sudo apt-get install nagios-full -y

<https://packages.altlinux.org/ru/sisyphus/binary/nagios-full/x86_64/>

<https://phoenixnap.com/blog/nagios-monitoring-tutorial>

**Настройка сервера мониторинга**

**На сервере:**

установить пакеты

apt-get install -y nagios-full nagios-www-apache2 nagios-addons-nrpe nagwad-templates nagwad-actions apache2-mod\_ssl nagiosdigger perl-DBD-mysql

Для каждого наблюдаемого узла в директории /etc/nagios/objects

нужно создать его конфигурационный файл, например, для узла host-100 создадим файл

vim /etc/nagios/objects/host-100.cfg

со следующим содержимым:

define host {

host\_name host-100

use linux-server

alias nagios-node

address 192.168.51.110

hostgroups nagwad-nodes

}

Критически важным является указание hostgroups nagwad-nodes. Все проверки, которые обеспечивает пакет nagwad и описаны в шаблоне /etc/nagios/templates/50-nagwad.cfg будут выполняться именно для этой группы хостов:

less /etc/nagios/templates/50-nagwad.cfg

**Установим СУБД для хранения статистики нарушений**

apt-get install -y mariadb

systemctl start mariadb

Создаем БД с именем nagiosdigger для хранения статистики нарушений. Для этого подключаемся к СУБД командой mysql:

mysql

и вводим следующие команды:

CREATE DATABASE nagiosdigger;

EXIT;

Затем в БД nagiosdigger создаем все необходимые таблицы скриптом:

cat /usr/share/doc/nagiosdigger-0.9.1/create\_tables\_mysql.sql | mysql -B nagiosdigger

Затем нужно снова подключиться к СУБД командой mysql и ввестиследующие команды:

GRANT INSERT,SELECT ON nagiosdigger.logs TO nagioslogs@localhost

IDENTIFIED BY 'пароль';

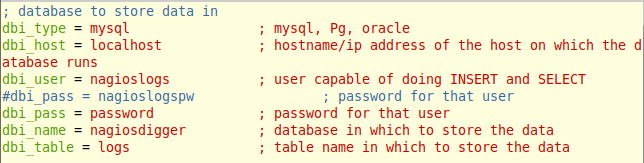
FLUSH PRIVILEGES;

EXIT;

указав в качестве пароля желаемый пароль для доступа к БД статистики нарушений.

Чтобы собирающее статистику нарушений ПО имело возможность чтения и записи статистики нарушений, использованный при конфигурации БД пароль необходимо прописать в конфигурационный файл /etc/nagios/nagiosdigger/config.ini (строка dbi\_pass)

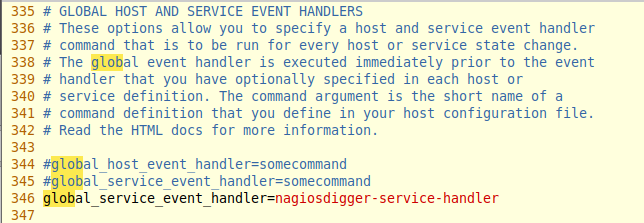
vim /etc/nagios/nagiosdigger/config.ini



Включаем копирование записей о событиях в БД, записав в конфигурационный файл /etc/nagios/nagios.cfg строку:

global\_service\_event\_handler=nagiosdigger-service-handler

vim /etc/nagios/nagios.cfg



Ставим в автозагрузку службы:

systemctl enable mariadb

systemctl enable nagios

systemctl enable httpd2

На сервере создаем ключ (в данном примере не ставим пароль на файл)

ssh-keygen

И отправляем открытый ключ на наблюдаемый хост (хосты):

ssh-copy-id 192.168.51.110

Проверяем возможность подключения:

ssh '192.168.51.110'

exit

Проверяем конфиг на отсутствие ошибок (иначе сервис не запустится):

/usr/sbin/nagios -v /etc/nagios/nagios.cfg

Запускаем сервис

systemctl start nagios

Устанавливаем программу Nagstamon. **Nagstamon** is a Nagios status monitor

Nagstamon — это монитор состояния Nagios, который отображается в системном трее или на рабочем столе (GNOME, KDE) в виде плавающей панели состояния, чтобы информировать вас в режиме реального времени о состоянии вашей контролируемой Nagios сети.

apt-get install -y nagstamon

Перезагрузить ОС

**На клиенте:**

На удаленном хосте, за которым необходимо наблюдать, установить пакеты:

nagwad и nagios-nrpe, и добавить их в автозагрузку:

# apt-get install nagwad -y

# apt-get install nagios-nrpe -y //устанавливается как зависимость предыдущего пакета видимо.

Запустить службы:

systemctl enable osec.timer

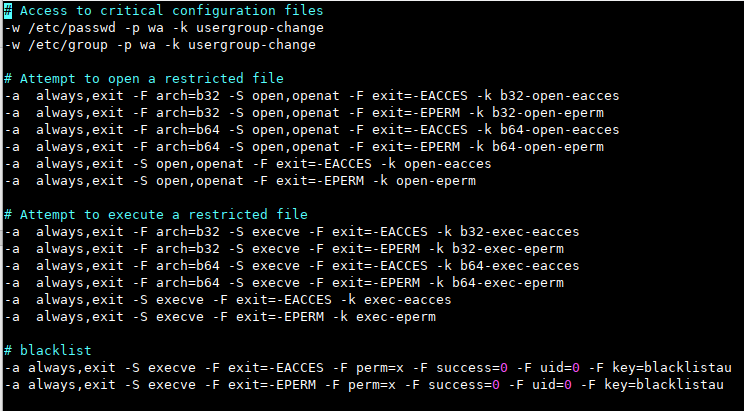
systemctl enable nagwad

systemctl enable nrpe

**Привести к указанному виду содержимое конфигурационного файла**

**/etc/audit/rules.d/50-nagwad.rules:**

vim /etc/audit/rules.d/50-nagwad.rules



Добавим блок:

# blacklist

-a always,exit -S execve -F exit=-EACCES -F perm=x -F success=0 -F uid=0 -F key=blacklistau

-a always,exit -S execve -F exit=-EPERM -F perm=x -F success=0 -F uid=0 -F key=blacklistau

В директории /etc/nagwad/

cd /etc/nagwad/

проверить конфигурационный файл

audit.regexp на предмет наличия следующего содержимого:

open-eacces

open-eperm

exec-eacces

exec-eperm

В директорию /etc/nagwad/ добавить конфигурационный файл

blacklist.regexp со следующим содержимым:

blacklistau

В конфигурационном файле /etc/nagios/nrpe.cfg, в строке server\_address= необходимо добавить **IP-адрес сервера** мониторинга Nagios:

server\_address=**192.168.51.1**

В файле /etc/nagios/send\_nsca.cfg установить:

host\_address=192.168.51.1 #сервер мониторинга с Nagios

Перезапустить систему:

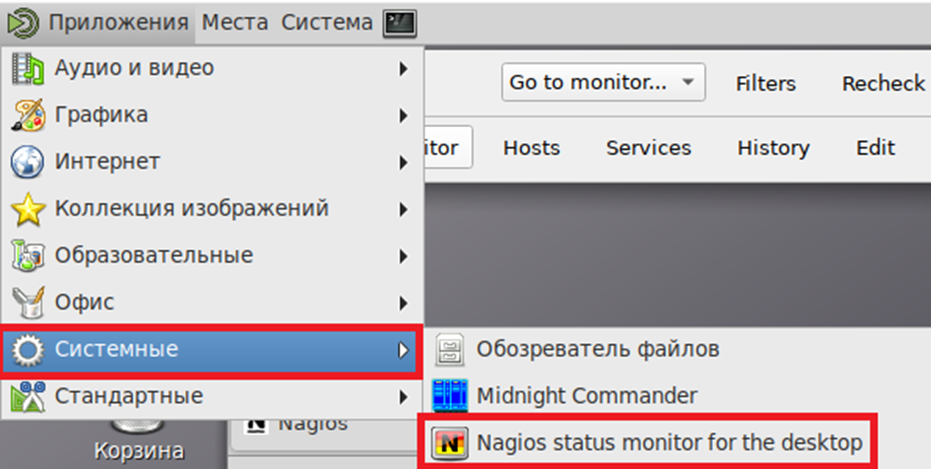
Reboot

echo "PermitRootLogin yes" >> /etc/openssh/sshd\_config

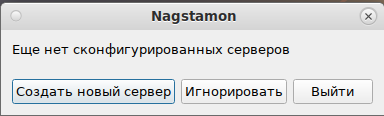
service sshd restart

**На сервере мониторинга**

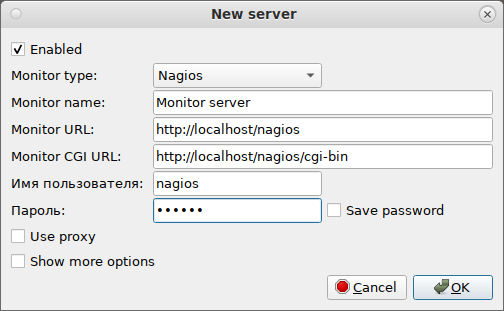
Запустить Nagstamon:



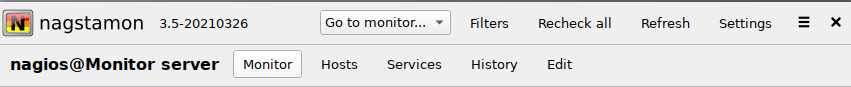
Нажать кнопку «Создать новый сервер»



Подключиться к серверу (**пароль nagios**):



Появится панель мониторинга Nagstamon



Nagstamon – утилита, которая может подключаться к серверам мониторинга, например, к nagios, для того, чтобы обеспечить в режиме реального времени информацию о состоянии узлов и служб. Nagstamon в виде небольшой настраиваемой строчки может висеть в любом месте экрана, отображая количество проблем в сети. При наведении на нее мышкой, выпадает список проблем.

**Открыть в браузере веб-консоль** (**пароль nagios**):

<http://localhost/nagios/>

