SMART-SOFT
ГРУППА КОМПАНИЙ

TRAFFIC INSPECTOR NEXT GENERATION

Инструкция по настройке
Center Management System
в Traffic Inspector Next Generation

www.smart-soft.ru

1. Обзор

Center Management System – система централизованного управления распределенной инфраструктурой сетевых шлюзов Traffic Inspector Next Generation. В рамках инфраструктуры, шлюз Traffic Inspector Next Generation может выполнять одну из двух ролей:

- Мастер-узел (master node) – шлюз Traffic Inspector Next Generation, устанавливаемый в центральном офисе учреждения. Мастер-узел позволяет осуществлять централизованное администрирование, диагностику и сбор данных с сетевых шлюзов, расположенных в удаленных офисах.
- Подчиненный узел (slave node) – шлюз Traffic Inspector Next Generation, устанавливаемый в каждом из удаленных офисов учреждения. Подчиненный узел получает свои настройки от назначенного мастер-узла. Подчиненный узел полностью контролирует и защищает сетевое взаимодействие между компьютерами удаленного офиса и сетью Интернет.

В процессе развертывания, администратор осуществляет настройки на каждом из узлов будущей инфраструктуры. Подчиненные узлы подготавливаются для взаимодействия с мастер-узлом. На мастер-узле производится регистрация подчиненных узлов. Сетевое взаимодействие между мастер-узлом и подчиненным узлом осуществляется по защищенным соединениям. После настройки инфраструктуры, администратор может инициировать передачу настроек на выбранный подчиненный узел и получать диагностические сообщения с подчиненных узлов.

Примечания. Только один шлюз может выступать в качестве мастер-узла в инфраструктуре. Количество подчиненных узлов не ограничено. Мастер-шлюз

может совмещать функции центра управления для удаленных шлюзов и функции обычного контролирующего шлюза.

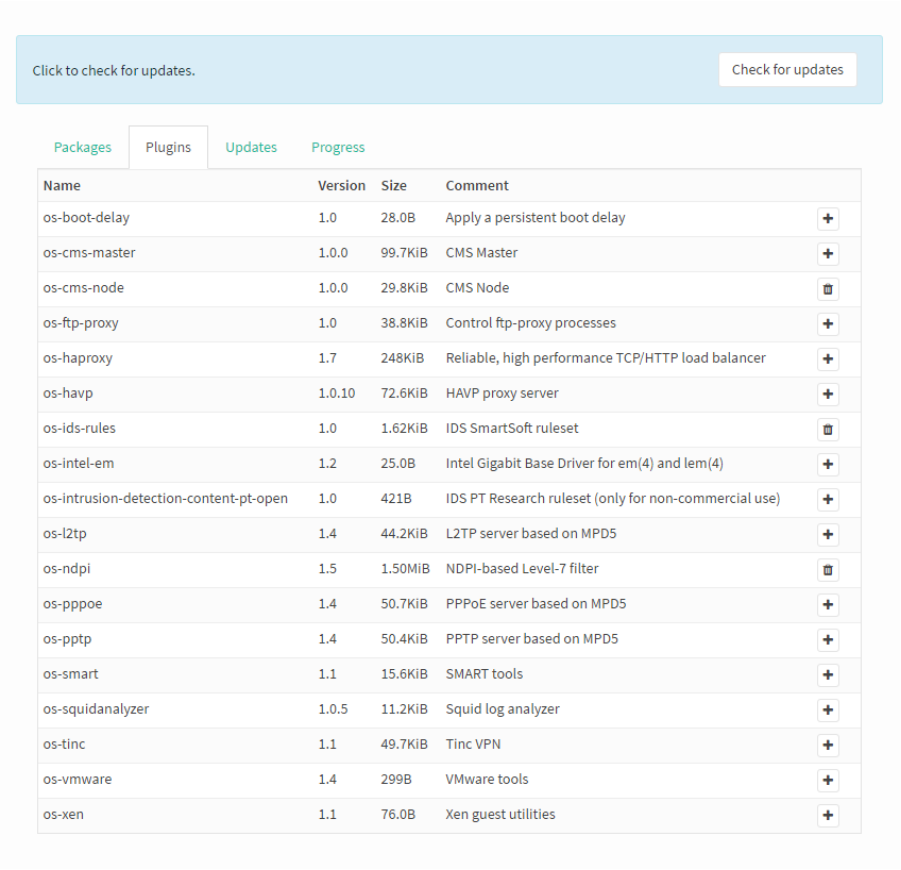
2. Настройка подчиненного нода

1.1. Установка сертификата для доступа к репозиторию

Установите приобретенный лицензионный сертификат. В разделе Сводка –> Сертификат укажите файл сертификата и файл ключа.

1.2. Установка плагина os-cms-node

Пройдите в раздел Система -> Прошивка -> Обновления, и нажмите Проверить наличие обновлений. Нажмите на иконку + напротив плагина os-cms-node для его установки.

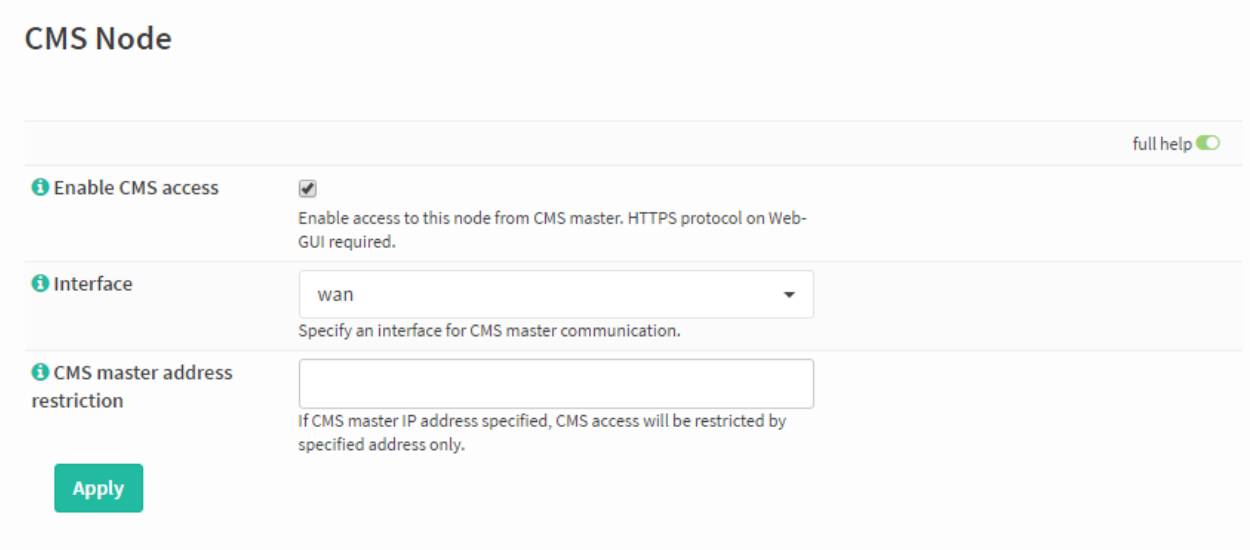


Name	Version	Size	Comment
os-boot-delay	1.0	28.0B	Apply a persistent boot delay
os-cms-master	1.0.0	99.7KiB	CMS Master
os-cms-node	1.0.0	29.8KiB	CMS Node
os-ftp-proxy	1.0	38.8KiB	Control ftp-proxy processes
os-haproxy	1.7	248KiB	Reliable, high performance TCP/HTTP load balancer
os-havp	1.0.10	72.6KiB	HAVP proxy server
os-ids-rules	1.0	1.62KiB	IDS SmartSoft ruleset
os-intel-em	1.2	25.0B	Intel Gigabit Base Driver for em(4) and lem(4)
os-intrusion-detection-content-pt-open	1.0	421B	IDS PT Research ruleset (only for non-commercial use)
os-l2tp	1.4	44.2KiB	L2TP server based on MPD5
os-ndpi	1.5	1.50MiB	NDPI-based Level-7 filter
os-pppoe	1.4	50.7KiB	PPPoE server based on MPD5
os-pptp	1.4	50.4KiB	PPTP server based on MPD5
os-smart	1.1	15.6KiB	SMART tools
os-squidanalyzer	1.0.5	11.2KiB	Squid log analyzer
os-tinc	1.1	49.7KiB	Tinc VPN
os-vmware	1.4	299B	VMware tools
os-xen	1.1	76.0B	Xen guest utilities

Примечание. Для успешной установки плагина в вашем устройстве должен быть установлен лицензионный сертификат.

3. Настройка параметров подчиненного узла

Пройдите в раздел System -> Access -> CMS node и осуществите настройку параметров подчиненного узла.



Установите флажок Enable CMS access для активации функционала подчиненного узла.

В поле Interface выберите интерфейс, через который подчиненный узел будет взаимодействовать с мастер-узлом.

В поле CMS master address restriction можно ограничить возможность подключения мастер-узла только с обозначенных IP-адресов.

Примечание. В результате осуществленных настроек подчиненный узел подготавливается для входящих подключений от мастер-узла. В частности, в сетевой экран подчиненного узла добавляются два правила для доступа по протоколам HTTPS и SSH (указанный IP-адрес будет отличаться в вашем случае):

pass in quick on igb1 inet proto tcp from any to 10.1.1.161 port = https flags S/SA keep state label "Allow CMS access on HTTPS"

pass in quick on igb1 inet proto tcp from any to 10.1.1.161 port = ssh flags S/SA keep state label "Allow CMS access on SSH"

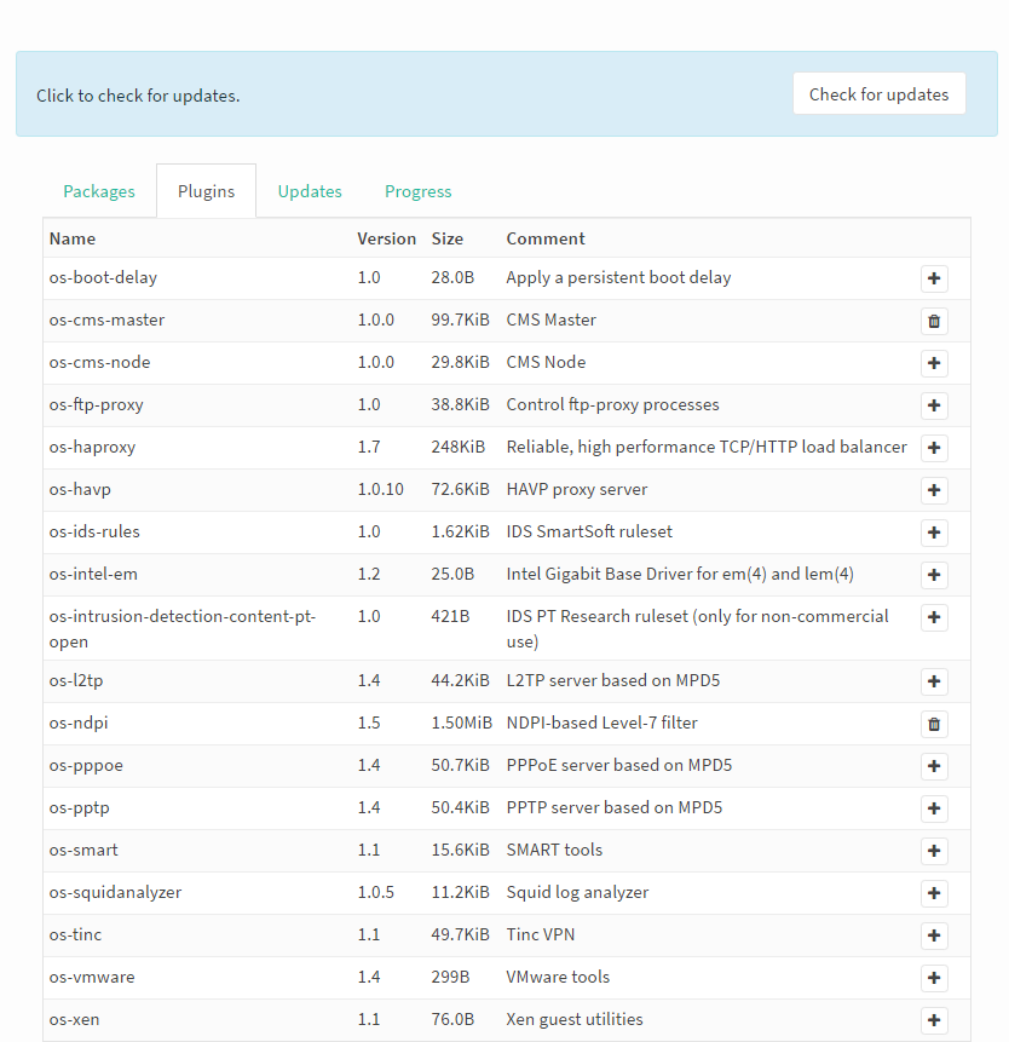
4. Настройка мастер-узла

3.1. Установка сертификата для доступа к репозиторию

Установите приобретенный лицензионный сертификат. В разделе Сводка –> Сертификат укажите файл сертификата и файл ключа.

3.2. Установка плагина os-cms-master

Пройдите в раздел Система -> Прошивка -> Обновления, и нажмите Проверить наличие обновлений. Нажмите на иконку + напротив плагина os-cms-master для его установки.



Name	Version	Size	Comment
os-boot-delay	1.0	28.0B	Apply a persistent boot delay
os-cms-master	1.0.0	99.7KiB	CMS Master
os-cms-node	1.0.0	29.8KiB	CMS Node
os-ftp-proxy	1.0	38.8KiB	Control ftp-proxy processes
os-haproxy	1.7	248KiB	Reliable, high performance TCP/HTTP load balancer
os-havp	1.0.10	72.6KiB	HAVP proxy server
os-ids-rules	1.0	1.62KiB	IDS SmartSoft ruleset
os-intel-em	1.2	25.0B	Intel Gigabit Base Driver for em(4) and lem(4)
os-intrusion-detection-content-pt-open	1.0	421B	IDS PT Research ruleset (only for non-commercial use)
os-l2tp	1.4	44.2KiB	L2TP server based on MPD5
os-ndpi	1.5	1.50MiB	NDPI-based Level-7 filter
os-pppoe	1.4	50.7KiB	PPPoE server based on MPD5
os-pptp	1.4	50.4KiB	PPTP server based on MPD5
os-smart	1.1	15.6KiB	SMART tools
os-squidanalyzer	1.0.5	11.2KiB	Squid log analyzer
os-tinc	1.1	49.7KiB	Tinc VPN
os-vmware	1.4	299B	VMware tools
os-xen	1.1	76.0B	Xen guest utilities

Примечание.

Для успешной установки плагина в вашем устройстве должен быть установлен лицензионный сертификат.

3.3. Создание служебного пользователя для инфраструктуры

Пройдите в раздел CMS -> Nodes и осуществите настройку параметров подчиненного нода. Нажмите на кнопку Set CMS Admin account.

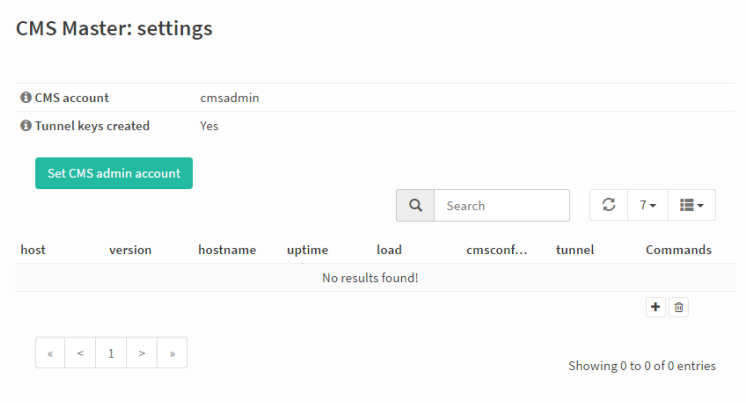
Это служебный пользователь, который будет присутствовать на всех узлах в инфраструктуре. Под этим пользователем мастер логинится на подчиненные узлы и управляет ими. Служебный пользователь *не должен* совпадать с локальными пользователями, существующими на мастер-узле.

3.4. Создание ключей для туннеля

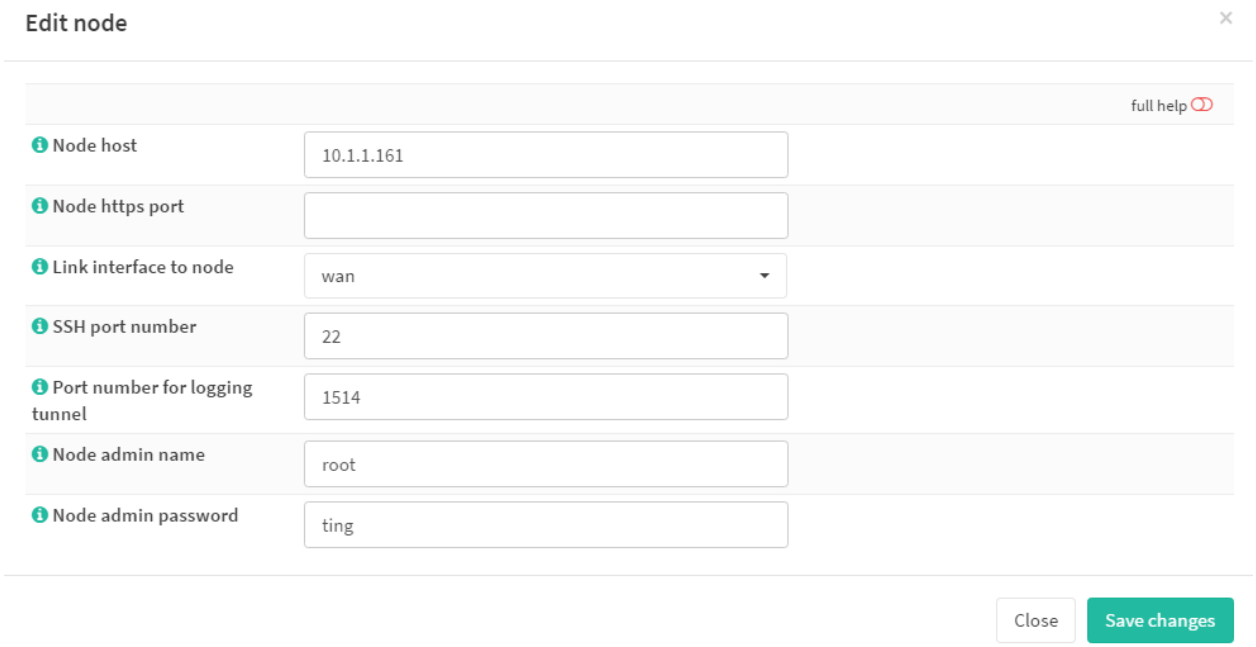
Нажмите на кнопку Create tunnel keys. Произойдет генерация SSH-ключей для туннеля.

3.5. Добавление подчиненных узлов на мастер-узле

Произведите добавление подчиненных узлов на мастер-узле. Для этого, кликните на значок +.



В окне добавления подчиненного узла, нужно задать ряд настроек:



Поле Node host. В данном поле указывается IP-адрес или DNS-имя подчиненного узла.

Поле Node https port. В данном поле указывается номер HTTPS-порта, который слушает веб-сервер на подчиненном узле. По HTTPS-каналу осуществляется работа с веб-интерфейсом подчиненного узла, и передаются команды на подчиненный узел. Соединение по HTTPS открывается только тогда, когда в web-интерфейсе на мастере нажимается какая-либо кнопка, связанная с получением или передачей информации на подчиненный узел. После передачи соединение сразу же закрывается.

Поле Link interface to node. В данном поле указывается через какой интерфейс мастер-узел будет подключаться к подчиненному узлу.

Поле SSH port number. В данном поле указывается номер SSH-порта, который слушает служба sshd на подчиненном узле. По SSH-каналу туннелируются сообщения от syslog службы подчиненного узла. Соединение по SSH постоянно находится в установленном состоянии.

Поле Port number for logging tunnel. В данном поле указывается номер порта, который будет использован для туннелирования syslog-сообщений.

Поле Node admin name. В данном поле указывается имя пользователя-администратора, существующего на подчиненном устройстве.

Поле Node admin password. В данном поле указывается пароль пользователя-администратора, существующего на подчиненном устройстве.

Примечание. В процессе настроек на мастер-узле, мы дважды задавали имя пользователя и пароль: (1) в общих настройках мастер-узла и (2) в настройках каждого добавляемого подчиненного узла. Данные учетные записи используются следующим образом.

(1) Учетная запись в общих настройках мастер-узла

Здесь настраивается служебный пользователь, необходимый для функционирования CMS. Служебный пользователь будет создан на всех узлах, добавленных в инфраструктуру. Служебный пользователь *не должен* совпадать с локальными пользователями, существующими на мастер-узле.

Служебный пользователь появляется на подчиненном узле при нажатии на кнопку "Сохранить изменения" в диалоговом окне добавления подчиненного узла (см. ниже). Если в этот момент подчиненный узел был недоступен, то нужно будет удалить созданный подчиненный узел и повторить его добавление заново.

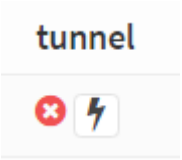
(2) Учетная запись в настройках добавляемого подчиненного узла

Здесь указывается логин / пароль пользователя-администратора на подчиненном узле. Мастер-узел использует данный логин / пароль однократно, для того, чтобы создать на подчиненном узле служебного пользователя.

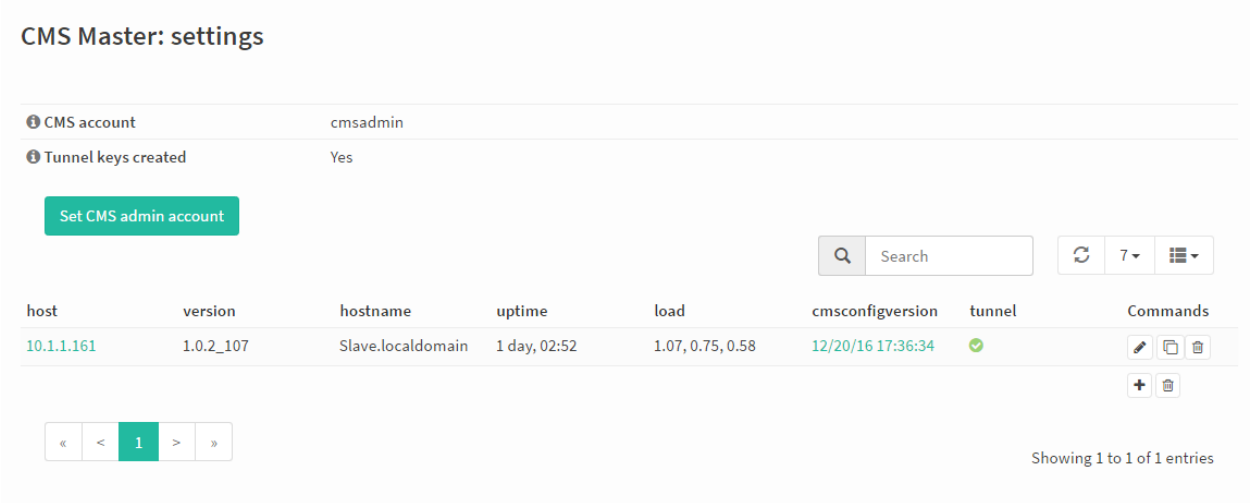
3.6. Установка SSH-туннеля между мастер-узлом и подчиненным узлом

В результате удачного добавления подчиненного узла, он будет отображен в интерфейсе со статусом online.

После добавления подчиненного узла, нужно установить туннель между мастер-узлом и подчиненным узлом. Для этого, в разделе CMS -> Nodes нужно выбрать запись, соответствующую нужному подчиненному узлу, и нажать на иконку в виде молнии в колонке tunnel.

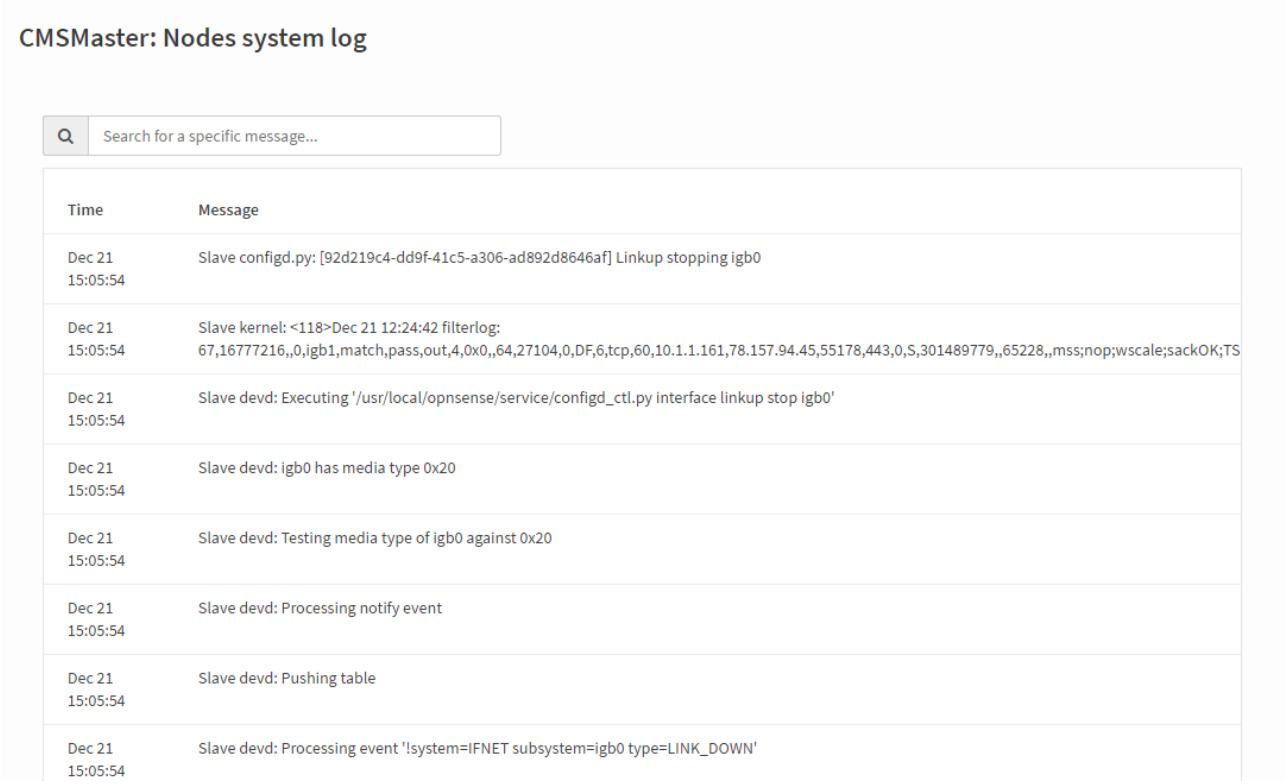


После успешной установки туннеля в колонке tunnel должен отобразится зеленый чекбокс.



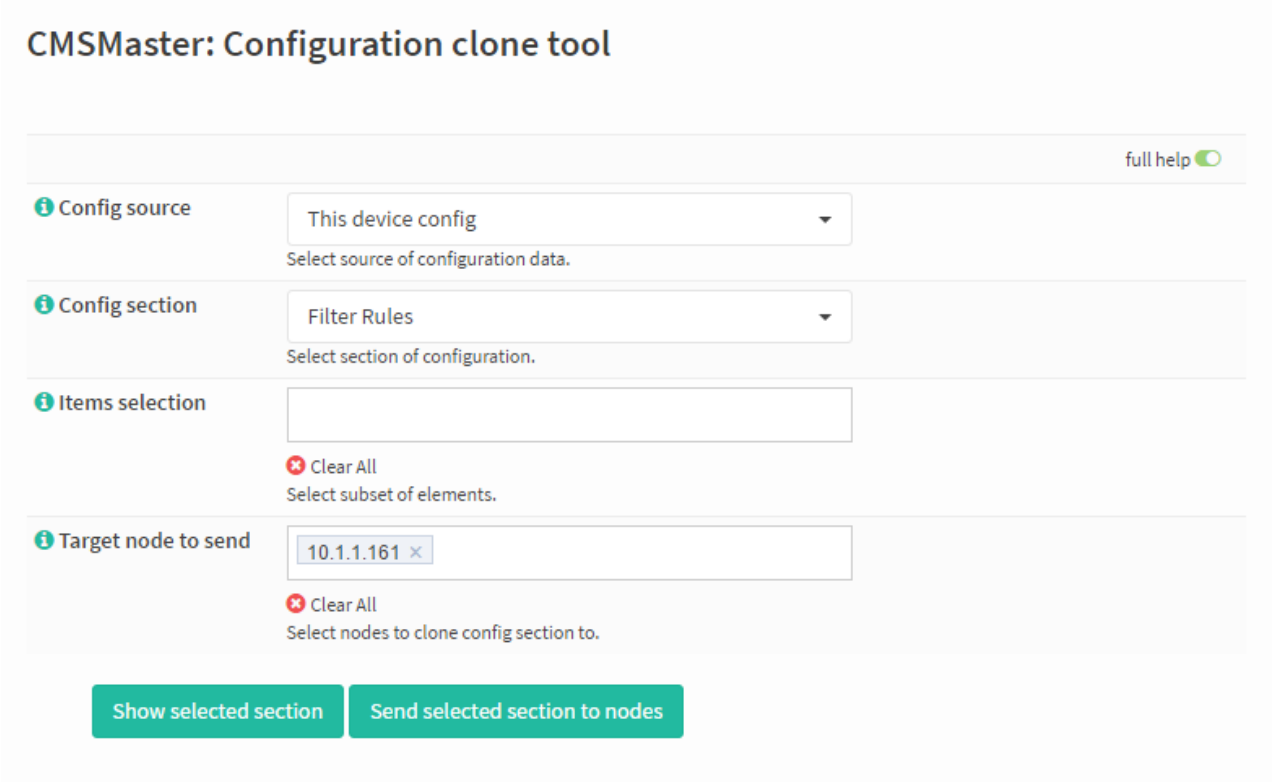
3.7. Просмотр логов с подчиненного устройства

После установки SSH-туннеля между мастер-узлом и подчиненным узлом, с последнего на первый начинают приходить syslog-сообщения, которые можно просматривать в разделе CMS -> Logs.



3.8. Передача настроек на подчиненные узлы

Из раздела CMS -> Config cloner можно осуществлять передачу настроек от мастер-узла подчиненным узлам. Для передачи, нужно определить следующие настройки:



Поле Config source. В данном поле указывает узел-источник настроек.

Поле Config section. В данном поле указывается секция конфигурационного файла, подлежащая передаче.

Поле Items selection. В данном поле можно выбрать отдельные элементы из секции конфигурационного файла.

Поле Target node to send. В данном поле указывается узел-получатель настроек (подчиненный узел).

Кнопка Show selected section. Данная кнопка позволяет просмотреть выбранную секцию конфигурационного файла в текстовом виде.

Кнопка Send selected section to nodes. Данная кнопка инициирует отправку настроек на узел-получатель.

3.9. Просмотр сертификатов

В разделе CMS -> Certificates можно увидеть сводную таблицу сертификатов с подчиненных узлов. Отображаются основные сертификаты и сертификаты на все модули.

3.10. Установка плагинов

В разделе CMS -> Plugins можно осуществить удаленную установку плагинов на подчиненном узле. Для этого нужно установить чекбокс на пересечении идентификатора нужного подчиненного узла и имени нужного плагина.

3.11. Установка обновлений

В разделе CMS -> Updates можно осуществить удаленную установку обновлений на подчиненном узле. Для того, чтобы инициировать обновление на подчиненном узле, нужно нажать на кнопку в колонке update.