Конфигурационный файл

Для WNAM версии 1.6 конфигурационный файл wnam.properties не используется, и вы можете пропустить это раздел. Все нижеописанные настройки доступны в веб-интерфейсе.

Предыдущие версии WNAM полностью настраиваются через административный веб-интерфейс, за исключением небольшого числа базовых параметров, которые вы вряд ли захотите часто изменить. Эти параметры установлены в файле wnam.properties. Файл расположен в каталогах:

/etc/ - для WNAM версии 1.4 и ниже

/home/wnam/ - для WNAM версии 1.5

В конфигурационном файле определены параметры приложения WNAM. Поскольку данный конфигурационный файл перечитывается при запуске приложения, изменения в этом файле требуют перезапуска приложения WNAM (перезапуском сервера tomcat, либо сервиса wnam).

Параметры работы с базой данных (не в кластерной конфигурации, которая описана дополнительно):

```
mongodb_host=localhost
mongodb_port=27017
mongodb_user=
mongodb_password=
mongodb_path=    (     ,    . WNAM    %     .)
```

(manager) Tomcat, WNAM (tomcat-manager):

```
admin_user=tomcat8
admin_password=tomcat8
```

Параметры доступа к RADIUS-серверу с целью периодический проверки времени его отклика. Обычно это тот же самый сервер, где работает WNAM:

```
radius_host=127.0.0.1
radius_secret=secret
```

При использовании WNAM в конфигурации Linux-маршрутизатора или с контроллером Unifi, когда RADIUS не требуется, укажите параметр radius_host=disabled

Пароль для взаимодействия с агентом уведомления о DHCP-событиях:

```
password=password
```

Рекомендуется ограничить доступ к административному интерфейсу и статистике WNAM путём указания разрешенных хостов и сетей, откуда такой доступ позволен (список через запятую, подсеть указывается с маской в виде "/" - число единичных бит в маске):

```
allowed_subnets=192.168.100.0/24, 188.224.13.78, 195.208.224.0/22
```

Параметры взаимодействия с порталом перехвата, организованном на том же сервере Linux (путь до скрипта управления, тайм-аут сессии):

```
linuxcp_leasescheck_script=/usr/local/bin/wnam-leases.pl
linuxcp_session_timeout=1200
```

Этот параметр включает учёт трафика (счётчики байт в сессиях) на основе статистики NetFlow, которую вы должны собирать на том же Linux-сервере:

```
is_netflow_acct=true
```

Параметры кэширования данных

Для решения проблем с "зависшими" сессиями абонентов (например, для случая перезагрузки сервера доступа) устанавливается абсолютный тайм-аут сессии, равный по умолчанию 6 часам (21600 сек.). Если сессия длится больше заданного времени, она сбрасывается из WNAM (даже если RADIUS-трафик по ней продолжает поступать). При установке параметра в 0 авто-сброса сессии не будет. Его можно настроить через следующий параметр:

```
session_max_lifetime=21600
```

Следующий параметр позволяет контролировать сброс сессии, если RADIUS-трафик по ней не поступает дольше указанного времени. При установке параметра в 0 проверка не производится.

```
session_max_interim=1800
```

Следующий параметр заставляет принудительно отправлять стоп-запрос (через RADIUS CoA, PoD или API) в сторону

сервера доступа при принудительном сбросе сессии в случае наступления абсолютного/interim таймаута по описанным выше двум критериям. По умолчанию выключено.

```
session_stop_expired=false
```

Время жизни закэшированной записи о выделении IP-адреса сервером DHCP (сек.)

```
dhcp_cache_timeout=43200
```

Время жизни закэшированной записи о созданной, но не авторизованной сессии на маршрутизаторе Cisco ISG (сек.)

```
isg_cache_timeout=43200
```

Время жизни закэшированной записи о созданной, но не авторизованной сессии в пользовательском разделе портала WNAM (/cp/...) (сек.)

```
connection_cache_timeout=300
```

Максимальный интервал времени между попыткой инициированного абонентом входа в сеть (веб-логина) и соответствующего RADIUS Auth запроса от сервера доступа (сек.). Если RADIUS Auth поступает позже этого момента (определенного в параметре lastUsed записи об абоненте), WNAM считает поступивший запрос попыткой MAC-авторизации, и применяет соответствующие правила обработки.

```
mac_auth_interval=60
```

Расширять длину идентификатора сессии (в RADIUS-данных) для уменьшения вероятности коллизии, например audit-session-id=0aab400a0000000a5aa90792 будет преобразован в 0aab400a0000000a5aa90792-341f5c

```
extend_session_id=true
```

Более строгая проверка привязки MAC и IP адреса

```
strict_ip_mac_check=false
```

Параметры взаимодействия с системой отправки СМС, локально утилитой gammu (указывается путь до исполняемого файла), или до шлюза kannel (настройки smsbox):

```
gammu_path=
kannel_host=127.0.0.1
kannel_port=13003
kannel_user=wnam_user
kannel_password=wnam_pass
```

```
intl_src_number=
```

Задаёт номер телефона, который будет подставляться вместо имени отправителя СМС при отправке через шлюз kannel (метод SMPP) сообщений зарубежным получателям (номера которых НЕ начинаются на 79). Требуется, чтобы зарубежные пользователи в роуминге смогли принимать СМС, т.к. для них обычно буквенные идентификаторы отправителя запрещены.

```
check_sms_balance=true
```

Устанавливает необходимость пытаться проверить баланс счета СМС-провайдера (только для SMSC и WebSMS), по умолчанию включено.

Параметры почтового сервера (для отправки уведомления о завершении рекламных кампаний, тестового письма, письма со ссылкой для входа и сброса пароля):

```
smtp_server=localhost
smtp_port=25
smtp_user=
smtp_password=
email_from=admin@localhost
```

Ссылка на веб-интерфейс (адрес сервера) пользователя личного кабинета/администратора, доступный "извне", которая появится в письме с ссылкой для входа после сброса пароля.

```
email_wnam_ref=https://wnam.provider.net/
```

Названия для отображения в личном кабинете владельца площадки:

```
owning_company=\\u041E\\u041E\\u041E
"\\u041D\\u0435\\u0442\\u0430\\u043C\\u0441-\\u043E\\u0431\\u043B\\u0430\\u043A\\u043E"
owning_company_url=http://cloud.wnam.ru
owning_logo=wnam_logo_owner.png
```

Путь до скрипта, занимающегося генерацией миниатюрных изображений предпросмотра из конструктора страниц:

```
render_script=/usr/local/bin/render.sh
```

Параметры работы встроенного RADIUS-сервера (только для версии WNAM 1.5)

```
radiusd_enable=true
,  ,  RADIUS-.     ,      FreeRADIUS
```

radiusd_networks=127.0.0.1,10.0.0.0/8
Список сетей, из которых разрешен доступ к RADIUS-серверу. Как минимум оставьте здесь сам сервер WNAM (127.0.0.1, для внутренней проверки), и перечислите сети, в которых у вас установлены ваши сервера доступа (роутеры-хотспоты).

radiusd_secret=secret
Секретный ключ по умолчанию, для проверки взаимодействия с WNAM, и для работы с хотспотами

```
radiusd_logdir=/home/wnam/radiuslog
```

Путь до каталога с лог-файлами RADIUS-сервера

Вы можете получить оригинальный файл wnam.properties из набора дополнительных файлов на сервере http://www.netams.com/files/wnam/misc/, либо взяв дистрибутивный файл после установки WNAM из каталога /var/lib/tomcat8/webapp/ROOT/classes/ (для версий младше 1.5)

После внесения изменений сохраните файл wnam.properties в каталог /etc/ на вашем сервере.

Настройки в файле /etc/wnam.properties имеют бóльший приоритет, чем в /var/lib/tomcat8/webapp/ROOT/classes/wnam.properties (для WNAM 1.4 и младше), таким образом они сохранятся при обновлении дистрибутива WNAM.

Изменения в файле требуют перезапуска приложения WNAM (через рестарт сервера tomcat, /etc/init.d/tomcat8 restart) для WNAM 1.4.

Остальные настройки WNAM производятся через веб-интерфейс http://server/wnam/home с логином и паролем по умолчанию admin (смените, пожалуйста, пароль сразу после установки).