Настройка аудита VMware ESXi и vCenter

VMware ESXi

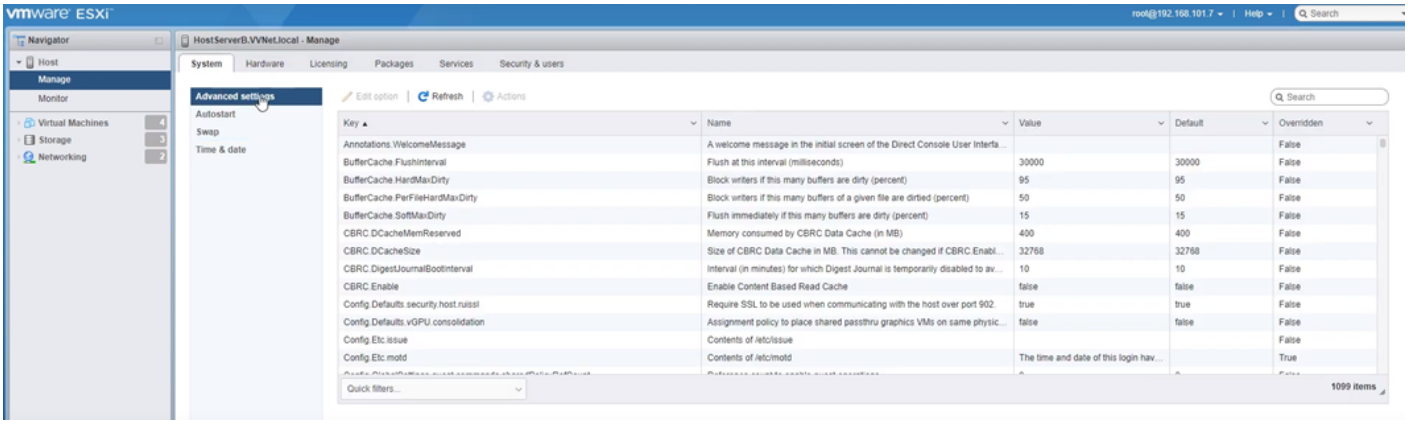
Через веб-интерфейс

Проверьте корректность настроек времени и часового пояса, проверить синхронизацию с NTP-сервером (принять во внимание, что ОС VMware ESXi работает только по UTC).

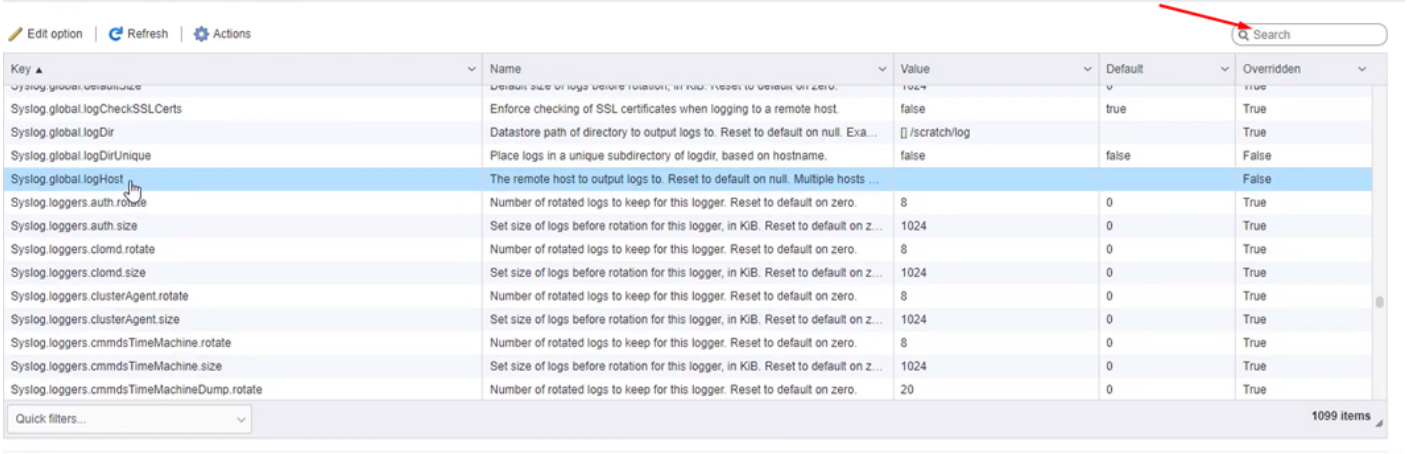
Выполнить резервное копирование конфигурации ESXi-хоста.

Через web-интерфейс подключиться к ESXi-хосту используя учетную запись root.

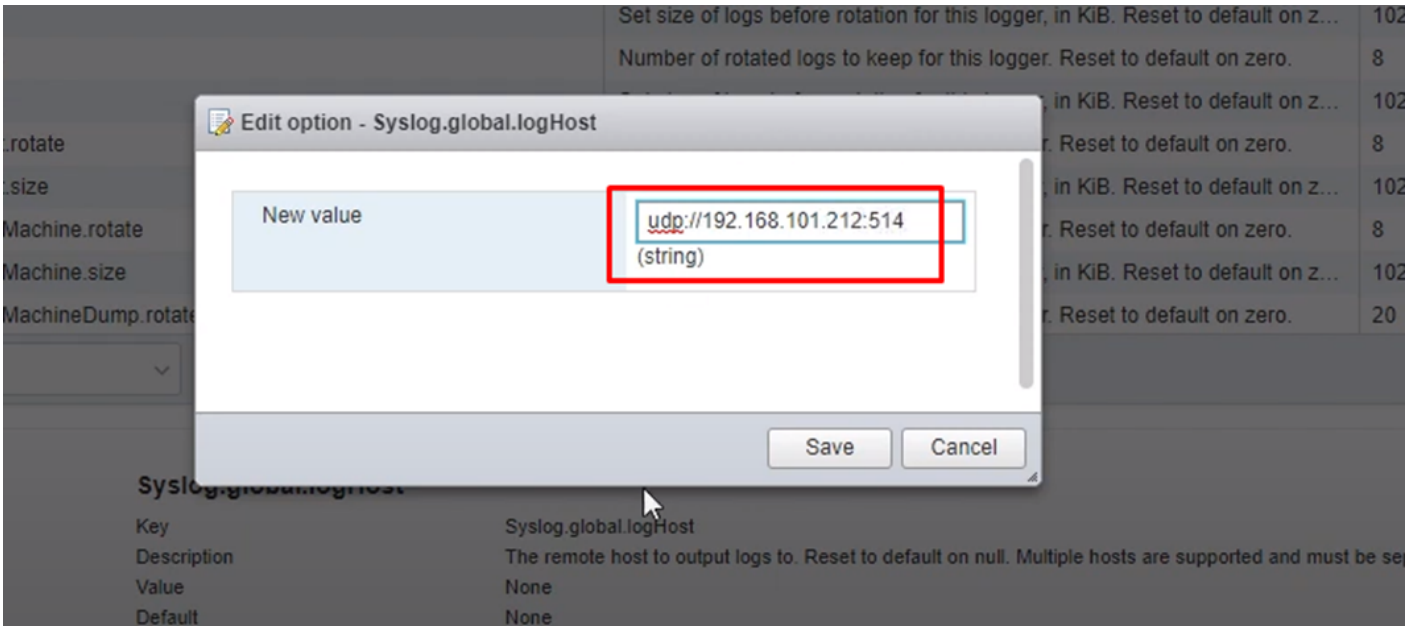
В главном меню в разделе навигации развернуть вкладку Host и перейти по пути: **Host – Manage – Advanced Settings**.



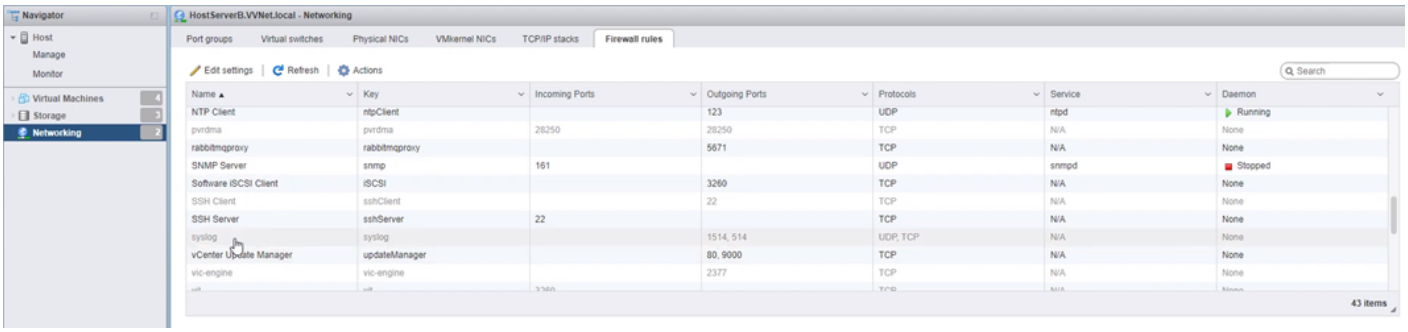
В окне поиска набрать **Syslog.global.LogHost**, выбрать параметр Syslog.global.LogHost и отредактировать его.



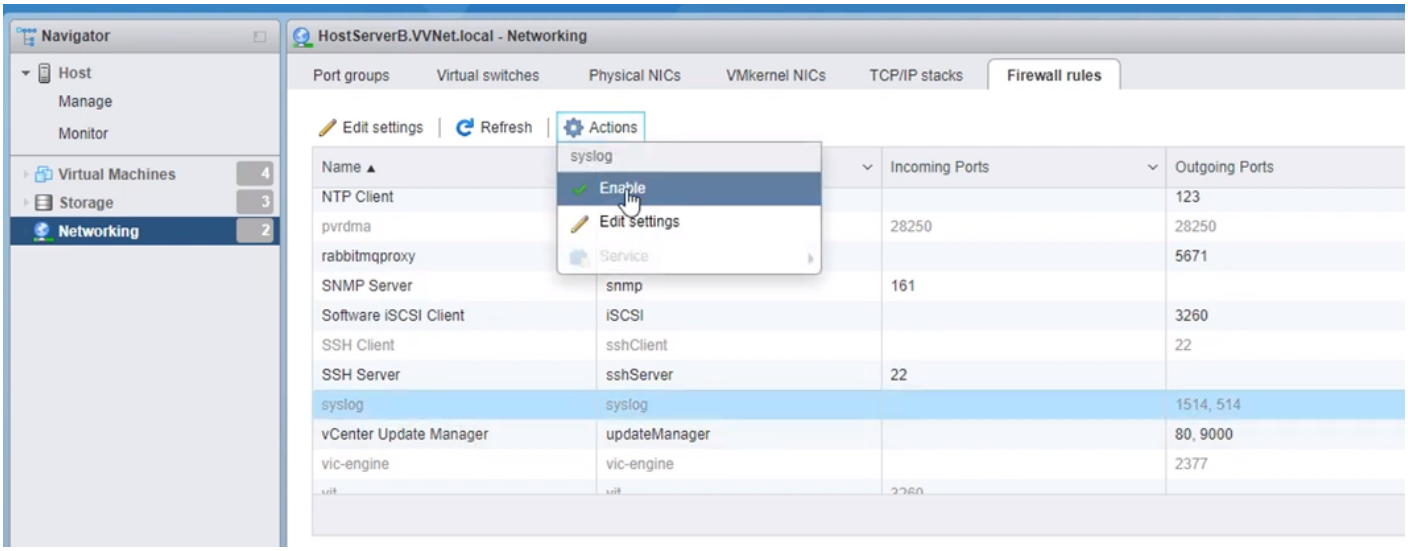
Укажите протокол, адрес и порт коллектора KUMA и нажмите **Save**.



Далее перейдите на вкладку **Networking – Firewall rules**.

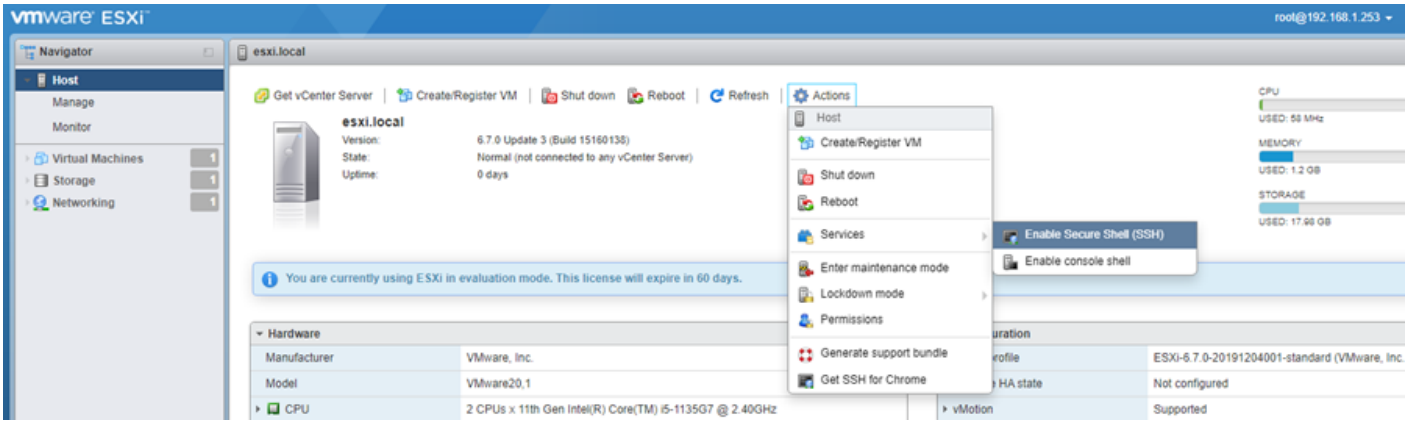


Найдите правило syslog, выделите его (можно воспользоваться поиском) и включите его, нажав на **Actions – Enable**.



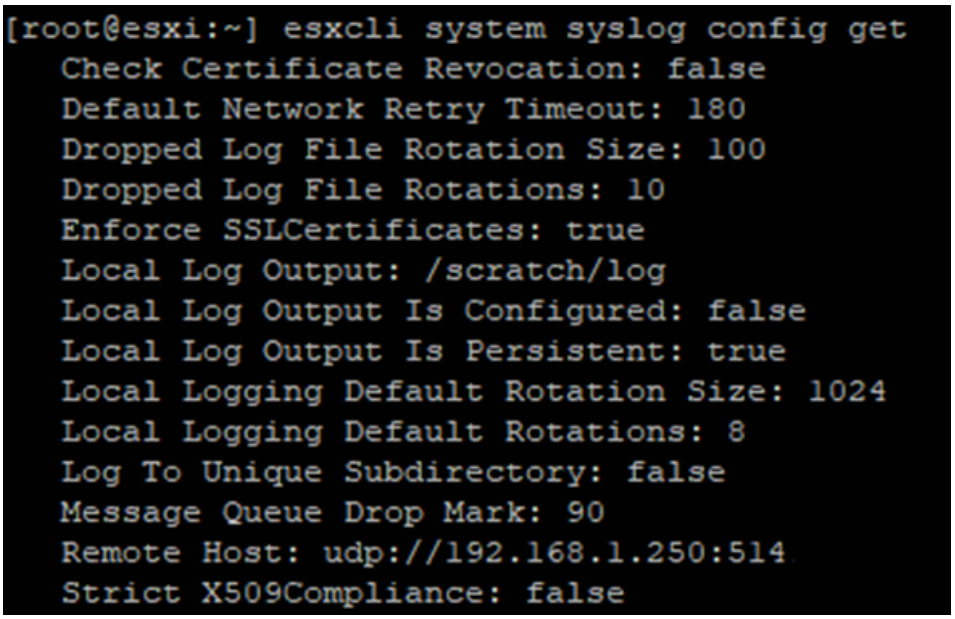
Через SSH

Настройку аудита можно выполнить через SSH. Включить доступ по SSH на ESXi-хосте, перейти по пунктам: **Host – Actions – Services – Enable Secure Shell (SSH)**.



Подключитесь к ESXi-хосту по SSH используя учетную запись root (например через Putty).

- Наберите команду: `esxcli system syslog config set --loghost=udp://192.168.1.250:514` (конфигурирование подключения к syslog-серверу, ip-адрес в команде не является легитимным и указан исключительно для примера).
- Наберите команду: `esxcli network firewall ruleset set --ruleset-id=syslog --enabled=true` (включение разрешающего правила фильтрации для syslog).
- Наберите команду: `esxcli network firewall refresh` (обновление настроек межсетевого экрана ESXi-хоста).
- Наберите команду: `esxcli system syslog config get` (проверка настроек syslog-службы ESXi-хоста):



- Набрать команду: `esxcli system syslog reload` (перезагрузка syslog-службы ESXi-хоста).
- Авторизоваться на ESXi-хосте, через его web-интерфейс под учетной записью с административными правами и **отключить доступ по SSH** (примечание: Согласно рекомендациям VMware, доступы по SSH и к ESXi-shell нужны только во время диагностических и аварийных работ).

(Опционально) Если необходимо отправлять события **Syslog на другой порт назначения**, необходимо добавить правило для МЭ ESXi, для этого зайдите на хост по SSH.

Создайте файл (используются классические Linux команды) со следующим содержимым, например для порта 5140 (назовем файл syslogPort-5140.xml):

```
<!-- /etc/vmware/firewall/syslogPort-5140.xml -->
<!-- remote syslog configuration -->
<ConfigRoot>
  <service>
    <id>syslogPort-5140</id>
    <rule id='0000'>
      <direction>outbound</direction>
      <protocol>udp</protocol>
      <porttype>dst</porttype>
      <port>5140</port>
    </rule>

    <rule id='0001'>
      <direction>outbound</direction>
```

```
    <protocol>tcp</protocol>
    <porttype>dst</porttype>
    <port>5140</port>
   </rule>

   <enabled>false</enabled>
   <required>false</required>
  </service>
</ConfigRoot>
```

Для использования этого правила выполните команды ниже, и активируйте его:

- `cp syslogPort-5140.xml  /etc/vmware/firewall/`
- `esxcli network firewall unload`
- `esxcli network firewall load`

VMware vCenter

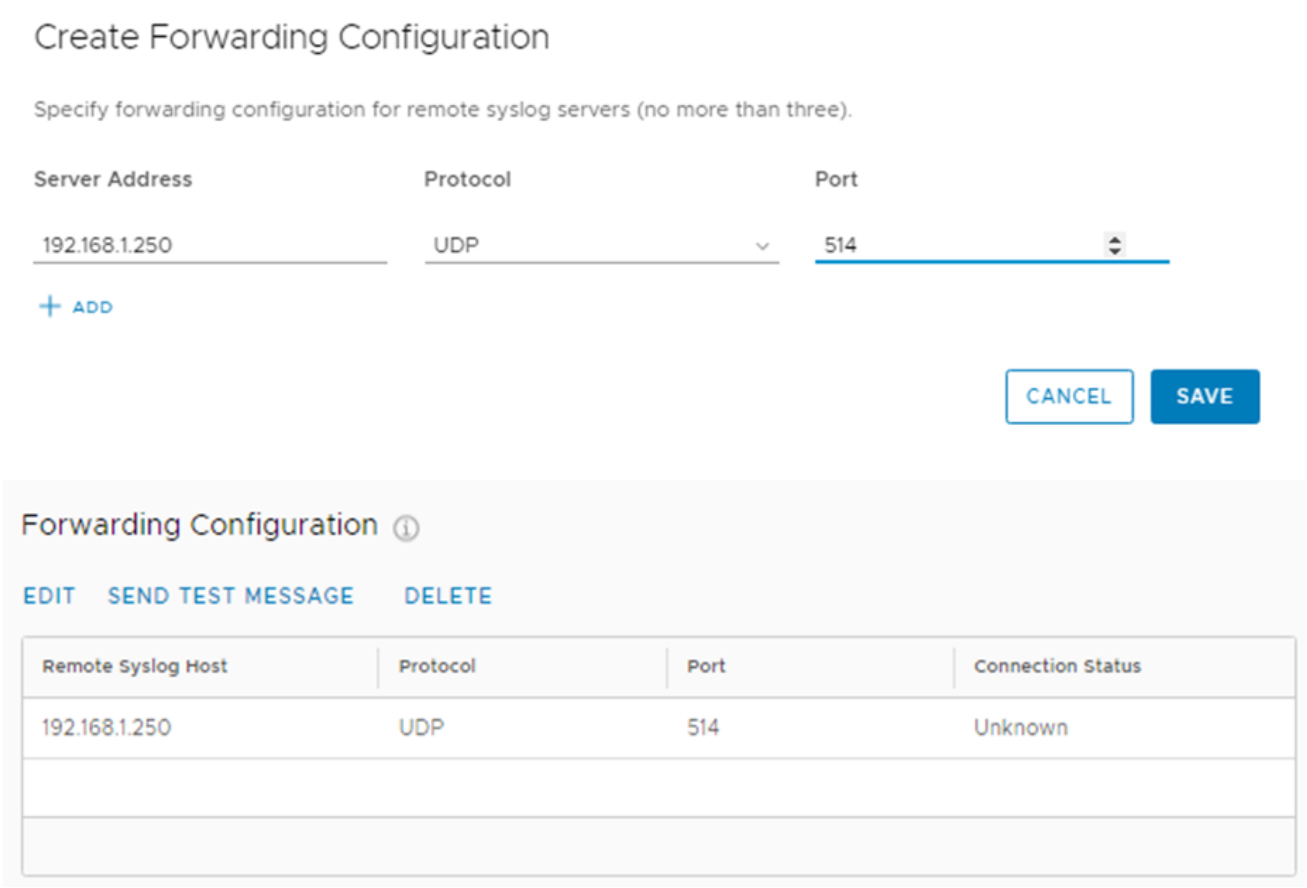
Сделайте snapshot или выполните резервное копирование vCenter.

Через web-браузер подключитесь к vCenter Server Appliance Management Inteface (VAMI) используя административную учетную запись (например, administrator@vsphere.local).

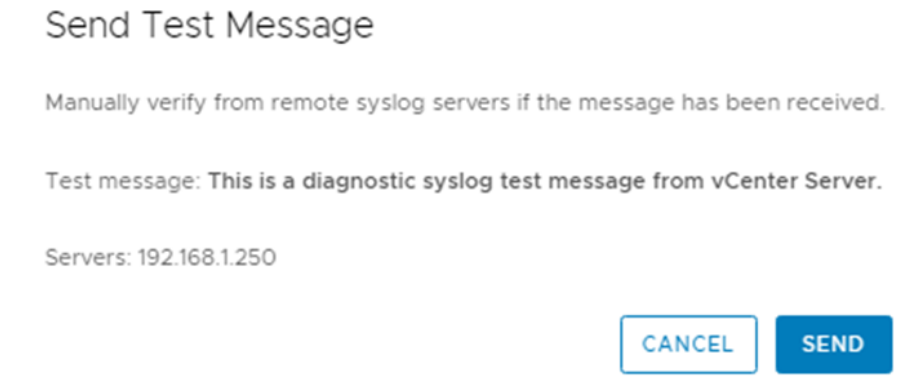
Наберите в web-браузере: https://vcenter.test.local:5480 и ввести административные учетные данные (имя vcenter.test.local не является легитимным и указан для примера).

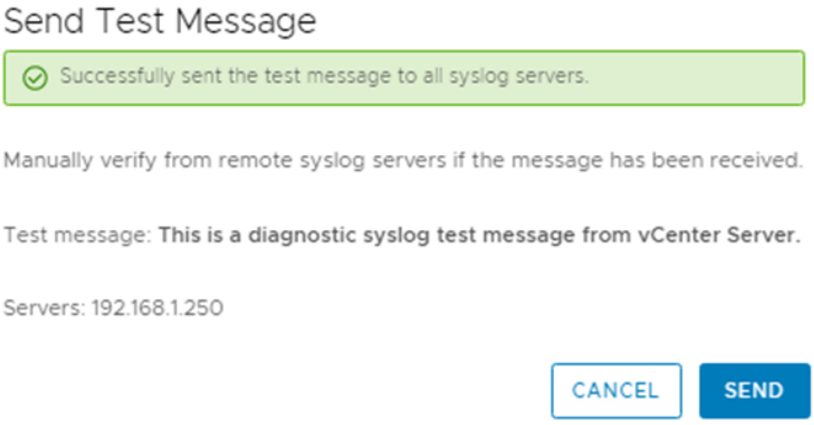
Убедитесь в корректности настроек времени в разделе Time (часовой пояс указан в качестве примера, а тип синхронизации в «Филиале» будет индивидуально зависеть от указанных местных настроек).

Перейти в раздел **Syslog**, чтобы настроить Forwarding. Нажать кнопку **CONFIGURE**, укажите протокол, адрес и порт коллектора KUMA и нажмите **Save**.



Отправьте тестовое сообщение:





Revision #2
Created 14 November 2023 09:50:12 by Boris Rzr
Updated 21 October 2024 15:09:46 by Koala