.db каждой записи об источнике назначается умолчательная агрегирующая функция LAST.</i></p>



Поле	Значение
	<p><i>Для ряда величин рекомендуется ее поменять. Например, для</i></p> <p><i>if_octets:rx</i></p> <p><i>if_octets:tx</i></p> <p><i>поменять <u>Aggregated function = AVG</u></i></p>
User defined function	Функция пользователя
Datasource description	Текстовое описание записи

### SNMP-plugin. Конфигурация Datablocks.

Пункт меню Datablocks позволяет сформировать конфигурацию SNMP-плагина CollectdV для определения списка/таблицы величин, которые будут опрашиваться плагином по SNMP (Data block в руководстве collectd-snmp(5)). Воспользуйтесь формой Datablocks из плагина iqmm-collectd. Форма вызывается через пункт меню:

*Configuration – Collectd – Datablocks*

The screenshot shows the 'Edit (Datablocks)' configuration page in the NetProbe interface. The breadcrumb path is 'Configuration – Collectd – Datablocks'. The page title is 'IQMM - [logged as admin] - Collectd plugin: Collectd plugin'. The main heading is 'Edit (Datablocks)'. Below the heading is a toolbar with icons for add, fill form, download CSV, view, change, delete, clear, expert, and filter. The configuration form consists of a table with the following fields:

Parameter	Value	Default
Multiconf	Выберите файл <input type="text"/> Файл не выбран Separation char <input type="text"/> Quotation char <input type="text"/>	Enter CSV configuration file
ID*	traffic	
Datablock name*	traffic	
Plugin name	snmp	snmp
Instance exists	YES	YES
Instance aggregated ds	NO	NO
Dataset*	if_octets	
Datablock description	Traffic value	

On the right side of the form, there is a preview of the generated XML configuration:

```
<Plugin snmp>
  <Data "traffic">
    Type "if_octets"
    Table true
    Instance "XXXX"
    Values "OID" "OID"
    # InstancePrefix String
    # Scale 1.0
    # Shift 0.0
  </Data>
</Plugin>
```

At the bottom of the page, the copyright notice reads: 'Copyright (C) 2008, LLC Network Probe. All rights reserved.'

Рисунок 68 Форма конфигурации Data block для SNMP-плагина CollectdV

При заведении объекта Datablock в базе, так же при заполнении формы конфигурационными значениями для выбранного идентификатора, в правом блоке формы выдается текстовая конфигурация для плагина (см. Рисунок 68), которая с минимальными корректировками должна быть перенесена в файл /etc/collectdV.d/snmp.conf.

```
LoadPlugin snmp
<Plugin snmp>
  <Data "traffic">
    Type "if_octets"
    Table true
    Instance "IF-MIB::ifDescr"
    Values "IF-MIB::ifInOctets" "IF-MIB::ifOutOctets"
  # InstancePrefix String
  # Scale 1.0
  # Shift 0.0
  </Data>

  <Host "iqmm">
    Address "192.168.0.2"
    Community "public"
    Version 2
    Collect "traffic"
    Interval 60
  </Host>
</Plugin>
```

После изменения конфигурации плагина требуется перезагрузить CollectdV.

```
[root@CO6 ~]# service collectdV restart
Останавливается collectdV: [ OK ]
Запускается collectdV: [ OK ]
[root@CO6 ~]#
```

Если блок конфигурации Host не определен, перезагрузка коллектора не требуется.

Поля формы имеют следующие значения:

Поле	Значение
Multiconf	Поле используется для осуществления массовой конфигурации источников для наборов данных. Введите путь к CSV файлу, содержащий конфигурацию. Подробнее о формате файла см. а разделе Режим массовой конфигурации.
ID	Идентификатор, транслированный в Datablock name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Datablock name	Обязательное для заполнения поле. Уникальное символическое имя для записи Datablock.
Plugin name	Имя плагина, для которого формируется конфигурация. <ul style="list-style-type: none"> <li>• snmp</li> <li>• cru</li> <li>• network</li> </ul> Внесение изменений в конфигурацию /etc/collectdV.d/snmp.conf с последующей перезагрузкой CollectdV требуется только для snmp-плагина.
Instance exists	YES - таблица значений NO - список
Instance aggregated ds	Агрегируемые экземпляры
Dataset	Набор данных (см. раздел Types.db. Управление именами наборов данных.)
Datablock description	Текстовое описание записи

### SNMP-plugin. Конфигурация Hosts.

Пункт меню Hosts позволяет сформировать конфигурацию SNMP-плагина CollectdV для определения хостов, подлежащих опросу по SNMP (Host block в руководстве collectd-snmp(5)). Воспользуйтесь формой Hosts из плагина iqmm-collectd. Форма вызывается через пункт меню:

*Configuration – Collectd – Hosts*

Parameter	Value	Default
Multiconf	<input type="text" value="Выберите файл"/> <input type="text" value="Файл не выбран"/> Separation char <input type="text"/> Quotation char <input type="text"/>	Enter CSV configuration file
ID*	iqmm	
Host name*	iqmm	
Host IP address*	192.168.0.2	
SNMP profile*	public	
Zone*	Столицы	
Datablocks*	cpu traffic traffic2	
Interval	60	60
Device description	IQMM	
Status	UP	UP
Customer	--undef--	
Geolocation		

```

<Plugin snmp>
  <Host "iqmm">
    Address "192.168.0.2"
    Community "public"
    Version 2
    Collect "traffic"
    Interval 60
  </Host>
</Plugin>
    
```

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 69 Форма конфигурации Host block для SNMP-плагина CollectdV

При заведении объекта Host в базе, так же при заполнении формы конфигурационными значениями для выбранного идентификатора, в правом блоке формы выдается текстовая

конфигурация для плагина (см. Рисунок 68), которая должна быть перенесена в файл `/etc/collectdV.d/snmp.conf`.

```
LoadPlugin snmp
<Plugin snmp>
  <Data "traffic">
    Type "if_octets"
    Table true
    Instance "IF-MIB::ifDescr"
    Values "IF-MIB::ifInOctets" "IF-MIB::ifOutOctets"
  # InstancePrefix String
  # Scale 1.0
  # Shift 0.0
  </Data>

  <Host "iqmm">
    Address "192.168.0.2"
    Community "public"
    Version 2
    Collect "traffic"
    Interval 60
  </Host>
</Plugin>
```

После изменения конфигурации плагина требуется перезагрузить CollectdV.

```
[root@CO6 ~]# service collectdV restart
Останавливается collectdV: [ OK ]
Запускается collectdV: [ OK ]
[root@CO6 ~]#
```

Поля формы имеют следующие значения:

Поле	Значение
Multiconf	Поле используется для осуществления массовой конфигурации источников для наборов данных. Введите путь к CSV файлу, содержащий конфигурацию. Подробнее о формате файла см. а разделе Режим массовой конфигурации.
ID	Идентификатор, транслированный в Host name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Host name	Обязательное для заполнения поле. Уникальное символическое имя для записи Host.
Host IP address	IP адрес устройства, подлежащего SNMP опросу.
SNMP profile	Профиль SNMP, определяющий параметры протокола для проведение опроса, в частности community. Управление SNMP-профилями осуществляется через пункт меню:  <a href="#"><u>Configuration --&gt; SNMP profiles</u></a>
Zone	Географическая зона, в которой устройство размещено. См. Управление зонами.
Datablocks	Список данных, структур Datablocks, которые надо запрашивать у устройства. Необходимо наличие опрашиваемых структур в конфигурационном файле <code>/etc/collectdV.d/snmp.conf</code> . См. SNMP-plugin. Конфигурация Datablocks.
Interval	Интервал опроса в секундах. По умолчанию устанавливается минимально разумное значение 60 сек. Приблизительно соответствует периоду обновления счетчиков на интерфейсах. Проведение опроса с большей частотой приведет к повышению нагрузки на сервер, сеть и само устройство, при этом меньшая

Поле	Значение
	гранулярность достигнута не будет.
Device description	Текстовое описание устройства, которое будет опрашиваться по SNMP
Status	Операционный статус устройства
Customer	Идентификатор клиента
Geolocation	Географические координаты

### Datablock instances. Экземпляры блоков данных.

Назначенные для пороса блоки данных могут содержать множество экземпляров (instances) объектов, по которым допускается сбор статистики. Так, например, таблица интерфейсов может содержать несколько интерфейсов, в зависимости от их физического наличия и логической конфигурации. Оператору предоставлена возможность выбора всей таблицы либо ограниченного списка экземпляров для отображения в результатах теста.

После создания объектов Data block, Host block, переноса их конфигурации в /etc/collectdV.d/snmp.conf и рестарта коллектора коллектор начнет опрос данных с заданных устройств. Список полученных экземпляров из считанных с устройств блоков данных система автоматически будет заносить в таблицу Instances. Время, требуемое на автоматическое заполнение таблицы, зависит от объема запрашиваемых данных, периодичности опроса и производительности устройств, сети и сервера. Таким образом, предлагаемая форма служит для контроля работы коллектора. Имя экземпляра формируется как:

*<Host block name>:<Data block name>:<Instance name>*

---

- Host block name - имя блока Host (см. SNMP-plugin. Конфигурация Datablocks.).
- Data block name - имя блока Data (см. SNMP-plugin. Конфигурация Hosts.).
- Instance name - имя экземпляра, получаемое из таблицы, определяемой параметром Instance (например, "IF-MIB::ifDescr").


Пункт меню Datablock instances позволяет просмотреть экземпляры блоков данных, которые впоследствии могут быть использованы при отображении результатов измерений для условного теста. Воспользуйтесь формой Datablock instances из плагина iqmm-collectd. Форма вызывается через пункт меню:

*Configuration – Collectd – Instances*

---

The screenshot displays the 'Edit (Datablock instances)' page in the IQM Manager. At the top, there is a navigation menu with various categories: Administration, Configuration, Statistics, Graphics, IP TV, Group reports, Custom reports, and SNMP profile. Below this, there are sub-menus for IQM Agents, Collectd, Alarm actions, SLA Policy, Custom reports, and SNMP profile. Further down, there are buttons for Types.db, Types.db DS, Data block, Hosts, Instances, and Tests. The main header indicates the user is logged as 'admin' and is viewing the 'Collectd plugin' configuration. The central part of the page is a form titled 'Edit (Datablock instances)'. Above the form is a toolbar with icons for adding, filling, downloading CSV, viewing, changing, deleting, clearing, expert mode, and filtering. The form itself has three columns: 'Parameter', 'Value', and 'Default'. The 'Multiconf' parameter has a file selection button and text 'Выберите файл' and 'Файл не выбран', with a note 'Enter CSV configuration file'. Other parameters include 'ID\*' (dropdown), 'Instance full name\*' (text input), 'Host\*' (dropdown), 'Datablock\*' (dropdown), and 'Instance short name\*' (text input). At the bottom of the page, there is a copyright notice: 'Copyright (C) 2008, LLC Network Probe. All rights reserved.'

Рисунок 70 Форма управления Datablock instances

В наличии новых экземпляров можно убедиться просмотрев их в списке ID, либо нажатием на кнопку  View.

Поля имеют следующие значения:

Поле	Значение
Multiconf	Поле используется для осуществления массовой конфигурации источников для наборов данных. Введите путь к CSV файлу, содержащий конфигурацию. Подробнее о формате файла см. а разделе Режим массовой конфигурации.
ID	Идентификатор, транслированный в Instance full name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Instance full name	Обязательное для заполнения поле. Уникальное символическое имя для экземпляра блока данных.
Host	имя блока Host (см. SNMP-plugin. Конфигурация Datablocks.).
Datablock	имя блока Data (см. SNMP-plugin. Конфигурация Hosts.).
Instance short name	имя экземпляра, получаемое из таблицы, определяемой параметром Instance (например, "IF-MIB::ifDescr").

### Tests. Формирование трестов.

После определения блоков Data и Host в файле /etc/collectdV.d/snmp.conf SNMP-плагина CollectdV и перегрузки коллектора, коллектор начнет опрос хостов, определенных в блоках Hosts по SNMP. Данные, собираемые коллектором передаются в документ-ориентированную базу mongoDB через write\_mongodb-плагин. Данные от коллектора складываются в базе collectd в коллекции snmp. В поступлении данных можно убедиться с помощью клиента mongo:

```
$ mongo
> use collectd
> db.snmp.find()
> db.snmp.count()
```

```
$ mongo
MongoDB shell version: 2.4.8
connecting to: test
Server has startup warnings:
Fri Oct 30 11:08:23.603 [initandlisten]
Fri Oct 30 11:08:23.603 [initandlisten] ** NOTE: This is a 32 bit MongoDB binary.
Fri Oct 30 11:08:23.603 [initandlisten] **      32 bit builds are limited to less than 2GB of
data (or less with --journal).
Fri Oct 30 11:08:23.603 [initandlisten] **      Note that journaling defaults to off for 32 bit
and is currently off.
Fri Oct 30 11:08:23.603 [initandlisten] **      See http://dochub.mongodb.org/core/32bit
Fri Oct 30 11:08:23.604 [initandlisten]
> use collectd
switched to db collectd
> db.snmp.find()
{ "_id" : ObjectId("58612d404fe138688a994796"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "Vlan1", "values" : [ 2 ], "dstypes" : [ "gauge" ],
"dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a994797"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "Vlan20", "values" : [ 1 ], "dstypes" : [ "gauge" ],
"dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a994798"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "Vlan451", "values" : [ 1 ], "dstypes" : [ "gauge" ],
"dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a994799"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_1", "values" : [ 2 ], "dstypes" : [
"gauge" ], "dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a99479a"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_2", "values" : [ 1 ], "dstypes" : [
"gauge" ], "dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a99479b"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_3", "values" : [ 2 ], "dstypes" : [
"gauge" ], "dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a99479c"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_4", "values" : [ 1 ], "dstypes" : [
"gauge" ], "dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a99479d"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_5", "values" : [ 1 ], "dstypes" : [
"gauge" ], "dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a99479e"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_6", "values" : [ 2 ], "dstypes" : [
"gauge" ], "dsnames" : [ "value" ] }
```



```

{ "_id" : ObjectId("58612d404fe138688a99479f"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_7", "values" : [ 1 ], "dstypes" : [
"gauges" ], "dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a9947a0"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_8", "values" : [ 1 ], "dstypes" : [
"gauges" ], "dsnames" : [ "value" ] }
{ "id" : ObjectId("58612d404fe138688a9947a1"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_9", "values" : [ 2 ], "dstypes" : [
"gauges" ], "dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a9947a2"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "GigabitEthernet0_10", "values" : [ 1 ], "dstypes" : [
"gauges" ], "dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a9947a3"), "time" : ISODate("2016-12-26T14:44:24.946Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "Null0", "values" : [ 1 ], "dstypes" : [ "gauges" ],
"dsnames" : [ "value" ] }
{ "_id" : ObjectId("58612d404fe138688a9947a4"), "time" : ISODate("2016-12-26T14:46:24.901Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" : "if_octets",
"type_instance" : "Vlan1", "values" : [ 0, 0 ], "dstypes" : [ "gauges", "gauges" ], "dsnames" :
[ "rx", "tx" ] }
{ "id" : ObjectId("58612d404fe138688a9947a5"), "time" : ISODate("2016-12-26T14:46:24.901Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" : "if_octets",
"type_instance" : "Vlan20", "values" : [ 0, 0 ], "dstypes" : [ "gauges", "gauges" ], "dsnames" :
[ "rx", "tx" ] }
{ "_id" : ObjectId("58612d404fe138688a9947a6"), "time" : ISODate("2016-12-26T14:46:24.901Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" : "if_octets",
"type_instance" : "Vlan451", "values" : [ 36.875128794057616, 44.050153854325096 ], "dstypes" :
[ "gauges", "gauges" ], "dsnames" : [ "rx", "tx" ] }
{ "_id" : ObjectId("58612d404fe138688a9947b2"), "time" : ISODate("2016-12-26T14:46:24.947Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "Vlan1", "values" : [ 2 ], "dstypes" : [ "gauges" ],
"dsnames" : [ "value" ] }
{ "id" : ObjectId("58612d404fe138688a9947b3"), "time" : ISODate("2016-12-26T14:46:24.947Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "Vlan20", "values" : [ 1 ], "dstypes" : [ "gauges" ],
"dsnames" : [ "value" ] }
{ "id" : ObjectId("58612d404fe138688a9947b4"), "time" : ISODate("2016-12-26T14:46:24.947Z"),
"host" : "customer-sw-5200", "plugin" : "snmp", "plugin_instance" : "", "type" :
"if_oper_status", "type_instance" : "Vlan451", "values" : [ 1 ], "dstypes" : [ "gauges" ],
"dsnames" : [ "value" ] }
Type "it" for more
>

```

MongoDB представляет промежуточное хранилище, в котором складываются временные данные, полученные по SNMP. За передачу данных из MongoDB в MySQL в соответствии с тестовой конфигурацией отвечает `iqm-mongodb-mysqld` - демон из состава пакета `iqmm-collectd`.

Пункт меню Tests позволяет сгруппировать собираемые данные для отображения в едином блоке. Воспользуйтесь формой `Collectd tests` из плагина `iqmm-collectd`. Форма вызывается через пункт меню:

### [Configuration – Collectd – Tests](#)



Administration Configuration Statistics Graphics Group reports Map (hour) Help

IQM Agents Collectd Custom Alarm actions SLA Policy SNMP profiles

Types.db Types.db DS Data block Hosts Instances Tests

MY-BOOK - [logged as admin] - Collectd plugin:  
Collectd plugin

Edit (Collectd tests)

+ add fill form download CSV view change delete clear expert filter

Deploy on:  
 On agent  
 On DB  
 Drop statistics when deleting

Parameter	Value	Default
Multiconf	Выберите файл Файл не выбран Separation char Quotation char	Enter CSV configuration file
ID*	..._port0_7	
Test name*	..._port0_7	
Test aggregated function	NONE	NONE
Test aggregated user-defined function		
Status	UP	UP
Policy	--undef--	
Datablocks	localdomain:CPU status if_octets	
Instances	:GigabitEthernet0_4 :GigabitEthernet0_5 :GigabitEthernet0_6 :GigabitEthernet0_7	
Test description	Ge0/7	
Source host for map	--undef--	
Destination host for map	--undef--	
Customer	--undef--	

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 71 Форма конфигурации SNMP-теста

Поля имеют следующие значения:

Поле	Значение
Multiconf	Поле используется для осуществления массовой конфигурации источников для наборов данных. Введите путь к CSV файлу, содержащий конфигурацию. Подробнее о формате файла см. а разделе Режим массовой конфигурации.

Поле	Значение
ID	Идентификатор, транслированный в Test name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Test name	Обязательное для заполнения поле. Уникальное символическое имя теста, представляющего набор данных для отображения в одном отчете.
Test aggregated function	Агрегирующая функция теста
Test aggregated user-defined function	Пользовательская агрегирующая функция теста
Status	Операционный статус
Policy	Профиль политики контроля. Позволяет назначить на тест политику контроля параметров, определенных в разделе <b>Ошибка! Источник ссылки не найден..</b>
Datablocks	Полный список/таблица величин (см. Data block в руководстве collectd-snmp(5)), которые будут переноситься из временной базы MongoDB в MySQL для формирования отчетов
Instances	В случае, если существуют экземпляры блоков данных (Instances), параметр позволяет выбрать конкретные интересующие экземпляры, например, выбрать нужные интерфейсы на конкретном устройстве.
Test description	Необязательное поле. Краткое описание теста.
Source host for map	Агент-источник для отображения на карте
Destination host for map	Агент-получатель для отображения на карте
Customer	Идентификатор клиента

После создания теста, данные начнут переноситься в постоянные таблицы MySQL и будут доступны для формирования отчетов.

### Отчеты по SNMP-тестам

SNMP-обвязка для системы управления IQM содержит в предустановленные базовые отчеты. Блок меню Statistics -> Collectd содержит пункты позволяющие просмотреть результаты измерений для условных SNMP-тестов в графическом режиме, получить табличные данные. Для получения доступа к агрегированным данным воспользуйтесь одной из форм Collectd <aggregation period> statistics. Для получения доступа к сырым не усредненным данным воспользуйтесь формой Collectd raw statistics из плагина iqmm-collectd. Форма вызывается через пункт меню:

*Statistics – Collectd – RAW*

---

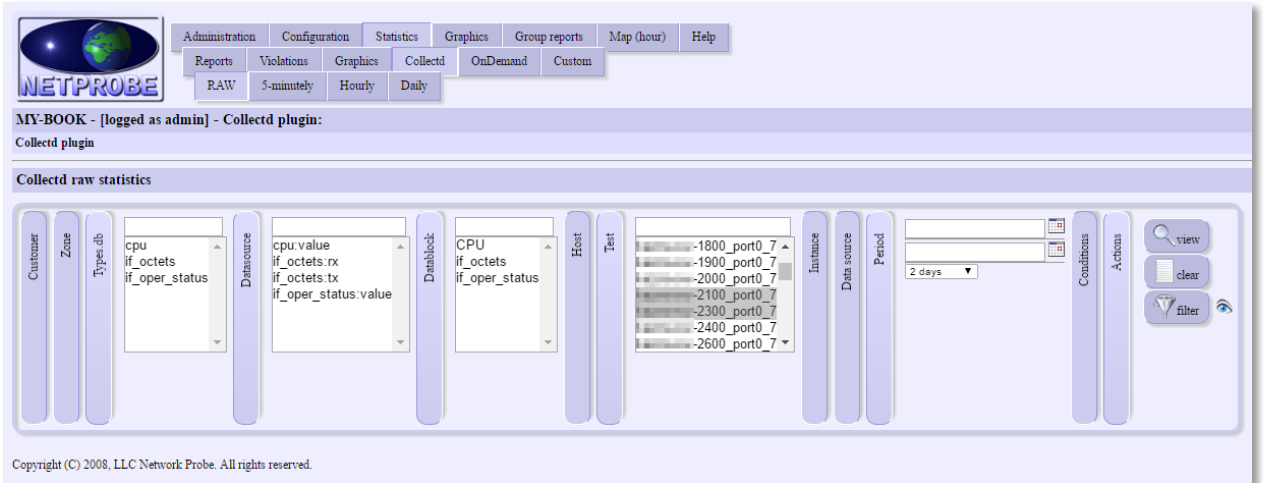


Рисунок 72 Фильтр формы запроса графических отчетов по SNMP-тестам

Форма содержит инструментарий (см. раздел Фильтры) для фильтрации запрашиваемых данных по различным признакам: клиентам, зонам, наборам данных (types db), источникам данных (datasources), блокам данных (datablocks), хостам, SNMP-тестам, экземплярам данных.

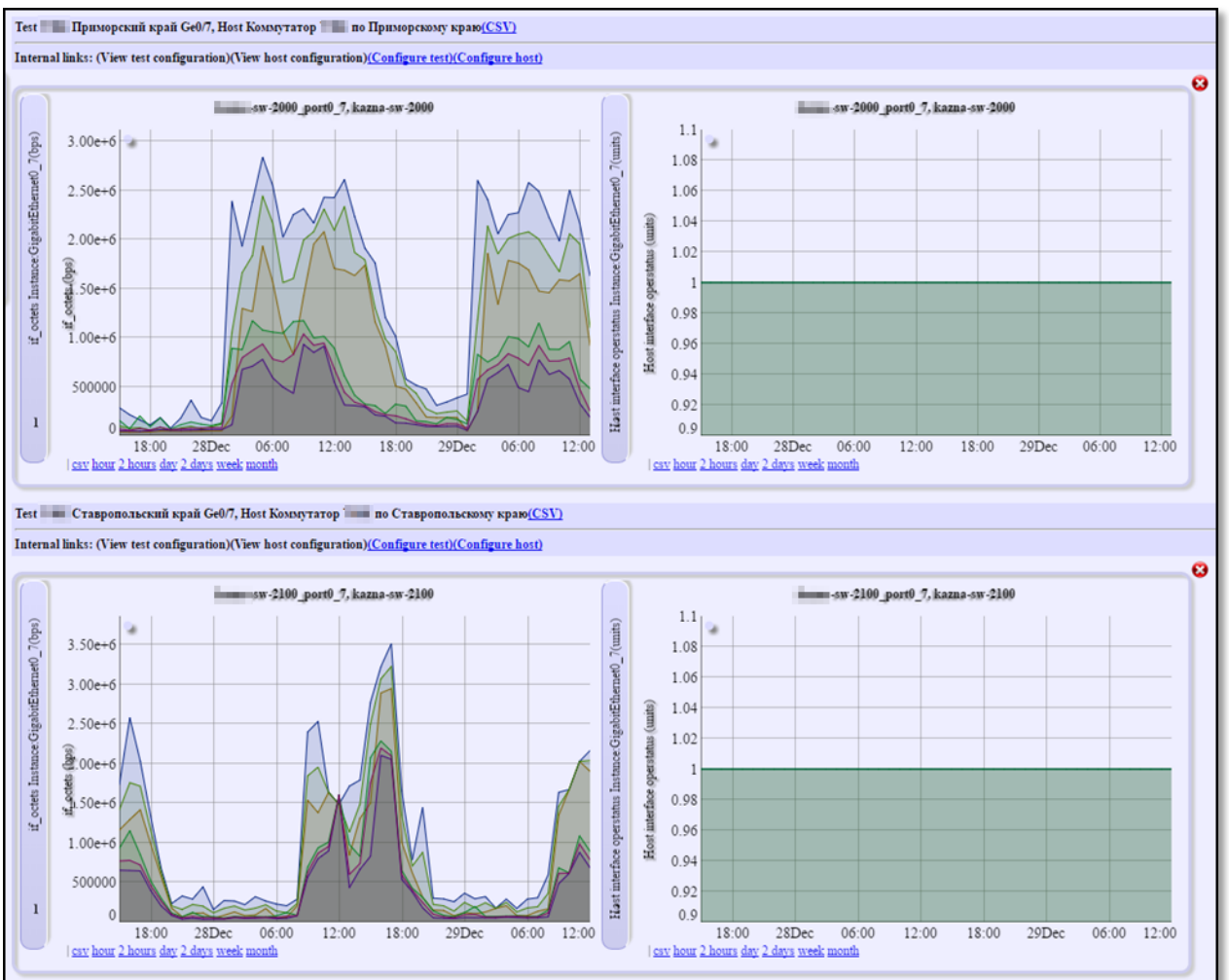


Рисунок 73 Графические отчеты по SNMP-тестам

## Диагностирование неисправностей в работе SNMP-плагина

Процесс сбора данных по SNMP задействует несколько независимых программных и технических средств. При возникновении сбоев в получении SNMP-данных для поиска неисправного звена требуется понимание всего процесса получения и обработки данных. Обратитесь к разделу Программное обеспечение для получения подробностей.

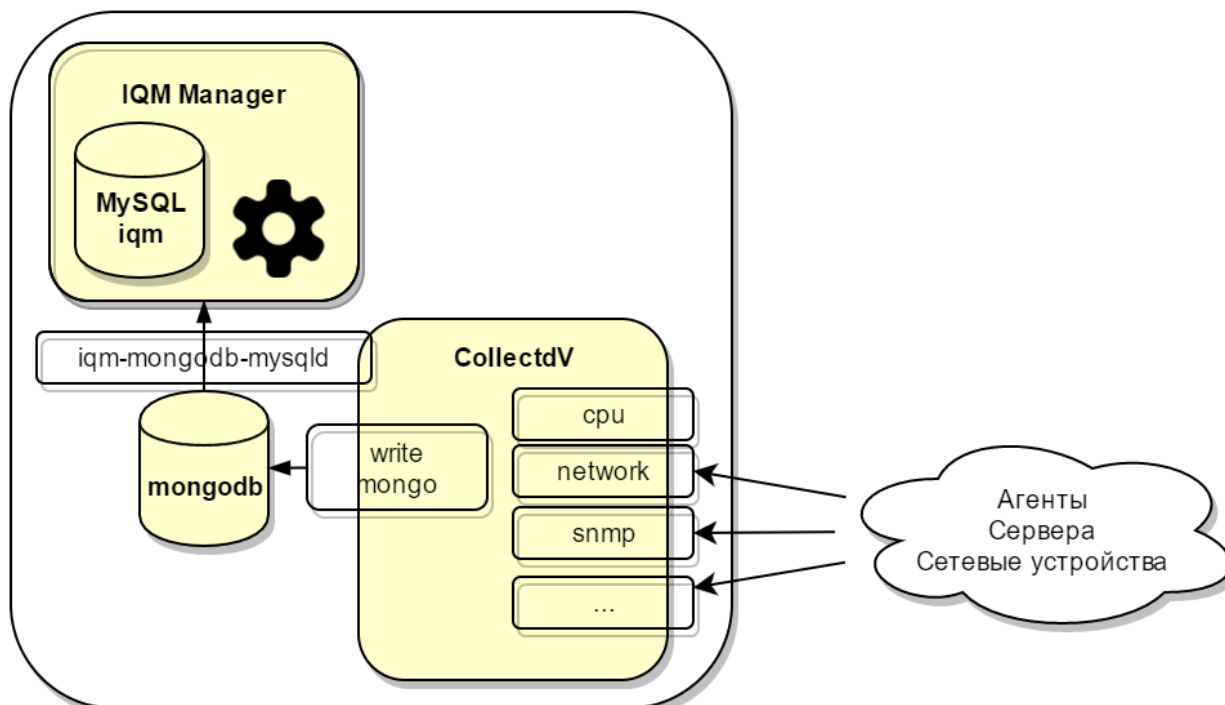


Рисунок 74 Информационные потоки между IQMM, MongoDB, CollectdV и сетевыми источниками

- Данные формируются на сетевых устройствах. Запрашиваются по сети с использованием SNMP-протокола. Проверки подлежат:
  - Сетевая доступность устройств-источников данных, проверка осуществляется с сервера системы управления IQMM, используются утилиты
    - ping
    - traceroute, tracert
    - nc
    - telnet <port>
    - ssh
  - Работоспособность устройств-источников данных
    - используйте средства проверки работоспособности, рекомендованные производителем
  - Наличие и работоспособность SNMP-сервиса на устройствах-источниках данных. Процесс для SNMP-сервиса должен быть запущен, привязан к заданному порту, должен корректно авторизовывать и отвечать на запросы, приходящие на прослушиваемый порт.
    - используйте средства проверки работоспособности, рекомендованные производителем устройства, доступные в соответствующей программной среде
- Данные запрашиваются SNMP-плагином CollectdV.

- Запросы SNMP должны проходить по сети и возвращаться на сервер, используйте утилиты:
  - `snmpget`, `snmpwalk`, etc
  - `nc`
- SNMP-плагин должен отправлять SNMP-запросы на нужные хосты, для проверки воспользуйтесь утилитами:
  - `tcpdump`
  - `wireshark`
- Анализ журнальных файлов `CollectdV`
  - `/var/log/messages` (уточните по текущей конфигурации куда направляются лог-файлы)
- Опрошенные данные передаются во временное хранилище MongoDB.
  - Наличие процесса, и прослушивание им нужного порта проверяется утилитами:
    - `ps`
    - `netstat`
    - `lsof`
  - Наличие данных во временном хранилище проверяется с использованием клиента `mongo` и специфических запросов к коллекциям. Следует понимать, что данные в хранилище находятся небольшой промежуток времени, после чего они перемещаются в MySQL базу, а в MongoDB удаляются. Для получения уверенности, что данные не удалены штатным порядком можно временно остановить сервис `iqmm-collectd`, после проверки запустить его заново.
    - `service iqmm-collectd stop`
    - `$ mongo`
    - `> use collectd`
    - `> db.snmp.find()`
    - `> db.snmp.count()`
    - `service iqmm-collectd start`
  - Анализ журнальных файлов MongoDB
    - `tail -f /var/log/mongodb/mongod.log`
- Данные из MongoDB перемещаются в MySQL процессом `iqmm-collectd`
  - Наличие процесса `iqm-mongodb-mysqld.pl` проверяется утилитами:
    - `ps ax|grep iqm-mongodb-mysqld.pl`
    - `service iqmm-collectd status`
  - Работоспособность базы MySQL:
    - `ps ax|grep mysqld`
    - `service mysqld status`
  - Анализ журнальных файлов `iqmm-collectd`:
    - `tail -f /home/iqm/log/iqm-mongodb-mysqld.log`
  - Наличие данных в базе MySQL проверяется SQL-апросами с использованием клиента `mysql`
- Данные из базы передаются в браузер клиента
  - Проверка наличия запросов от клиента на стороне сервера
    - анализ `http`-логов
    - `tcpdump`
  - Проверка со стороны клиента:
    - Проверка связанности с системой управления: `ping`, `trace...`

- Проверка работы браузера, проверьте настройки проху, используйте встроенный отладчик

## Блокировки mongodb

Локи mongodb находятся в /var/lib/mongo/

## Логи mongodb

tail -f /var/log/mongodb/mongod.log

```
[root@iqm ~]# mongo
MongoDB shell version: 2.6.11
connecting to: test
Server has startup warnings:
2015-09-07T14:59:49.310+0300 [initandlisten]
2015-09-07T14:59:49.310+0300 [initandlisten] ** NOTE: This is a 32 bit MongoDB binary.
2015-09-07T14:59:49.310+0300 [initandlisten] **      32 bit builds are limited to less than 2GB
of data (or less with --journal).
2015-09-07T14:59:49.310+0300 [initandlisten] **      Note that journaling defaults to off for 32
bit and is currently off.
2015-09-07T14:59:49.310+0300 [initandlisten] **      See http://dochub.mongodb.org/core/32bit
2015-09-07T14:59:49.311+0300 [initandlisten]
> use collectd
switched to db collectd
> show collections
cpu
snmp
system.indexes
>
```

## Логи collectdV

Логи collectdV в /var/log/messages

"/etc/collectdV.conf"

```
7 #####
8 # Global #
9 #-----#
10 # Global settings for the daemon. #
11 #####
12
13 #Hostname "localhost"
14 #Hostname "iqmm.msk1" # должно совпадать с названием хоста в конфиге
15 #FQDNLookup true
16 #FQDNLookup false
17 #BaseDir "/var/lib/collectdV"
18 #PIDFile "/var/run/collectdV.pid"
19 #PluginDir "/usr/lib/collectdV"
...
55 #LoadPlugin syslog
56 #LoadPlugin logfile
57
58 #<Plugin logfile>
59 #   LogLevel info
60 #   File STDOUT
61 #   Timestamp true
62 #   PrintSeverity false
63 #</Plugin>
64
65 <Plugin syslog>
66     LogLevel notice
67 </Plugin>
```

## Включение дебага в iqmm-collectd

/home/iqm/iqmm/scripts/iqm-mongodb-mysqld.pl:

```
59 my $server = NetProbe::IQM::Collect::Daemon->new ({
60     'pidfile' => sprintf(NETPROBE_PIDFILE,$short_program_name),
```

```
61 'localpath' => sprintf (NETPROBE_SOCKETFILE,$short_program_name),
62 # 'localpath' => '/tmp/socket-iqmm',
63 'proto' => 'unix',
64 # 'user' => 'netprobe',
65 # 'loop-child' => 1,
66 'loop-timeout' => 20,
67 'mode' => 'fork',
68 'logfile' => $log_file,
69 'listen' => 10,
70 'debug' => 1,
```

## Работа с отчетами

Система управления IQMM содержит богатый набор предустановленных отчетов. Жестко-закодированные отчеты не подлежат принципиальному изменению. Так же в системе предусмотрены пользовательские отчеты, они могут быть изменены, скопированы, на их базе оператор может построить собственные отчеты.

## Доступ к отчетам

### Графические отчеты

Для просмотра графических отчетов воспользуйтесь формой Custom reports. Форма вызывается через пункт меню верхнего уровня:

#### *Graphics*



Рисунок 75 графические отчеты

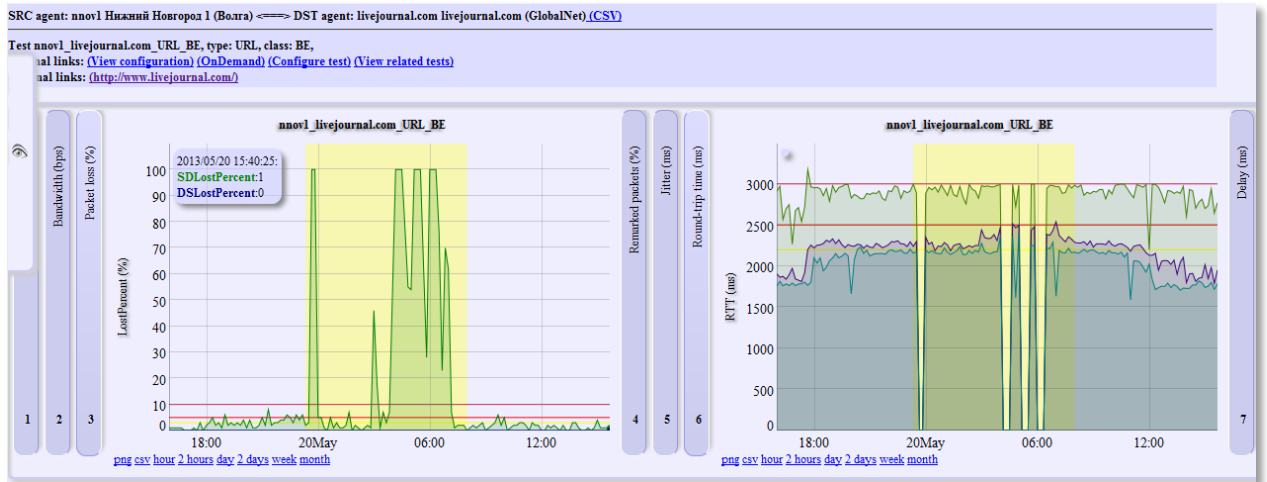


Рисунок 76 графические отчеты с отображением пороговых значений и окна регламентных работ

### Комбинированные графические отчеты

Для облегчения анализа измеренных агентами качественных характеристик в системе предусмотрена возможность комбинирования измерений, осуществленных различными тестами. В частности предоставлена возможность совмещения графиков. Приведем для примера серию графиков:

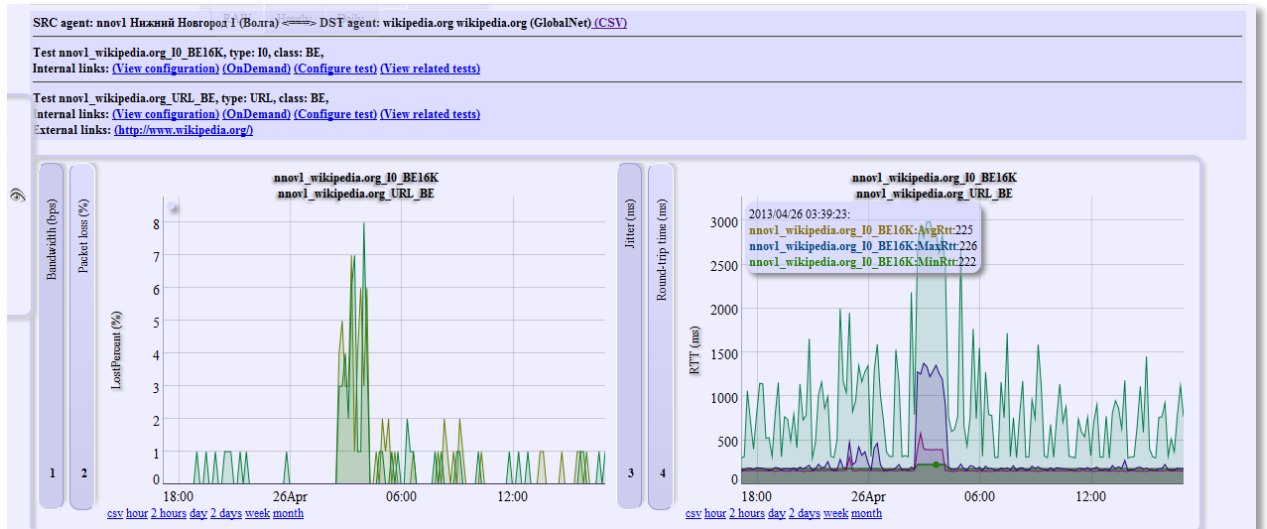


Рисунок 77 комбинированные графические отчеты

Приведенный скриншот демонстрирует наложение данных, измеренных тестами, производимых на транспортном и на прикладном уровнях. Наложение отчетов по потерям, возникшим при тестировании ресурса wikipedia на транспортном и прикладном уровнях, позволяют сделать заключение, о том, что возникшие потери на транспортном уровне явились причиной плохой доступности HTTP сервиса.



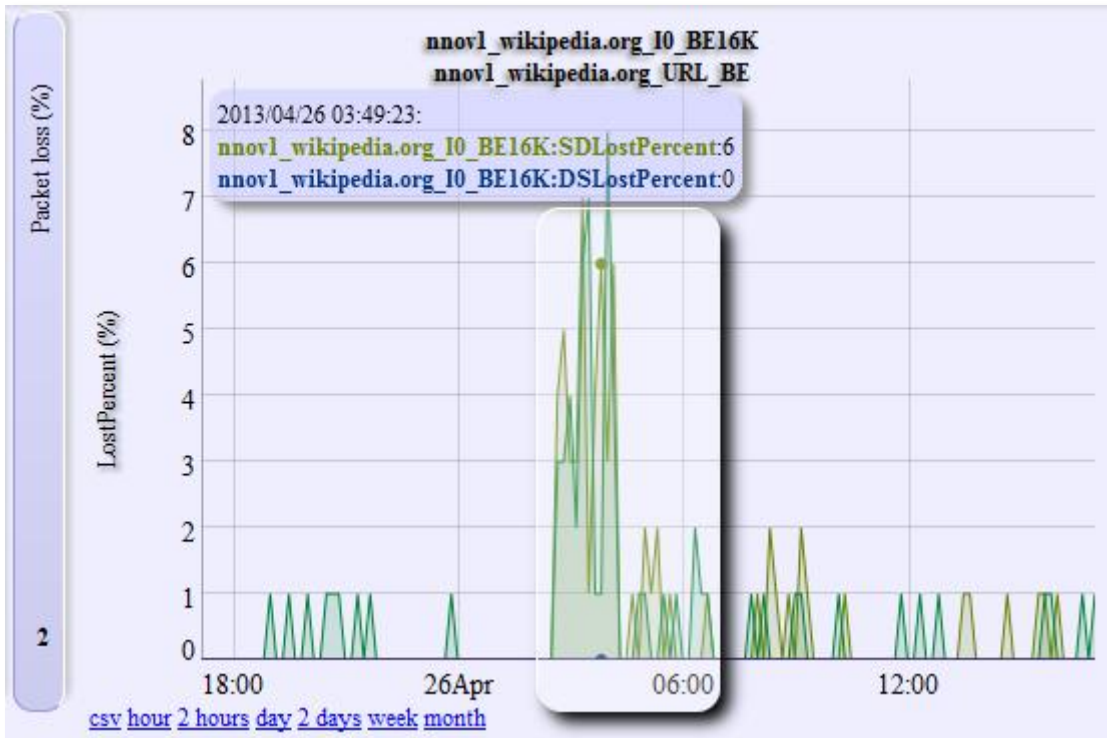


Рисунок 78 комбинированные графические отчеты

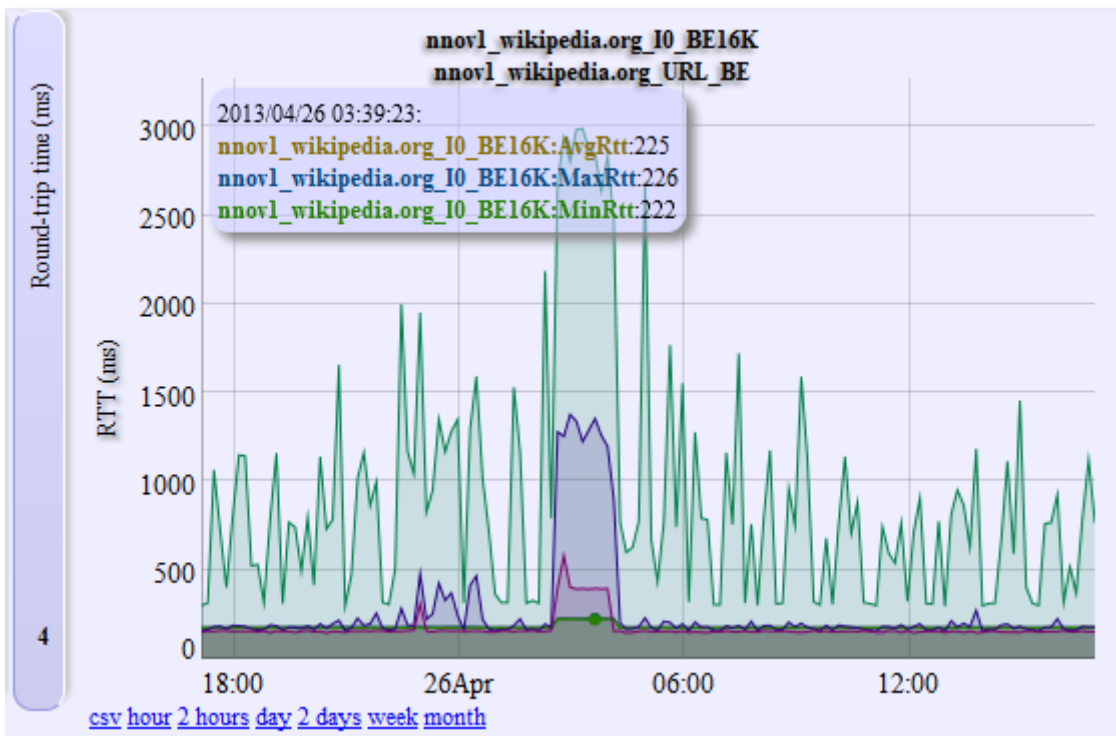


Рисунок 79 комбинированные графические отчеты

На приведенном графике виден минимальный порог задержки получения страницы с сайта wikipedia, он определяется возможностями транспортной среды, что подтверждается результатами соответствующего теста и видно на графике.

Под графиками расположены якоря, позволяющие изменить глубину запрошенных данных «по месту».

Графические отчеты так же организованы в блоках аккордеонов, с возможностью раскрытия/свертывания нужного отчета. Легенды отображены в отдельных блоках, не засоряя т.о. пространство графика. Оператору предоставлена возможность изменения масштаба графика. На графиках может быть скомбинированы отчеты как по разным параметрам одного теста, так и по различным тестам.

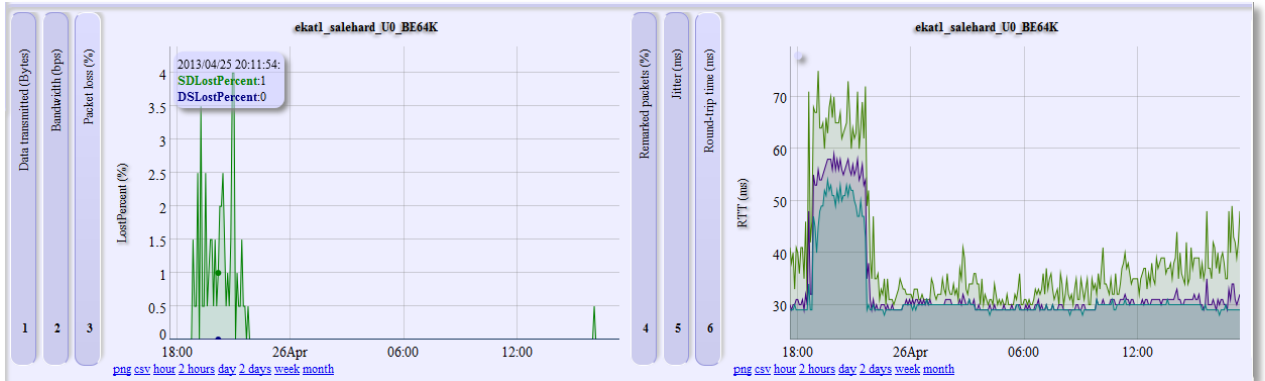


Рисунок 80 графические отчеты встроенные в "аккордеон"

Info Administration Configuration Statistics Graphics Map (hour) Map (filter) Help

Reports Violations Graphics OnDemand

QoS reports QoS reports (accel.) QoS reports TopX SLA reports (src zone) SLA reports

**RTC - [logged as admin] - QoS reports from 2013-04-04 16:51:44 to 2013-04-05 16:51:44:**

QoS reports from 2013-04-04 16:51:44 to 2013-04-05 16:51:44

Customer

SRC zone

DST zone

SRC agent

DST agent

Test ID

astrakhan\_dentv.ru\_I0\_BE16K

astrakhan\_dentv.ru\_URL\_BE

belgorod\_dentv.ru\_I0\_BE16K

belgorod\_dentv.ru\_URL\_BE

cheboksary\_dentv.ru\_I0\_BE16K

cheboksary\_dentv.ru\_URL\_BE

chelyabinsk\_dentv.ru\_I0\_BE16K

chelyabinsk\_dentv.ru\_URL\_BE

dolgoprudny\_dentv.ru\_I0\_BE16K

dolgoprudny\_dentv.ru\_URL\_BE

ekat1\_chelyabinsk\_U0\_BE1M

Class

Parameters

Bytes

BW

LostPercent

RemarkedPercent

Jitter

RttMax

RttAvg

RttMin

MaxDelay

AvgDelay

MinDelay

Data source

Period

2013-04-04 16:51:44

2013-04-05 16:51:44

day

Conditions

Actions

view

clear

filter

Number	SRC agent	DST agent	Test name	Parameters	Minimum	Average	Maximum
1	astrakhan	dentv.ru	astrakhan_dentv.ru_I0_BE16K	Packet loss (%)	0.00	0.01	1.00
				Jitter (ms)	0	0.00	0
				Maximum round-trip time (ms)	29	30.03	32
				Average round-trip time (ms)	29	29.00	29
				Minimum round-trip time (ms)	28	28.31	29
2	astrakhan	dentv.ru	astrakhan_dentv.ru_URL_BE	Packet loss (%)	0.00	0.01	1.00
				Jitter (ms)	43	70.27	218
				Maximum round-trip time (ms)	443	589.08	1922

Рисунок 81 табличные отчеты по значениям параметров

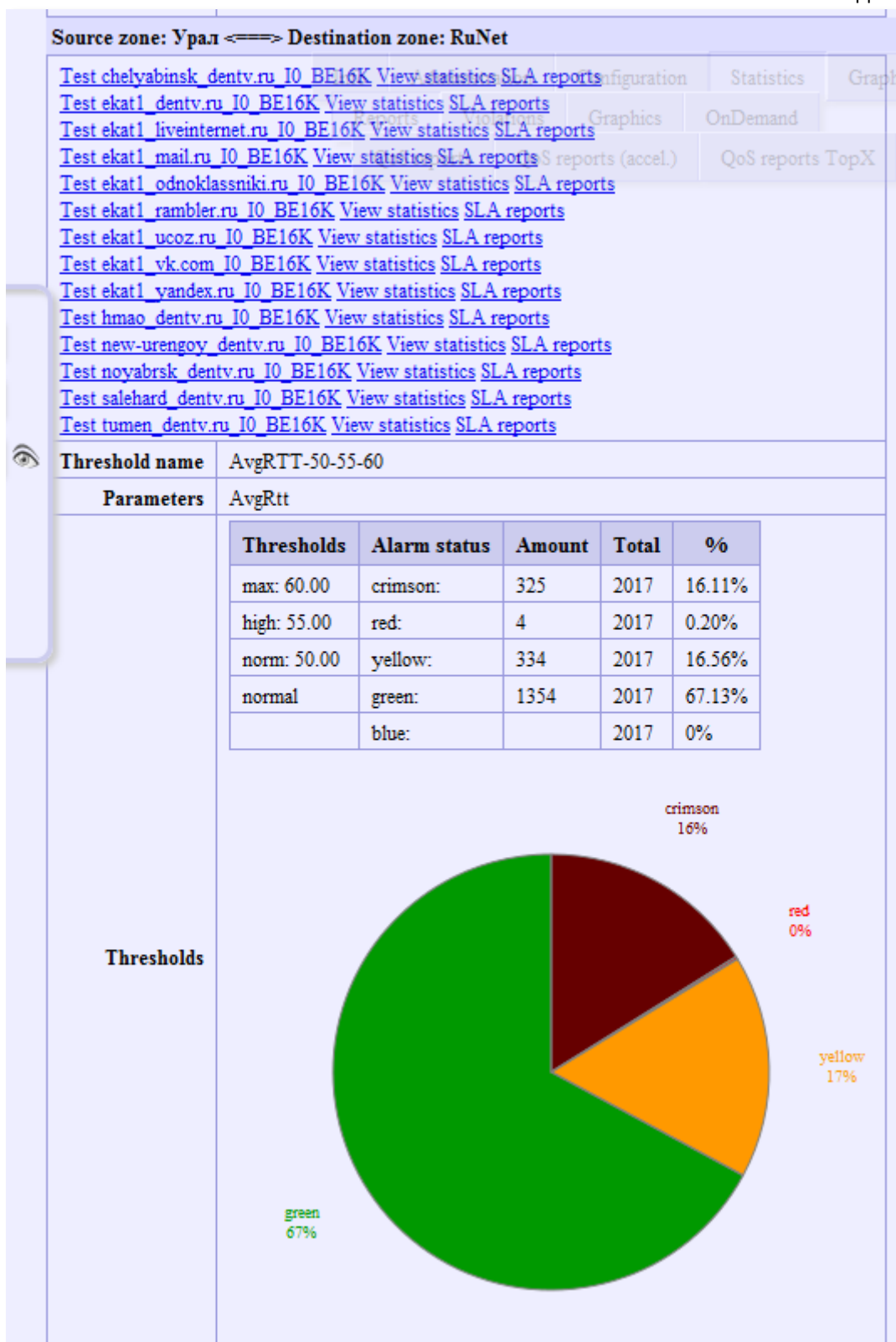


Рисунок 82 Зональные отчеты по соответствию контролируемых параметров нормам SLA

### Отчеты с группировкой

Отчеты с группировкой позволяют формировать различные суммарные отчеты для группы тестов. Объединение в группы происходит по тем же признакам, которые

используются для фильтрации запрашиваемых результатов (зоны, архитектурные уровни, агенты, тесты и прочие). В одну группу попадает множество измерений, с одинаковыми значениями признаков, определенных в критериях группировки. Для просмотра отчетов с группировкой воспользуйтесь формой Group reports. Форма вызывается через пункт меню верхнего уровня:

### Group reports

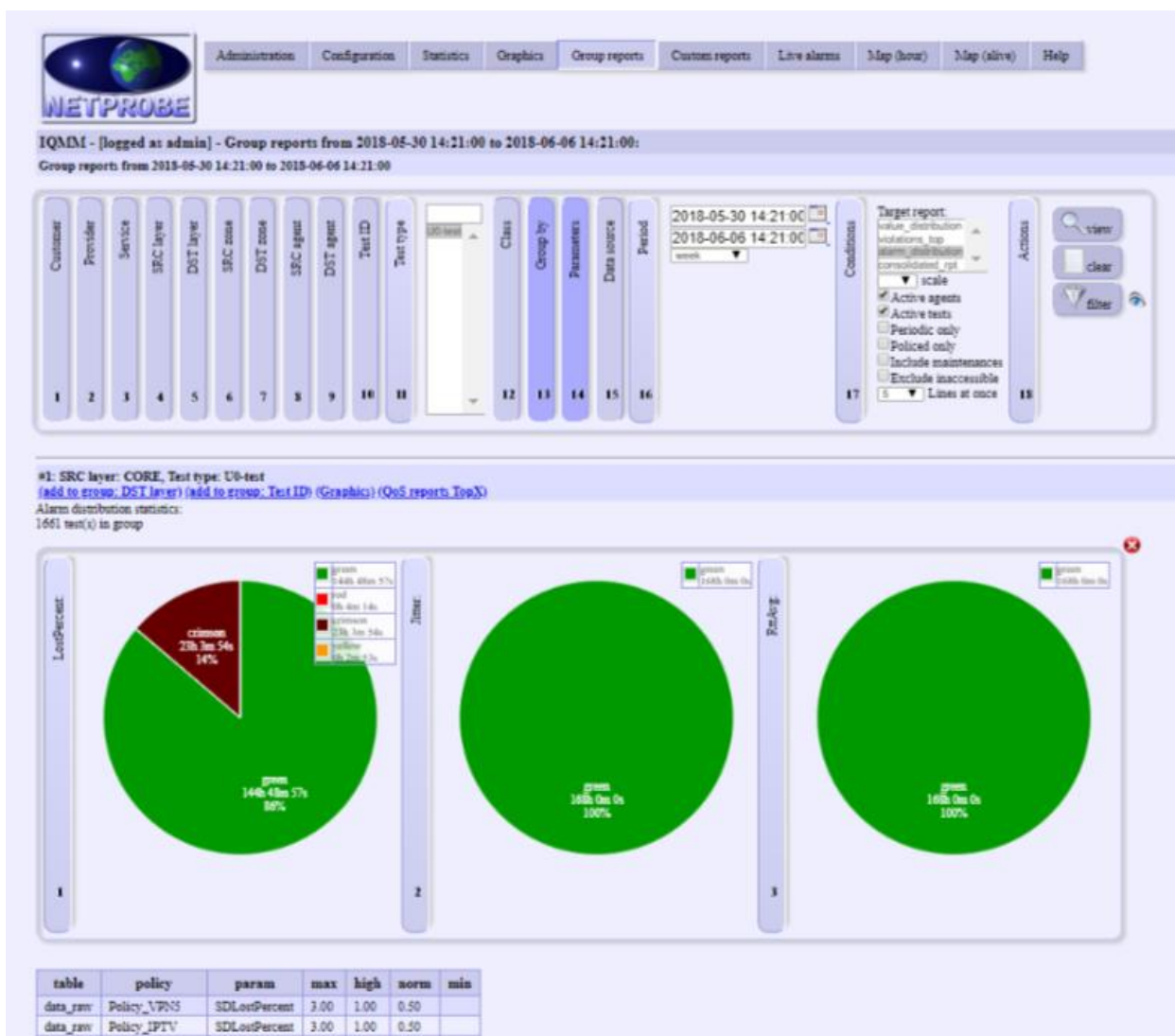


Рисунок 83 Пример отчета с группировкой. Отчет по алармам

Целевой отчет отчета с группировкой выбирается во вкладке «Conditions». Доступны следующие целевые отчеты с группировкой:

- Value\_distribution: отчет по распределениям значений измеряемых параметров для групп. Отчет представляет частотное распределение значений запрошенных параметров для группы тестов на отчетном периоде. Демонстрирует частоту нахождения параметра в диапазоне значений (в процентах). Рисунок 84 частотное распределение значений круговых и односторонних задержек показывает пример отчета по частотному распределению параметров. В примере запрошены 6 параметров: круговая и односторонняя задержки минимальные, средние и максимальные значения. Видно, что измеренная средняя круговая задержка в большинстве случаев принимала значения от 0.9 до 1.5 секунды, измерения проводились на спутниковом канале.

- **violations\_top**: работает по фактам превышения пороговых значений, но не учитывает частоту срабатывания, определенную в политике. Берутся все измерения, по параметрам подвергаемым контролю (с учетом или без учета периодов регламентных работ), их значения сравниваются с действующими порогами, факты превышения считаются как нарушения. Одно нарушение считается как соответствующая деградация, длящаяся в течение одного периода между проведениями двух последовательных тестов. Гранулярность - период теста. Отчет представляется в виде круговой диаграммы для параметров (см. Рисунок 85 violations\_top или alarm\_distribution с детализацией по тестам).
- **alarm\_distribution**: работает по фактически проведенным алармам, с учетом частоты срабатывания. Производится выборка по истории алармов для заданной группы тестов. Суммируются периоды пребывания в зонах одинаковой критичности, состояния дополняются нормальным состоянием, результат представляется в виде круговых диаграмм (см. Рисунок 85 violations\_top или alarm\_distribution с детализацией по тестам). Гранулярность - горизонт наблюдений, используемый при журнализации событий. Горизонты могут быть разными для разных тестов, однако, это не мешает им попасть в одну группу в отчете.
- **Consolidated\_report**: Сводный (консолидированный) отчет представляет в табличной форме (см. Рисунок 86 консолидированный отчет). Данные консолидированного отчета экспортируются в табличный формат, для этого вверху отчета приведен блок соответствующих кнопок. Поля консолидированного отчета:
  - Num (Num) – порядковый номер
  - Test (Тест) – идентификатор теста
  - Rate (Скорость) – скорость инициирования тестового потока
  - SRC agent (Иницирующий агент) – агент-инициатор теста
  - SRC layer (Уровень инициатора) – архитектурный уровень инициатора
  - SRC zone (Зона инициатора) – зона инициатора
  - DST agent (Сопряженный агент) – сопряженный агент
  - DST layer (Уровень сопряженного) – архитектурный уровень сопряженного агента
  - DST zone (Зона сопряженного) – зона сопряженного агента
  - Service (Сервис) – тип контролируемого сервиса
  - Test type (Тип теста) – механизм тестирования
  - Class (Класс сервиса)
  - Period h:m:s (Период ч:м:с) – отчетный период
  - Downtime h:m:s (Недоступен ч:м:с) – период недоступности (100% потерь)
  - Uptime h:m:s (Доступен ч:м:с) – период доступности (менее 100% потерь)
  - Availability (%) (Доступность (%)) – доступность в процентах
  - Минимальные, средние, максимальные значения запрошенных параметров за отчетный период (без учета периодов полной недоступности)
  - Policy (Политика) – идентификатор политики, контролирующей измеряемые значения параметров, если есть
  - Пороговые значения, определенные в политике для запрошенных параметров (Thresholds: low|norm|high|max) (Пороги: low|norm|high|max)
  - Нарушения, обнаруженные политиками для каждого из запрошенных параметров. Приводятся периоды нахождения параметра в каждой зоне критичности во временных характеристиках и в процентных. (Violations: parameter:severity:hh:mm:ss) (Нарушения: параметр:важность:чч:мм:сс), например SDLostPercent:green:22:46:59(96.13%)|yellow:00:55:01(3.87%)

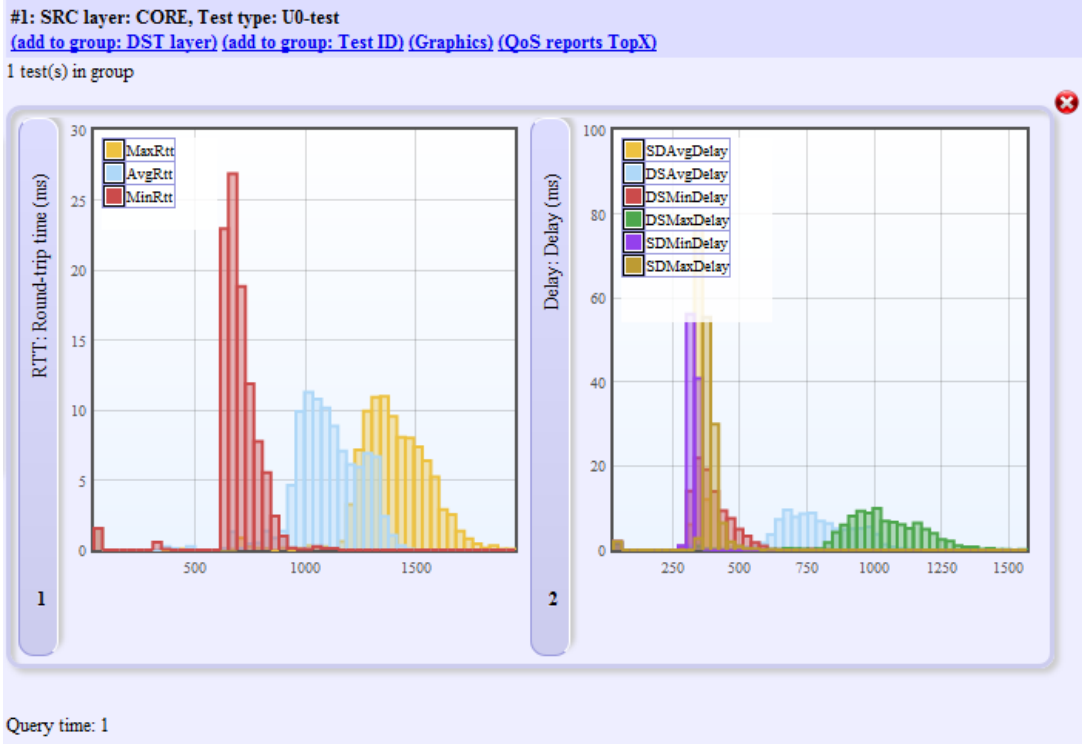


Рисунок 84 частотное распределение значений круговых и односторонних задержек

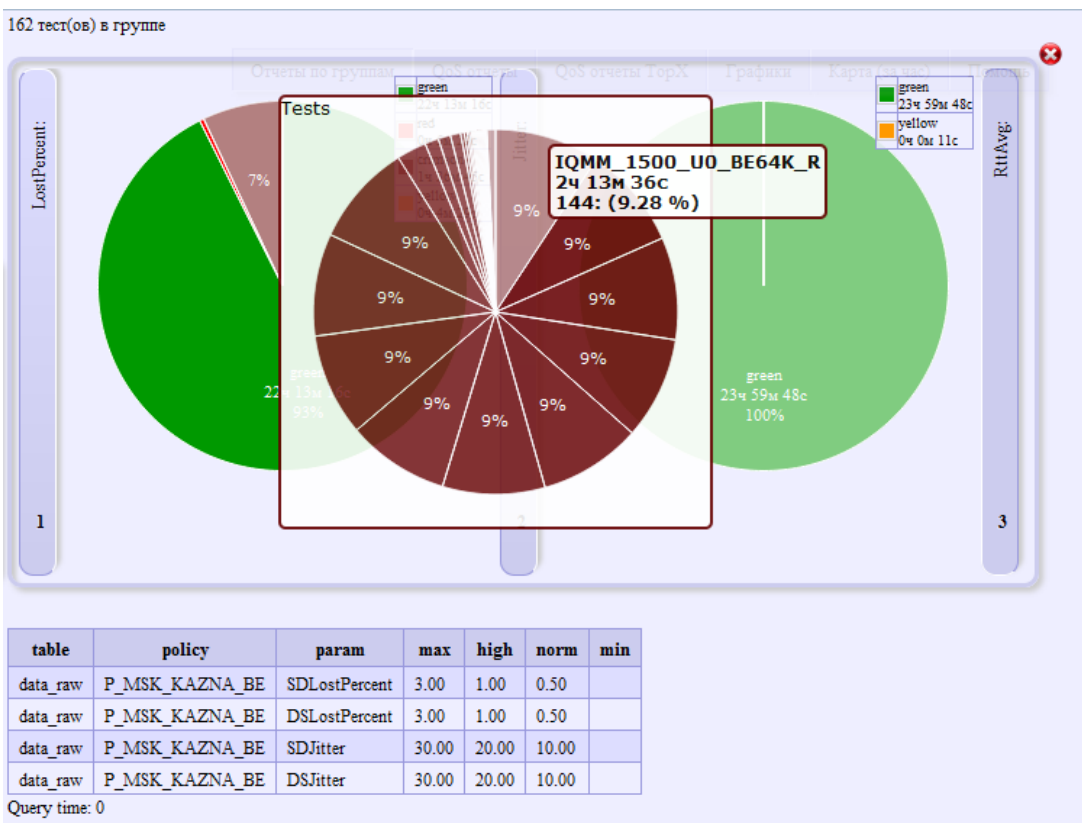


Рисунок 85 violations\_top или alarm\_distribution с детализацией по тестам

162 тест(ов) в группе

XLS CSV CSV export CSV report expert сброс фильтра

Консолидированный отчет

Num	Тест	Скорость	Соприженный агент	Уровень сопряженного	Зона сопряженного	Сервис	Тип теста	Класс сервиса	Период ч:м:с	Недоступен ч:м:с	Доступен ч:м:с	Доступность (%)	Потери пакетов (%)	Вариация задержки (ms)	Среднее значение
1	IQMM_0100_U0_BE64K_M	64 Кб/с	kazna_sla2_0100 (УФК по Республике Башкортостан)	Ядро	Агенты Казначейства (Агенты Казначейства)	L3 IP VPN	U0 (транспорт)	BE	23:52:00	00:00:00	23:52:00	100	0/01 0/00	0/00 0/00	2627
2	IQMM_0100_U0_BE64K_R	64 Кб/с	kazna_sla2_0100 (УФК по Республике Башкортостан)	Ядро	Агенты Казначейства (Агенты Казначейства)	L3 IP VPN	U0 (транспорт)	BE	23:52:00	00:00:00	23:52:00	100	0/0.16 0/00	0/00 0/00	2627
3	IQMM_0200_U0_BE64K_M	64 Кб/с	kazna_sla2_0200 (УФК по Республике Бурятия)	Ядро	Агенты Казначейства (Агенты Казначейства)	L3 IP VPN	U0 (транспорт)	BE	23:52:00	00:00:00	23:52:00	100	0/00 0/00	0/00 0/00	1821
4	IQMM_0200_U0_BE64K_R	64 Кб/с	kazna_sla2_0200 (УФК по Республике Бурятия)	Ядро	Агенты Казначейства (Агенты Казначейства)	L3 IP VPN	U0 (транспорт)	BE	23:42:00	23:42:00	00:00:00	0	100/100/100 100/100/100	0/00 0/00	0/00
5	IQMM_0300_U0_BE64K_M	64 Кб/с	kazna_sla2_0300 (УФК по Республике Дагестан)	Ядро	Агенты Казначейства (Агенты Казначейства)	L3 IP VPN	U0 (транспорт)	BE	23:42:00	00:00:00	23:42:00	100	0/00 0/00	0/00 0/00	4444

Рисунок 86 консолидированный отчет

## Мониторинг на ГИС

Система управления IQMM позволяет отображать структуру контролируемых каналов и агентов в наложении на ГИС. ГИС – гео-информационная система представляет собой многослойную географическую карту с возможностью включения-выключения слоев. Для проведения мониторинга состояния каналов и объектов на ГИС необходимо:

- Совершить геопривязку в конфигурации агентов (см. Форма конфигурации агентов параметр Longitude and Latitude),
- Сконфигурировать автоматические тесты между агентами (см. Создание тестов),
- Создать и наложить политику контроля на результаты измерений (см. Контроль параметров и далее).

Карта отображает состояния контролируемых агентов и каналов с часовой глубиной (за последний час). Вызывается через пункт меню:

### *Statistics – Violations – Map (XXX)*

- Map (hour) – отображение всех объектов мониторинга
- Map (filter) – карта с формой предварительной фильтрации (см. Фильтры)
- Map (alive) – отображение каналов между доступными агентами (операционное состояние - UP)

Карта содержит элементы управления, которые позволяют: изменить ее масштаб, переместиться на интересующий район, получить ссылку, включить/выключить слой. На карте отображаются агенты разных типов, они отличаются иконками, используемыми при отображении, их операционное состояние кодируется цветом. Состояние контролируемых каналов, так же индицируется цветом.



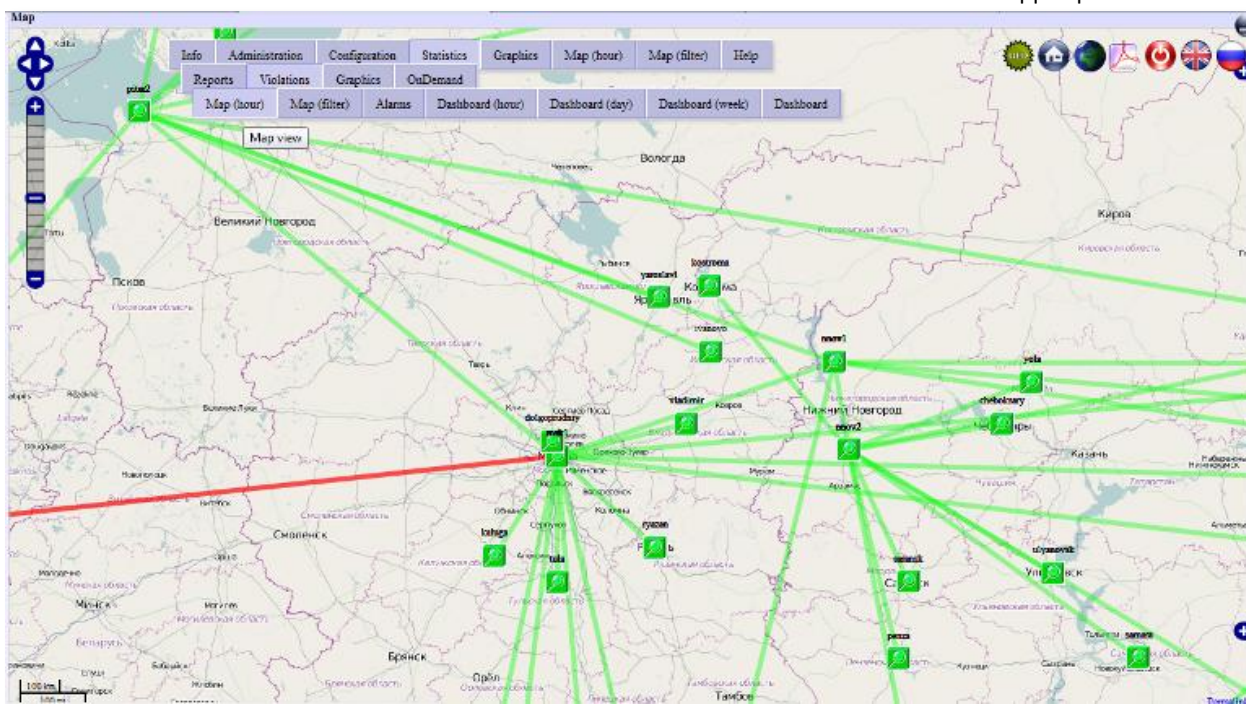


Рисунок 87 Табло мониторинга на географической карте

Для получения дополнительной информации об агенте необходимо кликнуть на его иконке левой кнопкой мыши, появится всплывающее окно с дополнительной информацией об агенте (см. Рисунок 88).

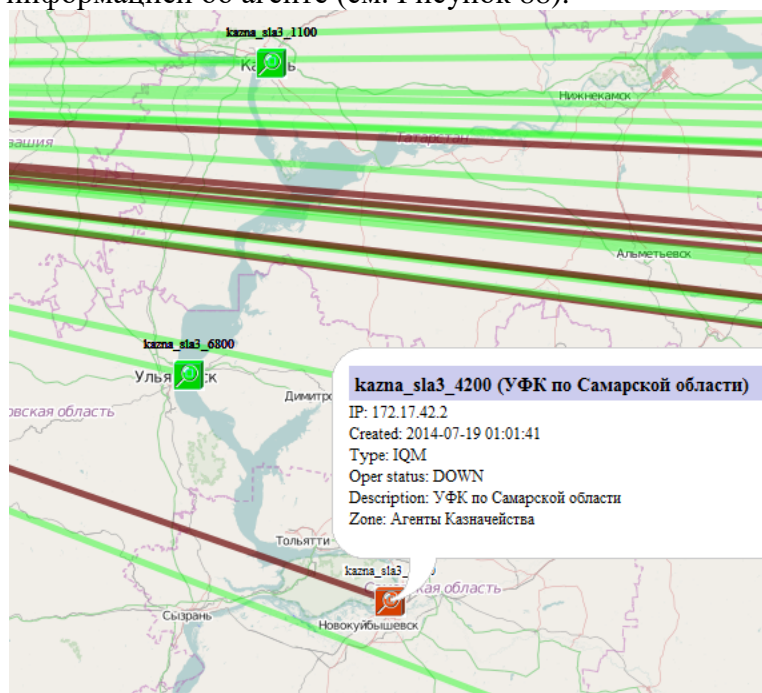


Рисунок 88 информация об агенте во всплывающем окне

На карте линиями отображаются тесты (см. Рисунок 89), цвет сигнализирует о наличии или отсутствии нарушения: зеленый (нет нарушения), желтый (обнаружено превышение порога нормального уровня), красный (обнаружено превышение порога высокого уровня), малиновый (обнаружено превышение порога максимального уровня), синий (обнаружено принижение порога минимального уровня). Для получения дополнительной информации о состоянии теста необходимо кликнуть на нем левой кнопкой мыши, появится



всплывающее окно с дополнительной информацией о тесте. В окне будет отображена таблица с данными последнего измерения, средними, минимальными и максимальными значениями за час, так же будут приведены графики со статистикой по параметрам за сутки и ссылками на соответствующие данные в формате CSV. Содержимое карты будет периодически обновляться.

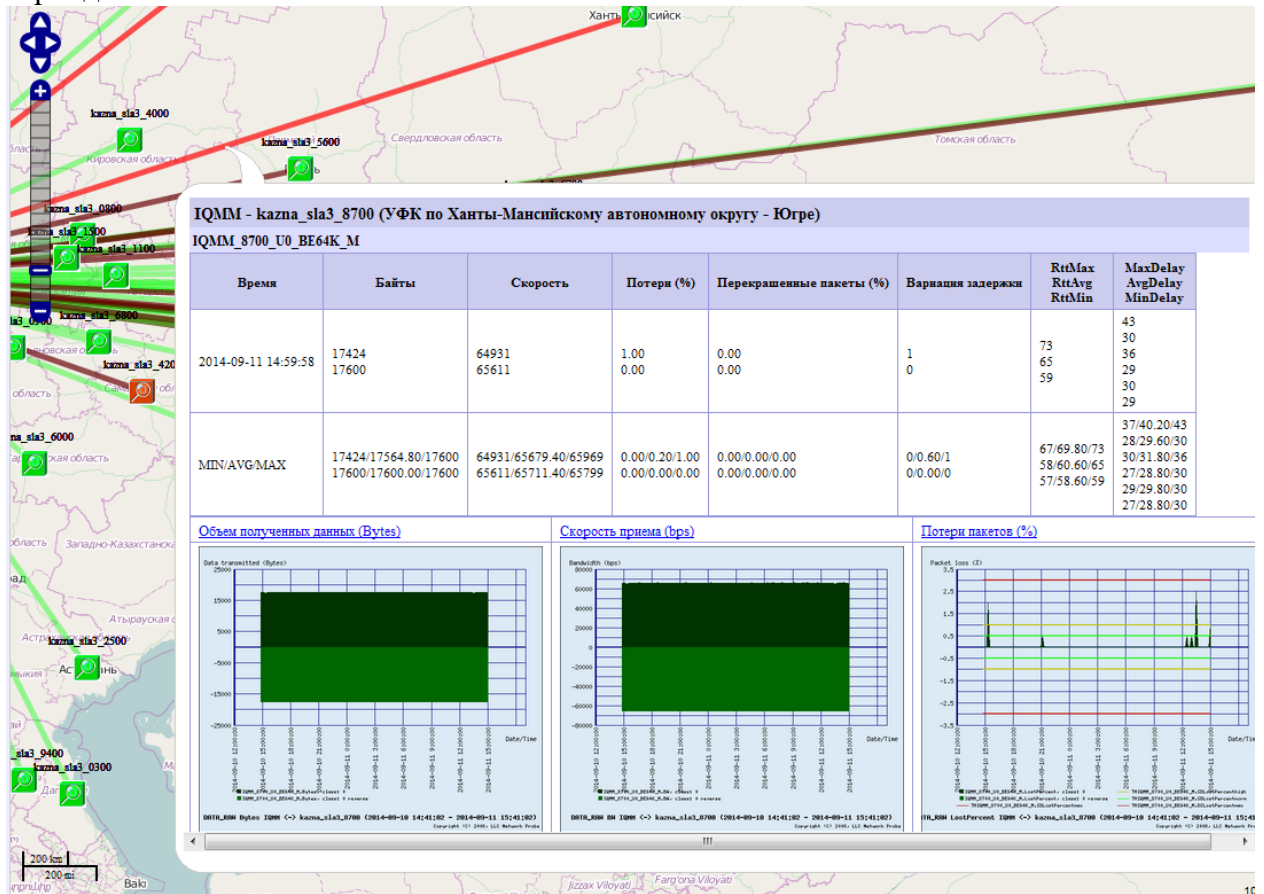


Рисунок 89 информация о измерениях во всплывающем окне

### Звуковая сигнализация на ГИС

В системе предоставлена возможность проведения звуковой сигнализации об изменении состояния отображаемых каналов на ГИС. Контролируемые каналы группируются по зональному признаку сопряженного агента. Скриптовая обвязка ГИС анализирует количество каналов, находящихся в различных состояниях для каждой из отображаемых групп. При увеличении количества каналов, находящегося в определенном состоянии проводится звуковая сигнализация в порядке приоритета: 'crimson', 'blue', 'red', 'yellow', 'green'. Проигрывается заданный в конфигурации файл. Если в группе обнаружено одновременно несколько переходов в разные состояния, то проигрывается звуковой файл, соответствующий приоритетному состоянию. Например: если в группе тестов на зону «Петушки» обнаружен одновременный прирост состояний 'crimson', 'blue' и 'red', то будет проигран только один звуковой файл для 'crimson'.

Звуковые уведомления определены в файле конфигурации /home/iqm/iqmm/iqmm-cfg.pl:

```
%gMapAudioAlarms = (
    crimson => 'img/alarms/Beethoven5.mp3',
    red      => 'img/alarms/Beethoven5.mp3',
    yellow  => 'img/alarms/Beethoven5.mp3',
    green   => undef,
    blue    => 'img/alarms/Beethoven5.mp3'
);
```

В качестве значения ключа передается URL либо, сокращенный URI, если аудио-файл размещен на том же хосте, что и интерфейс системы управления IQMM.

### Операционные состояния агентов

На карте, операционное состояние агента отображается цветом иконки, для каждого типа агента используется своя иконка. Перечень возможных состояний для типов IQM и UDP приведен далее.

#### Операционные состояния агентов IQM



UP – агент прошел проверки, находится в работе



TEST – соответствует административному состоянию TEST. Реальное состояние не проверяется, пока не будет изменено административное состояние.



UNKNOWN – состояние не проверялось, но будет проверено, скорее всего агент недавно заведен.



NOT\_AVAILABLE – агент доступен по ICMP, но не отвечает тестовый протокол IQM.



NO\_DATA – ожидается, что от агента должны приходить результаты тестов, но их нет. Однако, по тестовому протоколу агент доступен. Возможна проблема с доставкой CDR-ов.



DOWN – агент не доступен.

#### Операционные состояния агентов UDP-echo



UP – агент прошел проверки, находится в работе



TEST – соответствует административному состоянию TEST. Реальное состояние не проверяется, пока не будет изменено административное состояние.



UNKNOWN – состояние не проверялось, но будет проверено, скорее всего агент недавно заведен.



NOT\_AVAILABLE – агент доступен по ICMP, но не отвечает тестовый протокол UDP-echo.



DOWN – агент не доступен.

## QoS отчеты

QoS отчеты доступны в форме QoS reports в пунете меню:

*Statistics → Reports → QoS reports*

---

Отчеты QoS предоставляют информацию о минимальных, средних и максимальных значениях контролируемых параметров за заданный отчетный период для каждого теста. При расчете не учитываются измерения проведенные в моменты полной недоступности канала/агента, когда возникали 100% потери.

Number	SRC agent	DST agent	Test name	Parameters	Minimum	Average	Maximum
1	IQMM	kazna_sla3_0100	IQMM_0100_U0_BE64K_R	Packet loss (%)	0.00 0.00	0.00 0.00	0.00 0.00
				Jitter (ms)	0 0	0.00 0.00	0 0
				Average round-trip time (ms)	26	28.39	57
2	IQMM	kazna_sla3_0200	IQMM_0200_U0_BE64K_M	Packet loss (%)	0.00 0.00	0.22 0.00	17.00 0.00
				Jitter (ms)	0 0	0.01 0.00	1 0
				Average round-trip time (ms)	170	185.32	199
3	IQMM	kazna_sla3_0200	IQMM_0200_U0_BE64K_R	Packet loss (%)			
				Jitter (ms)			
				Average round-trip time (ms)			
4	IQMM	kazna_sla3_0300	IQMM_0300_U0_BE64K_M	Packet loss (%)	0.00 0.00	0.01 0.00	0.50 0.00
				Jitter (ms)	0 0	0.00 0.00	0 0
				Average round-trip time (ms)	44	44.09	45
5	IQMM	kazna_sla3_0300	IQMM_0300_U0_BE64K_R	Packet loss (%)	0.00 0.00	0.00 0.00	0.50 0.00
				Jitter (ms)	0 0	0.00 0.00	0 0
				Average round-trip time (ms)	43	43.49	44

Рисунок 90 QoS отчет по значениям параметров

*Statistics → Reports → QoS reports (accel.) – отчет аналогичен QoS reports. Отличается механизм запроса базы, который в QoS reports (accel.) отчете оптимизирован для больших таблиц, однако выдача данных в нем осуществляется разом по всем тестам, а не построчно, как это делается в отчете QoS reports.*

*В связи с появлением механизма Custom reports все штатные табличные отчеты считаются устаревающими.*

---

## Отчет с TopX

Для просмотра TopX отчетов воспользуйтесь формой TopX QoS reports. Форма вызывается через меню:

TopX QoS отчеты – демонстрируют TopX самых неблагоприятных направлений по выбранным параметрам на заданном периоде. Расчет осуществляется по средним значениям параметров. Отчет полезен для оперативного наблюдения за состоянием множества направлений. При необходимости, в фильтре определяются дополнительные условия запроса. Например:

*Для того, чтобы убрать из отчета недоступные каналы можно нужно во вкладке **Conditions (Условия)** установить флаг **Exclude inaccessible (Исключить недоступные)** – исключить измерения со 100% потерями, т.е. проведенные в моменты, когда связности между агентами не было по той или иной причине.*

На выходе будет отчет с графиками по каждому запрошенному параметру. Графики будут отсортированы в порядке убывания средней величины значения параметра. В качестве примера рассмотрим Рисунок 91 TopX отчет. Отчет сформирован на основе L7 тестов, в отчете запрошены лидеры с максимальной скоростью загрузки страниц, с максимальным количеством потерь, с максимальной задержкой. Как видно, наивысшая скорость отдачи по HTTP у mail.ru, в лидеры по потерям попали одноклассники, сайт которых был не доступен по техническим причинам, наибольшие задержки от ЖЖ до Хабаровска.

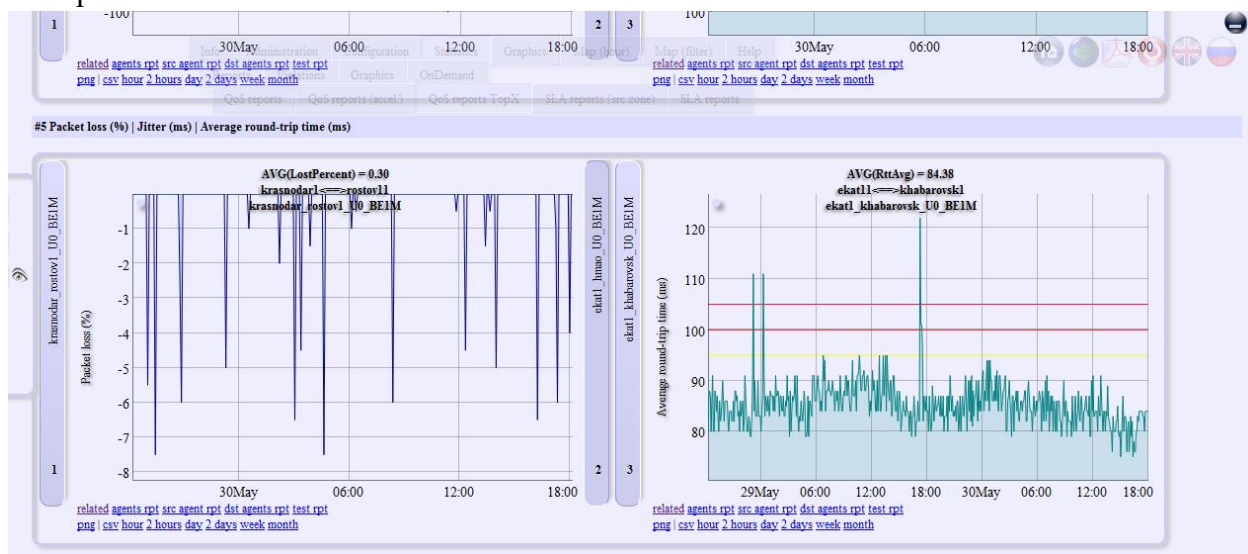


Рисунок 91 TopX отчет

## Табло сигналов о нарушениях

Таблица сигналов нарушений предоставляет оператору доступ к списку сигналов, позволяет проанализировать возникшую проблему, поменять статус сигнала, добавить комментарий, удалить сигнал.

Для получения доступа к форме запроса сигналов нарушений – выберите пункт меню

Появится фильтр-форма:

The screenshot shows the 'Alarms from 2018-10-30 19:48:29 to 2018-10-30 20:48:29' section. A filter bar is visible above the table. The table contains the following data:

Severity	Count	Percentage
yellow	2	50.00%
red	1	25.00%
crimson	1	25.00%

Time begin	Time end	Test ID	Class	Policy ID	Table	Value	Threshold	Status	Severity	Info	History	Action
2018-10-30 18:31:06	2018-10-30 20:41:06	iqmm_twitich_tv_URL (View) (OnDemand) (Config) (Related)	BE	Policy_URL (Config)	data_raw	AvgRtt	100.00	UP	YELLOW		1 events (View)	
2018-10-30 13:58:09	2018-10-30 20:41:07	iqmm_valve.com_URL (View) (OnDemand) (Config) (Related)	BE	Policy_URL (Config)	data_raw	AvgRtt	100.00	UP	YELLOW		1 events (View)	
2018-10-30 12:58:04	2018-10-30 20:41:05	iqmm_rutube.ru_URL (View) (OnDemand) (Config) (Related)	BE	Policy_URL (Config)	data_raw	AvgRtt	400.00	UP	RED		4 events (View)	
2018-10-30 12:47:05	2018-10-30 20:41:05	iqmm_microsoft.com_ID (View) (OnDemand) (Config) (Related)	BE	Policy_STB1962 (Config)	data_raw	SDLonPercent	3.00	UP	CRIMSON		2 events (View)	

Рисунок 92 Табло алармов

Наряду со стандартными критериями выборки фильтр предлагает следующие дополнительные критерии:

Поле	Значение
Severity	<p>Зона критичности, возможны несколько уровней:</p> <p><b>GREEN (зеленый):</b> значение параметра находится в пределах нормы.</p> <p><b>YELLOW (желтый):</b> значение параметра находится в пределах между нормальным и высоким значением. <i>Предлагаемая интерпретация: Критичность желтого сигнала соответствует предупреждению. Значение контролируемого параметра пока не влияет на жизнеспособность сетевых сервисов, но приближается к критическому значению.</i></p> <p><b>RED (красный):</b> значение параметра находится в пределах между высоким и максимальным значением. <i>Предлагаемая интерпретация: Критичность красного сигнала говорит о значительной деградации качества. Многие сетевые сервисы могут страдать, но продолжают работать.</i></p> <p><b>CRIMSON (красный):</b> значение параметра превышает максимальное значение. <i>Предлагаемая интерпретация: Критичность кровавого сигнала говорит о наличии аварийной ситуации в контролируемом направлении. Сетевые сервисы, критичные к данному параметру качества перестают работать.</i></p> <p><b>BLUE (синий):</b> значение оказывается ниже минимального значения. Голубая зона критичности предназначена для сигнализации о недостатке ресурса,</p>

Поле	Значение
	например, для контроля доступной полосы пропускания.
Status	<p>Состояние сигнала. Отображает текущий статус проблемы. Возможны значения:</p> <p>UP – проблема обнаружена, требует разбирательства.</p> <p>DOWN – проблема очищена но сигнал не удален (после статуса UP).</p> <p>PROGRESS – проблема существует, находится в работе (после статуса UP).</p> <p>RESOLVED – проблема устранена (после статуса PROGRESS).</p> <p>NEGLECTED – проблема игнорируется (после статуса UP).</p> <p>Изначально, в момент обнаружения нарушения, сигналу присваивается состояние UP. В дальнейшем состояние сигнала меняет оператор в процессе его отработки.</p>

Форма сигналов нарушений обновляется автоматически. Цвет строки, описывающей параметры события, соответствует важности события, при условии, если его статус UP или Progress. Статусы DOWN и RESOLVED отображаются зеленым независимо от важности. Статус NEGLECTED – отображается серым цветом независимо от важности. Поле History позволяет просмотреть историю изменений статуса сигнала. Состояния в истории соотносятся к одному сигналу, если тревожные состояния идут подряд или если период зеленого состояния между ними не превышает значения горизонта наблюдений.

Alarm ID	Alarm time	Policy	Horizon (min)	Threshold	Count	Test	Class	Table	Value	Severity	History
33407	2013-04-05 16:17:05	Russia_GlobalNet	60	5.00	2	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	RED	1 events (View)
33406	2013-04-05 16:13:05	Russia_GlobalNet	60	3.00	5	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	YELLOW	1 events (View)
33397	2013-04-05 15:47:06	Russia_GlobalNet	60	5.00	2	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	RED	1 events (View)
33390	2013-04-05 15:23:05	Russia_GlobalNet	60	3.00	2	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	YELLOW	1 events (View)
33388	2013-04-05 15:17:06	Russia_GlobalNet	60	5.00	2	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	RED	1 events (View)
33371	2013-04-05 15:12:05	Russia_GlobalNet	60	3.00	2	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	YELLOW	1 events (View)
33350	2013-04-05 12:42:05	Russia_GlobalNet	60	5.00	4	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	RED	1 events (View)
33322	2013-04-05 10:37:05	Russia_GlobalNet	60	10.00	2	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	CRIMSON	1 events (View)
33320	2013-04-05 10:37:06	Russia_GlobalNet	60	5.00	2	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	RED	1 events (View)
33311	2013-04-05 09:37:06	Russia_GlobalNet	60	3.00	2	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	YELLOW	1 events (View)
33299	2013-04-05 09:23:04	Russia_GlobalNet	60	0.00	0	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	GREEN	7 events (View)
33271	2013-04-05 07:47:05	Russia_GlobalNet	60	3.00	2	snov1_google.com_URL_BE	BE	data_srv	SDLossPercent	YELLOW	12 events (View)

Рисунок 93 Табло алармов с историей по отдельному объекту



## Создание пользовательских отчетов

Функционал отчетов, определяемых пользователем, позволяет создавать собственные структуры табличных отчетов. В поставку системы уже включен ряд пользовательских отчетов (см. раздел Предустановленные пользовательские отчеты).

Для создания собственного пользовательского отчета требуется сформировать SQL-запрос или серию SQL-запросов к данным, размещенным в базе IQM.

*Подробнее о структуре таблиц IQM и значениях полей см. [sql-base-structure-guide.pdf](#) (IP Quality Monitor: Структура базы данных. Руководство администратора), см. так же [/home/iqm/iqmm/sql/create\\_cfg\\_tables.sql](#).*

В процессе выполнения серии запросов будет формироваться требуемая структура данных, необходимая для итоговой выборки. Последний запрос должен выполнять выборку данных. На основе данных итоговой выборки будет сформирован отчет в интерфейсе пользователя.

Для обработки и хранения промежуточных данных во временных таблицах, необходимых для формирования пользовательского отчета предусмотрена выделенная база данных с именем `iqm_reports`:

```
drop database IF EXISTS iqm_reports;  
CREATE DATABASE IF NOT EXISTS iqm_reports DEFAULT CHARACTER SET 'utf8';
```

Пользователь `iqmweb` имеет права на создание временных таблиц в базе `iqm_reports`:

```
GRANT SELECT, INSERT, UPDATE, DELETE, CREATE TEMPORARY TABLES  
ON `iqm_reports`.* TO 'iqmweb'@'localhost'
```

Для создания и отладки SQL-скрипта удобно пользоваться GUI инструментарием MySQL Workbench. Доступны дистрибутивы для различных операционных систем Windows, Linux, MacOS.

*Дистрибутивы, документация а так же исходные коды MySQL Workbench доступны на сайте разработчика:  
<https://www.mysql.com/products/workbench/>*

По умолчанию, доступ к MySQL базе данных IQM разрешен для пользователя `iqmweb` с `localhost`. Для подключения GUI клиента к базе данных MySQL рекомендуется воспользоваться SSH-тоннелем (см.Рисунок 94).

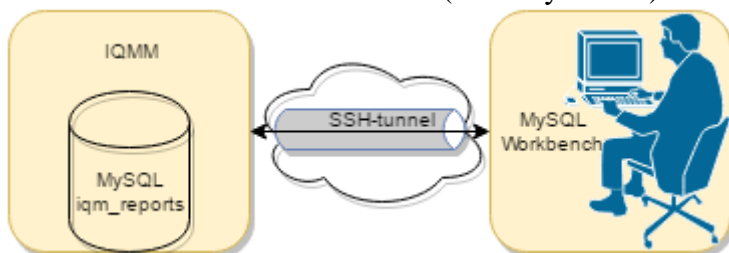


Рисунок 94 Доступ к MySQL базе IQMM через SSH-туннель

Разумеется, выбор MySQL-клиента и способа его подключения оставляется на усмотрение пользователя.

Для формирования пользовательского отчета воспользуйтесь формой REPORTS CONFIGURATION. Форма вызывается через пункт меню:

*Configuration – Custom reports*

Administration Configuration Statistics Graphics IP TV Group reports  
 IQM Agents Collectd Alarm actions SLA Policy Custom reports

NETPROBE

IQMM - [logged as admin] - REPORTS CONFIGURATION:  
 REPORTS CONFIGURATION

+ add ↻ fill form CSV 🔍 view ✓ change ✗ delete 🗑 clear ⚙ expert

Parameter	Value	Default
Report ID	<input type="text"/>	
Report name	<input type="text"/>	
Description	<input type="text"/>	
Query	<input type="text"/>	
Fields definition: field_name:filter_type field_name:filter_type...	<input type="text"/>	
Customer ID	<input type="text"/>	

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 95 Форма конфигурации пользовательских отчетов

Значения полей описаны в таблице ниже:

Поле	Значение
Report ID	Идентификатор, транслированный в Report name. Используется при операциях просмотра, изменения, заполнения формы и удаления.
Report name	Обязательное для заполнения поле. Уникальное символическое обозначение пользовательского отчета. Допускается использование алфавитно-цифровых символов, пробелы.
Description	Текстовое описание.
Query	SQL-скрипт. SQL-запрос или серия SQL-запросов к данным, размещенным в базе IQM. В процессе выполнения серии запросов будет формироваться требуемая структура данных, необходимая для итоговой выборки. Последний запрос должен выполнять выборку



Поле	Значение
	<p>данных. На основе данных итоговой выборки будет сформирован отчет в интерфейсе пользователя.</p> <p>Для обработки и хранения промежуточных данных во временных таблицах, необходимых для формирования пользовательского отчета предусмотрена выделенная база данных с именем <code>iqm_reports</code>.</p> <p>Пользователь <code>iqmweb</code> имеет права на создание временных таблиц в базе <code>iqm_reports</code>.</p>
Fields definition	<p>При необходимости параметр позволяет задать тип полей в итоговой таблице для организации фильтрации по строкам итоговой выборки. Описание следует задавать в формате:</p> <p style="text-align: center;"><u><i>field_name:filter_type field_name:filter_type...</i></u></p> <p>Пример:  <code>agent_filial:select agent_region:select agent_description:text class_name:select bandwidth:number</code></p> <p>Порядок следования полей в определении должен соответствовать порядку, в котором будет осуществлена их выборка. Допускается не задавать тип полей, для которых не требуется фильтрация, эти поля должны идти после полей с определенным типом.</p> <p>Допустимые значения типов полей:</p> <ul style="list-style-type: none"> <li>• <code>select</code> - поля имеют значения из строго определенного набора, будет добавлен выпадающий список, фильтрация строк будет осуществляться по точному совпадению значения поля в строке с заданным значением из списка (см. Определение списка значений для <code>select</code>),</li> <li>• <code>text</code> - текстовое поле, будет добавлено редактируемое поле, фильтрация строк будет осуществляться по частичному совпадению значения поля в строке с введенным в поле значением,</li> <li>• <code>number</code> - числовое поле</li> </ul>
Customer ID	Идентификатор пользователя. Если задан, отчет будет доступен в личном кабинете пользователя.

Пример фильтра в отчете:

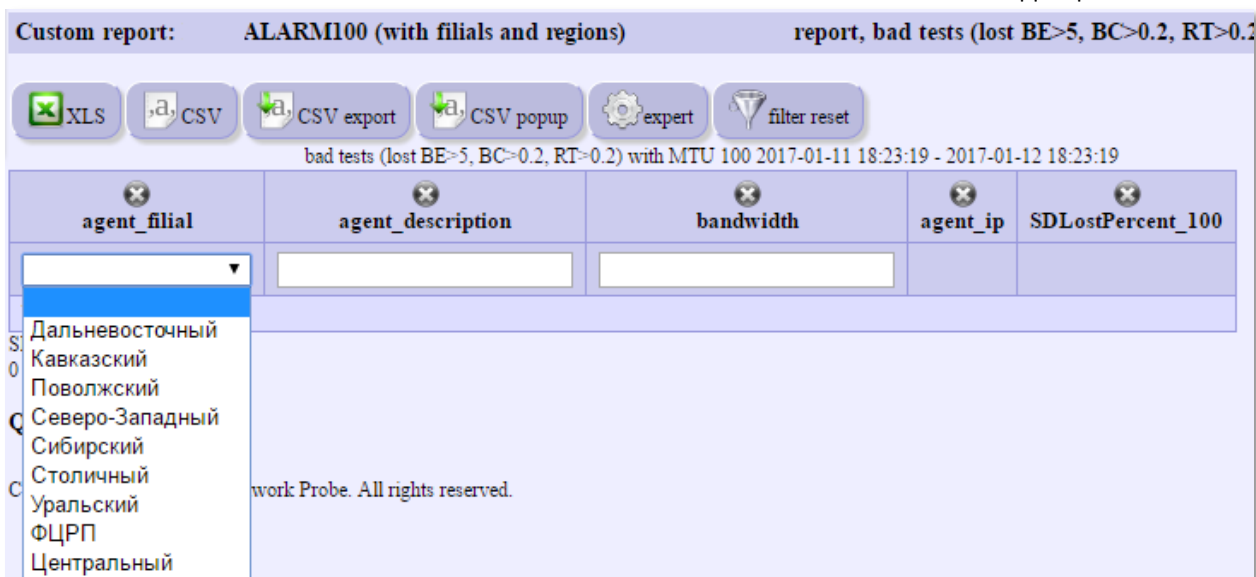


Рисунок 96 Пример полей для фильтрации данных в пользовательских отчетах

## Определение списка значений для select-поля

Для определения набора значений, которыми будет заполнен фильтр для поля типа select потребуется создать VIEW-таблицу в базе `iqm_reports` с полями `id` и `name`. Имя таблицы должно быть определено как `iqm_reports.filter_view_<field_name>`. Например для списка филиалов для фильтрации поля `agent_filial`:

```
use iqm_reports;
CREATE VIEW `filter_view_agent_filial`
AS select `filials`.`name` AS `id`,`filials`.`name` AS `name` from `filials`
```

а для списка классов сервиса для поля `class_name`:

```
use iqm_reports;
CREATE VIEW `filter_view_class_name`
AS select `iqm`.`classes`.`class_name` AS `id`,`iqm`.`classes`.`class_name` AS `name`
from `iqm`.`classes`
```

## Привязка к фильтру и времени

Для привязки запроса в пользовательском отчете к фильтру (см. Фильтры) используйте специальные значения `__TID_LIST__` и/или `__TID_VAL_LIST__`, вместо которых будет совершена подстановка.

`__TID_LIST__`

в запросе будет заменен на:

`test_id IN (<список тестов соответствующих выборке по критериям фильтра>)`

`__TID_VAL_LIST__`

в запросе будет заменен на:

`IN (<список тестов соответствующих выборке по критериям фильтра>)`

Для привязки запроса в пользовательском отчете ко времени, определенному в фильтре (см. Фильтры), используйте специальные значения `__START_DATE__` и/или

\_\_END\_DATE\_\_ вместо которых будет совершена подстановка на значения даты-времени, заданном в фильтре.

Специальные значения \_\_AND\_\_, \_\_OR\_\_, \_\_<ANYTEXT>\_\_ будут заменены на AND, OR, ANYTEXT в случае, если пользователем будут определены критерии в фильтре.

### Пример пользовательского отчета

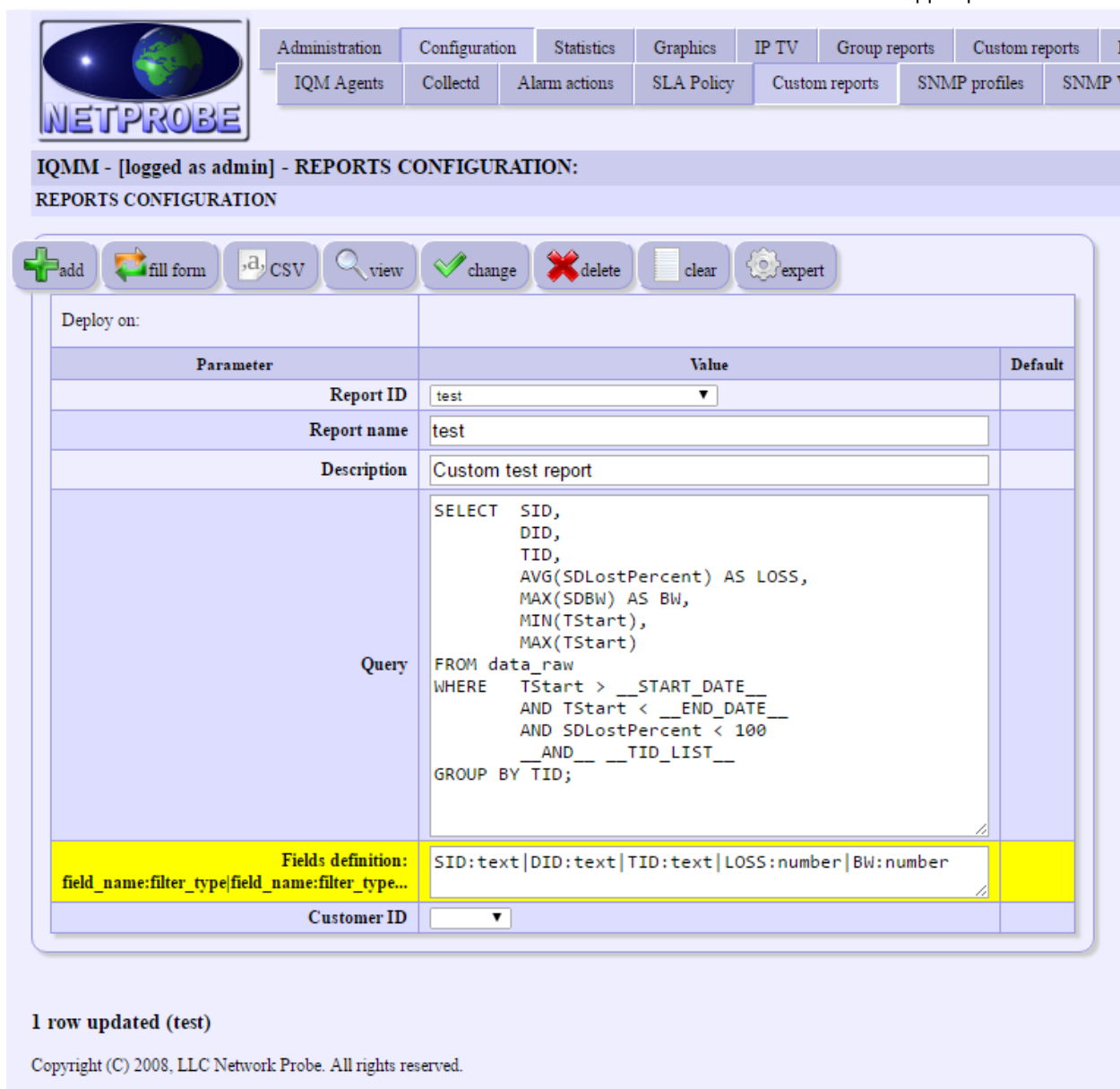
Приведем пример простейшего пользовательского отчета. Отчет будет выводит средние потери в одном направлении и среднюю скорость приема для тестов, соответствующих критериям, заданным в фильтре за заданный период. SQL-скрипт будет состоять из одного запроса, таблица iqm\_report не будет задействована, поскольку данные предварительно не обрабатываются, а выбираются из IQM-базы напрямую. Запрос будет иметь вид:

```
SELECT SID,
       DID,
       TID,
       AVG(SDLostPercent) AS LOSS,
       MAX(SDBW) AS BW,
       MIN(TStart),
       MAX(TStart)
FROM data raw
WHERE TStart >  START DATE
      AND TStart < __END_DATE__
      AND SDLostPercent < 100
      __AND__ __TID_LIST__
GROUP BY TID;
```

для организации фильтрации по строкам итогового запроса параметр Fields definition следует определить как:

```
SID:text|DID:text|TID:text|LOSS:number|BW:number
```

См. Рисунок 97 Пример пользовательского отчета:



Administration Configuration Statistics Graphics IP TV Group reports Custom reports I

IQM Agents Collectd Alarm actions SLA Policy Custom reports SNMP profiles SNMP V

**NETPROBE**

**IQMM - [logged as admin] - REPORTS CONFIGURATION:**  
REPORTS CONFIGURATION

+ add ↻ fill form CSV 🔍 view ✅ change ❌ delete 🗑 clear ⚙ expert

Deploy on:

Parameter	Value	Default
Report ID	test	
Report name	test	
Description	Custom test report	
Query	<pre>SELECT SID,       DID,       TID,       AVG(SDLostPercent) AS LOSS,       MAX(SDBW) AS BW,       MIN(Tstart),       MAX(Tstart) FROM data_raw WHERE Tstart &gt; __START_DATE__       AND Tstart &lt; __END_DATE__       AND SDLostPercent &lt; 100       __AND__ __TID_LIST__ GROUP BY TID;</pre>	
Fields definition: field_name:filter_type field_name:filter_type...	SID:text DID:text TID:text LOSS:number BW:number	
Customer ID		

1 row updated (test)

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 97 Пример пользовательского отчета

## Просмотр пользовательских отчетов

Для просмотра отчета воспользуйтесь формой Custom reports. Форма вызывается через пункт меню верхнего уровня:

### *Custom reports*

Во вкладке Conditions следует выбрать идентификатор нужного отчета. В случае, если отчет поддерживает привязку к датам и к фильтру (см. Привязка к фильтру и времени) определите критерии фильтрации и временные границы (см. Фильтры).

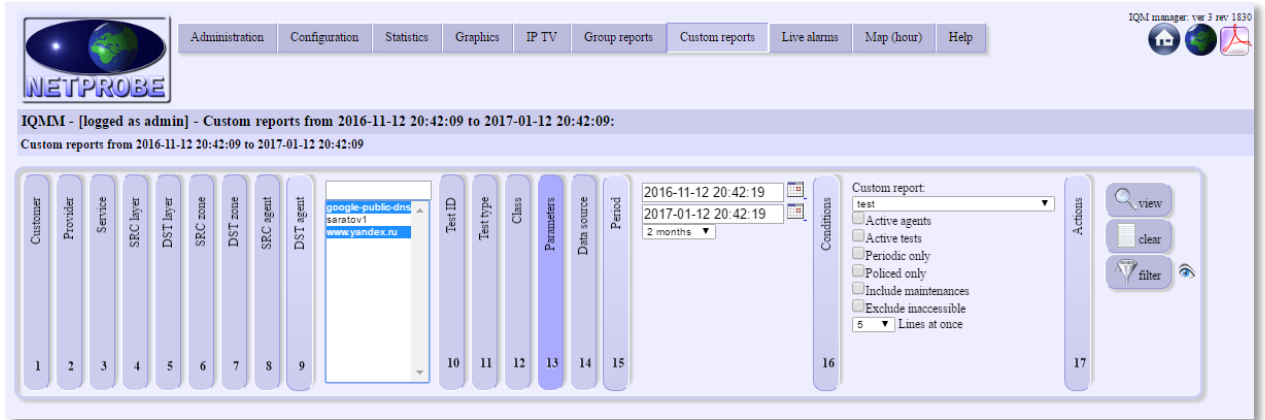



Рисунок 98 Фильтр пользовательских отчетов

После нажатия на кнопку  View система выполнит заданный для отчета SQL-скрипт и выдаст результат выполнения в форме таблицы. Рисунок 99 иллюстрирует вывод отчета, созданного на примере из раздела Пример пользовательского отчета.

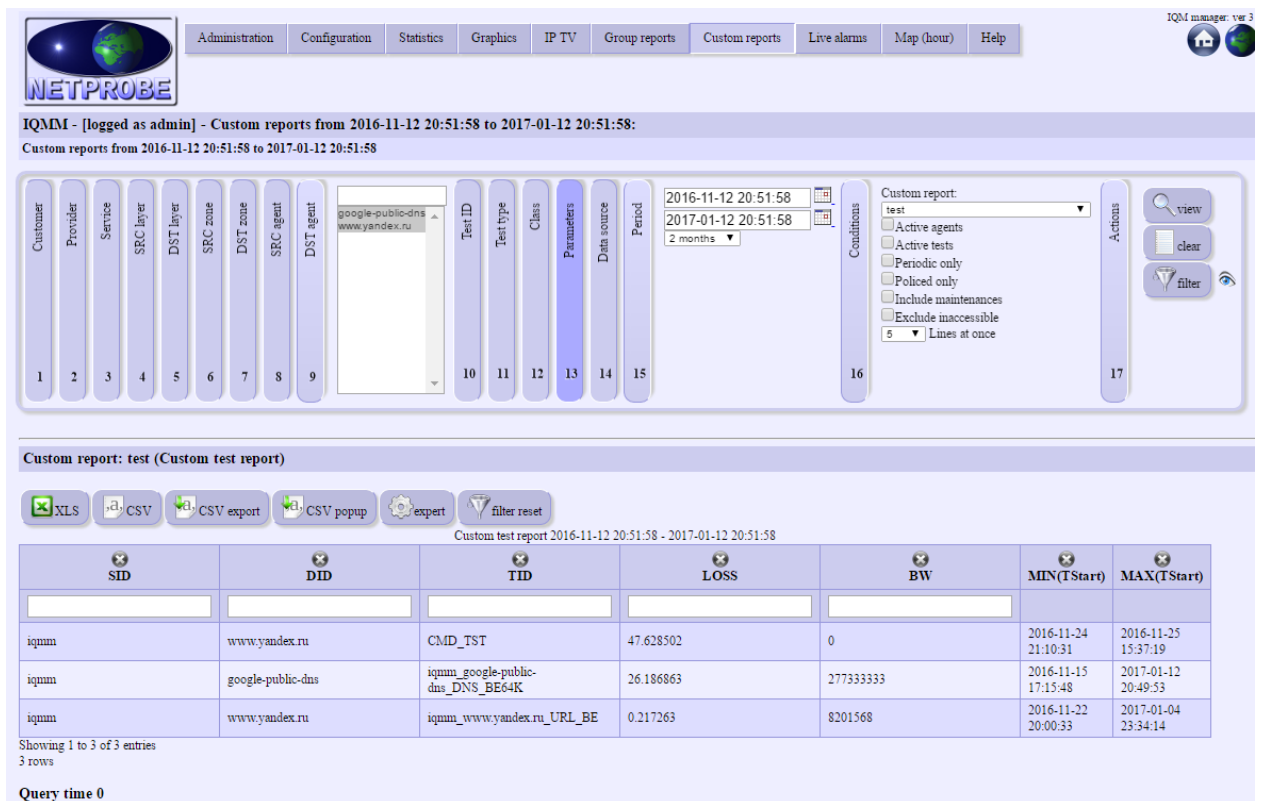


Рисунок 99 Вывод тестового пользовательского отчета

## Предустановленные пользовательские отчеты

## alarms db (alarms dashboard)

Custom report: alarms db (alarms dashboard)

XLS
 CSV
 CSV export
 CSV popup
 expert
 filter reset

alarms dashboard 2017-01-10 19:23:20 - 2017-01-11 19:23:20

Test descr	SDLost (%)	DSLost (%)	AvgRtt (ms)	SDJitter (ms)	DSJitter (ms)	Graph
iqmm_google-public-dns_DNS_BE64K	26.00 CRIMSON 07:39:00 <a href="#">alarm history png csv</a>	0.00	6 GREEN 05:15:00 <a href="#">alarm history png csv</a>	4 CRIMSON 06:37:59 <a href="#">alarm history png csv</a>	0	<a href="#">Graphics</a>
iqmm_www.yandex.ru_URL_BE	100.00 CRIMSON 07:39:00 <a href="#">alarm history png csv</a>	0.00	0	0	0	<a href="#">Graphics</a>

2 rows

Query time 2

Copyright (C) 2008, LLC Network Probe. All rights reserved.

Рисунок 100 Пользовательский отчет alarms db (alarms dashboard)

Отчет представляет список тестов с нарушениями на текущий момент. Приводятся значения параметров.

## point db (point dashboard)

Custom report: point db (point dashboard)

XLS
 CSV
 CSV export
 CSV popup
 expert
 filter reset

point dashboard 2017-01-10 19:17:51 - 2017-01-11 19:17:51

Test descr	Date	SDLost (%)	DSLost (%)	AvgRtt (ms)	SDJitter (ms)	DSJitter (ms)	Graph
iqmm_google-public-dns_DNS_BE64K	2017-01-11 19:17:09	26.00	0.00	5	3	0	<a href="#">Graphics</a>
iqmm_www.yandex.ru_URL_BE	2017-01-11 19:03:39	100.00	0.00	0	0	0	<a href="#">Graphics</a>

2 rows

Рисунок 101 Пользовательский отчет point db (point dashboard)

Отчет представляет текущие значения параметров для каждого контролируемого направления, при наличии нарушения параметр подсвечивается в цвет тревоги (Даже, если текущее значение параметра возвратилось в норму).

## SLA Lost (SLA lost packets report)

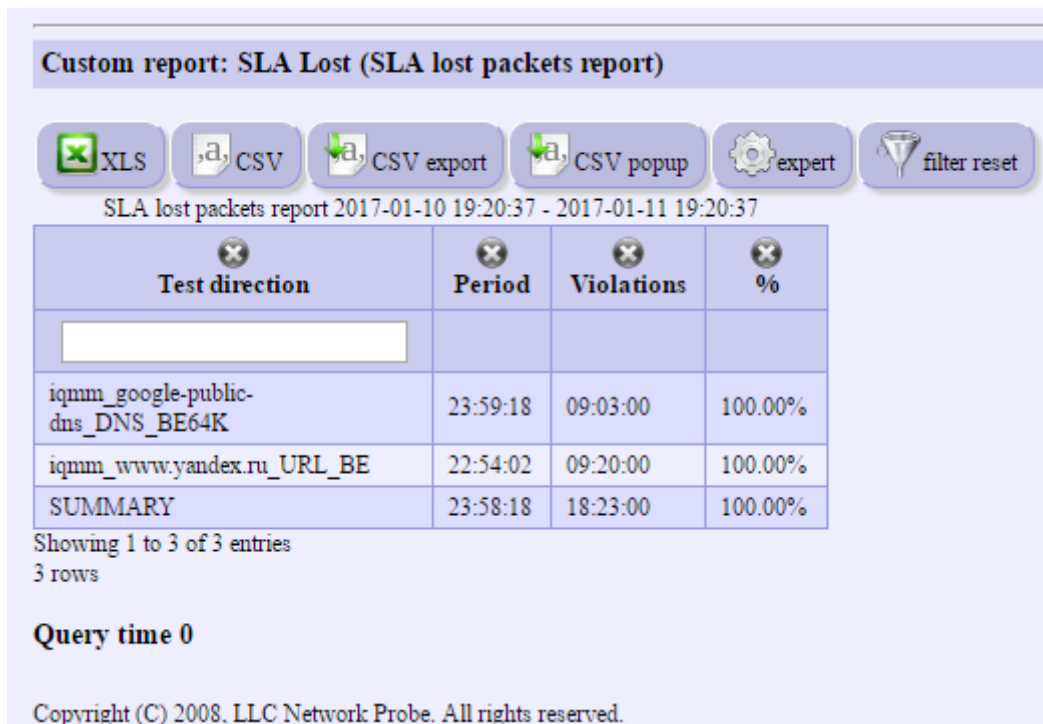


Рисунок 102 Пользовательский отчет SLA Lost (SLA lost packets report)

Отчет SLA Lost выполняет расчет периодов с нарушениями SLA по параметру Lost.

## Params report #1 (Граничные значения параметров для транспортных тестов #1)

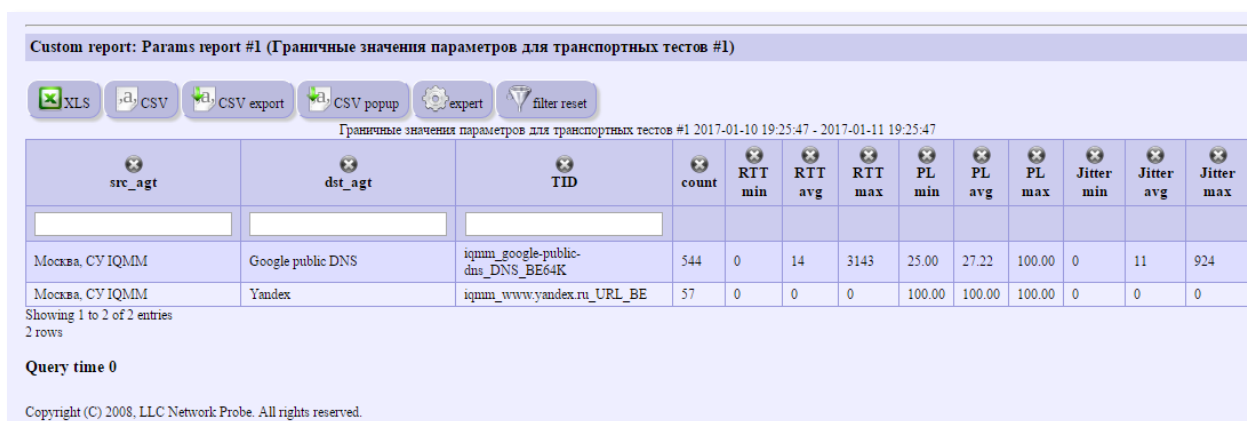


Рисунок 103 Пользовательский отчет Params report #1 (Граничные значения параметров для транспортных тестов #1)

Отчет по параметрам представляет граничные значения потерь, круговых задержек и вариации задержек для заданного временного периода. Отражаются минимальные, средние и максимальные значения, количество проведенных измерений.

Аналогичные отчеты:

- Params report #1 (without 100% loss) - исключены измерения с 100% потерь
- Params report #1 (SD and DS) - с расчетом для каждого направления передачи

## Пользовательское табло мониторинга

Пользовательское табло мониторинга состоит из двух пользовательских отчетов:

- `_NP_ALARMS_DB_` (Alarms dashboard (NetProbe)) - отчет по алармам
- `_NP_LIVE_ALARMS_DB_` (Live alarms (NetProbe)) - отчет по срочным алармам

Оба отчета скомбинированы на отдельной странице с возможностью включения и выключения нужных отчетов, выбора режима обновления. Панель доступна через пункт меню верхнего уровня:

### Live alarms

Панель автоматически обновляется (при включенном `autoupdate (min)`) и позволяет наблюдать поступление срочного аларма и его последующий переход в системный.

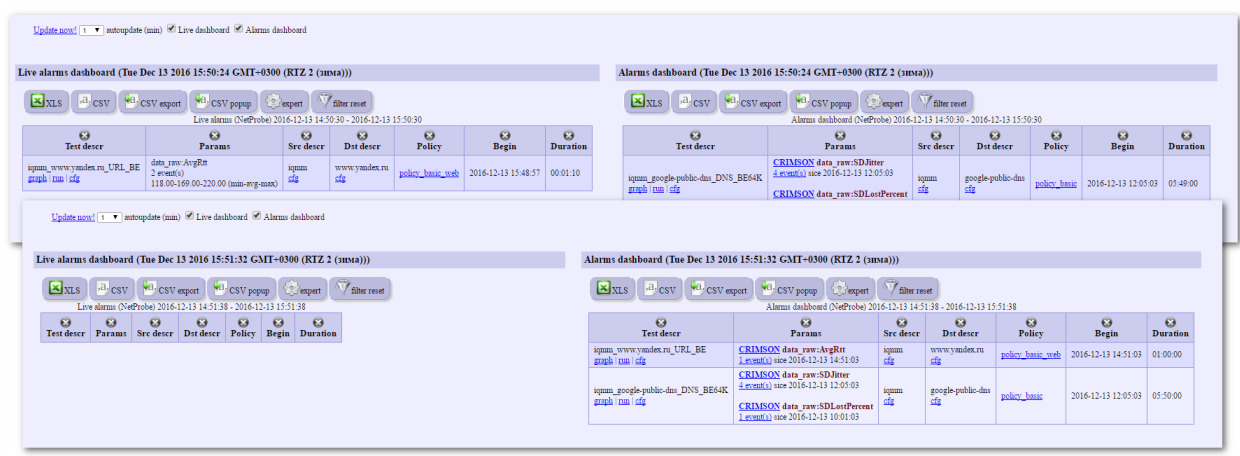


Рисунок 104 Пользовательское табло мониторинга

## Список документов

1. Обзор решения IP Quality Monitor (IQM). Файл `IQM-overview-new-v<редакция>.pdf`.
2. IP Quality Monitor (IQM). Реализованные функции. Файл `IQM-implemented-features-v<редакция>.pdf`.
3. IQM: часто задаваемые вопросы. Файл `IQM-FAQ-v<редакция>.pdf`.
4. IQM Manager - руководство пользователя. Файл `IQM-Manager-UG-v<редакция>.pdf`.
5. IP Quality Monitor: Структура базы данных. Руководство администратора. Файл `sql-base-structure-guide.pdf`.
6. IQM: запуск мониторинга IP TV. Файл `IQM-IPTV-INIT-v<редакция>.pdf`.
7. Аппаратные платформы IQMA. Спецификации. Файл `Спецификации на пробники v<редакция>.pdf`.
8. IP Quality Monitor. Настройка ip-адресов устройства `ipplug`. Руководство пользователя. Файл `iqm-ipplug-ip-address-set-v3-0.pdf`.
9. IQM Agent: конфигурация агента на платформе SLAX. Файл `IQMA-CG v<редакция>-slax_rus.doc`
10. Личный кабинет. IQMM v3. Файл `IQMM-personal-account-v<редакция>.pdf`.