



Сетевое управление и мониторинг

Управление логами



These materials are licensed under the Creative Commons *Attribution-Noncommercial 3.0 Unported* license
(<http://creativecommons.org/licenses/by-nc/3.0/>)

Основы Syslog

Использует протокол UDP, порт 514

У сообщений syslog есть два атрибута (в дополнение к собственно сообщению):

<u>Тип (Facility)</u>		<u>Уровень (Level)</u>
Auth	Security	Emergency (0)
Authpriv	User	Alert (1)
Console	Syslog	Critical (2)
Cron	UUCP	Error (3)
Daemon	Mail	Warning (4)
Ftp	Ntp	Notice (5)
Kern	News	Info (6)
Lpr		Debug (7)
Local0 ... Local7		

Дополнительно есть еще понятие "приоритета", являющегося комбинацией типа и уровня. См. <http://en.wikipedia.org/wiki/Syslog#Priority>.

Больше информации о syslog

- **RFC 3164:** *BSD Syslog Protocol*
<http://tools.ietf.org/html/rfc3164>
- **RFC 5426:** Transmission of Syslog Messages over UDP
<http://tools.ietf.org/html/rfc5426>
- Transmission of syslog messages over UDP draft-ietf-syslog-transport-udp-00
<http://tools.ietf.org/html/draft-ietf-syslog-transport-udp-00>
- Wikipedia Syslog Entry
<http://en.wikipedia.org/wiki/Syslog>

Cisco Press: *An Overview of the Syslog Protocol*

<http://www.ciscopress.com/articles/article.asp?p=426638>

Управление логами и мониторинг

- Храните логи в защищенном месте, где они легко могут быть проверены.
- Проверяйте ваши файлы логов.
- Они содержат важную информацию:
 - Случается многое, и кто-то должен проверять логи.
 - Непрактично делать это вручную.

Управление логами и мониторинг

На роутерах и маршрутизаторах

```
Sep  1 04:40:11.788 INDIA: %SEC-6-IPACCESSLOGP: list 100 denied tcp  
79.210.84.154(2167) -> 169.223.192.85(6662), 1 packet
```

```
Sep  1 04:42:35.270 INDIA: %SYS-5-CONFIG_I: Configured from console by pr on  
vty0 (203.200.80.75)
```

```
%CI-3-TEMP: Overtemperature warning
```

```
Mar  1 00:05:51.443: %LINK-3-UPDOWN: Interface Serial1, changed state to down
```

На серверах

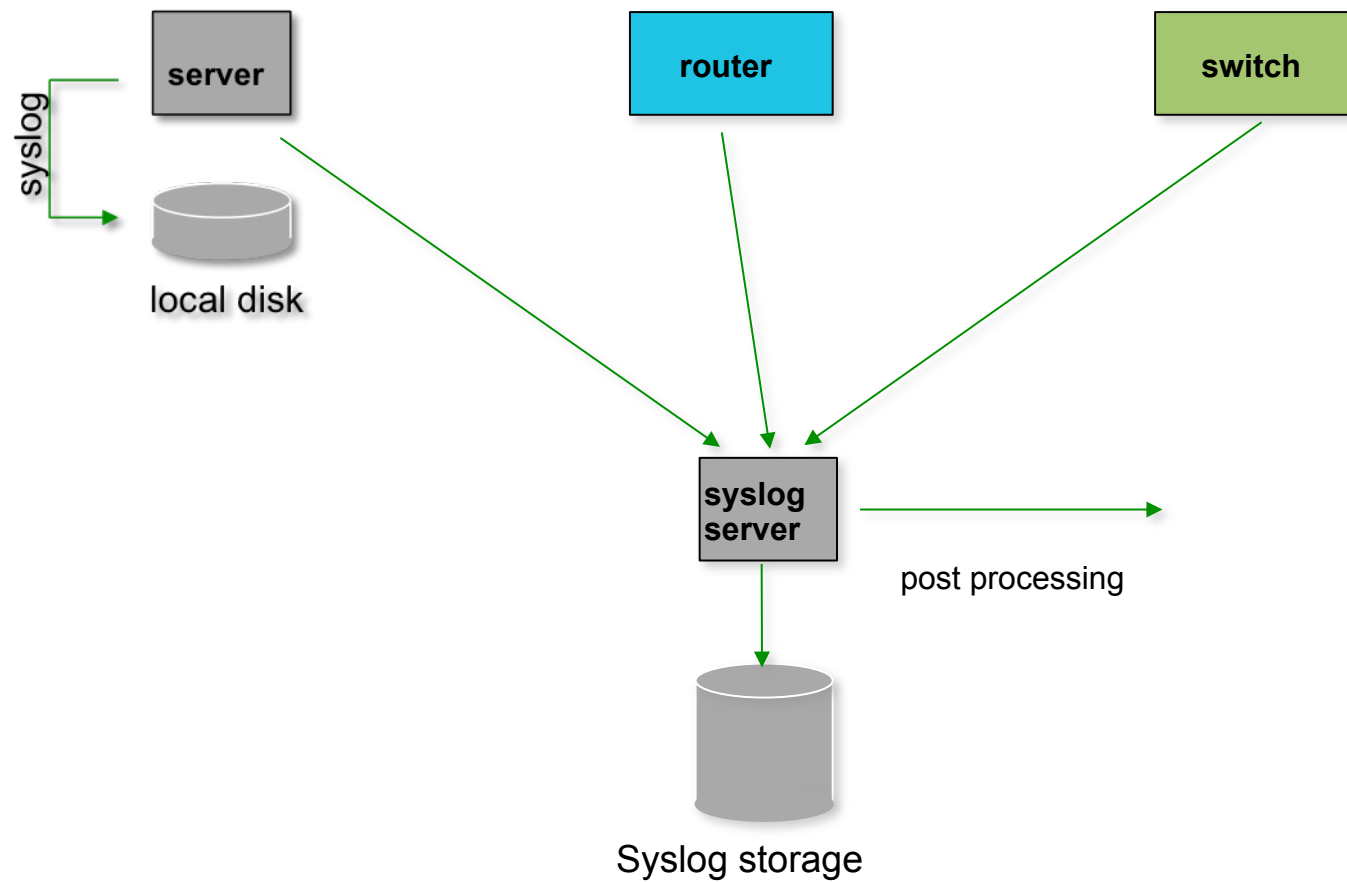
```
Aug 31 17:53:12 ubuntu nagios3: Caught SIGTERM, shutting down...
```

```
Aug 31 19:19:36 ubuntu sshd[16404]: Failed password for root from  
169.223.1.130 port 2039 ssh2
```

Управление логами

- Централизовать и объединять файлы логов
- Отправлять все сообщения от роутеров, маршрутизаторов и серверов на один узел – *сервер логов*.
- Любое сетевое оборудование и серверы UNIX/Linux могут мониториться используя какую-либо версию *syslogd* (мы используем либо `syslog-ng`, либо `rsyslog` на семинаре).
- Windows также может использовать syslog с дополнительными инструментами.
- Храните копию логов локально, но также сохраняйте их на центральном сервере.

Централизованное логирование



Настройка централизованного логирования

Устройства Cisco

– По минимуму:

```
logging ip.of.logging.host
```

Узлы Unix and Linux

– В syslogd.conf, или в rsyslog.conf, добавьте:

```
*.* @ip.of.log.host
```

– Перезапустите syslogd, rsyslog, или syslog-ng

Другое оборудование имеет похожие параметры

– Параметры для изменения *типа (facility)* и *уровня (level)*

Получение сообщений – **syslog-ng**

- Определить *тип (facility)*, который оборудование будет использовать для отправления сообщений.
- Перенастроить *syslog-ng* слушать в сети*
 - В Ubuntu измените `/etc/syslog-ng/syslog-ng.conf`
- Создайте файл*
 - `/etc/syslog-ng/conf.d/10-network.conf`
- Создайте новый каталог для логов:
 - `# mkdir /var/log/network`
- Перезапустите сервис *syslog-ng*:
 - `# service syslog-ng restart`

*См. упражнения

Если вы используете *rsyslog*

- *rsyslog* включен в Ubuntu по умолчанию (хотя бы предпочитаем *syslog-ng*). Его конфигурация немного другая – у нас есть лабораторные работы и для *rsyslog*:
- Изменить `/etc/rsyslog`
- Создать следующий файл
`/etc/rsyslog.d/30-routerlogs.conf`
- Создать новый каталог для логов и поменять права доступа к этому каталогу
`# mkdir /var/log/network`
`# chown syslog:adm /var/log/network`
- Перезапустить сервис *rsyslog*
`# service rsyslog restart`

Группировка логов

- Используя *тип (facility)* и *уровень (level)* можно группировать логи по категориям в разных файлах.
- С помощью таких программ как *rsyslog* можно группировать по машинам, датам и т.д. автоматически в разных каталогах.
- Можно использовать *grep* для фильтрации логов.
- Можно использовать стандартные утилиты UNIX для группировки и фильтрации логов:

```
egrep -v '(list 100 denied|logging rate-limited)' mylogfile
```

- Можно ли делать это автоматически?

Tenshi

- Простой и гибкий инструмент мониторинга логов
- Сообщения распределяются по очередям, используя регулярные выражения
- Каждая очередь может быть настроена чтобы отправлять письмо со сводкой за какое-то время
 - Например, вы можете сказать Tenshi отправлять сводку всех подходящих сообщений раз в пять минут, чтобы не переполнить почтовый ящик

Пример конфигурации Tenshi

```
set uid tenshi  
set gid tenshi
```

```
set logfile /log/dhcp
```

```
set sleep 5  
set limit 800  
set pager_limit 2  
set mailserver localhost  
set subject tenshi report  
set hidepid on
```

```
set queue dhcpd tenshi@localhost sysadmin@noc.localdomain [*/10 * * * *]
```

```
group ^dhcpd:  
dhcpd ^dhcpd: .+no free leases  
dhcpd ^dhcpd: .+wrong network  
group_end
```

Ссылки

Rsyslog

<http://www.rsyslog.com/>

SyslogNG

<http://www.balabit.com/network-security/syslog-ng/>

Windows Log в Syslog

<http://code.google.com/p/eventlog-to-syslog/>

<http://www.intersectalliance.com/projects/index.html>

Tenshi

<http://www.inversepath.com/tenshi.html>

Другие программы

<http://sourceforge.net/projects/swatch/>

<http://www.crypt.gen.nz/logsurfer>

<http://simple-evcorr.sourceforge.net/>

Вопросы?

?