

Лабораторная работа №15

Настройка сетевого журналирования

Газизянов Владислав Альбертович

Содержание

1 Цель работы	5
2 Задание	6
3 Выполнение лабораторной работы	7
3.1 Настройка сервера сетевого журнала	7
3.2 Настройка клиента сетевого журнала	9
3.3 Просмотр журналов событий	10
3.4 Автоматизация развертывания	14
4 Контрольные вопросы	16
5 Выводы	18

Список иллюстраций

3.1	Создание конфигурационного файла сервера	7
3.2	Конфигурация TCP-приёмника rsyslog	7
3.3	Перезапуск службы rsyslog	8
3.4	Проверка открытых портов rsyslog	8
3.5	Настройка firewall для сетевого журналирования	9
3.6	Создание конфигурационного файла клиента	9
3.7	Настройка перенаправления логов на сервер	9
3.8	Перезапуск rsyslog на клиенте	10
3.9	Мониторинг журнала сообщений в реальном времени	11
3.10	Просмотр журналов через gnome-system-monitor	12
3.11	Установка просмотрщика журналов lnav	12
3.12	Анализ журналов с помощью lnav	13
3.13	Скрипт настройки сервера журналирования	14
3.14	Конфигурация Vagrantfile для журналирования	15

Список таблиц

1 Цель работы

Получение практических навыков по работе с журналами системных событий, настройке централизованного сетевого журналирования и мониторинга событий в распределённой среде.

2 Задание

1. Настроить сервер сетевого журналирования событий
2. Настроить клиент для передачи системных сообщений в сетевой журнал
3. Просмотреть журналы системных событий с помощью различных инструментов
4. Разработать скрипты автоматизации для развертывания системы журналирования

3 Выполнение лабораторной работы

3.1 Настройка сервера сетевого журнала

3.1.1 Подготовка конфигурации

На серверной машине создан файл конфигурации сетевого хранения журналов в каталоге /etc/rsyslog.d/. Создан файл netlog-server.conf для настройки параметров сервера журналирования.

```
[root@server.vagazizianov.net ~]# cd /etc/rsyslog.d
[root@server.vagazizianov.net rsyslog.d]# touch netlog-server.conf
```

Рисунок 3.1: Создание конфигурационного файла сервера

3.1.2 Конфигурация TCP-приёмника

В файл конфигурации добавлены директивы для включения приёма записей журнала по TCP-порту 514. Загружен модуль imtcp и активирован TCP-сервер на указанном порту.

```
GNU nano 8.1                               /etc/rsyslog.d/netlog-server.conf
$ModLoad imtcp
$InputTCPServerRun 514
```

Рисунок 3.2: Конфигурация TCP-приёмника rsyslog

3.1.3 Перезапуск службы rsyslog

Выполнен перезапуск службы rsyslog для применения новых настроек. Проверено состояние службы и прослушиваемые порты, связанные с rsyslog.

```
[root@server.vagazizianov.net rsyslog.d]# nano /etc/rsyslog.d/netlog-s  
[root@server.vagazizianov.net rsyslog.d]# systemctl restart rsyslog
```

Рисунок 3.3: Перезапуск службы rsyslog

3.1.4 Проверка открытых портов

С помощью команды lsof проверено, что rsyslog прослушивает TCP-порт 514, что подтверждает корректность настройки сервера сетевого журналирования.

```
server.vagazizianov.net:35156->93.243.107.34.bc.googleusercontent.com:https (ESTABLISHED)  
rsyslogd 10920 root 4u IPv4 66566 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 root 5u IPv6 66567 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10922 in:imjour root 4u IPv4 66566 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10922 in:imjour root 5u IPv6 66567 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10923 in:imtcp root 4u IPv4 66566 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10923 in:imtcp root 5u IPv6 66567 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10924 in:imtcp root 4u IPv4 66566 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10924 in:imtcp root 5u IPv6 66567 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10925 in:imtcp root 4u IPv4 66566 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10925 in:imtcp root 5u IPv6 66567 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10926 in:imtcp root 4u IPv4 66566 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10926 in:imtcp root 5u IPv6 66567 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10927 in:imtcp root 4u IPv4 66566 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10927 in:imtcp root 5u IPv6 66567 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10928 rs:main root 4u IPv4 66566 0t0 TCP  
*:shell (LISTEN)  
rsyslogd 10920 10928 rs:main root 5u IPv6 66567 0t0 TCP  
*:shell (LISTEN)
```

Рисунок 3.4: Проверка открытых портов rsyslog

3.1.5 Настройка межсетевого экрана

Настроены правила firewall для разрешения входящих соединений на TCP-порт 514. Добавлены как временные, так и постоянные правила для обеспечения сетевой безопасности.

```
*:shell (LISTEN)
[root@server.vagazizianov.net rsyslog.d]# firewall-cmd --add-port=514/tcp
success
[root@server.vagazizianov.net rsyslog.d]# firewall-cmd --add-port=514/tcp --permanent
success
```

Рисунок 3.5: Настройка firewall для сетевого журналирования

3.2 Настройка клиента сетевого журнала

3.2.1 Подготовка клиентской конфигурации

На клиентской машине создан файл конфигурации netlog-client.conf в каталоге /etc/rsyslog.d/. Файл содержит настройки для перенаправления сообщений журнала.

```
[root@client.vagazizianov.net ~]# cd /etc/rsyslog.d
[root@client.vagazizianov.net rsyslog.d]# touch netlog-client.conf
```

Рисунок 3.6: Создание конфигурационного файла клиента

3.2.2 Конфигурация перенаправления сообщений

В файл конфигурации добавлена директива для перенаправления всех системных сообщений (.) на сервер журналирования через TCP-порт 514 с использованием двойного символа @@ для TCP-соединения.

```
GNU nano 8.1                               /etc/rsyslog.d/netlog-client.conf
*.* @@server.vagazizia.net:514
```

Рисунок 3.7: Настройка перенаправления логов на сервер

3.2.3 Перезапуск клиентской службы

Выполнен перезапуск службы rsyslog на клиенте для применения новой конфигурации. Проверен статус службы для подтверждения корректной работы.

```
[root@client.vagazizianov.net ~]# systemctl restart rsyslog
```

Рисунок 3.8: Перезапуск rsyslog на клиенте

3.2.4 Проверка соединения

Проверена возможность установления TCP-соединения между клиентом и сервером журналирования. Убедились в доступности порта 514 на сервере.

3.3 Просмотр журналов событий

3.3.1 Мониторинг системных сообщений

На сервере выполнена проверка файла /var/log/messages с использованием команды tail -f для отслеживания поступающих сообщений в реальном времени. Проанализированы записи с различных хостов.

```
[sudo] password for vagazizianov.
[root@server vagazizianov ~]# tail -f /var/log/messages
Dec 13 07:47:31 server systemd[1]: Started systemd-hostnamed.service - Hostname Service.
Dec 13 07:47:31 client ptyxis[10742]: context mismatch in svga_surface_destroy
Dec 13 07:47:31 client ptyxis[10742]: context mismatch in svga_surface_destroy
Dec 13 07:47:31 client ptyxis[10742]: context mismatch in svga_surface_destroy
Dec 13 07:47:31 client ptyxis[10742]: context mismatch in svga_surface_destroy
Dec 13 07:47:31 server systemd-coredump[11275]: Process 11265 (VBoxClient) of user 1001 dumped core.
#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libX11.so.6 from rpm libX11-1.8.10-1.el10.x86_64#012Module libffi.so.8
from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 11268:#012#0 0x00000000041db4b n/a (n/a + 0x0)#012#1 0x0000000000041dac4 n/a (n/a + 0x0)#012#2 0x00000000000450a8c n/a (n/a + 0x0)#012#3 0x0000000000435890 n/a (n/a + 0x0)#012#4 0x00007ff4ff231b68 start_thread (libc.so.6 + 0x94b68)#012#5 0x00007ff4ff2a26bc __clone3
(libc.so.6 + 0x1056bc)#012#0 0x00007ff4ff2a04bd syscall (libc.so.6 + 0x1034bd)#012#1 0x0000000004347a2 n/a (n/a + 0x0)#012#2 0x00000000004506d6 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007ff4ff1c730e __libc_start_call_main (libc.so.6 + 0x2a30e)#012#5 0x00007ff4ff1c73c9 __libc_start_main@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 13 07:47:31 server systemd[1]: systemd-coredump@150-11271-0.service: Deactivated successfully.
Dec 13 07:47:32 client kernel: traps: VBoxClient[11139] trap int3 ip:41db4b sp:7f32458b6cd0 error:0 in VBoxClient[1db4b,400000+bb000]
Dec 13 07:47:32 client systemd-coredump[11140]: Process 11136 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP_processing...
```

Рисунок 3.9: Мониторинг журнала сообщений в реальном времени

3.3.2 Использование графического монитора

Запущена графическая программа gnome-system-monitor для просмотра системных журналов. Проанализированы различные категории событий и сообщения от клиентских устройств.

Process Name	User	% CPU	ID	Memory	Disk read total	Disk write
at-spi2-registryd	vagazizianov	0.03	8173	524.3 kB	N/A	
at-spi-bus-launcher	vagazizianov	0.03	8165	524.3 kB	N/A	
bash	vagazizianov	0.03	10693	2.0 MB	319.5 kB	
bash	vagazizianov	0.03	11216	1.8 MB	N/A	
bash	vagazizianov	0.03	11372	2.0 MB	N/A	
cataonit	vagazizianov	0.03	10630	N/A	663.6 kB	
dbus-broker	vagazizianov	0.09	8048	1.8 MB	N/A	
dbus-broker	vagazizianov	0.05	8172	262.1 kB	N/A	
dbus-broker-launch	vagazizianov	0.03	8038	262.1 kB	N/A	
dbus-broker-launch	vagazizianov	0.03	8171	262.1 kB	N/A	
dconf-service	vagazizianov	0.09	8199	393.2 kB	77.8 kB	20
evolution-addressbook-factory	vagazizianov	0.03	8540	3.7 MB	2.3 MB	53
evolution-alarm-notify	vagazizianov	0.03	8266	8.5 MB	1.2 MB	
evolution-calendar-factory	vagazizianov	0.03	8489	3.5 MB	1.6 MB	
evolution-source-registry	vagazizianov	0.03	8406	3.9 MB	2.8 MB	
firefox	vagazizianov	0.94	9159	343.9 MB	270.3 MB	138.1
gdm-wayland-session	vagazizianov	0.03	8032	393.2 kB	4.1 kB	

Рисунок 3.10: Просмотр журналов через gnome-system-monitor

3.3.3 Установка специализированного просмотрщика

Установлен просмотрщик журналов lnav, предоставляющий расширенные возможности для анализа и фильтрации системных сообщений.

```
success
[root@server.vagazizianov.net rsyslog.d]# dnf -y install lnav
Extra Packages for Enterprise L      [ == ] --- B/s | 0 B --:-- ETA
```

Рисунок 3.11: Установка просмотрщика журналов lnav

3.3.4 Анализ журналов через lnav

Запущен lnav для просмотра и анализа журналов. Использованы возможности цветового выделения, фильтрации и поиска для эффективной работы с большими объёмами логов.

The screenshot shows a terminal window titled 'root@server.vagazizianov.net /var/log/messages' with the command 'sudo -i' running. The log output is as follows:

```

ture: AMD x86-64
Dec 13 09:09:40 client systemd[1]: systemd-coredump@976-21354-0.service: Deactivated successfully.
Dec 13 09:09:41 server systemd-coredump[143075]: Process 143063 (VBoxClient) of user 1001 dumped core
.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libXi.so.6 from rpm libXi-1.8.10-1.el10.x86_64#012Stack trace of thread 143066:#012#0 0x000000000041db4b n/a (n/a + 0x0)#012#1 0x000000000041dac4 n/a (n/a + 0x0)#012#2 0x0000000000450a8c n/a (n/a + 0x0)#012#3 0x0000000000435890 n/a (n/a + 0x0)#012#4 0x00007ff4ff231b68 pthread_cancel@GLIBC_2.2.5 (libc.so.6 + 0x93b68)#012#012Stack trace of thread 143063:#012#0 0x00007ff4ff2a04bd preadv64v2 (libc.so.6 + 0x1024bd)#012#012Stack trace of thread 143065:#012#0 0x00007ff4ff2a04bd preadv64v2 (libc.so.6 + 0x1024bd)#012#012Stack trace of thread 143064:#012#0 0x00007ff4ff2a04bd preadv64v2 (libc.so.6 + 0x1024bd)#012#012ELF object binary architecture: AMD x86-64
Dec 13 09:09:41 server systemd[1]: systemd-coredump@834-143067-0.service: Deactivated successfully.
Dec 13 09:09:45 client kernel: traps: VBoxClient[21364] trap int3 ip:41db4b sp:7f32458b6cd0 error:0 in VBoxClient[1db4b,400000+bb000]
Dec 13 09:09:45 client systemd-coredump[21365]: Process 21361 (VBoxClient) of user 1001 terminated abnormally with signal 5/TRAP, processing...
Dec 13 09:09:45 client systemd[1]: Started systemd-coredump@977-21365-0.service - Process Core Dump PID 21365/UID 0.
Dec 13 09:09:45 client systemd-coredump[21366]: Process 21361 (VBoxClient) of user 1001 dumped core.#012#012Module libXau.so.6 from rpm libXau-1.0.11-8.el10.x86_64#012Module libxcb.so.1 from rpm libxcb-1.17.0-3.el10.x86_64#012Module libXi.so.6 from rpm libXi-1.8.10-1.el10.x86_64#012Module libffi.so.8 from rpm libffi-3.4.4-9.el10.x86_64#012Module libwayland-client.so.0 from rpm wayland-1.23.0-2.el10.x86_64#012Stack trace of thread 21364:#012#0 0x000000000041db4b n/a (n/a + 0x0)#012#1 0x000000000041dac4 n/a (n/a + 0x0)#012#2 0x0000000000450a8c n/a (n/a + 0x0)#012#3 0x0000000000435890 n/a (n/a + 0x0)#012#4 0x00007f3253f5fb68 start_thread (libc.so.6 + 0x94b68)#012#5 0x00007f3253fd06bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 21362:#012#0 0x00007f3253fce4bd syscall (libc.so.6 + 0x1034bd)#012#1 0x0000000000434ef0 n/a (n/a + 0x0)#012#2 0x000000000045126b n/a (n/a + 0x0)#012#3 0x000000000043592a n/a (n/a + 0x0)#012#4 0x0000000000450a8c n/a (n/a + 0x0)#012#5 0x0000000000435890 n/a (n/a + 0x0)#012#6 0x00007f3253f5fb68 start_thread (libc.so.6 + 0x94b68)#012#7 0x00007f3253fd06bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 21363:#012#0 0x00007f3253fce4bd syscall (libc.so.6 + 0x1034bd)#012#1 0x00000000004347a2 n/a (n/a + 0x0)#012#2 0x00000000004506d6 n/a (n/a + 0x0)#012#3 0x0000000000416449 n/a (n/a + 0x0)#012#4 0x0000000000404860 n/a (n/a + 0x0)#012#5 0x0000000000417c5a n/a (n/a + 0x0)#012#6 0x0000000000435890 n/a (n/a + 0x0)#012#7 0x0000000000450a8c n/a (n/a + 0x0)#012#8 0x0000000000435890 n/a (n/a + 0x0)#012#9 0x00007f3253f5fb68 start_thread (libc.so.6 + 0x94b68)#012#10 0x00007f3253fd06bc __clone3 (libc.so.6 + 0x1056bc)#012#012Stack trace of thread 21361:#012#0 0x00007f3253fce4bd syscall (libc.so.6 + 0x1034bd)#012#1 0x00000000004347a1 n/a (n/a + 0x0)#012#2 0x00000000004506d6 n/a (n/a + 0x0)#012#3 0x0000000000405123 n/a (n/a + 0x0)#012#4 0x00007f3253ef530e __libc_start_main (libc.so.6 + 0x2a30e)#012#5 0x00007f3253ef53c9 __libc_start_main@@GLIBC_2.34 (libc.so.6 + 0x2a3c9)#012#6 0x00000000004044aa n/a (n/a + 0x0)#012ELF object binary architecture: AMD x86-64
Dec 13 09:09:45 client systemd[1]: systemd-coredump@977-21365-0.service: Deactivated successfully.
Dec 13 09:09:46 server kernel: traps: VBoxClient[143133] trap int3 ip:41db4b sp:7ff4f0b88cd0 error:0 in VBoxClient[1db4b,400000+bb000]
Dec 13 09:09:46 server systemd-coredump[143134]: Process 143130 (VBoxClient) of user 1001 terminated

```

Рисунок 3.12: Анализ журналов с помощью Inav

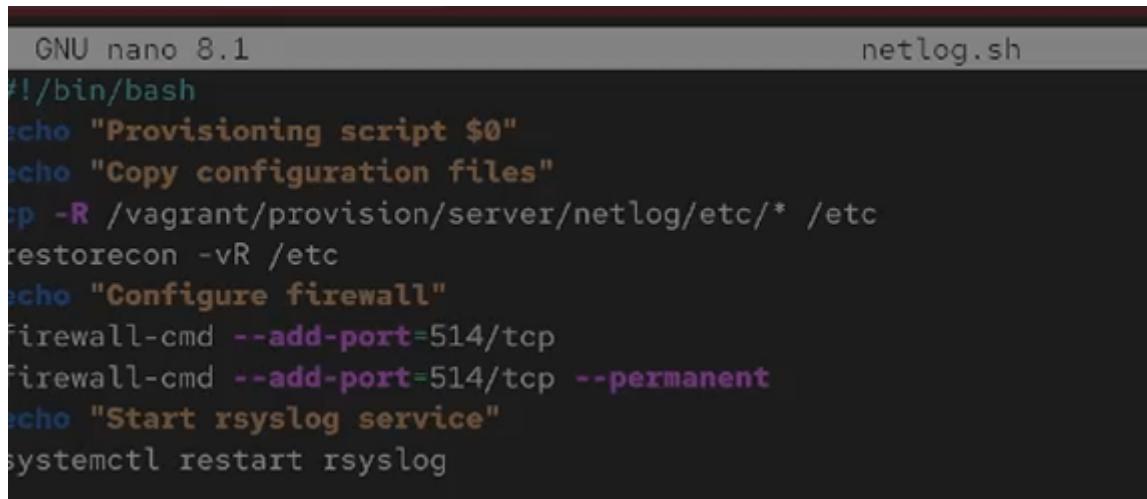
3.3.5 Диагностика системных проблем

Проанализированы сообщения о некорректной работе сервисов. Выявлены и исправлены ошибки в настройках соответствующих служб на основе информации из журналов.

3.4 Автоматизация развертывания

3.4.1 Разработка скриптов provisioning

Созданы исполняемые скрипты для автоматической настройки сервера и клиента системы сетевого журналирования. Скрипты включают копирование конфигурационных файлов и настройку служб.



The screenshot shows a terminal window with a nano editor session for a file named 'netlog.sh'. The title bar indicates 'GNU nano 8.1' and the file name 'netlog.sh'. The script content is as follows:

```
#!/bin/bash
echo "Provisioning script $0"
echo "Copy configuration files"
cp -R /vagrant/provision/server/netlog/etc/* /etc
restorecon -vR /etc
echo "Configure firewall"
firewall-cmd --add-port=514/tcp
firewall-cmd --add-port=514/tcp --permanent
echo "Start rsyslog service"
systemctl restart rsyslog
```

Рисунок 3.13: Скрипт настройки сервера журналирования

3.4.2 Организация конфигурационных файлов

Создана структура каталогов для хранения конфигурационных файлов сервера и клиента. Выполнено копирование рабочих конфигураций в соответствующие директории.

3.4.3 Интеграция с Vagrant

Настроены секции provisioning в конфигурационном файле Vagrant для автоматического выполнения скриптов при развертывании виртуальных машин.

```
server.vm.provision "SMB server",
  type: "shell",
  preserve_order: true,
  path: "provision/server/smb.sh"

server.vm.provision "server netlog",
  type: "shell",
  preserve_order: true,
  path: "provision/server/netlog.sh"

server.vm.provision "server firewall",
  type: "shell",
  preserve_order: true,
  path: "provision/server/firewall.sh"

end
```

Рисунок 3.14: Конфигурация Vagrantfile для журналирования

3.4.4 Тестирование работы автоматизации

Протестирована работа скриптов автоматизации при создании виртуальных машин. Проверена корректность настройки всех компонентов системы журналирования.

3.4.5 Проверка передачи журналов

Проверена передача сообщений от клиента на сервер журналирования. Убедились в корректной записи клиентских логов в централизованное хранилище.

4 Контрольные вопросы

1. **Какой модуль rsyslog вы должны использовать для приёма сообщений от journald?**

Модуль imjournal используется для приёма сообщений от journald.

2. **Как называется устаревший модуль, который можно использовать для включения приёма сообщений журнала в rsyslog?**

Устаревший модуль - imuxsock.

3. **Чтобы убедиться, что устаревший метод приёма сообщений из journald в rsyslog не используется, какой дополнительный параметр следует использовать?**

Следует использовать параметр RateLimit.Interval=0 в конфигурации imjournal.

4. **В каком конфигурационном файле содержатся настройки, которые позволяют вам настраивать работу журнала?**

Настройки содержатся в файле /etc/systemd/journald.conf.

5. **Каким параметром управляется пересылка сообщений из journald в rsyslog?**

Параметром ForwardToSyslog в файле /etc/systemd/journald.conf.

6. **Какой модуль rsyslog вы можете использовать для включения сообщений из файла журнала, не созданного rsyslog?**

Модуль imfile позволяет читать сообщения из произвольных файлов.

7. **Какой модуль rsyslog вам нужно использовать для пересылки сообщений в базу данных MariaDB?**

Модуль ommysql используется для пересылки сообщений в базу данных MariaDB.

8. **Какие две строки вам нужно включить в rsyslog.conf, чтобы позволить текущему журнальному серверу получать сообщения через TCP?**

\$ModLoad imtcp и \$InputTCPServerRun 514.

9. **Как настроить локальный брандмауэр, чтобы разрешить приём сообщений журнала через порт TCP 514?**

Использовать команды: firewall-cmd –add-port=514/tcp и firewall-cmd –add-port=514/tcp –permanent.

5 Выводы

- Освоены практические навыки настройки сервера сетевого журналирования с использованием rsyslog
- Приобретён опыт конфигурации клиентских устройств для передачи системных сообщений в централизованное хранилище
- Изучены различные инструменты для просмотра и анализа журналов системных событий
- Освоены методы диагностики системных проблем на основе информации из журналов
- Получены навыки настройки сетевой безопасности для системы журналирования
- Разработана система автоматизации развертывания инфраструктуры сетевого журналирования
- Изучены особенности работы с различными форматами журналов и инструментами их анализа
- Приобретён опыт настройки мониторинга системных событий в распределённой сетевой среде