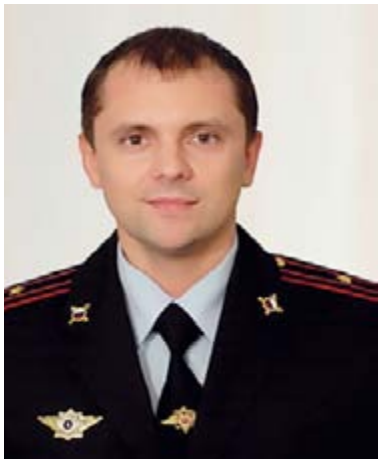

Универсальная система мониторинга работоспособности сети и параметров каналов передачи «Zabbix»

Алексеев
Александр Владимирович,
заместитель начальника – начальник ОИТ ЦИТСиЗИ
ГУ МВД России по Ростовской области,
майор внутренней службы

Применение современных информационных технологий играет все большую роль в решении задач, возложенных на органы внутренних дел. Использование в служебной деятельности информационно-телекоммуникационной инфраструктуры прописано в Федеральном законе №3-ФЗ от 7 февраля 2011 года «О полиции». При этом объем технологических решений и сервисов, применяемых в повседневной деятельности органов внутренних дел, постоянно растет, и, следовательно, повышаются требования к качеству предоставляемых телекоммуникационных услуг и надежности функционирования инфраструктуры связи. К сожалению, аварий и сбоев в работе телекоммуникационного оборудования не избежать, а значит одной из основных задач подразделений информационных технологий, связи и защиты информации на современном этапе развития является минимизация времени «простоя» телекоммуникационного оборудования и соответствующих последствий. В этой связи особое внимание следует уделить вопросам контроля работоспособности не только телекоммуникационного оборудования, эксплуатируемого в территориальных органах и подразделениях системы МВД России, но и бесперебойной работе каналов связи, в том числе предоставляемых сторонними операторами связи, соответствия предоставляемых каналов установленным параметрам качества. Круглосуточный контроль бесперебойного функционирования отдельных составных частей информационно-технологической инфраструктуры (маршрутизаторов, коммутаторов, IP-станций, каналов связи) — непосильная задача для администратора.

Для реализации задач мониторинга оборудования и каналов связи ведомственного сегмента сети передачи данных в ГУ МВД России по Ростовской области используется программно-аппаратный комплекс на базе системы мониторинга и контроля работоспособности каналов передачи данных «Zabbix».

«Zabbix» состоит из нескольких частей:

- сервера мониторинга, обеспечивающего обработку получаемых данных, их анализ, запуск скриптов оповещения;
- базы данных (MySQL, PostgreSQL, SQLite или Oracle);
- Web-интерфейса на PHP;
- агента — демона, который запускается на отслеживаемых (контролируемых) объектах и предоставляет данные серверу. Агент опционален, мониторинг можно производить не только с помощью него, но и по SNMP (версий 1, 2, 3), запуском внешних скриптов, выдающих данные, и нескольких видов предопределенных встроенных проверок, таких как ping, запрос по http, ssh, ftp и другим протоколам, а также измерением времени ответа этих сервисов.

Основная логическая единица — узел сети (host), сервер или маршрутизатор, находящиеся под наблюдением (рис. 1). Каждому узлу сети присваивается описание и адрес (dns или ip, можно оба, причем с возможностью выбирать, что использовать для соединения).

Узлы объединяются в группы (например, маршрутизаторы, серверы или ip-станции). Группы служат для вывода только определенных объектов при наблюдении (рис. 2).

Рис.1 Узлы сети ГУ МВД России по Ростовской области

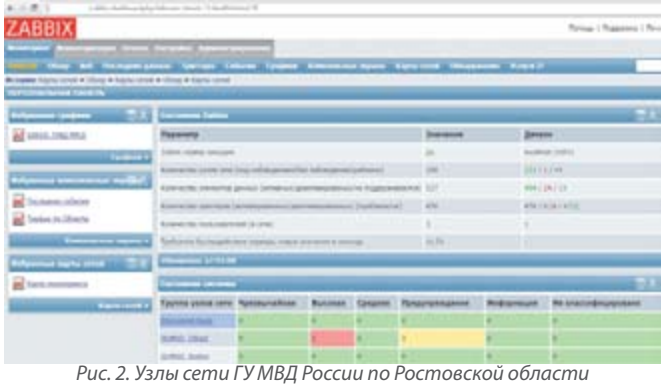

Рис. 2. Узлы сети ГУ МВД России по Ростовской области

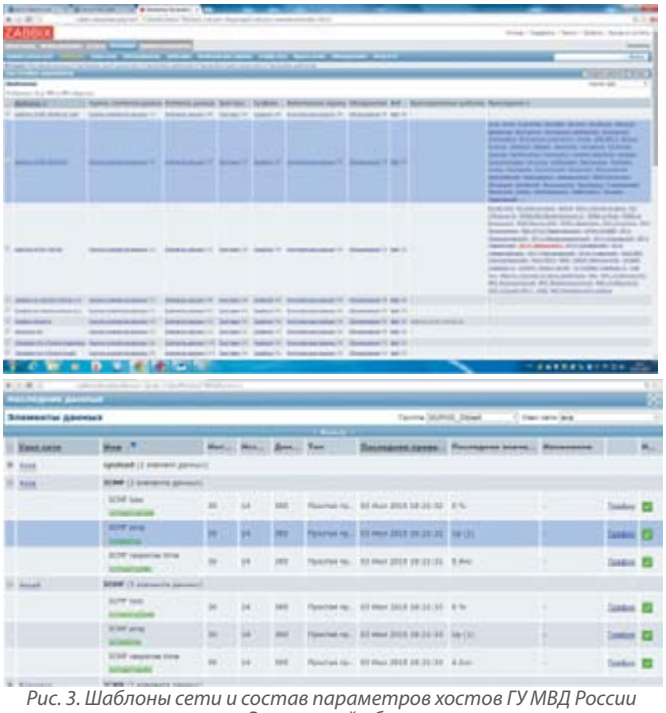

Рис. 3. Шаблоны сети и состав параметров хостов ГУ МВД России по Ростовской области

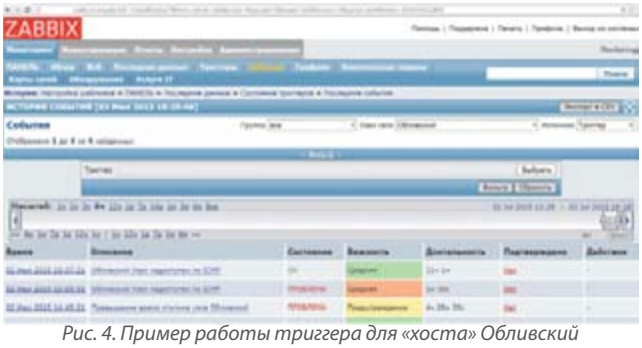

Рис. 4. Пример работы триггера для «хоста» Обливский

Рис. 5. График изменения трафика для отдела Таганрог

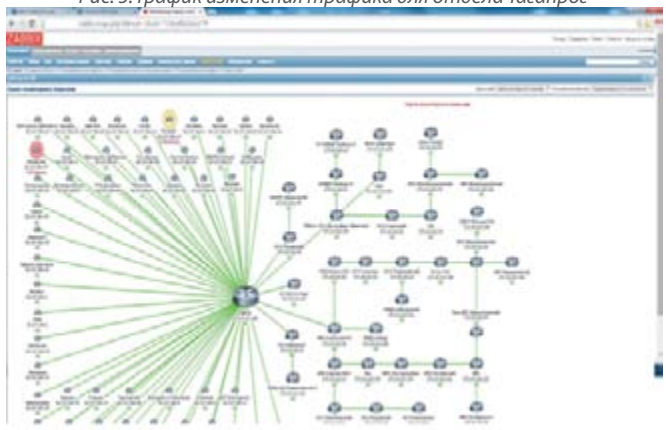

Рис. 6. Фрагмент карты сети ГУ МВД России по Ростовской области

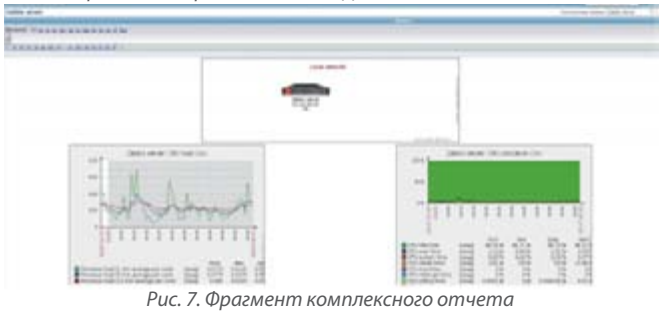

Рис. 7. Фрагмент комплексного отчета

Создавать элементы данных для каждого из множества маршрутизаторов сложно, поэтому можно создать узлы-шаблоны. Эти узлы тоже содержат элементы данных, но они не «мониторятся» напрямую. Вместо этого реальный хост связывается с одним или несколькими шаблонами, и все параметры шаблона автоматически наследуются хостом. Так, элемент ping хранится именно в шаблоне и просто связывает все хосты с шаблоном, например — шаблон «ICMP ОБЛАСТЬ» (рис. 3).

Человек — не робот, следить за тысячами параметров и думать, не выходит ли это значение за допустимые границы, просто нереально. «Zabbix» предоставляет гибкие возможности по настройке условий — триггеров, которые включаются при авариях и неполадках. Система начинает «моргать лампочками», показывая администратору, что имеется неисправность. В упомянутом выше шаблоне есть триггер, который реагирует на отсутствие «пинга» (рис. 4).

Если администратора нет на месте, «Zabbix» достаточно самостоятелен и сможет отправить уведомление о неисправности на электронную почту, или sms-сообщение с помощью gsm-модема и даже попытаться самостоятельно восстановить сервис, выполнив заранее определенный алгоритм действий, которые запускаются при срабатывании определенных триггеров.

По данным любого параметра система сможет построить график изменения, причем не за предопределенные и жестко заданные временные интервалы, а за любой промежуток времени с максимальным разрешением.

Можно создавать и более сложные графики, отображающие на одном поле несколько параметров.

Для отображения логической структуры сети можно создавать карты сети, отображающие расположение узлов сети и связей между ними. Естественно, состояние узлов (доступен или недоступен) отображается и на карте (рис. 6).

Кроме того, для более удобного обзора есть различные комплексные отчеты, которые позволяют на одном экране просматривать сразу несколько сущностей — графики, данные, триггеры (рис. 7).

Zabbix — довольно мощная и обширная система, в запасе у нее есть еще полдесятка функций, которые позволяют еще больше упростить наблюдение за сетью, серверами и хостами сети.

Использование системы Zabbix в ГУ МВД России по Ростовской области позволяет оперативно и своевременно реагировать на сбои в работе технологического оборудования, всегда иметь актуальную информацию о сети в целом и возможность анализа в случае аварии, а также сократить количество привлекаемого личного состава ЦИТСиЗИ ГУ МВД России по Ростовской области для оценки состояния и времени реагирования.