Смена мастер-ключей в сетях с ViPNet Coordinator HW

Руководство администратора

infotecs

АО «ИнфоТеКС»

127083, Москва, улица Мишина, д. 56, стр. 2, этаж 2, помещение IX, комната 29

Телефон: +7 (495) 737-6192, 8-800-250-0260 — бесплатный звонок из России (кроме Москвы)

Веб-сайт: infotecs.ru

Служба технической поддержки: hotline@infotecs.ru

Содержание

Введение

О документе

В документе указан порядок действий администратора сети ViPNet и администратора ViPNet Coordinator HW при смене мастер-ключей в сети ViPNet.

О том, что такое мастер-ключи и в каких случаях может потребоваться их сменить, см. документ «ViPNet Удостоверяющий и ключевой центр. Руководство администратора».

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте ИнфоТеКС:

- Информация о продуктах ViPNet.
- Информация о решениях ViPNet.
- Часто задаваемые вопросы.
- Форум пользователей продуктов ViPNet.

Контактная информация

Если у вас есть вопросы, свяжитесь со специалистами ИнфоТеКС:

- Единый многоканальный телефон:

  +7 (495) 737-6192,

  8-800-250-0-260 — бесплатный звонок из России (кроме Москвы).

- Служба поддержки: hotline@infotecs.ru.

  Форма для обращения в службу поддержки через сайт.

  Телефон для клиентов с расширенной поддержкой: +7 (495) 737-6196.

- Отдел продаж: soft@infotecs.ru.

Если вы обнаружили уязвимости в продуктах компании, сообщите о них по адресу security-notifications@infotecs.ru. Распространение информации об уязвимостях продуктов компании ИнфоТеКС регулируется политикой ответственного разглашения.

Подготовка к смене мастер-ключей

Перед сменой мастер-ключей выполните следующие действия:

1 Для корректной смены мастер-ключей на вашем ViPNet Coordinator HW должно быть установлено ПО версии 4.3.2 и выше.

Если на ViPNet Coordinator HW установлено ПО версии 3.x, обновите его сначала до версии 4.2.1 (подробнее см. документ «ViPNet Coordinator HW 4. Инструкция по обновлению ViPNet Coordinator HW 3 до ViPNet Coordinator HW 4»), а затем до версии 4.3.2 (подробнее см. документ «ViPNet Coordinator HW 4. Настройка с помощью командного интерпретатора», раздел «Обновление программного обеспечения»).

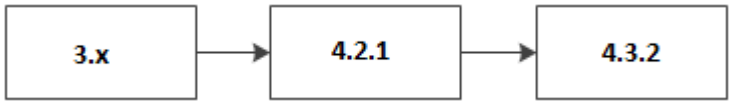

Рисунок 1. Порядок обновления версий ПО ViPNet Coordinator HW

2 Убедитесь, что пароли пользователя `user` на сетевом узле ViPNet Coordinator HW и в программе ViPNet Удостоверяющий и ключевой центр совпадают. Если пароли не совпадают, то необходимо на ViPNet Coordinator HW для пользователя `user` задать тот же пароль, который задан в программе ViPNet Удостоверяющий и ключевой центр.

Смена мастер-ключей при использовании ViPNet Administrator 4.6.4

Для смены мастер-ключей:

1 За несколько дней до обновления мастер-ключей на ViPNet Coordinator HW проверьте, что у вас есть резервный набор персональных ключей (РНПК). Для этого выполните команду:

```
hostname> iplir show key-info
```

Если в выводе команды будет информация о ключах в секции `Spare personals key set info`, это значит, что на вашем ViPNet Coordinator HW есть РНПК.

При этом важно, чтобы совпадали:

- дата создания мастер-ключа для персонального ключа и дата создания мастер-ключа для РНПК;
- номер мастер-ключа для персонального ключа и номер мастер-ключа для РНПК.

```
Current personal key info:
Master personal key date : 2019-01-17 17:49:37 MSK
Master personal key number: 4
...
Spare personals keys set info:
Master personal key date : 2019-01-17 17:49:37 MSK
Master personal key number: 4
```

Если РНПК нет, или даты создания мастер-ключа для персонального ключа и для РНПК отличаются:

1.1 Убедитесь, что пароли пользователя `user` на сетевом узле ViPNet Coordinator HW и в программе ViPNet Удостоверяющий и ключевой центр (УКЦ) совпадают. Если пароли не совпадают, то необходимо на ViPNet Coordinator HW для пользователя `user` задать тот же пароль, который задан в ViPNet УКЦ.

1.2 В ViPNet УКЦ сохраните РНПК сетевого узла ViPNet Coordinator HW в файл и скопируйте его на USB-носитель.

1.3 На сетевом узле ViPNet Coordinator HW импортируйте РНПК с USB-носителя с помощью команды:

```
hostname# admin add spare keys
```

2 На ViPNet Coordinator HW проверьте, что у вас отсутствуют неприменившиеся обновления ключей:

2.1 Перейдите в режим администратора с помощью команды `enable`.

2.2 Перейдите в командную оболочку Linux с помощью команды `admin escape`.

2.3 Выполните команду:

```
find /opt/vipnet/ccc/ -name "k*.*".
```

Если в результате в командной строке появятся пути к файлам, это значит, что на вашем ViPNet Coordinator HW есть не применившиеся обновления ключей. Чтобы исправить ситуацию, в ViPNet Центр управления сетью (ЦУС) заново отправьте справочники и ключи по сети на ViPNet Coordinator HW, дождитесь, когда они примут статус **Приняты** и повторите шаги 2.1-2.3 для проверки успешности обновления.

Внимание! Если после выполнения шагов 2.1-2.3 на вашем ViPNet Coordinator HW остались не применившиеся обновления ключей, прекратите процесс обновления ключей и обратитесь в службу поддержки «ИнфоТеКС».

3 На ViPNet Coordinator HW выполните экспорт справочников, ключей и настроек (в файл `*.vbe`) с помощью команд:

```
hostname# iplir stop
hostname# mftp stop
```

```
hostname# admin export keys binary-encrypted usb
```

Подробнее об экспорте см. документ «ViPNet Coordinator HW. Руководство администратора», раздел «Экспорт справочников, ключей и настроек».

4 В ViPNet УКЦ смените мастер-ключи. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр 4. Руководство администратора», разделы «Смена мастер-ключей защиты и обмена» и «Смена мастер-ключа персональных ключей».

Внимание! После смены мастер-ключей не выполняйте в ViPNet УКЦ никакие действия кроме описанных ниже (в том числе не выпускайте файлы DST). Неправильный порядок действий может привести к нарушению работоспособности ViPNet Coordinator HW.

5 После смены мастер-ключей:

5.1 В ViPNet УКЦ создайте ключи для всех пользователей и передайте их в ЦУС.

5.2 В ViPNet УКЦ создайте ключи для всех сетевых узлов и передайте их в ЦУС.

5.3 В ViPNet ЦУС отправьте все обновления ключей по сети отложенным способом (на несколько дней), чтобы обновления успели получить все узлы сети, включая самые дальние.

5.4 Проконтролируйте доставку и применение обновлений на всех узлах — в программе ViPNet ЦУС для всех узлов статус обновлений должен быть **Приняты**.

5.5 Проверьте работоспособность сети.

5.6 На ViPNet Coordinator HW выполните экспорт справочников и настроек в файл `*.vbe`.

Смена мастер-ключей при способе аутентификации «устройство»

Если в программе ViPNet Adminsitrator для сетевого узла ViPNet Coordinator HW выбран способ аутентификации «устройство», то после смены мастер-ключей вы не сможете авторизоваться.

Поэтому после смены мастер-ключей:

1 В программе ViPNet Adminsitrator выполните процедуру «выдать новый дистрибутив ключей».

При этом на «устройство (персональный ключ)» будут записаны новые ключи пользователя. Подробнее см. документ «ViPNet Удостоверяющий и ключевой центр 4. Руководство администратора», раздел «Создание дистрибутивов ключей».

2 Авторизуйтесь на ViPNet Coordinator HW используя это «устройство (персональный ключ)».

Разворачивать новый дистрибутив ключей на ViPNet Coordinator HW не требуется.

Особенности смены мастер-ключей в кластере горячего резервирования

При смене мастер-ключей для ViPNet Coordinator HW, работающем в кластере горячего резервирования изменения применяются только на активном узле кластера. На пассивном узле изменения применяются при последующем перезапуске службы `mftp` либо при смене состояния кластера.

В связи с этим после смены мастер-ключей может возникнуть ошибка удаленного обновления ПО ViPNet Coordinator HW в кластере, если состояние кластера не менялось перед попыткой обновления ПО.

Для устранения ошибки удаленного обновления ПО после смены мастер-ключей, выполните перезагрузку пассивного узла кластера горячего резервирования, либо перезапустите службу `mftp` на пассивном узле кластера, выполнив команды:

```
#mftp stop
```

```
#mftp start
```