Пользовательские статьи

В данной книге зарегистрированные пользователи могут создавать свои собственные статьи. После прохождения модерации такие статьи могут быть перенесены в существующие разделы базы знаний.

Балансировка UDP трафика (L3-L4) средствами службы Nginx

> Информация, приведенная на данной странице, является разработкой команды pre-sales и/или community KUMA и **НЕ** является официальной рекомендацией вендора.

> Официальная документация по данному разделу приведена в Онлайн-справке на продукт: Управление потоком событий с помощью nginx (kaspersky.com)

Чтобы настроить балансировку трафика между коллекторами KUMA:

1. Установите nginx на сервере, предназначенном для управления потоком событий (предпочтительно выделенные сервера, не менее двух)

- Команда для установки в Oracle Linux 8.6:
  `$sudo dnf install nginx`
- Команда для установки в Ubuntu 20.4:
  `$sudo apt-get install nginx`
  При установке из sources, необходимо собрать с параметром `-with-stream`:
  `$sudo ./configure -with-stream -without-http_rewrite_module -without-http_gzip_module`

2. Подготавливаем конфигурационный файл nginx.conf, где блоки выделенные красным меняем (название\ip адреса\порт) под свою задачу.

```
{
      upstream back_FW_ASA {
      server 10.11.17.145:514;
      server 10.11.18.145:514;
      }
```

и

```
server {
            listen 514 udp;
            proxy_pass back_FW_ASA;
```

```
        proxy_bind $remote_addr transparent;
    }
```

При помощи данного файла nginx будет "прозрачно" для коллекторов пробрасывать оригинальный сетевой пакет трафика, позволяя передать реальный адрес\имя устройства, которое передало лог.

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;
# Load dynamic modules. See /usr/share/doc/nginx/README.dynamic.
include /usr/share/nginx/modules/*.conf;
events {
    worker_connections 1024;
}
stream {
        upstream back_FW_ASA {
        server 10.11.17.145:514;
        server 10.11.18.145:514;
        }
        server {
                listen 514 udp;
                proxy_pass back_FW_ASA;
                proxy_bind $remote_addr transparent;
        }
}
```

3. Укажите адреса коллекторов KUMA и порт, в примере их адреса\порты - 10.11.17.145:514 ? 10.11.18.145:514, ???????????? ???????? ????????? ????? ??????? ? ???????????? 50:50 (??? ???????????? ???? ????????????).

4. Служба балансировщика будет "прослушивать" 514 порт со всех IP адресов сервера, для большей отказоустойчивости служб предлагается использовать службу keepalived на двух серверах. Настройка keepalived

VIP адрес для использования с балансировками

> Информация, приведенная на данной странице, является разработкой community KUMA и **НЕ** является официальной рекомендацией вендора.

Чтобы настроить балансировку трафика между коллекторами KUMA:

1. Установите nginx на сервере, предназначенном для управления потоком событий (предпочтительно выделенные сервера, не менее двух)

- Команда для установки в Oracle Linux 8+:
  `$sudo dnf install keepalived`
- Команда для установки в Ubuntu 20.4:
  `$sudo apt-get install keepalived`

2. Подготавливаем конфигурационный файл **/etc/keepalived/keepalived.conf** под свою задачу. **Обратите внимание, конфига два! Нужно раскидать конфиг по серверам ACTIVE\BACKUP**

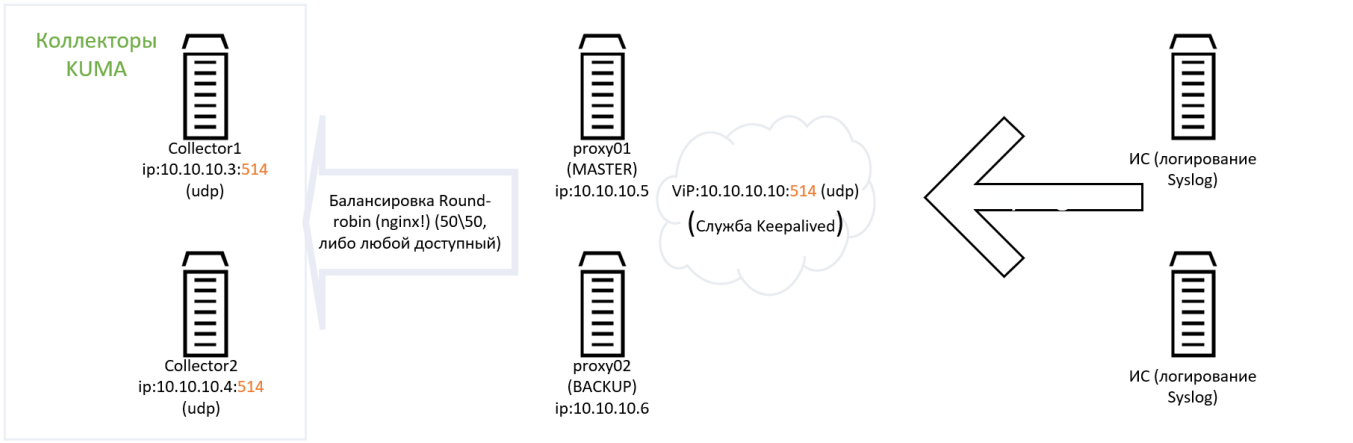
```
#CONFIG FOR MASTER SERVER


! Barebones conf File for keepalived


 global_defs {
   notification_email {
     your_mail@testmailcompany.ru
   }
   notification_email_from keepalived@testmailcompany.ru
   smtp_server mail.testmailcompany.ru
   smtp_connect_timeout 60
 }
```

```
  vrrp_instance VI_1 {
     state MASTER
     interface ens192 #меняем под свой интерфейс
     virtual_router_id 100
     priority 100
     advert_int 1
     authentication {
        auth_type PASS
        auth_pass 12345678 #меняем пароль!
     }
     virtual_ipaddress {
        10.10.10.10
     }
  }



#CONFIG FOR BACKUP SERVER

! Barebones conf File for keepalived

  global_defs {
    notification_email {
      your_mail@testmailcompany.ru
    }
    notification_email_from keepalived@testmailcompany.ru
    smtp_server mail.testmailcompany.ru
    smtp_connect_timeout 60
  }

  vrrp_instance VI_1 {
     state BACKUP
     interface ens192 #меняем под свой интерфейс
     virtual_router_id 100
     priority 100
     advert_int 1
     authentication {
        auth_type PASS
        auth_pass 12345678 #меняем пароль!
     }
```

```
    virtual_ipaddress {
        10.10.10.10
    }
}
```

3. Запускаем службу командой `sudo systemctl start keepalived` на двух серверах, при выводе ip -a можем наблюдать на MASTER сервере - дополнительный адрес - 10.10.10.10, для проверки "переезда" адреса можем остановить службу на MASTER сервере командой `sudo systemctl stop keepalived`, виртуальный адрес поднимется на BACKUP сервере.

4. Настраиваем по статье балансировку средствами nginx и получается следующая отказоустойчивая схема приёма логов на коллекторах:



Включение IPv6 Oracle\CentOS\RedHat

> Информация, приведенная на данной странице, является разработкой community KUMA и **НЕ** является официальной рекомендацией вендора.

Для того, чтобы включить IPv6 нам понадобится:

1. Проверить наличие трех полей по части IPv6 с правильным атрибутом (no\yes), в файле `/etc/sysconfig/network-scripts/ifcfg-` `ens192` (имя интерфейса может меняться, точный необходимо уточнять командой ip a) как в примере, если их нет - добавляем их (при необходимости правим значения.):

   ```
   IPV6INIT=yes
   IPV6_DEFROUTE=yes
   IPV6_FAILURE_FATAL=no
   ```

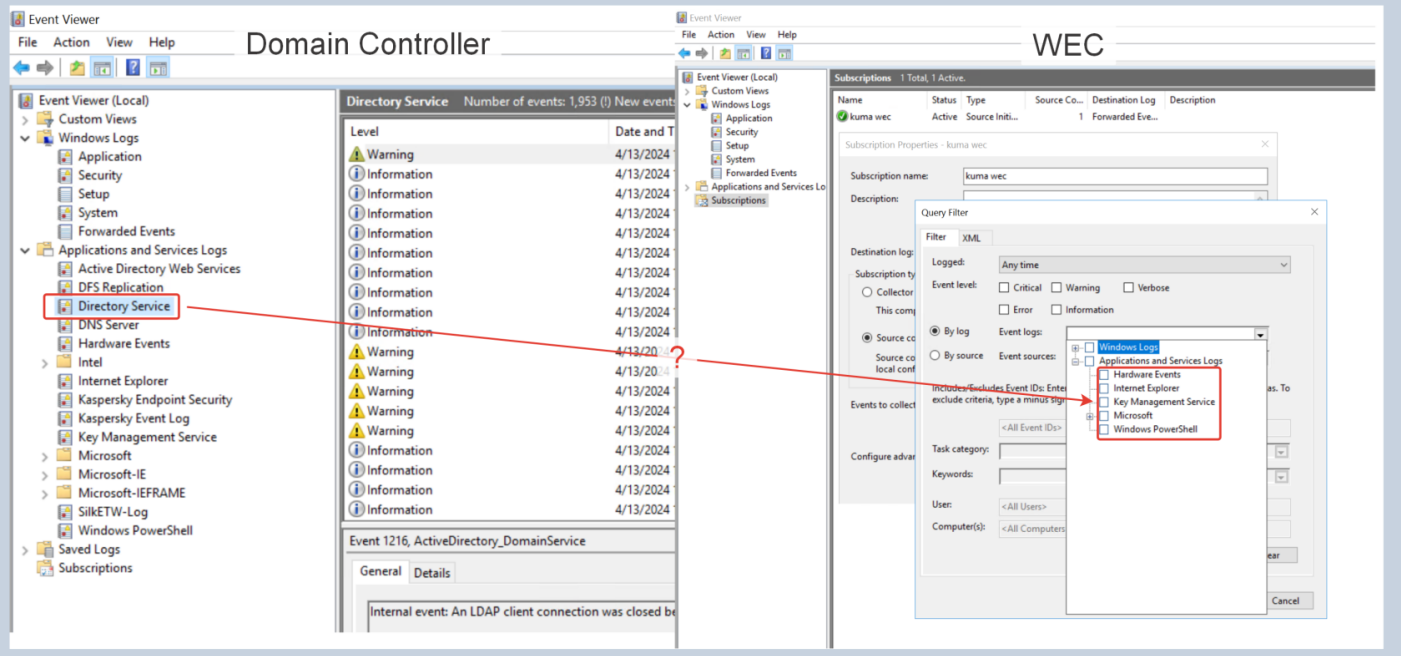
2. Проверяем папку `/etc/sysctl.d/*` на наличие файлов, если они есть - ищем в них следующие строки конфигурации. Обычно используются:

   ```
   net.ipv6.conf.lo.disable_ipv6 = 1
   net.ipv6.conf.all.disable_ipv6 = 1
   net.ipv6.conf.default.disable_ipv6 = 1
   ```

   Если файлов **.conf в папке* /etc/sysctl.d/ нет, или отсутствуют строки, касающиеся работы IPv6 - идем в файл /etc/sysctl.conf и ищем в нем данные строки, если нашли - комментируем их (#перед строкой).
3. Вводим команду `sysctl -p`, IPv6 локальный должен появится. Проверяем командой ip -6 addr
4. Если адрес не появился, проверяем файл `/etc/default/grub`
   в строке GRUB_CMDLINE_LINUX добавляем `ipv6.disable=0`
   Должно получиться: `GRUB_CMDLINE_LINUX="ipv6.disable=0"`, также в этой строке могут быть другие параметры, не стираем их, а добавляем. Запятую ставить не нужно.
5. Запускаем команду `sudo grub2-mkconfig` и `sudo init 6`. Сервер перезагрузится.
6. Проверяем командой `ip -6 addr`

Настройка подписки WEC с использованием XML фильтра

При настройке подписки WEC через графический интерфейс не получится выбрать нужные для сбора журналы, если на сервере с WEC не установлены соответствующие роли Windows Server или ПО.

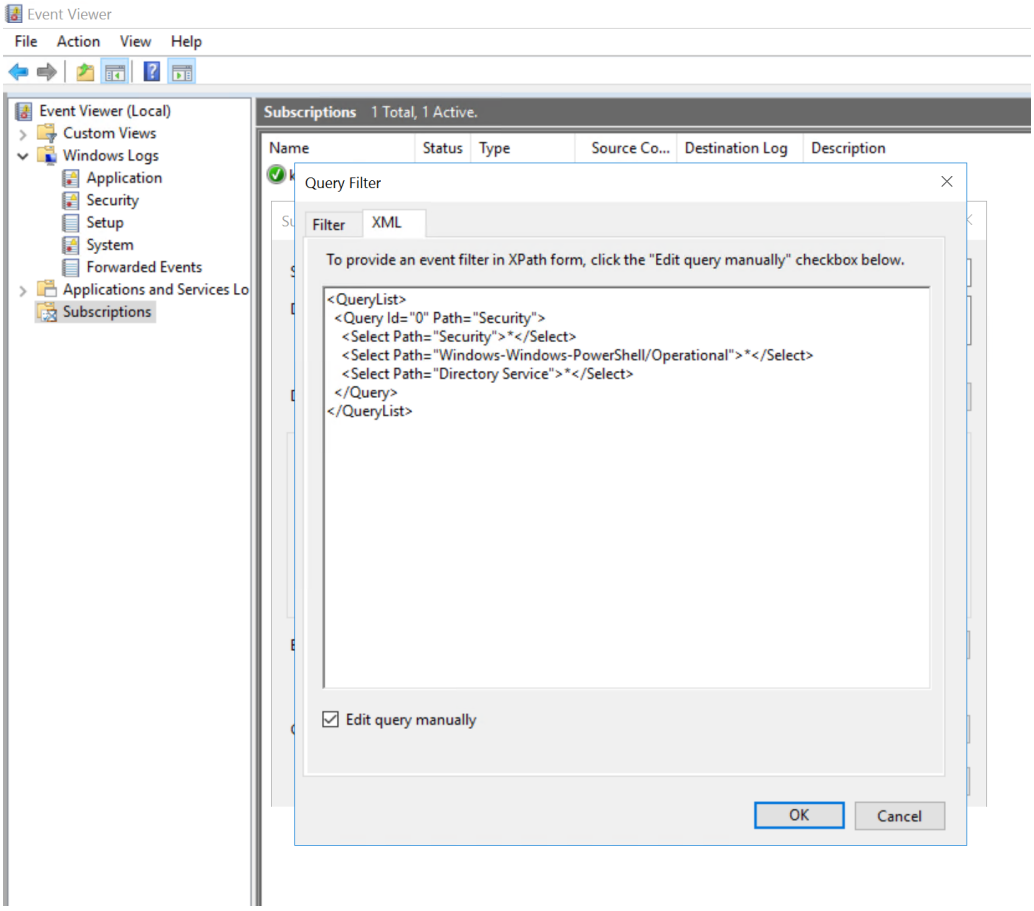


Чтобы выбрать журналы, которые фактически присутствуют на удаленном сервере, но не доступны для выбора на WEC, можно воспользоваться XML фильтром.

Ниже приведен пример XML фильтра для сбора событий из стандартного журнала Security, а также из журнала, который присущ только контроллеру домена - Directory Service.

```
<QueryList>
  <Query Id="0" Path="Security">
    <Select Path="Security">*</Select>
    <Select Path="Windows-Windows-PowerShell/Operational">*</Select>
    <Select Path="Directory Service">*</Select>
  </Query>
```

```
</QueryList>
```



В результате данной настройки WEC начнет собирать события из журнала контроллера домена Directory Service.

Аналогичном образом можно настроить сбор событий из других специфических журналов, а также использовать XML фильтры, если требуется выполнить настройку большого количества подписок WEC.