Визитка

СЕРГЕЙ ЯРЕМЧУК, фрилансер. Автор более 800 статей и шести книг. С «СА» с первого номера. Интересы: сетевые технологии, защита информации, свободные ОС

Система мониторинга Zenoss Core

Системы мониторинга наблюдают за состоянием устройств в сети и позволяют предупредить проблемы еще до их появления. Zenoss даст фору многим проприетарным продуктам

В сетях даже небольших организаций насчитывается не один десяток устройств самого разного назначения. Некоторые из них должны быть доступны 24 часа семь дней в неделю, другие время от времени. Но выход из строя или проблемы с любым из них означают прерывание бизнес-процессов, потерю или недовольство клиентов, а значит, упущенную прибыль. Постоянный мониторинг сервисов и ресурсов позволяет определить большую часть проблем и среагировать еще до того, как произойдет сбой. Если же аварийная ситуация произошла, то подобные системы автоматически оповестят админа, который может среагировать раньше, а значит, и недовольных будет меньше.

В журнале уже рассматривались различные системы мониторинга, доступные под открытой лицензией, – Nagios [1], GroundWork Monitor [2], Cacti [3], Zabbix [4] и другие. Каждая из них обладает интересными возможностями, имеет многочисленных как сторонников, так и противников. Но возможность выбора – это всегда хорошо, особенно что касается Open Source, поскольку можно подобрать наиболее подходящее для конкретных условий решение. В данной статье познакомимся с возможностями и основными настройками системы мониторинга Zenoss Core [5].

Возможности Zenoss Core

Распространяемая под лицензией GPL система мониторинга сетевой инфраструктуры Zenoss Core, несмотря на бесплатность, – это серьезное решение уровня предприятия. Начало разработок датируется 2002 годом, новый проект позиционировался как открытая альтернатива таким популярным решениям, как IBM Tivoli, HP OpenView, BMC Patrol. Но в открытом доступе на SourceForge.net Zenoss Core появился лишь спустя четыре года, когда была уже практически готова версия 1.0. С тех пор различные релизы с этого сайта скачаны более миллиона раз, что косвенно подтверждает популярность и доверие пользователей. За этот период была образована Zenoss Inc., которая впоследствии стала продвигать коммерческую ветку продукта Zenoss Enterprise, отличающуюся наличием дополнительных модулей и официальной поддержкой. Кстати, Zenoss Enterprise используется в таких известных компаниях, как VMware, NASA, Motorola, ATI. Также Zenoss Inc. обеспечивает финансовую поддержку и разработку GPL-версии системы. Кроме оригинальных разработок, в Zenoss Core для сбора и анализа информации используются другие открытые решения – Net-SNMP, RRDtool, Twisted. Написан на языке Python с использованием сервера приложений Zope, данные хранятся в MySQL.

Система, построенная на Zenoss Core, обеспечивает следующие возможности:

- мониторинг сетевых устройств с помощью SNMP, SSH, WMI, JMX, Ping/ICMP и Syslog;
- мониторинг сетевых сервисов – HTTP, POP3, NNTP, SNMP, FTP;
- мониторинг системных ресурсов популярных операционных систем;
- мониторинг производительности устройств;
- система оповещения с настраиваемыми событиями, реакцией и обнаружением взаимосвязи;
- возможность расширения функциональности за счет плагинов собственной разработки ZenPack и плагинов системы мониторинга Nagios.

Функция автообнаружения позволяет быстро собрать информацию обо всех активных системах в сети. При этом ядро Zenoss умеет анализировать среду, что дает возможность быстро разобраться с большим количеством специфических устройств. Параметры, собранные разными способами, нормализуются с использованием шаблонов и приводятся к единому виду.

В случае обнаружения проблем Zenoss может не только отправить сообщение администратору, но и, например, выполнить команду на перезапуск сервиса.

Список ZenPacks, доступных на сайте проекта, довольно внушительный и насчитывает более 200 наименований. Здесь можно найти расширения для мониторинга ряда устройств (APC, Cisco, Dell), сервисов (Asterisk, VMware, Ganglia, MySQL, Microsoft IIS) и многого другого. Относительно недавно в этом списке появились ZenPacks, добавляющие возможность управления и мониторинга удаленных систем с помощью Puppet [8] и Cfengine [9].

Для установки сервера Zenoss потребуется компьютер, работающий под управлением Linux, FreeBSD, Solaris/OpenSolaris, Mac OS X или VMware Appliance.

На клиентских компьютерах программа-агент не устанавливается, это упрощает развертывание. Для построения карт сетей и обнаружения систем и сервисов применяется автоматическое сканирование. Управление производится с помощью веб-интерфейса. Полностью поддерживаются браузеры Firefox 3 и Internet Explorer 7 и 8, для остальных заявлена лишь частичная совместимость.

При написании статьи автор несколько дней работал с Chromium 9.0, особых проблем не заметил. Интерфейс в настоящее время не локализован, вероятно, потому, что в этом нет особого смысла. Все термины общеупотребляемы, поэтому человек с базовым английским может разобраться с настройками в Zenoss без особого труда. При желании локализацию можно провести самостоятельно.

Чтобы получать сообщения в реальном времени на рабочий стол, отдельно устанавливаются специальные аплеты Zapplet [10] или ZenTrayIcon. При этом работа Zapplet возможна только на Linux (в будущем планируется порт под Windows), ZenTrayIcon [11] протестирован под Fedora 7 и Windows XP.

Также хочется отметить вполне подробную документацию на английском языке и наличие своего канала на YouTube [12].

Установка Zenoss в Ubuntu 10.04 LTS

На сайте Zenoss, кроме исходных текстов, доступны x86- и x64-пакеты под популярные дистрибутивы Linux: RHEL, CentOS, Fedora, Ubuntu, Debian, Debian и SUSE/openSUSE в двух вариантах: Stack и Native. Их функциональность одинакова, но Stack – это двоичный универсальный .bin-инсталлятор, позволяющий задать в процессе дополнительные параметры и имеющий, в числе прочего, графический интерфейс. Вариант Native – обычный deb- или rpm-пакет, устанавливаемый с помощью штатного пакетного менеджера дистрибутива. Кроме того, для Debian/Ubuntu разработчики предлагают репозитарий, подключаемый в /etc/apt/sources.list строкой:

```
deb http://dev.zenoss.org/deb main stable
```

Далее будет рассмотрена установка в вариантах Stack и Native. Начнем со Stack как с более универсального.

Минимальные системные требования, которые даны на сайте проекта, двухядерный CPU, 4 Гб RAM и 300 Гб жесткий диск, соответствуют мониторингу 1 – 250 устройств.

В дальнейшем будем рассматривать установку Zenoss в Ubuntu 10.04 LTS.

С помощью APT ставим MySQL и компоненты SNMP:

```
30 17 * * * /mnt/sdb1/datadir.tar.gz /home/user/datadir
```

Настроим SNMP:

```
$ sudo cp /etc/snmp/snmpd.conf /etc/snmp/snmpd.conf.bak
```

Генерируем файл, копируем его на место и перезапускаем сервис:

```
$ sudo snmpconf
$ sudo cp snmpd.conf /etc/snmp/
$ sudo service snmpd restart
```

Проверяем работу:

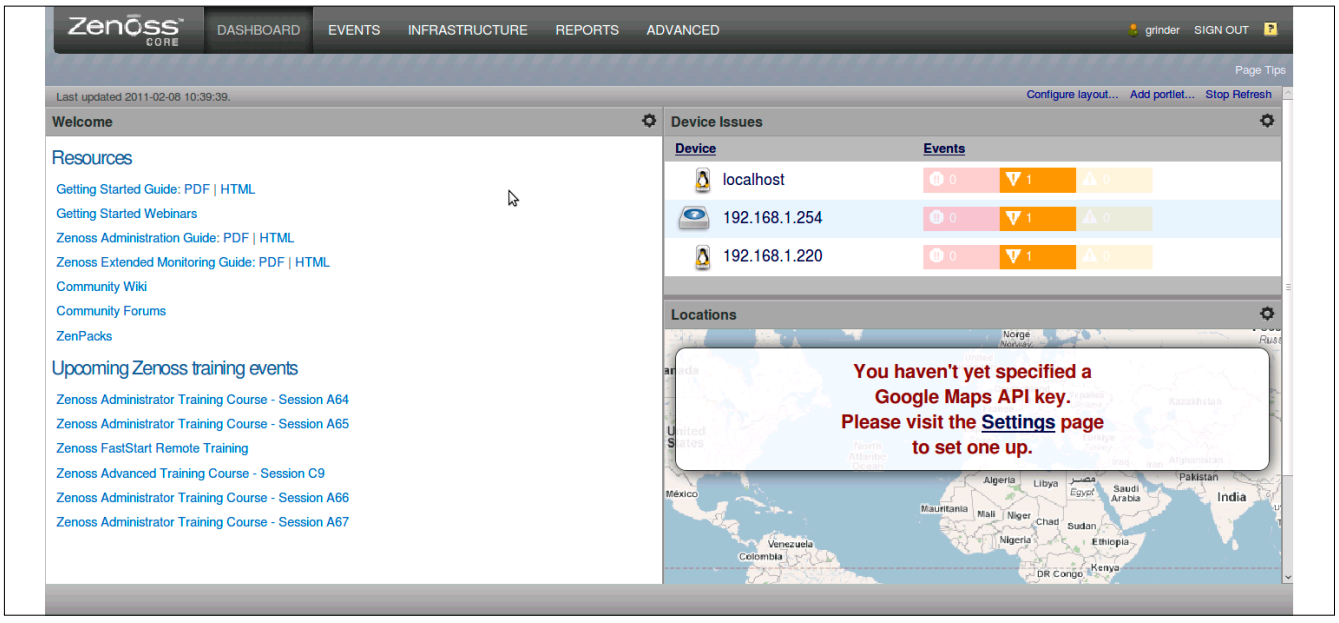
```
$ snmpwalk -v2c -c public 127.0.0.1 system
```

Скачиваем по ссылке на сайте проекта установочный файл и запускаем:

```
$ chmod +x zenoss-stack-3.0.3-linux-x64.bin
$ sudo ./zenoss-stack-3.0.3-linux-x64.bin
```

Появляется мастер установки, продвигаясь по шагам, указываем каталог, в который устанавливается Zenoss (по умолчанию /usr/local/zenoss), и пароль доступа пользо-

Рисунок 1. Панель Zenoss по умолчанию



вателя root к MySQL. После этого начнется процесс распаковки пакета, установка и создание базы данных.

Скрипт с расширением bin удобен тем, что поддерживает несколько дополнительных ключей и режимов. Полный список можно получить с помощью параметра -help. Так, по умолчанию для управления Zenoss через веб-интерфейс используется порт 8080, в случае если он свободен, скрипт не выдаст запрос, иначе одним из шагов установки предстоит указать номер порта. Используя ключ --zope_server_port, номер порта можно указать сразу на этапе установки, при работе в текстовом терминале используется --mode=text. Также возможно использование подготовленного файла ответов.

Если выбран deb-пакет, то команда стандартна:

```
$ sudo dpkg -i ./zenoss-stack-3.0.3_x64.deb
```

При использовании репозитария следует просто установить пакет zenoss-stack:

```
$ sudo apt-get update
$ sudo apt-get install zenoss-stack
```

Если сервер MySQL установлен на другом компьютере, следует указать его данные с помощью ключей -mysql* (для bin) или вручную прописать данные в файле zenoss/bin/zenoss_init_pre:

```
# environment variable
export OS_USERNAME="zenoss"
export OS_UID="1001"
export ZENHOME="/usr/local/zenoss/zenoss"
export MYSQLHOST="localhost"
export MYSQLPORT="3307"
export MYSQLROOTUSER="root"
export MYSQLROOTPASSWD="myslq_passwd"
export MYSQLUSER="zenoss"
export MYSQLPASS="zenoss"
```

Данные, указанные в MYSQLUSER и MYSQLPASS в Zenoss, устанавливаются по умолчанию, в целях безопасности пароль лучше изменить.

Также документация проекта рекомендует увеличить значения некоторых системных параметров в /etc/sysctl.conf:

```
$ sudo nano /etc/sysctl.conf
net.core.rmem_default=1048576
net.core.rmem_max=1048576
net.core.wmem_default=1048576
net.core.wmem_max=1048576
```

В правилах межсетевого экрана следует открыть порты 8080 (веб-интерфейс Zenoss), 514 (Syslog) и 162 (SNMP).

Проверяем, слушается ли нужный порт:

```
$ netstat -ant | grep 8080
```

Если нет, то запускаем Zenoss:

```
$ sudo service zenoss-stack start
```

И обеспечиваем автозапуск:

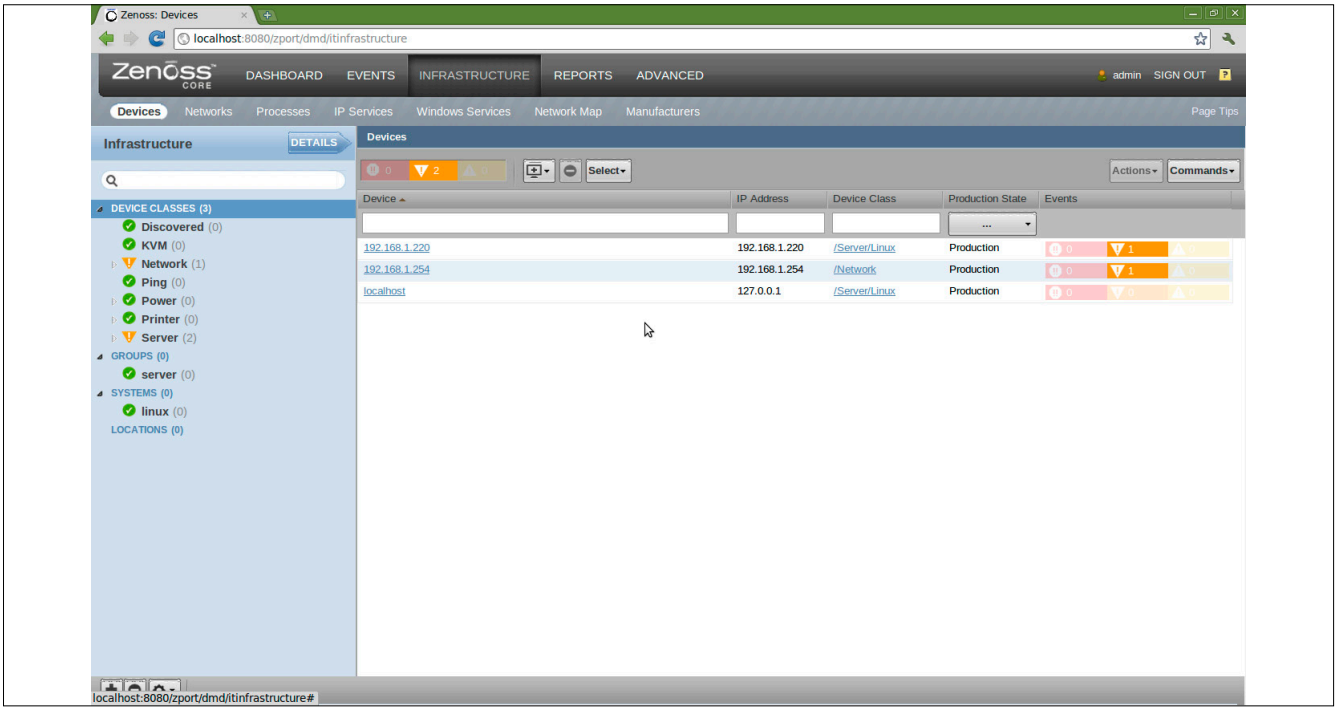
```
$ sudo update-rc.d zenoss-stack enable S
```

Открываем в веб-браузере страницу Zenoss (http://localhost:8080) и приступаем к предварительным настройкам. Необходимо пройти всего два шага. Выбираем Get Started и на Set Up Initial Users, вводим пароль администратора (admin) и создаем новую учетную запись обычного пользователя.

Следующий шаг позволяет добавить устройства для мониторинга. Здесь доступны два варианта: ручной (Manually find devices) и автоматический (Autodiscover devices) поиск.

В первом случае необходимо указывать имя или IP-адрес системы, и в окне справа выбрать тип SNMP (Linux Server, Windows Server или Generic Switch/Router).

Рисунок 2. Найденные при сканировании сети устройства и системы



В случае автоматического поиска устройств необходимо задать диапазон IP, указать пароль root для доступа к UNIX-системам через SSH или пароль администратора Windows. Локальная система будет добавлена автоматически. При желании можно отказаться на этом этапе от добавления устройств. Подтверждаем выбор, после чего загрузится панель Zenoss.

Если для работы выбран VMware, всего этого нет, для регистрации через веб-интерфейс используем логин root и пароль zenoss.

Панель администрирования Zenoss

Панель Zenoss состоит из нескольких меню. После регистрации пользователь попадает в Dashboard, в котором выводится основная информация. Состоит Dashboard из сменных панелей-портлетов (portlets), которые можно удалять, устанавливать и настраивать по своему усмотрению. По умолчанию это панели Welcome (ссылки на документацию), Device Issues (статистика по устройствам) и Locations (показывает расположение устройств на Google Maps). Для корректности работы последнего потребуется ключ Google Maps API [11]. В правом углу портлета находится кнопка, нажатие на которую вызовет меню настроек, откуда можно в том числе и удалить портлет с панели. Расположение портлетов изменяется с помощью кнопки Configure Layot, при нажатии Add portlet получим список из девяти возможных портлетов, просто выбираем нужный, он появляется в поле, и затем перетаскиваем на свое место.

Список портлетов, доступных пользователям с разными правами, настраивается в Advanced → Setting → Portlets.

Добавляем устройства

Начинать работу надо с меню Infrastructure, в котором собраны все системы и устройства, известные Zenoss. Для удобства они разбиты по классам (автоматически), группам, системам и расположению. Напротив каждого устройства показывается значок, говорящий о его состоянии. Чтобы добавить новое устройство или компьютер, достаточно нажать кнопку с изображением знака «+», выбрать вариант (один или несколько компьютеров) и затем указать параметры поиска. Всплывающая подсказка сообщит, что новое задание выполняется. По завершении можно получить доступ к найденным устройствам, просто выбрав их в окне программы. По умолчанию все системы автоматически распределяются по классам (Device Classes), в случае ошибки класс можно изменить, просто перетащив мышкой ярлык на свое место.

В подменю Modelles Plugins перетаскиванием можно добавить дополнительные параметры, которые будут отслеживаться с помощью текущего шаблона.

Локализация Zenoss

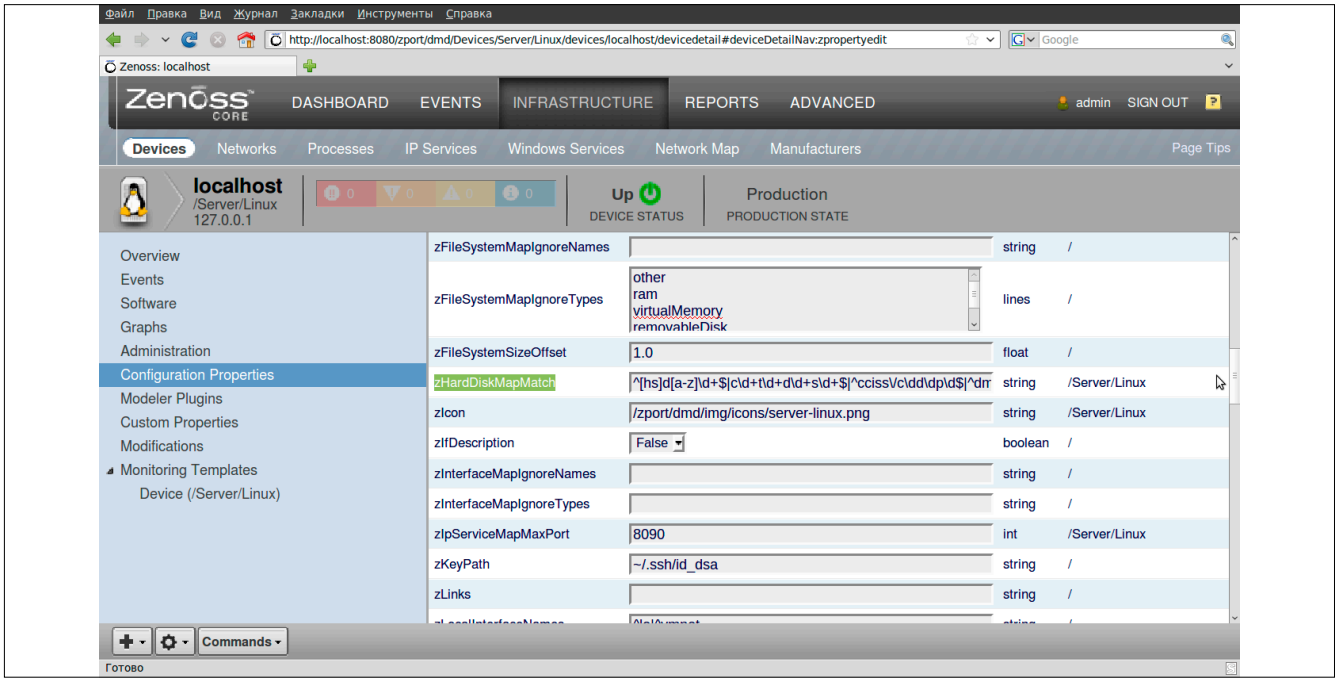
До недавнего времени разработчики не представляли удобных средств для локализации интерфейса. Возможно, в этом не было острой необходимости, ведь Zenoss ориентирован прежде всего на специалистов, которые обычно владеют необходимой терминологией. Но теперь все необходимое есть. Процесс локализации стандартен для приложений, использующих GNU Gettex. Все файлы собраны в каталоге $ZENHOME/zenoss/Products/ZenUI3/locales/, по умолчанию здесь два подкаталога en и fr, содержание которых можно взять за основу. Создаем подкаталог ru/LC_MESSAGES, в который копируем файл zenoss.po из французского перевода (в английском его нет). Формат записи внутри прост.

```
msgid "Reports"
msgstr "Отчеты"
```

Переводим последовательно все термины, затем компилируем в файл понятного Zenoss формата.

```
msgfmt -o zenoss.mo zenoss.po
```

Рисунок 3. Настройка свойств устройства



Также в Overview заполняем тэги, редактируем параметры производителя устройства, данные ОС и прочие. Все это позволит Zenoss правильно группировать системы.

Чтобы начать получать данные, необходимо подключить Zenoss к SNMP, для этого выберем в Devices устройство и затем пункт Configuration Properties. Здесь очень много настроек, с назначением которых предстоит разобраться, иначе мы не получим полную информацию. Назначение большинства из них понятно из контекста и примеров. Так, параметры для подключения к SNMP-демону прописываются в zSnmpCommunity и zSnmpPrivPassword, данные для удаленного выполнения команд через SSH – в zCommandUsername и zCommandPassword. Убедитесь также, что в zSnmpCommunities прописано значение из zSnmpCommunity.

Также стоит проверить значения шаблонов локальных параметров zLocalIpAddresses, zLocalInterfaceNames, zHardDiskMapMatch и других. И хотя значения, установленные по умолчанию, подходят для большинства ситуаций, в правилах бывают и исключения. Есть и специфические параметры. Например, в zNmapPortscanOptions указываются параметры для утилиты сканирования nmap.

В подменю Administration редактируются команды, которые затем можно вызвать, выбрав в меню Commands. Результат выполнения будет показан в отдельном прозрачном окне.

В подменю Network настраиваются сети: вы просто добавляете вручную IP подсети с указанием сетевой маски, в последующем в этих сетях Zenoss будет производить автопоиск устройств.

Обработка событий

В меню Events собраны все события с добавленных систем и устройств. Так как количество сообщений может быть большим, предусмотрены фильтры по статусу, важности, по каждой колонке плюс сортировка по алфавиту и колонкам.

Двойной щелчок позволяет просмотреть подробности, в которые администратор может добавить свои пометки. Предусмотрен также экспорт выбранных событий в файлы формата XML и CSV.

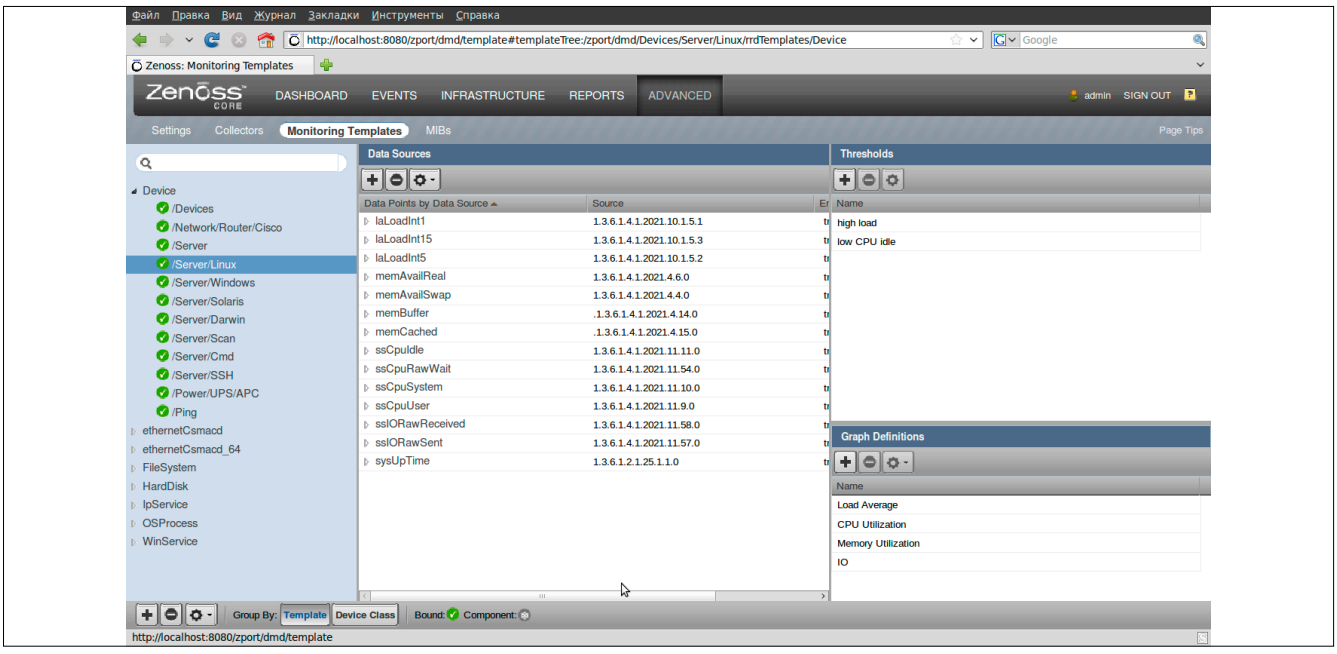
В других подменю доступны история, управление классами и подклассами событий и настройка кэширования. Отдельно хочу отметить подменю Event Manager, где настраиваются дополнительные поля таблиц базы данных, в которых будут записаны события, подключение к MySQL и триггеры (команды администратора, выполняемые при наступлении события).

Триггер создается в два этапа. Вначале в поле Event Manager – Command добавляем название новой команды, просто прописав ее в поле и нажав кнопку Add. Теперь выбираем ее в списке и редактируем, указав собственно команду, которая должна выполниться, время задержки, повтора и условие (система, событие, устройство, адрес и т.п.). По окончании устанавливаем Enabled в True и сохраняем результат.

После того как все устройства и сервисы будут добавлены, и начинает поступать информация, администратору необходимо отслеживать критические вопросы. Для этого Zenoss содержит большое количество готовых отчетов. Все они расположены в меню Reports. Отчеты разбиты по нескольким категориям – устройства, производительность, события, пользователи и другие. Естественно, предустановок скорее всего будет недостаточно, но добавить новый отчет очень просто. Нажимаем на значок с изображением «+» и в меню выбираем вариант отчета (Custom Device Reports, Graph и Multi-Graph Reports).

И, наконец, перейдя в Advanced, мы можем настроить подключение к SMTP-серверу (для отправки почтовых уведомлений), установить параметры приоритета, роли администрирования, настроить пользовательские команды, просмотреть журналы работы демонов, создать резервную копию БД.

Рисунок 4. Шаблоны в Zenoss можно отредактировать по своему усмотрению



Учетные данные и оповещения

Учетные записи пользователей и групп создаются в подменю Advanced → Users. Процесс, в общем, прост. Вначале указываем логин пользователя и его почтовый адрес, затем переходим к редактированию, где заполняем предложенные поля (пароль, роли и объекты, к которым будем иметь доступ).

Чтобы пользователь получал оповещение, необходимо создать правило в подменю Alerting Rules. Принцип тот же. Нажимаем кнопку с плюсом и вводим название, затем приступаем к редактированию записи. Добавляем задержку по времени (а вдруг оживет?), альтернативный почтовый адрес, в поле Action устанавливаем значение email, затем в Where набираем правило. Указав условия и фильтр с помощью раскрывающегося списка, меняем Enabled на True и сохраняем правило.

Администратор может создать любое количество правил, специфических для разных устройств. Чтобы сообщения отправлялись нескольким пользователям, следует использовать групповой адрес или создать группу, для которой затем создать свои Alerting Rules.

На сайте доступны расширения, позволяющие отправлять оповещения в твиттер или СМС. Кроме того, практически все настройки и правила можно легко импортировать в ZenPack, чтобы затем быстро повторить на другой системе или выложить в открытый доступ.

Рисунок 6. Настройка мониторинга IP-сервиса

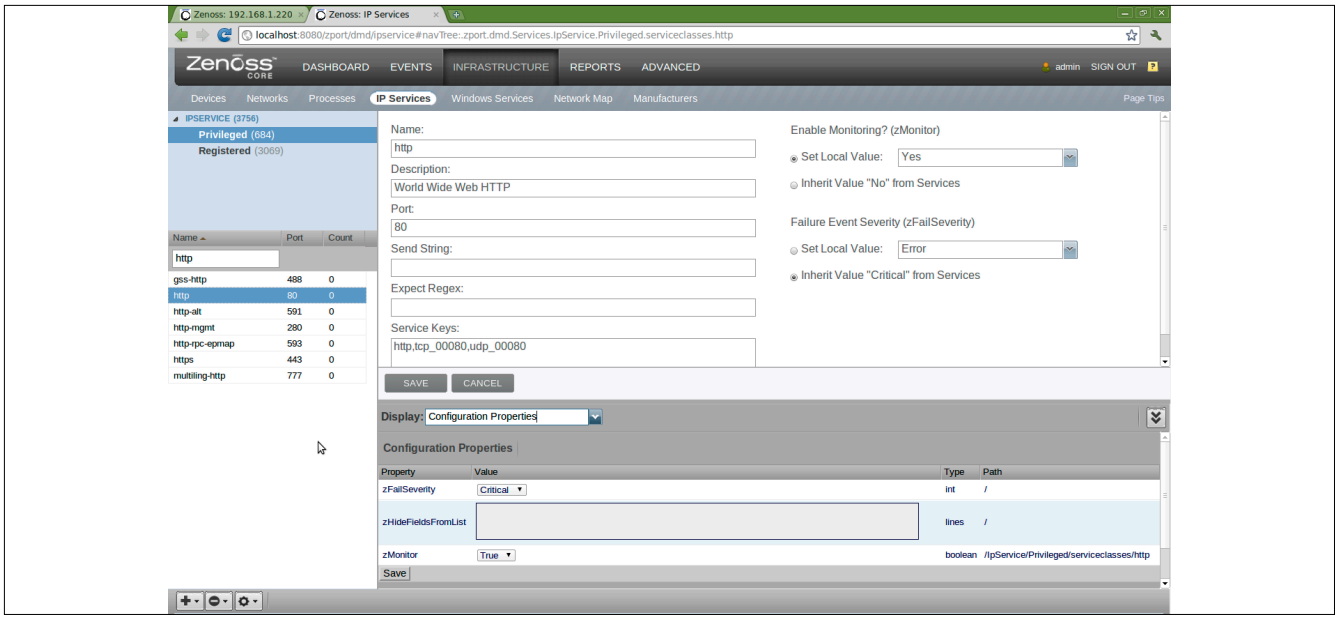
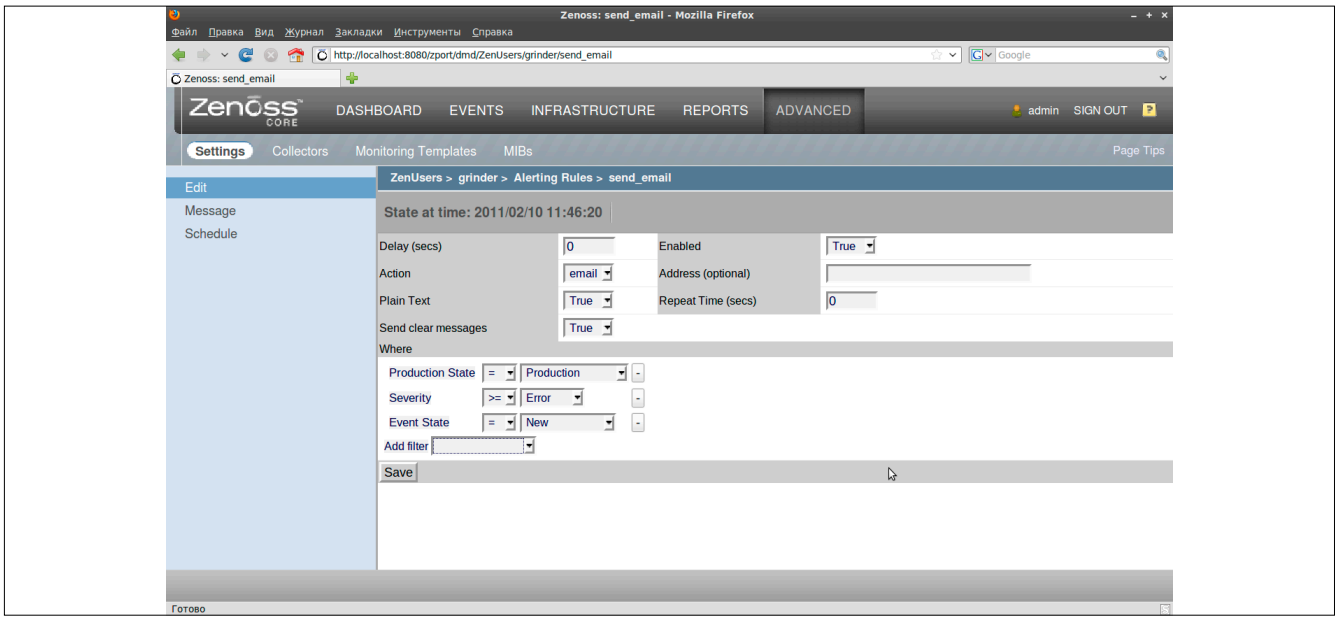


Рисунок 5. Создание правила для отправки почтового сообщения



По умолчанию правила работают круглосуточно, но мы можем указать время его действия в Schedule окна Alerting Rule.

Для упрощения развертывания системы мониторинга разработчики подготовили наборы шаблонов, в которых прописано, как и с какими параметрами опрашивать различные типы устройств, графики и так далее. Их полный список доступен в Advanced – Monitoring Templates. Опытный администратор может самостоятельно создать готовые шаблоны под любые условия. Процесс максимально упрощен. Вначале необходимо выбрать шаблон, который станет основой, затем заполнить источники, указать порог и данные для построения графиков. Конечно, здесь понадобится некоторый опыт, но все равно это намного проще, чем самостоятельно писать правила для SNMP и RRDTool.

Мониторинг процесса

Мониторинг общих параметров сервера, конечно, интересен, но администратору в большинстве случаев необходимо знать состояние конкретного сервиса. Выбираем устройство и переходим в меню Devices, в котором находим несколько подменю, где можно настроить контроль сервисов по состоянию процесса или по ответу, полученному с сетевого порта. После установки в IP Services и Windows Services доступно около 4000 готовых шаблонов, позволяющих судить о состоянии сервиса UNIX- и Windows-машин соответственно. Просто в настройках сервера выбираем Add IPService и указываем предопределенный параметр.

В Processes создаются правила, позволяющие отслеживать состояние отдельного процесса. Здесь поступаем аналогично другим настройкам. Добавляем новое название, например httpd, после чего вызываем окно редактирования. Основным параметром здесь является Regex, который определяет шаблон имени процесса. Вводим httpd, проверяем, чтобы zMonitor был установлен в True. Теперь осталось создать оповещение, как говорилось выше, и администратор будет уведомлен о проблемах.

Как уже было сказано, на сайте проекта доступны расширения. Устанавливаются они очень просто. Скачиваем файл и затем указываем на него в Advanced → ZenPacks.

***

Как видите, Zenoss очень простая в развертывании и настройках система мониторинга, обладающая большим количеством полезных функций, что делает ее достойным конкурентом коммерческим аналогам. EOF

1. Бешков А. Установка Nagios. //«Системный администратор», №2, 2003 г. – С. 6-14 (http://samag.ru/archive/article/74).
2. Яремчук С. GroundWork Monitor. //«Системный администратор», №6, 2008 г. – С. 4-11.
3. Яремчук С. Cacti – простой и удобный инструмент для мониторинга и анализа сети. //«Системный администратор», №4, 2007 г. – С. 14-17.
4. Денисов Ю. Знакомьтесь, Zabbix! Мониторинг активных устройств и рабочих станций. //«Системный администратор», №5, 2010 г. – С. 36-39.
5. GPL ветка Zenoss Community – http://community.zenoss.org.
6. Страница Zenoss – http://sourceforge.net/projects/zenoss.
7. Сайт проекта Zenoss – http://www.zenoss.com.
8. Яремчук С. Централизованная настройка UNIX-систем с помощью Puppet. //«Системный администратор», №7, 2007 г. – С. 58-61 (http://samag.ru/archive/article/779).
9. Яремчук С. Проект одного человека. Централизованное управление с помощью Cfengine. //«Системный администратор», №1-2, 2010 г. – С. 48-53 (http://samag.ru/archive/article/930).
10. Сайт Zapplet – http://sourceforge.net/projects/zapplet.
11. Страница ZenTraylcon – http://www.zenoss.com/community/wiki/user-contributed/ZenTraylcon.
12. Страница Zenoss IT Management на YouTube –http://www.youtube.com/user/zenossmonitoring.
13. Получение Google Maps API – http://www.google.com/apis/maps/signup.html.

Рисунок 7. Графики производительности Zenoss