Business Ecosystems

Руководство по установке

Console Management System

BE CMS Manager 4.6

Business Ecosystems
Март 2020

Аннотация

Руководство по установке BE CMS Manager содержит описание шагов по развертыванию системы

Введение

Содержит общую информацию о системе и ее основных функциях.

Эксплуатационные требования

Содержит перечень требований для установки Системы, а также описывает необходимые компетенции администратора развертывания Системы.

Архитектура системы

Содержит описание архитектуры Системы и краткое описание составных элементов.

Установка системы

Описывает шаги по развертыванию Системы.

Обслуживание системы

Содержит пароли доступа по умолчанию, а также процедуры резервного копирования, восстановления и обновления Системы.

Приложения

Содержит лицензионное соглашение и контакты службы технической поддержки Business Ecosystems.

История изменений

В **Таблице 1** представлена история изменений в документе. В первом столбе указана дата изменений, а во втором столбце описание изменений.

Таблица 1. История изменений в настоящем документе.

Дата изменения	Описание изменения
20 сентября 2015 г.	Создан настоящий документ.
10 января 2017 г.	Обновление документа в связи с выходом BE CMS Manager 3.0.
13 сентября 2017 г.	Обновлен раздел развертывания системы в связи с выходом BE CMS Manager 4.1.
05 февраля 2018 г.	Обновлен раздел развертывания системы в связи с выходом BE CMS Manager 4.2.
9 июня 2018 г.	Обновлен раздел развертывания системы в связи с выходом BE CMS Manager 4.4.
12 октября 2019 г.	Обновлен раздел развертывания системы в связи с выходом BE CMS Manager 4.5.
5 января 2020 г.	Обновление документа в связи с выходом BE CMS Manager 4.6.
15 марта 2020 г.	Исправление неточностей в документе.

Примечание

Использование специальных обозначений

Данное руководство содержит различные специальные обозначения.

> Текст, содержащийся в рамке серого цвета, означает дополнительную справочную информацию или ссылки на внешние источники.

Жирный текст обозначает название компонентов Системы, а также кнопки или пункты меню.
Курсивный текст обозначает команды, которые вводиться в режиме командной строки.

> Текст, содержащийся в рамке красного цвета, означает важную информацию или предупреждения о возникновении возможных проблем.

Содержание

Введение

Данный раздел содержит общую информацию о системе и основных функциях

Обзор системы

Business Ecosystems Console Management System (далее Becsys) является инструментом удаленного подключения к компьютерам, расположенными как в корпоративной сети так и за ее пределами. Becsys может быть использован для оказания технической поддержки пользователей и для удаленной работы сотрудников.

Целями внедрения Becsys являются повышение эффективности техподдержки, снижение рисков информационной безопасности и повышение доступности информационных ресурсов.

В состав системы входят следующие компоненты:

- **BE CMS Endpoint Client** (далее клиент Becsys) позволяет подключаться к рабочим станциям под управлением ОС Windows и выполнять администрирование в фоновом режиме через удаленную командную строку, удаленный реестр, диспетчер задач и менеджер файлов.
- **BE CMS Manager** (далее сервер Becsys) позволяет разграничивать доступ, управлять привилегиями администраторов, осуществлять аудит сеансов подключения, выполнять мониторинг доступности и централизованное управление клиентами Becsys.
- **BE CMS VPN** (далее сервер VPN) обеспечивает подключение клиентов Becsys из Интернет с использованием технологии VPN.

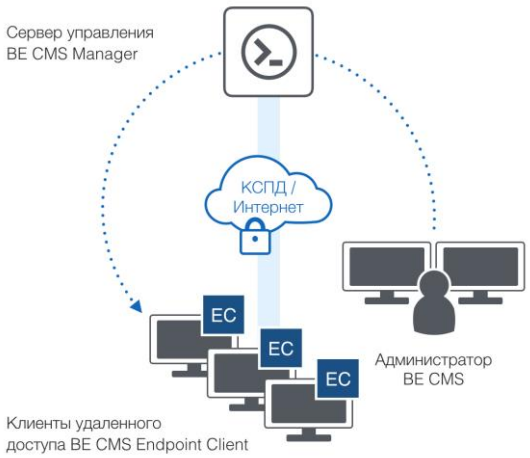

Рисунок 1. Компоненты системы **BE CMS**

Все подключения к рабочим станциям осуществляются только через сервер Becsys, обеспечивая полный контроль над трафиком управления.

Эксплуатационные требования

Данный раздел содержит перечень требований для установки Системы, а также описывает необходимые компетенции администратора для развертывания Системы

Программные требования

Система **BE CMS** поставляется в виде шаблона двух виртуальных машин под платформу VMware (OVF template, гостевая операционная система CentOS 7.2) для развертывания на VMware ESXi 6.0 и выше.

В настройках сетевого адаптера (технологического линка) между BE CMS Manager и BE CMS VPN должен быть разрешен Promiscuous Mode.

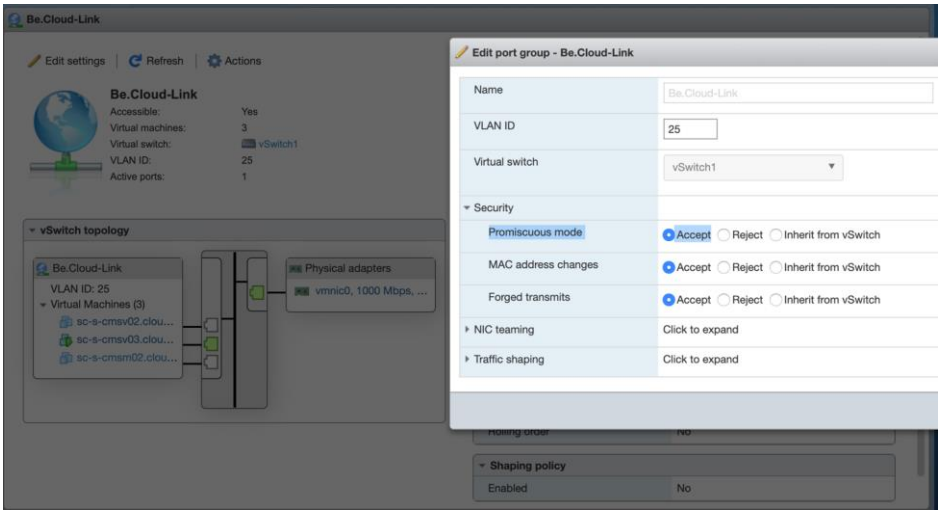

Рисунок 2. Настройки технологического линка между BE CMS Manager и BE CMS VPN

Аппаратные требования

Для эксплуатации системы **BE CMS** рекомендуется установка виртуальных машин на ресурсах:

- BE CMS Manager
  - Процессор Intel Xeon 2.5 ГГц (2 vCPU);
  - 8 ГБ оперативной памяти;
  - 100 ГБ свободного дискового пространства (SSD рекомендуется);
  - 2 сетевых адаптера.
- BE CMS VPN
  - Процессор Intel Xeon 2.5 ГГц (2 vCPU);
  - 8 ГБ оперативной памяти;
  - 32 ГБ свободного дискового пространства;
  - 2 сетевых адаптера.

Требования к сетевому окружению

Подключение из корпоративной сети

Для подключения клиентов Becsys к серверу управления из корпоративной сети необходимо обеспечить сетевой доступ к BE CMS Manager.

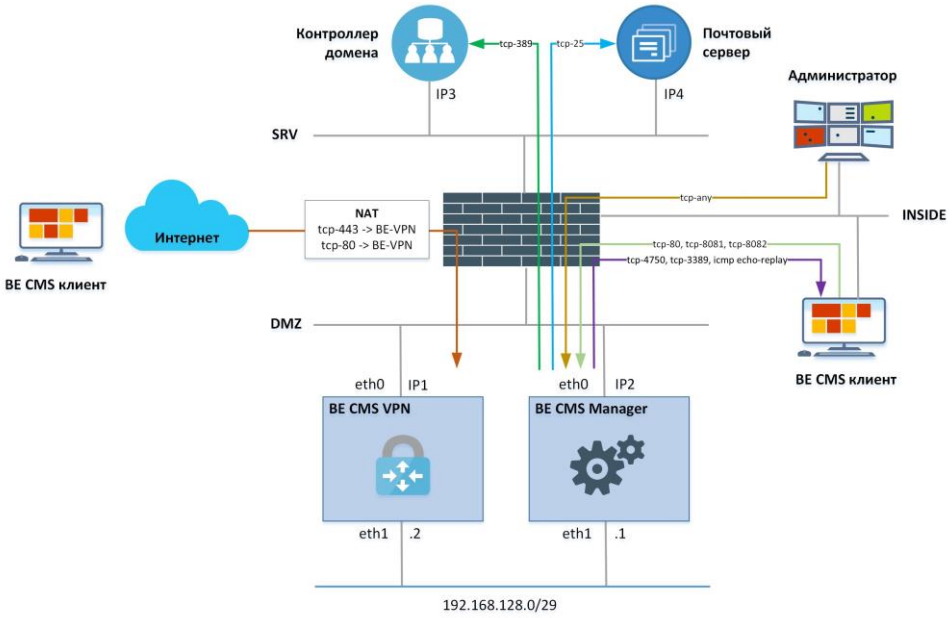

Рисунок 3. Схема взаимодействия компонентов BE CMS

Если на сети между клиентом BE CMS и сервером управления будет обнаружена трансляция сетевых адресов (NAT), то клиент автоматически переключиться к BE CMS VPN. В этом случае необходимо дополнительно обеспечить доступ к VPN серверу по порту tcp-443.

> Подключение администраторов и клиентов BE CMS с использованием HTTP прокси серверов не поддерживается в текущей версии. Для использования протокола L2TP (для WinXP) необходимо дополнительно открыть доступ к VPN серверу по портам udp-500 и udp-4500.

Подключение из Интернет

Для подключения клиента Becsys к серверу управления из Интернет необходимо обеспечить сетевой доступ к BE CMS VPN по указанным на Рисунке 3 правилам NAT.

Требования к администратору

Для успешного внедрения и обслуживания системы **BE CMS** администратору необходимо обладать следующими компетенциями:

- понимать основные принципы построения локальных вычислительных сетей;
- понимать модель ISO OSI и архитектуру стека протоколов TCP/IP;
- иметь начальные навыки работы с операционными системами на базе Linux;
- иметь начальные навыки работы с СУБД Oracle достаточные для понимания шагов в инструкции по обслуживанию базы данных;
- владеть английским языком в объеме достаточным для чтения технической документации и диагностических журналов.

Архитектура системы

Данный раздел содержит описание архитектуры Системы и краткое описание составных элементов

Система управления **BE CMS Manager** состоит из следующих компонентов:

- **База данных** – используется для хранения и обработки информации об объектах системы и выполнения пользовательских отчетов.

  > По умолчанию система **BE CMS** поставляется с СУБД Oracle Database 11g Express Edition Release 11.2.0.2.0 – 64bit. В целях повышения производительности системы и при наличии лицензии Oracle у Заказчика возможно использование Oracle Standard Edition.

- **Модуль управления** – веб-сервис с поддержкой протокола взаимодействия SOAP/XML для регистрации клиентов Becsys в системе.
- **Модуль доступа** – обрабатывает соединения администраторов к рабочим станциям, серверам и другим типам оборудования. Модуль реализует динамические управление листами контроля доступа и журналирование соединений.

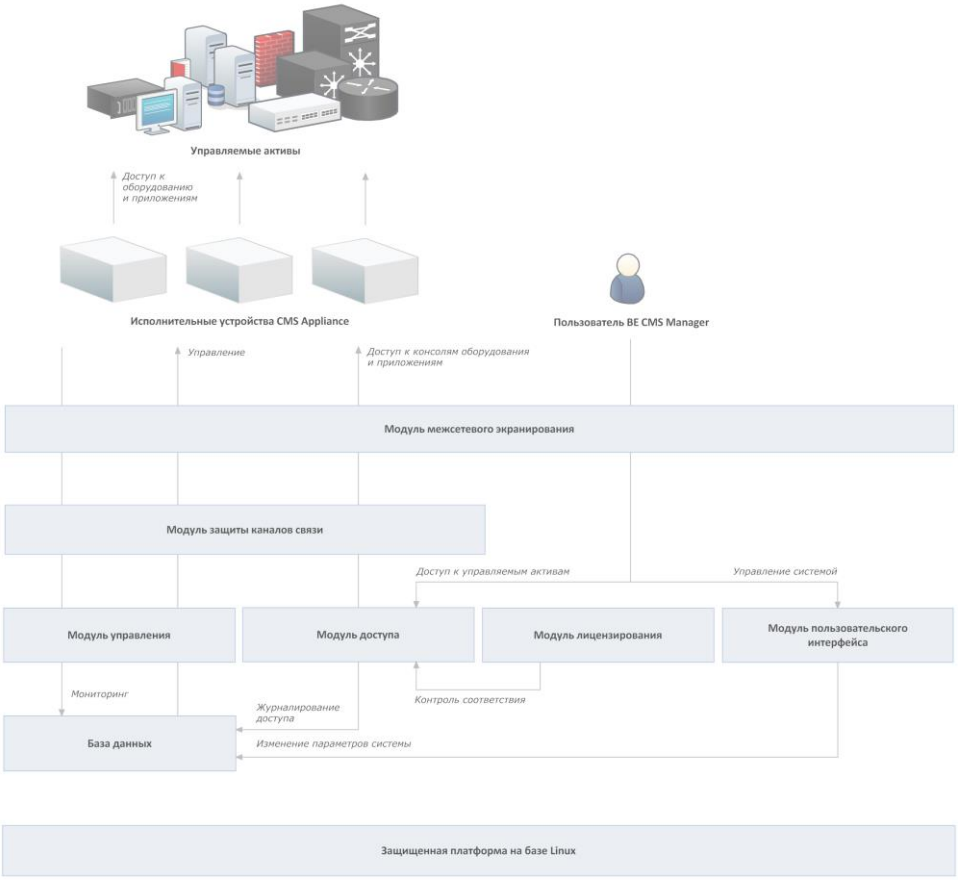

Рисунок 4. Программная архитектура системы **BE CMS**

- **Модуль лицензирования** – контролирует работу модуля доступа и в случае нарушения лицензионной политики останавливает его работу.

- **Модуль интерфейса пользователя** – WEB интерфейс управления системой на базе Oracle APEX. В интерфейсе управления выделяют следующие роли пользователей:
  - **Администратор системного контекста** – управляет системной рабочей областью APEX, в которой создается прикладной контекст **BE CMS Manager**;
  - **Администратор прикладного контекста** – управляет прикладной рабочей областью APEX, где создается и редактируется веб-интерфейс пользователя системы **BE CMS Manager**. Используется для обновления веб-интерфейса пользователя;
  - **Пользовательская учетная запись** – применяется для подключения к веб-интерфейсу **BE CMS Manager** пользователями системы.
- **Модуль межсетевого экранирования** – обеспечивает защиту от атак типа «отказ в обслуживании». Модуль реализован средствами операционной системы;
- **Модуль защищенной связи** – обеспечивает защищенный канал взаимодействия между клиентами BE CMS и сервером BE CMS, реализуется отдельным сервером BE VPN.
- **Защищенная платформа на базе Linux** – предварительно настроенная 64-битная операционная система CentOS 7.2, содержащая необходимый набор служб.

Более детальная информация об архитектуре решения предоставляется по запросу при наличии приобретенного пакета технической поддержки Business Ecosystems.

Развертывание системы

Данный раздел описывает шаги по развертыванию

Импорт шаблонов виртуальных машин

Система **BE CMS** поставляется в виде образов виртуальных машин VMware (OVF Template) и импортируется в существующую виртуальную среду VMware vSphere (или VMware ESXi):

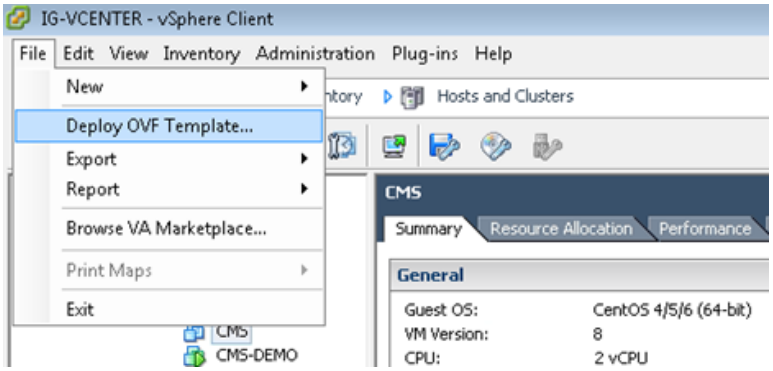

Рисунок 5. Фрагмент интерфейса VMware vSphere

После завершения импорта виртуальной машины, необходимо обновить информацию в конфигурационных файлах операционной системы, т.к. при импорте генерируется новый MAC адрес для интерфейсов **eth0** и **eth1**.

> Для подключения по SSH к BE CMS Manager необходимо воспользоваться учетной записью Администратора ОС. Логин/пароль указан в разделе «Обслуживание системы».

Настройка сетевых параметров

Для изменения IP адреса необходимо подключиться к системе с помощью доступного SSH клиента (например, putty), используя учетную запись администратора ОС и выполнить следующие действия (или используя интерфейс гипервизора):

1) Записать MAC-адреса интерфейсов ens32 и ens33 из вывода команды *ifconfig -a.*
2) Открыть в режиме редактирования файлы **ifcfg-ens32**, **route-eth0** и **ifcfg-ens33**, расположенные в директории **/etc/sysconfig/network-scripts**:
   - заменить текущий MAC адрес на адрес из вывода команды *ifconfig -a;*
   - Установить корректные сетевые настройки.

> Подробная инструкция по работе с редактором **vi** расположена по адресу http://www.washington.edu/computing/unix/vi.html.

```
[root@CMS ~]# vi /etc/sysconfig/network-scripts/ifcfg-ens32
HWADDR=[MAC]
IPADDR=[BE CMS IP]
PREFIX=[24]
GATEWAY=[GW]
```

```
DNS1=8.8.8.8
DEVICE=eth0
```

- Настройка маршрута для подключения к BE CMS администраторов из Интернет (опционально).

```
[root@CMS ~]# vi /etc/sysconfig/network-scripts/route-eth0
ADDRESS0=172.19.40.0
NETMASK0=255.255.255.0
GATEWAY0=[BE VPN IP + 1]
```

- Настройка технологического линка (при наличии клиентов за пределами корп. сети)

```
[root@CMS ~]# vi /etc/sysconfig/network-scripts/ifcfg-ens33
HWADDR=[MAC]
IPADDR=192.168.128.1
PREFIX=29
DEVICE=eth1
```

3) Выполнить перезагрузку системы командой *reboot*.

После перезагрузки системы необходимо проверить наличие интерфейсов **eth0** и **eth1** в выводе *ifconfig.*

Изменение имени хоста

Необходимо изменить имя сервера в соответствии с корпоративным стандартом.

```
[root@sc-s-cmsm01 ~]# vi /etc/hostname
sc-s-cmsm01.demo.becsys.ru
```

Необходимо изменить сопоставление службы **webservice**, которая отвечает за работу модуля управления, за IP адресом **eth0** в файле **/etc/hosts**, с помощью команды *vi /etc/hosts*

```
[root@sc-s-cmsm01 ~]# vi /etc/hosts
[CMS IP]  webservice
127.0.0.1   sc-s-cmsm01
127.0.0.1   sc-s-cmsm01.demo.becsys.ru
```

Необходимо изменить IP адрес и имя хоста в файлах параметров СУБД Oracle XE и сервера приложений **listener.ora**, **tnsnames.ora** и **catalina.properties**.

```
[root@ sc-s-cmsm01 ~]# vi /u01/app/oracle/product/11.2.0/xe/network/admin/listener.ora
    (ADDRESS = (PROTOCOL = TCP)(HOST = sc-s-cmsm01.demo.becsys.ru)(PORT = 1521))
[root@sc-s-cmsm01 ~]# vi /u01/app/oracle/product/11.2.0/xe/network/admin/tnsnames.ora | grep HOST
   (ADDRESS = (PROTOCOL = TCP)(HOST = sc-s-cmsm01.demo.becsys.ru)(PORT = 1521))
[root@sc-s-cmsm01 ~]# vi /u01/app/oracle/tomcat/conf/catalina.properties
spring.datasource.url=jdbc:oracle:thin:@[CMS IP]:1521/xe
swagger.host=[CMS IP]

[root@ sc-s-cmsm01 ~]# vi /etc/raddb/mods-enabled/sql | grep radius_db

radius_db = "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=sc-s-
cmsm01.demo.becsys.ru)(PORT=1521))(CONNECT_DATA=(SID=XE)))"
```

Настройка WEB сервера и Lsyncd

Для смены IP адреса WEB сервера **nginx** (при изменении сетевых настроек) необходимо изменить файл **/etc/nginx/conf.d/default.conf** с помощью команды *vi /etc/nginx/conf.d/default.conf*

```
[root@CMS ~]# vi /etc/nginx/conf.d/default.conf
```

```
server_name [CMS IP];

[root@CMS ~]# vi /etc/nginx/conf.d/ssl.conf
server_name  [CMS IP]  default_server;
```

Необходимо изменить IP адрес на [CMS IP] в файлах **title_en.js** и **title.js**, расположенных в директории /u01/app/oracle/tomcat/webapps/i/cms_ut/js/ и в файлах **title.js.tmpl** и **title_en.js.tmpl**, расположенных в директории /etc/proxyd/templates/.

Необходимо указать IP адрес VPN сервера в настройках **lsynd** и **authorized_keys**

```
[root@CMS ~]# vi /etc/lsyncd.conf
settings{logfile='/var/log/lsyncd/lsyncd.log', insist=true,}
sync{default.rsync, source="/usr/share/nginx/html", target="/opt/ramdrive",}
sync{default.rsyncssh, source="/usr/share/nginx/html", targetdir="/opt/ramdrive", host="[VPN IP]", delay=1}

[root@CMS ~]# vi /root/.ssh/authorized_keys
from="[VPN IP]" ssh-rsa AAAAB3NzaC…..
```

Выполнить перезагрузку системы командой reboot.

Установка SSL-сертификата

Для установки корпоративного SSL-сертификата необходимо:

1. Создать запрос на получение сертификата (в поле Common Name указать URL, по которому будет доступен BE CMS Manager).
   openssl req -new -newkey rsa:2048 -nodes -keyout private.key -out request.csr
2. При получении сертификата в формате DER (*.cer) его необходимо конвертировать в PEM (*.crt) https://www.sslshopper.com/ssl-converter.html
3. При использовании цепочки центров сертификации необходимо добавить их к *.crt файлу
   cat public.crt ca-keychain.crt > certificate.crt
4. Скопировать файлы открытого и закрытого ключей в директории /etc/ssl/certs/ и /etc/pki/tls/private/
5. Отредактировать содержимое файла /etc/nginx/conf.d/ssl.conf и перезапустить сервис *nginx*
   ssl_certificate /etc/ssl/certs/certificate.crt;
   ssl_certificate_key /etc/pki/tls/private/private.key;

> Сервер **BE CMS Manager** может эксплуатироваться с использованием самоподписанного SSL-сертификата. В этом случае при первом подключении на компьютере пользователя необходимо добавить этот сертификат в список доверенных.

Настройка отправки Pin-кодов

Pin-коды отправляются по email. Для отправки писем необходимо прописать адрес почтового сервера и учетные сведения для SMTP подключения.

```
root@sc-s-cmsm01 ~]# vi /u01/app/oracle/tomcat/conf/catalina.properties
#email
spring.mail.host=[smtp server hostname or IP address]
spring.mail.port=[smtp port]
spring.mail.username=[email]
spring.mail.password=[password]
```

Подключение к консоли

Подключиться к консоли **BE CMS Manager** можно двумя способами:

1. К консоли системы через протокол Secure Shell (SSH).
2. К веб-интерфейсу системы по адресу **http://<IP-address>**. При первом подключении необходимо довериться установленному на системе самоподписанному сертификату, затем ввести учетные данные в приветственной форме.

Для подключения к WEB интерфейсу BE CMS Manager необходима учетная запись Администратора BE CMS Manager. Логин/пароль указан в разделе «Обслуживание системы».

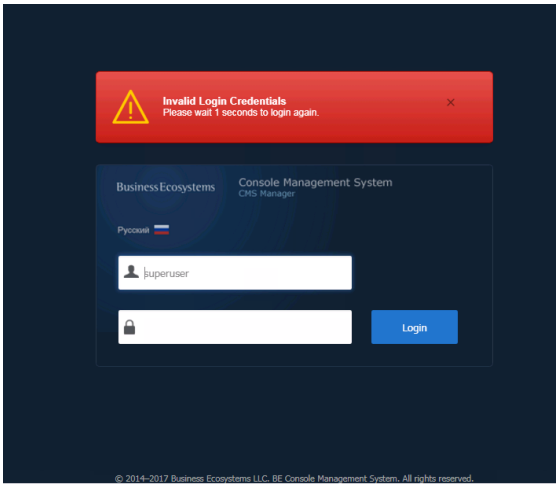

Рисунок 6. Форма ввода учетных сведений

В случае ввода неверных учетных сведений появится предупреждающее всплывающее окно.

Для выхода из системы необходимо нажать кнопку **Exit**, расположенную в правом верхнем углу страницы в подменю логина.

Управление лицензиями

Запрос лицензионного ключа

Перед началом эксплуатации системы **BE CMS** необходимо создать файл лицензионного запроса и передать его Business Ecosystems. Для скачивания файла запроса лицензионного ключа подключитесь к **BE CMS Manager** и скачайте его с помощью любого SCP-клиента (например, WinSCP).

```
[root@CMS ~]# request
Writing LRQ file...
[root@CMS ~]# ls -lah | grep lic
-rw-r--r--   1 root root  257 Jan 16 15:20 license.lrq
```

Рисунок 7. Процесс создания файла запроса лицензионного ключа

Файл запроса содержит информацию о параметрах операционной системы и об аппаратных компонентах серверного оборудования, на котором работает Система **BE CMS Manager**. При смене аппаратной платформы или изменении настроек операционной системы необходимо повторно создать запрос на получение лицензионного ключа.

Установка лицензионного ключа

Необходимо загрузить полученные от правообладателя файлы лицензионного ответа **license.lrs** и **device.lrs** через интерфейс BE CMS Manager, перейдя на вкладку **Licensing** раздела **System**.

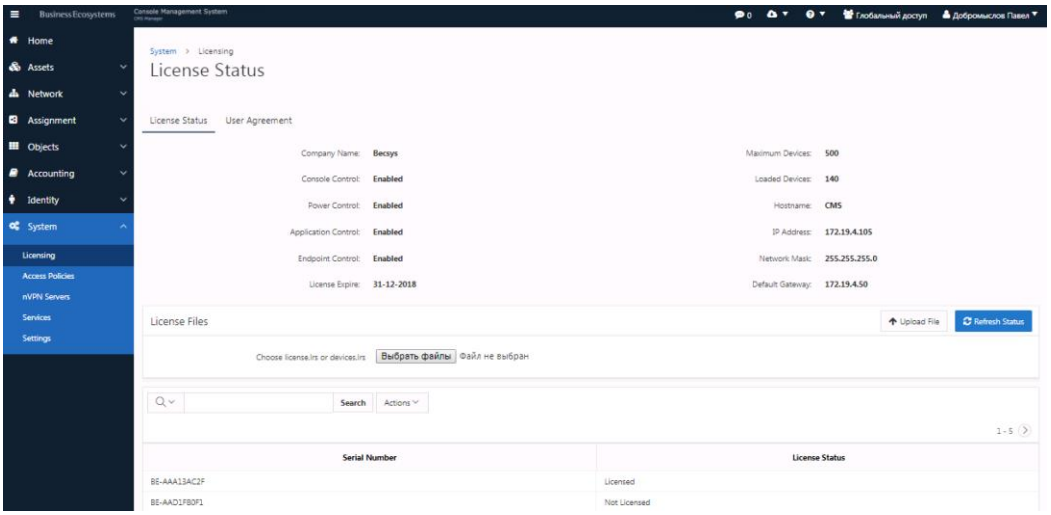

Рисунок 8. Загрузка лицензионного ключа

> Файл **device.lrs** содержит список серийных номеров Endpoint Client, приобретенных Заказчиком. Использование компьютеров, серийные номера которых не содержатся в файле **device.lrs** запрещено лицензионным соглашением.

После загрузки файлов необходимо выполнить запуск сервиса проксирования.

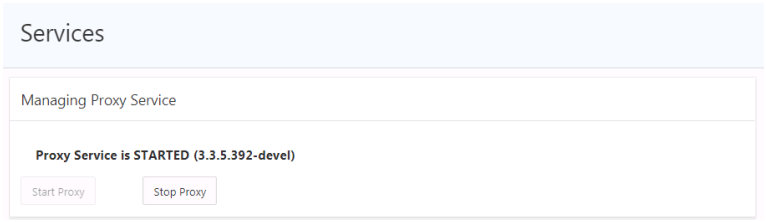

Рисунок 9. Запуск сервиса проксирования

> Выполните перезагрузку сервера BE CMS Manager если Proxy сервис не стартует.

Проверка лицензионного ключа

Для просмотра лицензионной информации необходимо в интерфейсе **BE CMS Manager** перейти на вкладку **Licensing** раздела **System**:

На вкладе **Licensing** можно получить следующую информацию:

- Сетевые настройки системы.
- Максимальное количество поддерживаемых системой устройств.
- Лицензированные функции (такие как **Endpoint Control** или **Application Control**).
- Срок действия лицензионного ключа.
- Список серийных номеров разрешенных устройств.
- Список нелицензированных серийных номеров устройств, но подключенных к системе.

Управление системными параметрами

Администратор **BE CMS Manager** обладает полномочиями на изменение системных параметров. Интерфейс управления системными параметрами расположен на вкладке **System -> Settings** (должны быть заполнены все параметры).

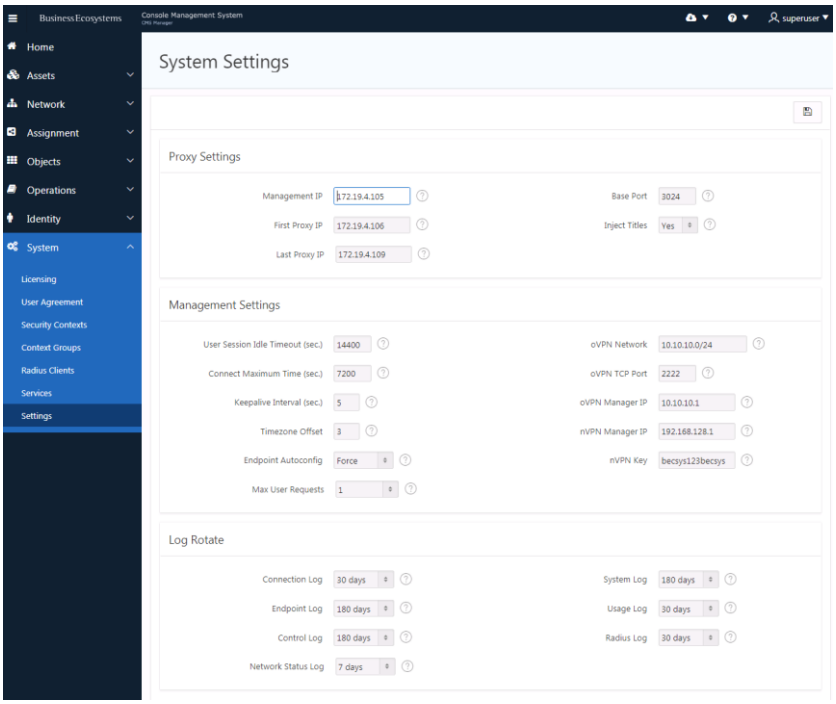

Рисунок 10. Системные параметры BE CMS Manager

Таблица 2. Настройки проксирования BE CMS Manager

Параметр	Описание
Management IP	IP адрес для подключения к BE CMS Manager, также используется как адрес источника RADIUS запросов.
First Proxy IP	Первый IP адрес диапазона, который будет использоваться для подстановки в ссылки подключений к Активам. На одном IP адресе поддерживается до 600 BE CMS Endpoint Client.
Last Proxy IP	Последний IP адрес диапазона, который будет использоваться для подстановки в ссылки подключений к Активам. Данный параметр может быть равен значению параметра First Proxy IP. Суммарное количество клиентов не должно превышать количество доступных слотов в системе, которые рассчитываются по формуле: **Кол-во слотов = (LastProxyIP – FirstProxyIP) x 600**
Base Port	Первый TCP порт для использования сервисом проксирования. Используются в формулах расчета сдвига порта для подключения к Активам при использовании одного адреса проксирования (для инсталляций до 500 клиентов).
Inject Titles [Yes | No]	Вставлять или нет подписи окна для подключения к telnet-приложениям и rs-232 устройствам (функция Console Control).
Outbound IP (выбирается автоматически)	IP адрес исходящих прокси соединений в зависимости от типа клиента: • Management IP для LanMode клиентов; • nVPN Manager IP для VPN клиентов.
Online Per Server	Максимальное количество подключенных Endpoint клиентов, которые может обслуживать сервер (kamgr).

Таблица 3. Системные настройки BE CMS Manager

Параметр	Описание
User Session Idle Timeout (sec.)	Максимальное время сессии пользователя в консоли BE CMS Manager. При достижении указанного порога происходит устаревание сессии.
Connect Maximum Time (sec.)	Максимальное время подключения BE CMS Endpoint Client к BE CMS Manager в режиме «По запросу». По достижении указанного порога происходит отправка запроса на отключение BE CMS Endpoint Client от системы.
Keepalive Interval (sec.)	Интервал отправки keepalive сообщений клиентами. При отсутствии keepalive сообщений в течение 3-х интервалов клиенты помечаются как неактивные.
Timezone Offset	Сдвиг часового пояса относительно UTC в журналах системы.
Endpoint Autoconfig [Enabled | Disabled | Force]	Включение опции автоматического создания Endpoint клиентов на основании настройки контекста безопасности. Значение Force разрешает заведение Endpoint клиентов с повторяющимися именами (к дубликату добавляется суффикс «_»).
oVPN Network	IP подсеть, которая используется для построения сети управления для oVPN клиентов. Адреса из данной подсети выдаются BE CMS Endpoint Client при подключении. **Параметр не используется для клиентов версии 3.5 и выше.**
oVPN TCP Port	TCP порт, который используются для построения oVPN туннеля. **Параметр не используется для клиентов версии 3.5 и выше.**
oVPN Manager IP	IP адрес интерфейса Менеджера для oVPN клиентов.
nVPN Manager IP	IP адрес интерфейса Менеджера для nVPN клиентов.
nVPN Key	Общий ключ для аутентификации по протоколу L2TP (для WinXP).
nVPN CA Cert SN	Серийный номер корневого сертификата удостоверяющего центра.
nVPN CA Cert MD5	Хэш сумма сертификата удостоверяющего центра.
Requests Per User	Максимальное количество Endpoint клиентов, которые может вызвать на связь пользователь с ролью Helpdesk.
Requests Per Server	Максимальное количество Endpoint клиентов, которые могут быть вызваны на сервере.
Users Per Server	Максимальное количество одновременных пользователей с ролью Helpdesk, которые могут работать в системе.

Указывается срок устаревания записей журнала. Все записи, старше указанного значения, удаляются.

Таблица 4. Настройки ротации журналов BE CMS Manager

Параметр	Описание
Connections [Disabled | 7 Days … 365 Days]	Содержит информацию о всех попытках подключения в системе.
Endpoint Actions [Disabled | 7 Days … 365 Days]	Содержит информацию об использовании RMC утилит, о файловых операциях, повышении привилегий и др.
Network [Disabled | 7 Days … 365 Days]	Содержит информацию о времени подключения и отключения клиентов.
Operations [Disabled | 7 Days … 365 Days]	Содержит информацию о действиях пользователя в системе, например о событиях входа/выхода и вызова клиента на связь.
System Objects [Disabled | 7 Days … 365 Days]	Содержит информацию о действиях администратора в системе, о редактируемых им объектах.

nVPN [Disabled | 7 Days … 365 Days]	Содержит информацию о длительности подключений nVPN клиентов (информация с nVPN сервера через Radius Accounting).
Usage [Disabled | 7 Days … 365 Days]	Содержит информацию о метриках использования системы. Данные журнала используются для построения графиков.

Администратор **BE CMS Manager** обладает полномочиями на изменение параметров аутентификации пользователей в системе на вкладке **Identity -> Authentication**.

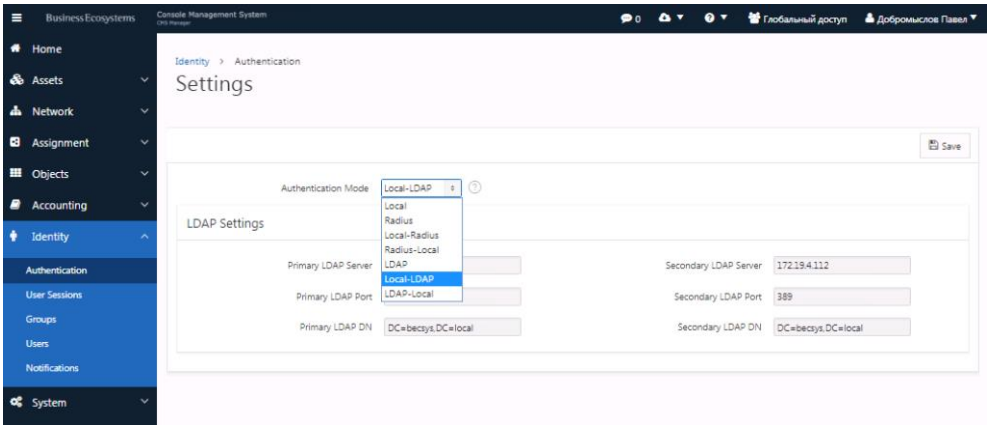

Рисунок 11. Параметры аутентификации BE CMS Manager

Таблица 5. Настройки аутентификации BE CMS Manager

Параметр	**Описание**
Authentication Mode	Режим аутентификации пользователей BE CMS Manager: ▪ Local – аутентифицировать пользователей только с помощью локальных учетных записей BE CMS Manager. ▪ Radius – аутентифицировать пользователей только через Radius протокол. ▪ Local-Radius – аутентифицировать пользователей с помощью локальных учетных записей BE CMS Manager, а в случае отсутствия соответствующей записи использовать Radius протокол. ▪ Radius-Local – аутентифицировать пользователей через Radius протокол, а в случае недоступности Radius серверов использовать локальные учетные записи.
Параметры RADIUS	
Primary AAA Server	IP адрес основного Radius сервера.
Primary Server Key	Общий ключ для основного Radius сервера.
Secondary AAA Server	IP адрес резервного Radius сервера. Данный параметр может быть равен значению параметра Primary AAA Server.
Secondary Server Key	Общий ключ для резервного Radius сервера. Данный параметр может быть равен значению параметра Primary Server Key
Radius Timeout (sec.)	Время ожидания ответа на запрос от Radius сервера.
Radius Retries	Количество попыток отправки запросов на Radius сервер.
Radius Deadtime (sec.)	Количество времени, в течение которого Radius сервер, не ответивший на запросы, игнорируется для дальнейших запросов. Radius сервер помечается неактивным после отсутствия ответов на запросы в течение (Radius Retries x Radius Timeout) сек.
Login Timeout (sec.)	Время ожидания ввода логин/пароль в рамках Radius запроса.

Login Tries	Количество попыток ввода логин/пароль перед разрывом сессии.
Параметры LDAP	
Primary LDAP Server	IP адрес основного LDAP сервера.
Primary LDAP Port	TCP порт основного LDAP сервера.
Primary LDAP Distinguished Name	Путь к контейнеру, где содержаться учетные записи пользователей, в формате «DC=becsys,DC=local»
Secondary LDAP Server	IP адрес резервного LDAP сервера. Данный параметр может быть равен значению параметра Primary LDAP Server.
Secondary LDAP Port	TCP порт резервного LDAP сервера.
Secondary LDAP Distinguished Name	Путь к контейнеру, где содержаться учетные записи пользователей, в формате «DC=becsys,DC=local»

Настройка RADIUS сервера

Для настройки RADIUS сервера на базе Windows Server 2008 R2 или старше необходимо:

1) создать группу(ы) безопасности в Active Directory согласно выбранной ролевой модели;
2) поместить необходимые учетные записи в соответствующие группы безопасности;
3) добавить RADIUS клиента на Network Policy Server, указав в качестве IP адреса значение глобального параметра **Management IP** (на вкладке Settings в интерфейсе BE CMS Manager), а в качестве пароля **Secret Key**;

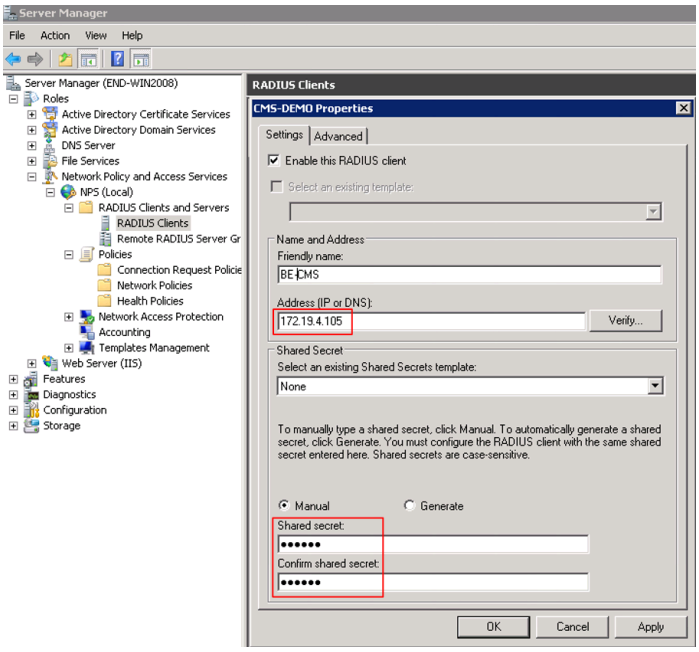

Рисунок 12. Окно добавления RADIUS клиента

4) Создать сетевую политику на Network Policy Server согласно Рис.16-19.
   - на вкладке Overview убедиться, что выбраны опции «Policy Enabled» и «Grant Access»;
   - на вкладке Conditions добавить созданную группу и RADIUS клиента;
   - на вкладке Constraints разрешить использование протоколов аутентификации;
   - на вкладке Settings добавить RADIUS атрибут **«Class = [BE CMS External Group]»**

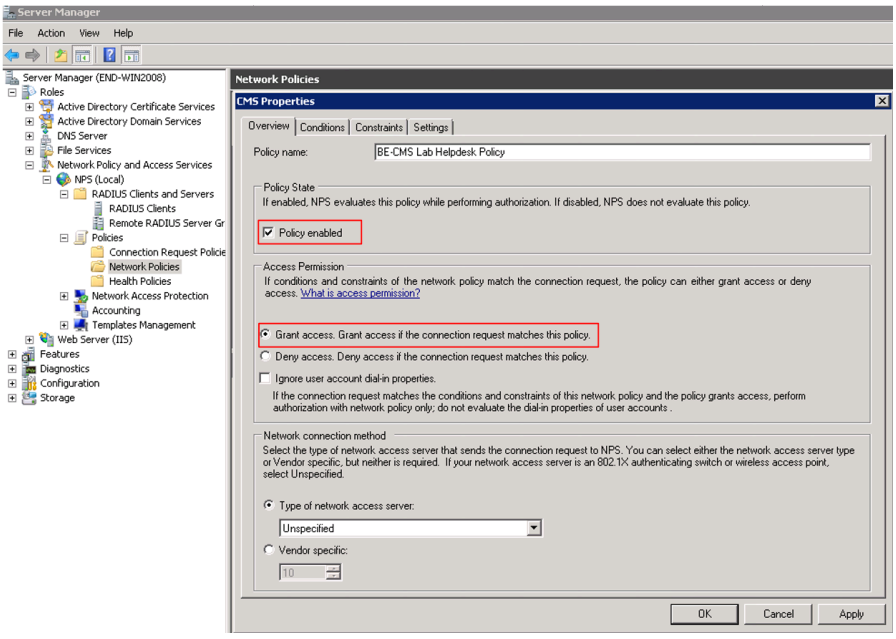

Рисунок 13. Окно создания сетевой политики. Вкладка Обзор

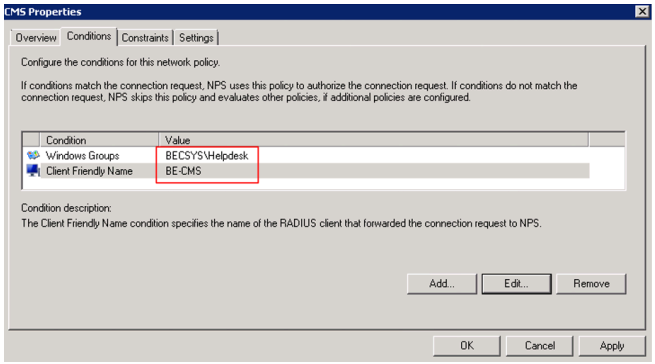

Рисунок 14. Окно создания сетевой политики. Вкладка Условия

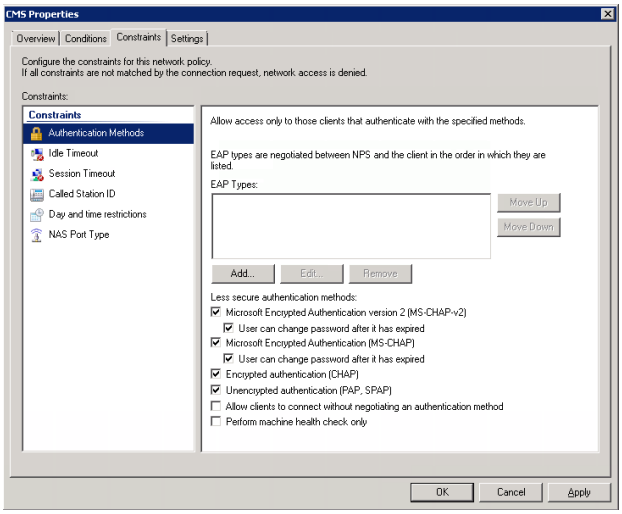

Рисунок 15. Окно создания сетевой политики. Вкладка Ограничения

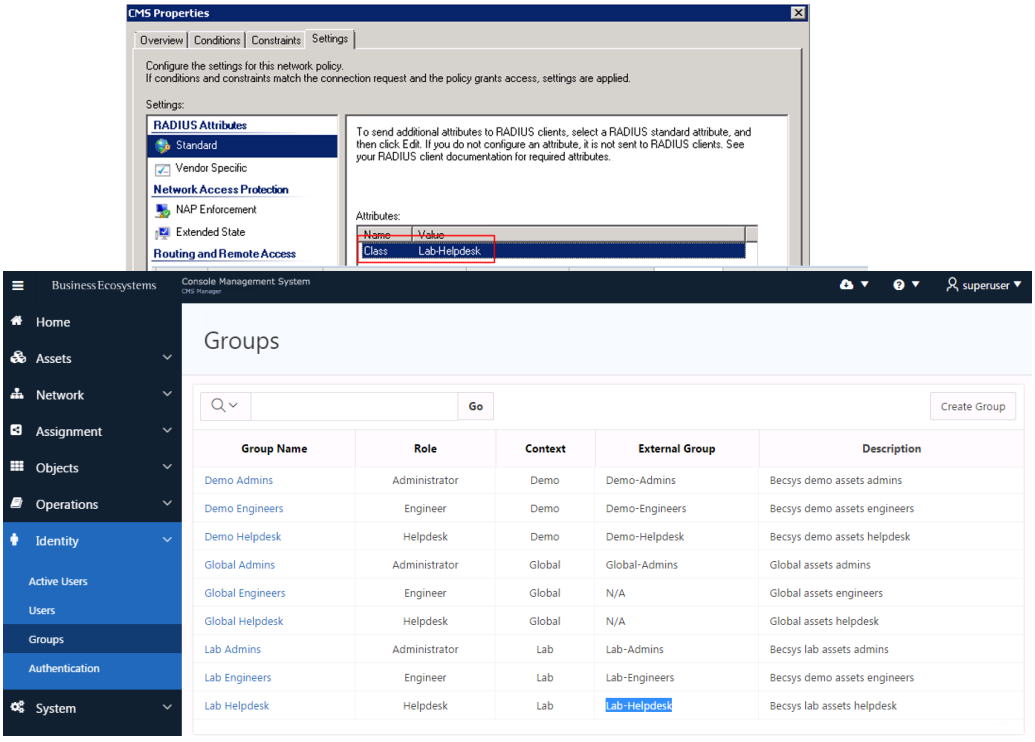

Рисунок 16. Окно создания сетевой политики. Вкладка Настройки

Настройка VPN сервера

Сетевые настройки

Для изменения IP адреса необходимо подключиться к системе с помощью доступного SSH клиента (например, putty), используя учетную запись администратора ОС и выполнить следующие действия (или используя интерфейс гипервизора):

1) Записать MAC-адреса интерфейсов ens32 и ens33 из вывода команды *ifconfig -a.*
2) Открыть в режиме редактирования файлы **ifcfg-ens32**, **route-eth0** и **ifcfg-ens33**, расположенные в директории **/etc/sysconfig/network-scripts**:
   - заменить текущий MAC адрес на адрес из вывода команды *ifconfig -a;*
   - Установить корректные сетевые настройки.

> Подробная инструкция по работе с редактором **vi** расположена по адресу http://www.washington.edu/computing/unix/vi.html.

```
[root@VPN ~]# vi /etc/sysconfig/network-scripts/ifcfg-ens32
HWADDR=[MAC]
IPADDR=[BE VPN IP]
PREFIX=[24]
GATEWAY=[GW]
DNS1=8.8.8.8
DEVICE=eth0
```

   - Настройка технологического линка (при наличии Интернет клиентов BE CMS)

```
[root@VPN ~]# vi /etc/sysconfig/network-scripts/ifcfg-ens33
HWADDR=[MAC]
IPADDR=192.168.128.2
PREFIX=29
DEVICE=eth1
```

3) Выполнить перезагрузку системы командой *reboot*.

После перезагрузки системы необходимо проверить наличие интерфейсов **eth0** и **eth1** в выводе *ifconfig.*

Изменение имени хоста и настройка Web-сервера

Необходимо изменить имя сервера в соответствии с корпоративным стандартом.

```
[root@VPN ~]# vi /etc/hostname
sc-s-cmsv01.demo.becsys.ru
```

Необходимо изменить сопоставление службы **webservice**, которая отвечает за работу модуля управления, за IP адресом **eth0** в файле **/etc/hosts**, с помощью команды *vi /etc/hosts*

```
[root@VPN ~]# vi /etc/hosts
127.0.0.1   sc-s-cmsv01
127.0.0.1   sc-s-cmsv01.demo.becsys.ru
```

Необходимо изменить адрес Web-сервера.

```
[root@VPN ~]# vi /etc/nginx/nginx.conf
   server {
      listen       [VPN IP]:80 default_server;
```

Настройки VPN

Для изменения настройки VPN сервиса необходимо выполнить следующие действия:

1) Необходимо изменить IP адрес в скрипте автостарта сервиса **/etc/rc.local** и **authorized_keys**.

```
[root@VPN ~]# vi /etc/rc.local
/opt/softether/vpncmd/vpncmd [BE VPN IP] /SERVER /PASSWORD:becsys /CMD SyslogEnable 2
/HOST:127.0.0.1
/usr/bin/rsync -av [BE CMS IP]:/usr/share/nginx/html/ /opt/ramdrive

[root@VPN ~]# vi /root/.ssh/authorized_keys
from="[CMS IP]" ssh-rsa AAAAB….
```

2) Включить ведение журналов подключений по RADIUS и SYSLOG:
   - для VPN хаба VPN-USERS

```
[root@VPN ~]# vi /opt/softether-radacct-endpoints/settings.php
$hubname = "VPN-USERS"; // softether hub name
$softetherip = "[BE VPN IP]"; // softether hub address
```

   - для VPN хаба VPN-ENDPOINTS

```
[root@VPN ~]# vi /opt/softether-radacct-endpoints2/settings.php
$hubname = "VPN-ENDPOINTS"; // softether hub name
$softetherip = "[BE VPN IP]"; // softether hub address
```

   - для SYSLOG событий "The new session" и "The session has been terminated"

```
[root@VPN ~]# vi /etc/syslog-ng/conf.d/syslog-ng_softether.conf
filter acctstart_127.0.0.1_vpnhub { host("[BE VPN IP]") and match("VPN-ENDPOINTS") and match("The
new session"); };
filter acctstop_127.0.0.1_vpnhub { host("[BE VPN IP]") and match("VPN-ENDPOINTS") and match("The
session has been terminated"); };
filter acctstart_127.0.0.1_vpnhub2 { host("[BE VPN IP]") and match("VPN-USERS") and match("The new
session"); };
filter acctstop_127.0.0.1_vpnhub2 { host("[BE VPN IP]") and match("VPN-USERS") and match("The
session has been terminated"); };
```

3) Разрешить управление VPN сервером с определенных IP адресов:

```
[root@VPN ~]# vi /opt/softether/adminip.txt
[BE VPN IP]
[IP MGMT PC]
127.0.0.1
```

4) Остановить VPN сервис перед редактирование конфигурационного файла:

```
[root@VPN ~]# ps -ef | grep vpn
root       979     1  0 Jul03 ?        00:00:00 /opt/softether/vpnserver/vpnserver execsvc
root       982   979  0 Jul03 ?        00:18:27 /opt/softether/vpnserver/vpnserver execsvc
root      3746  1270  0 08:07 pts/0    00:00:00 grep --color=auto vpn
root@VPN ~]# /opt/softether/vpnserver stop
[root@VPN ~]# ps -ef | grep vpn
root      3746  1270  0 08:07 pts/0    00:00:00 grep --color=auto vpn
```

В качестве альтернативы можно воспользоваться утилитой **kill [pid]**.

5) Отредактировать конфигурационный файл VPN сервиса:

```
[root@VPN ~]# vi /opt/softether/vpn_server.config
….
string ListenIP [BE VPN IP]
….
```

```
declare InterfaceList …
declare Interface0
{
  string HubName LAN-USERS
  string IpAddress [BE VPN IP + 1]
```

6) Выполнить перезагрузку системы командой reboot.

После перезагрузки системы необходимо проверить наличие интерфейсов **eth0** и **eth1** в выводе *ifconfig* и наличие процессов syslog и vpn:

```
[root@cs-s-cmsv01 ~]# ps -ef | grep syslog
root      929     1  0 09:57 ?        00:00:00 /usr/sbin/rsyslogd -n
root      940     1  0 09:57 ?        00:00:00 /usr/sbin/syslog-ng -F -p /var/run/syslogd.pid
[root@cs-s-cmsv01 ~]# ps -ef | grep vpn
root      992     1  0 09:57 ?        00:00:00 /opt/softether/vpnserver/vpnserver execsvc
root      994   992  2 09:57 ?        00:00:18 /opt/softether/vpnserver/vpnserver execsvc
```

7) Подключиться к графической консоли редактирования настроек VPN сервера.

За инструкцией по настройке VPN сервера через графическую консоль обратитесь в службу поддержки.

Настройки сертификатов

Дополнительно можно сгенерировать для VPN сервера новые сертификаты. За инструкцией по генерации и импорту новых сертификатов обратитесь в службу поддержки.

Обслуживание системы

Данный раздел содержит пароли доступа по умолчанию и описание параметров сервисов

Учетные сведения по умолчанию

В Системе BE CMS предусмотрены несколько типов учетных записей.

Таблица 6. Типы учетных записей в системе BE CMS

Роль	Описание
Администратор ОС	Выполняет настройку операционной системы, сетевых и системных параметров.
Администратор СУБД	Осуществляет резервное копирование и восстановление BE CMS Manager.
Администратор прикладного контекста Oracle APEX	Выполняет обновление интерфейса пользователя BE CMS Manager.
Администратор BE CMS Manager	Осуществляет настройку глобальных параметров BE CMS Manager и выполняет управление системой, являясь членом встроенного системного контекста.
Пользователь BE CMS Manager	Выполняет управление настройками системы BE CMS Manager в рамках своего контекста, а также осуществляет подключение к управляемым активам. Пользователя могут быть трех типов: ▪ Administrator – имеет права по настройки сети управления и активов, подключения к любым типам активов. ▪ Engineer – имеет права подключения к любым типам активов (Endpoint Clients, Applications, Devices). ▪ Helpdesk – имеет права подключения к только к клиентам Becsys.

Таблица 7. Учетные сведения BE CMS по умолчанию

Роль	Имя пользователя	Пароль
Администратор ОС	root	**********
Администратор СУБД	SYS	**********
Администратор Oracle APEX	ADMIN	**********
Администратор прикладного контекста Oracle APEX	CMS_APP/ADMIN	**********
Администратор BE CMS Manager	superuser	**********

Управление параметрами сервисов

В системе BE CMS существует ряд параметров, которые могут быть настроены только из интерфейса командной строки ОС. Конфигурационный файл **kamgr.conf** модуля управления расположен в директории **/etc/proxyd**.

```
[root@CMS ~]# cat /etc/proxyd/kamgr.conf
{
    "network": {
        "#comments#": "bind ip is a ipv4 address, 0.0.0.0 - all available interfaces"
        "bind": [
            {"ip": "10.10.10.1", "port": 8082},
            {"ip": "192.168.128.1", "port": 8082},
            {"ip": "172.19.4.105", "port": 8082}
        ]
    },
    "performance": {
        "#comments#": "increase server threads upto your CPU cores number in case of
        the server high loading",
        "server threads": 4
    },
    "timings": {
        "heartbeat (sec)": 10,
        "hold down attempts": 3,
        "sync gap (sec)": 30,
        "serials blacklist lookup (min)": 10
    },
    "logging": {
        "#comments#": "logging destination is one of the following: syslog, console
        or a path to log file",
        "destination": "syslog",
        "#comments#": "filter log messages below level, where levels are - critical,
        error, warning, notice, info and debug",
        "level": "notice"
    }
```

Рисунок 17. Редактирование конфигурационного файла сервиса **Keepalive Manager**

- **bind ip/port** – IP адрес и порт, на котором принимает запросы keepalive manager.
- **heartbeat (sec.)** – интервал отправки keepalive-сообщений Endpoint клиентами.
- **hold down attempts** – при отсутствии указанного количества keepalive-сообщений Endpoint Client помечаются как Offline.
- **sync gap (sec.)** – периодическая синхронизация статистики в базе данных (например, время последней регистрации клиентов).

Сервис обращается в БД (SID = XE) под учетной записью CMS.

```
[root@CMS]# cat /etc/proxyd/proxyd.conf
{
    "controller": {
        "#comments#": "bind ip is a ipv4 addres, 0.0.0.0
        - all available interfaces",
        "bind ip": "127.0.0.1",
        "bind port": 8083
    },
    "performance": {
        "#comments#": "increase server threads upto your
        CPU cores number in case of the server high loading",
        "listener threads": 2,
        "proxy threads": 6
    },
    "database": {
        "name": "XE",
        "user": "CMS",
        "password":
    },
    "logging": {
        "#comments#": "logging destination is one of the
        following: syslog, console or a path to log file",
        "destination": "syslog",

        "#comments#": "filter log messages below level,
        where levels are - critical, error, warning, notice,
        info and debug",
        "level": "notice"
    }
}
```

Рисунок 18. Редактирование конфигурационного файла сервиса **proxyd**

После изменения системных параметров необходимо перезапустить сервис **proxyd** с помощью команды командной стройки ОС: *[root@CMS ~]# service proxyd stop и [root@CMS ~]# service proxyd start*

Приложения

Данный раздел содержит лицензионное соглашение и
контакты службы технической поддержки Business Ecosystems

Лицензионное соглашение

Настоящее Лицензионное соглашение заключается между ООО «Company» (далее по тексту «Лицензиат») и ООО «Бизнес Экосистемс» (далее по тексту – «Правообладатель» или «Лицензиар»), являющимся обладателем интеллектуальных имущественных прав на использование программного обеспечения «BE-CMS» (далее по тексту – «Программное обеспечение» или «ПО»), в котором возможно использование разработок и технологий других производителей, права на которые предоставлены в соответствии с законодательством Российской Федерации и нормами международного права, о нижеследующем:

1. Все условия настоящего Лицензионного соглашения относятся к использованию Программного обеспечения, которое является объектом интеллектуальных прав Правообладателя. В случае если Лицензиат не согласен хотя бы с одним пунктом или условием настоящего Лицензионного соглашения, Лицензиат не имеете прав на использование ПО. Использование ПО с нарушением условий настоящего Лицензионного соглашения считается использованием ПО без согласия (разрешения) Правообладателя и влечет за собой гражданскую, а также административную или уголовную ответственность.

2. Исключительные права на Программное обеспечение принадлежат Правообладателю.

3. Лицензиар предоставляет Лицензиату право использования программного обеспечения (простая неисключительная лицензия) с сохранением за Лицензиаром права выдачи лицензий другим лицам.

4. Правомерно полученные Лицензиатом лицензионные файлы **licence.lrs** и **device.lrs** (расположенные в системной директории /etc/proxyd) используется для активации ПО и содержат информацию о системе (название Компании, параметры лицензии, системные параметры операционной системы, а также список серийных номеров приобретенных Лицензиатом Клиентов удаленного доступа BE CMS Endpoint Client).

5. Лицензиат имеете право использовать ПО при условии полного соблюдения условий настоящего Лицензионного соглашения:

5.1. Использование ПО возможно до ___.___._____, список поддерживаемых серийных номеров BE CMS Endpoint Client можно посмотреть на вкладке **System -> Licensing.** При покупке Клиентов удаленного доступа BE CMS Endpoint Client серийные номера вносятся Лицензиаром в файл лицензии **device.lrs**, который высылается Лицензиату.

5.2. В случае изменения системных параметров операционной системы ПО автоматически блокируется. Для восстановления работоспособности необходимо связаться со Службой технической поддержки Лицензиара или восстановить в исходное состояние системные параметры операционной системы.

5.3. В течение срока использования ПО Лицензиату предоставляется право обращаться в Службу технической поддержки Правообладателя либо распространителя ПО, имеющего соответствующий договор с Правообладателем.

5.4. Лицензиату не разрешается осуществлять распространение ПО в любой форме и любым способом, в том числе, путем продажи, сдачи в аренду, прокат или во временное пользование, предоставления взаймы, включая импорт, для любой из этих целей.

5.5. Лицензиату не разрешается изменять, декомпилировать, дизассемблировать, дешифровать и производить иные действия с объектным кодом ПО, имеющие целью получение информации о реализации алгоритмов, используемых в ПО, без письменного согласия на то Правообладателя, за исключением случаев, прямо предусмотренных действующим законодательством Российской Федерации.

5.6. Лицензиату не разрешается каким-либо образом модифицировать механизм внутренней защиты ПО (модуль лицензирования и его компонентов). Копирование ПО с заведомо устраненным или испорченным механизмом внутренней защиты, равно как неправомерное использование такого ПО, является незаконным.

5.7. ПО и сопутствующая ему документация (руководство пользователя и руководство администратора) предоставляются Лицензиату «AS IS», в соответствии с общепринятым в международной практике принципом. Это означает, что за проблемы и их последствия, возникающие в процессе установки, обновления, поддержки и эксплуатации Лицензиатом экземпляра ПО (в том числе: проблемы совместимости с другими программными продуктами, проблемы, возникающие из-за неоднозначного толкования Лицензиатом сопроводительной документации, несоответствия результатов использования ПО ожиданиям Лицензиата и т. п.), Правообладатель ответственности не несет.

6. Действие настоящего Лицензионного соглашения распространяется на все последующие обновления/новые версии Программного обеспечения. Установка обновления/новой версии ПО означает принятие Лицензиатом условий настоящего Лицензионного соглашения для соответствующих обновлений/новых версий Программы, если обновление/установка новой версии ПО не сопровождается иным Лицензионным соглашением.

Авторское право

Business Ecosystems предоставляет данный документ «AS IS». Разработчик оставляет за собой право выполнять изменения в данном руководстве, продукте или программах, являющихся частью продукта, в любое время без предупреждения пользователей. Данное руководство может содержать технические неточности или орфографические ошибки, которые могут быть устранены в следующих версиях документа. Право использования системы управления **BE CMS** предоставляется с сохранением за Правообладателем права выдачи лицензий другим лицам, т.е. система предоставляется с простой неисключительной лицензией.

В случае нарушения (превышения) со стороны Лицензиата положений Лицензии, Правообладатель согласно ст. 1252 ч. 4 Гражданского кодекса РФ имеет право на защиту исключительных прав путем предъявления требований:

- о признании права – к лицу, которое отрицает или иным образом не признает право, нарушая тем самым интересы Правообладателя;
- о пресечении действий, нарушающих право или создающих угрозу его нарушения – к лицу, совершающему такие действия или осуществляющему необходимые приготовления к ним;
- о возмещении убытков или выплате компенсации в размере от ста тысяч рублей до двух миллионов рублей – к лицу, неправомерно использовавшему результат интеллектуальной деятельности без заключения соглашения с правообладателем (бездоговорное использование) либо иным образом нарушившему его исключительное право и причинившему ему ущерб;
- о публикации решения суда о допущенном нарушении с указанием действительного правообладателя – к нарушителю исключительного права.

В системе управления **BE CMS Manager** реализована функция проверки установленных лицензионных ключей, а также проверки их годности. Работа системы автоматически блокируется в следующих случаях:

- изменение системных параметров операционной системы (например, сетевых настроек или смена аппаратных комплектующих сервера);
- истечение срока действия лицензионного ключа.

Для восстановления работы системы **BE CMS** необходимо обратиться в службу технической поддержки Business Ecosystems.

Техническая поддержка

Для получения технической поддержки по продукту необходимо написать на адрес support@becsys.ru электронное письмо с описанием вопроса, указав название организации и серийный номер инсталляции BE CMS Manager.

Business Ecosystems LLC.

ООО «Бизнес Экосистемс»
143026 Москва, Россия
Территория инновационного центра Сколково
ул. Малевича, 1, офис 5

info@becsys.ru
www.becsys.ru