

Zabbix умеет анализировать любой лог файл, сохранять его в свою базу, рассылать алерты по каким-то событиям. Я решил использовать эту возможность для анализа лог файла утилиты `apcupsd` для отправки оповещений об отключении электричества. Решается данная задача стандартным функционалом заббикса, описанного в документации.

Если у вас есть желание научиться работать с роутерами микротик и стать специалистом в этой области, рекомендую по программе, основанной на информации из официального курса **MikroTik Certified Network Associate**. Курс стоящий, все подробности читайте по ссылке. Есть бесплатные курсы.

Содержание:

- 1 Введение
- 2 Настройка мониторинга логов
- 3 Создание триггера на событие из лога
- 4 Заключение
- 5 Дополнительные материалы по Zabbix

Введение

Ранее я рассказывал об использовании утилиты управления upsами марки арс - **apcupsd**. Я показал, как установить `apcupsd` на `hyper-v` и `xenserver` для корректного завершения работы при отключении электричества. Рекомендую ознакомиться, если вас интересует этот вопрос. Его не всегда получается быстро и удобно решить. На помощь приходит `apcupsd`.

Указанные конфигурации у меня успешно работают, проверено годами. Я решил настроить отправку оповещений на почту через `zabbix` при пропадании электричества. Да и просто хочется хранить информацию об инцидентах в одном месте. Почтовые сообщения не всегда будут доставлены, нужно следить, чтобы на резервное питание были подключены все устройства, которые обеспечивают связь с интернетом. Частенько бывает, что при выключении

электричества у провайдера так же выключается оборудование и связи нет. Либо ваш свитч, к которому подключен сервер, выключится и сообщение не будет доставлено.

Заранее позаботьтесь об этих вещах. Пишу об этом, потому что сам недавно на одном объекте все запитал от упсов, но забыл про свитч. В итоге об отключении электричества я узнал уже после того, как его вернули назад и сервера автоматически поднялись. Если у вас еще не настроен сервер мониторинга, рекомендую мою подробную статью с видео об установке и настройке zabbix на centos 9 или установка zabbix 3.4 на debian 9.

Настройка мониторинга логов

Для того, чтобы мониторить лог файл, на сервере должен быть установлен zabbix agent, а сам сервер добавлен в панель мониторинга. Я буду следить за логом программы apcupsd, который располагается по пути `/var/log/apcupsd.events`. Идем в веб интерфейс заббикса и добавляем новый итем к интересующему нас хосту. Если у вас таких будет несколько, то создавайте сразу шаблон. В моем случае у меня один сервер, поэтому я буду добавлять новый элемент сразу на него.

На всякий случай сообщаю, что вся настройка проходит на zabbix server версии 3.2. Но информация актуальна и для других версий, так как используется стандартный функционал, который поддерживают все версии заббикса.

Создаем новый итем со следующими параметрами:

Name

Type

Key

Type of information

Update interval (in sec)

History storage period (in days)

Log time format

New application

Applications

- None-
- apcupsd**
- CPU
- Filesystems
- General
- ICMP
- Mdadm softraid
- Memory
- Network interfaces
- OS

Description

Enabled

serveradmin.ru

Name	Имя нового итема. Можете указать любое название.
Type	Тип элемента. Обязательно выбираем Zabbix agent (active). По-умолчанию будет другой тип стоять.
Key	Ключ данных, log - тип, в квадратных скобках путь до лог файла.
Type of information	Указываем тип информации, поступающей в итем.

Остальные параметры оставляете на свое усмотрение. Рекомендую время обновления итема ставить поменьше, чтобы оперативно получить информацию об инциденте. У меня стоит 30 секунд.

После того, как вы сохраните новый итем, через несколько минут начнут поступать данные. Проверять их как обычно в Latest data. В данной конфигурации будут сохраняться все строки из файла. В моем случае это не страшно, так как записей будет очень мало. Они создаются только по событиям в электро сети, а они случаются редко, поэтому я не стал делать фильтр по строкам или словам.

Но это только пол дела. Мы стали собирать логи, теперь нам нужно настроить отправку оповещения при пропадании электричества.

Создание триггера на событие из лога

Мы будем слать оповещение не только в момент отключения электричества, но и тогда, когда оно снова появится. Так что в триггере будут два условия:

1. Условие активации события.
2. И условие его прекращения.

Открываем вкладку с триггерами хоста и добавляем туда новый триггер со следующими параметрами:

Name

Severity Not classified Information Warning Average High Disaster

Problem expression

[Expression constructor](#)

OK event generation Expression Recovery expression None

Recovery expression

[Expression constructor](#)

PROBLEM event generation mode Single Multiple

OK event closes All problems All problems if tag values match


Tags

Allow manual close

URL

Description

Enabled



Name Имя триггера. Может быть любым.
Problem expression {xm-xen02:log[/var/log/apcupsd.events].str(Power failure.)}=1
Recovery expression {xm-xen02:log[/var/log/apcupsd.events].str(Power is back.)}=1

Рассказываю подробнее, что тут написано. **xm-xen02** - имя сервера. **Power failure.** - строка в лог файле, которая появляется при отключении электричества. Когда оно возвращается, появляется запись **Power is back.** В общем виде лог выглядит примерно следующим образом:

```
2016-11-07 23:17:23 +0300 Power failure.
2016-11-07 23:17:29 +0300 Running on UPS batteries.
2016-11-07 23:21:20 +0300 Mains returned. No longer on UPS batteries.
2016-11-07 23:21:20 +0300 Power is back. UPS running on mains.
2016-11-16 14:20:42 +0300 Power failure.
2016-11-16 14:20:48 +0300 Running on UPS batteries.
2016-11-16 14:20:51 +0300 Mains returned. No longer on UPS batteries.
2016-11-16 14:20:51 +0300 Power is back. UPS running on mains.
```

Становится понятно, почему я взял именно эти строки. На этом все. После сохранения триггера он начнет работать и следить за итемом, который собирает строки из лога. Как только появятся строки, попадающие под условие, вы получите оповещение.

Заключение

Отладить работу оповещения об отключении электричества достаточно трудно, так как дергать по этому поводу шнур с питанием не хочется. Я пошел другим путем. Во время отладки использовал общий лог файл `/var/log/messages` и останавливал службу `chronyd`. Во время остановки, она пишет информацию об этом в лог файл, а при запуске так же сообщает, что запустилась. Я просто настроил итем и триггер на нужные строки и убедился, что все работает как надо. После этого уже сделал по аналогии итемы и триггеры для `apcupsd`. Рекомендую поступить похожим образом и потестировать функционал.

Помогла статья? Подписывайся на telegram канал автора

Анонсы всех статей, плюс много другой полезной и интересной информации, которая не попадает на сайт.

Дополнительные материалы по Zabbix

Онлайн курс по Linux

Если у вас есть желание освоить операционную систему Linux, не имея подходящего опыта, рекомендую познакомиться с **онлайн-курсом Administrator Linux. Basic** в OTUS. Курс для новичков, адаптирован для тех, кто только начинает изучение Linux. Обучение длится 4 месяца. Что даст вам этот курс:

- Вы получите навыки администрирования Linux (структура Linux, основные команды, работа с файлами и ПО).
- Вы рассмотрите следующий стек технологий: Zabbix, Prometheus, TCP/IP, nginx, Apache, MySQL, Bash, Docker, Git, nosql, grafana, ELK.
- Умение настраивать веб-сервера, базы данных (mysql и nosql) и работа с сетью.
- Мониторинг и логирование на базе Zabbix, Prometheus, Grafana и ELK.
- Научитесь командной работе с помощью Git и Docker.

Смотрите подробнее программу по .

**Рекомендую полезные материалы по Zabbix:
Настройки системы**

- Установка 4.0
- Обновление 3.0 -> 3.2
- Обновление 3.4 -> 4.0
- Установка Zabbix Proxu
- Работа на NGINX

Видео и подробное описание установки и настройки Zabbix 4.0, а также установка агентов на linux и windows и подключение их к мониторингу.

Подробное описание обновления системы мониторинга zabbix версии 3.4 до новой версии 4.0.

Пошаговая процедура обновления сервера мониторинга zabbix 2.4 до 3.0. Подробное описание каждого шага с пояснениями и рекомендациями.

Подробное описание установки и настройки zabbix proxu для организации распределенной системы мониторинга. Все показано на примерах.

Подробное описание установки системы мониторинга Zabbix на веб сервер на базе nginx + php-fpm.

Мониторинг служб и сервисов

- Температура процессора
- Nginx и php-fpm
- Mysql репликация
- Службы Linux
- Рейд mdadm
- Транки Asterisk
- Synology

Мониторинг температуры процессора с помощью zabbix на Windows сервере с использованием пользовательских скриптов.

Настройка полноценного мониторинга web сервера nginx и php-fpm в zabbix с помощью скриптов и пользовательских параметров.

Мониторинг репликации mysql с помощью Zabbix. Подробный разбор методики и тестирование работы.

Описание настройки мониторинга tcp служб с помощью zabbix и его инструмента простых проверок (simple checks)

Настройка мониторинга рейда mdadm с помощью zabbix. Подробное пояснение принципа работы и пошаговая инструкция.

Подробное описание мониторинга регистраций транков (trunk) в asterisk с помощью сервера мониторинга zabbix.

Подробная инструкция со скриншотами по настройке мониторинга по snmp дискового хранилища synology с помощью сервера мониторинга zabbix.

Мониторинг различных значений

- Мониторинг сайта
- Мониторинг бэкапов
- Размер бэкапа
- Делегирование домена
- Значения из текстового файла
- Мониторинг логов

Настройка мониторинга web сайта в zabbix. Параметры для наблюдения - доступность сайта, время отклика, скорость доступа к сайту.

Один из способов мониторинга бэкапов с помощью zabbix через проверку даты последнего изменения файла из архивной копии с помощью vfs.file.time.

Подробное описание настройки мониторинга размера бэкапов в Zabbix с помощью внешних скриптов.

Пример настройки мониторинга за временем делегирования домена с помощью Zabbix и внешнего скрипта. Все скрипты и готовый шаблон представлены.

Пример распознавания и мониторинга за изменением значений в обычных текстовых файлах с помощью zabbix.

Описание мониторинга лог файлов в zabbix на примере анализа лога программы arpcpsd. Отправка оповещений по событиям из лога.