Cisco IOS

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

Настройка Cisco IOS

Войдите на источник Cisco IOS коммутатор или маршрутизатор.

Введите следующую команду для входа в маршрутизатор в привилегированный режим: `enable`

Переключитесь в режим конфигурации (configure terminal):

```
conf t
```

> Перед включением ведения журнала убедитесь, что ваш маршрутизатор правильно настроен для получения времени от сервера NTP, или настройте его вручную, чтобы получать время. Используйте команду `set clock` или `ntp server x.x.x.x` для синхронизации часов.

Включите журналирование:

```
logging on
```

Укажите IP-адрес коллектора и порт (можно использовать UDP или TCP транспорт):

```
logging host <IP-адрес коллектора> transport udp port <порт коллектора>
```

Укажите уровень важности событий (рекомендуется informational):

```
logging trap informational
```

Уровни критичности в CISCO:

Level Keyword	Level	Description	Syslog Definition
emergencies	0	Система нестабильна	LOG_EMERG
alerts	1	Требуются немедленные действия	LOG_ALERT

critical	2	Критические условия	LOG_CRIT
errors	3	Условия ошибки (по умолчанию)	LOG_ERR
warnings	4	Условия предупреждения	LOG_WARNING
notifications	5	Нормальное, но значимое состояние	LOG_NOTICE
informational	6	Только информационные сообщения	LOG_INFO
debugging	7	Отладка сообщений	LOG_DEBUG

Укажите интерфейса источника для отправки событий:

```
logging source-interface <Имя интерфейса>
```

<Имя интерфейса> - это имя интерфейса, например, dmz, lan, ethernet0 или ethernet1.

Настройте средство для системного журнала:

```
logging facility syslog
```

Настройте идентификатор событий:

```
logging origin-id ip
```

Настройте временные метки событий и идентификаторы событий в логировании:

```
service timestamps log datetime year show-timezone
service sequence numbers
```

> Маршрутизатор по умолчанию не проверяет, авторизован ли пользователь в консольном порту или к нему подключено устройство; если ведение журнала консоли включено, на консольный порт всегда отправляются сообщения, которые могут вызвать нагрузку на процессор. Поэтому ниже включим логирование только необходимых событий. (вместо включения `logging console warning`)

Включите регистрацию событий входа пользователей:

```
logging userinfo
login on-success log
login on-failure log
ip ssh logging events
```

Включите регистрацию событий выполнения конфигурационных команд:

```
archive
log config
logging enable
notify syslog contenttype plaintext
```

Опционально. Включите регистрацию событий VPN:

```
crypto logging ezvpn
crypto logging session
crypto logging ikev2
```

Выйдите из режима конфигурирования:

```
end
```

Сохраните изменения даже после перезагрузки:

на старых Cisco:

```
write memory
```

на новых Cisco (копирование рабочей конфигурации):

```
copy running-config startup-config
```

Чтобы отобразить состояние системного журнала (syslog) и содержимое стандартного буфера сообщений системного журнала, используйте команду из привилегированного режима:

```
show logging
```

Revision #3
Created 6 December 2023 11:14:27 by Boris Rzr
Updated 7 July 2024 08:51:36 by Koala