ViPNet MFTP Linux

Руководство администратора

ViPNet Virtual Private Network

infotecs

ФРКЕ.00031-04 90 03, Версия 3.6.5

ОАО «Инфотекс»

127287, г. Москва, Старый Петровско-Разумовский пр., дом 1/23, строение 1

Тел: (495) 737-61-96 (hotline), 737-61-92, факс 737-72-78

E-mail: hotline@infotecs.ru

WWW: http://www.infotecs.ru

Содержание

Введение

О данном документе

Данный документ предназначен для администраторов, отвечающих за настройку и эксплуатацию ПО ViPNet Coordinator Linux, в состав которого входит транспортный модуль ViPNet MFTP Linux. В нем содержится информация по настройке и работе с транспортным модулем.

Соглашения документа

Соглашения данного документа представлены в таблице ниже.

Таблица 1. Условные обозначения

Указатель	Описание
	**Внимание!** Указывает на обязательное для исполнения или следования действие или информацию.
	**Примечание.** Указывает на необязательное, но желательное для исполнения или следования действие или информацию.
	**Совет.** Содержит дополнительную информацию общего характера.

Обратная связь

Дополнительная информация

Сведения о продуктах и решениях ViPNet, распространенные вопросы и другая полезная информация собраны на сайте компании «Инфотекс». По предложенным ссылкам можно найти ответы на многие вопросы, возникающие в процессе эксплуатации продуктов ViPNet.

- Сборник часто задаваемых вопросов (FAQ) http://www.infotecs.ru/support/faq/.
- Законодательная база в сфере защиты информации http://www.infotecs.ru/laws/.
- Информация о решениях ViPNet http://www.infotecs.ru/solutions/vpn/.

Контактная информация

С вопросами по использованию продуктов ViPNet, пожеланиями или предложениями свяжитесь со специалистами компании «Инфотекс». Для решения возникающих проблем обратитесь в службу технической поддержки.

- Электронный адрес службы поддержки hotline@infotecs.ru.
- Форма запроса по электронной почте в службу поддержки http://www.infotecs.ru/support/request/.
- Форум компании «Инфотекс» http://www.infotecs.ru/forum.
- 8 (495) 737-6196 — «горячая линия» службы поддержки.
- 8 (800) 250-0260 — бесплатный звонок из любого региона России (кроме Москвы).

Общие сведения

Назначение и функциональность транспортного модуля

Транспортный модуль ViPNet MFTP Linux (далее - транспортный модуль) предназначен для обеспечения надежной и безопасной передачи транспортных конвертов между узлами сети ViPNet посредством протоколов TCP (этот канал передачи называется MFTP) и SMTP/POP3. Кроме того, транспортный модуль принимает непосредственное участие в удаленном обновлении адресных справочников и ключевых баз на узлах, в удаленном обновлении ПО ViPNet, а также в приеме политик безопасности открытой сети от Центра управления политиками безопасности (ЦУПБ). Транспортный модуль ViPNet MFTP Linux входит в состав программного обеспечения (ПО) ViPNet Coordinator Linux и обеспечивает выполнение Координатором функции Сервера-маршрутизатора.

Транспортные конверты (далее - конверты) представляют собой файлы с данными, которыми обмениваются между собой приложения, входящие в состав ПО ViPNet. Транспортный модуль передает конверты в соответствии с адресами получателей, прописанными в заголовках этих конвертов.

При связи по **каналу MFTP** устанавливается соединение TCP с узлом-получателем конвертов, проводится взаимная аутентификация узлов и осуществляется прием/передача конвертов друг для друга.

При связи по **каналу SMTP/POP3** транспортный модуль переадресует конверты для отправки модулю почтового обмена MailTrans (см. «Секция [mailtrans]» на стр. 21), который передает их через сервер SMTP, а также забирает с сервера POP3 конверты, предназначенные для данного узла.

Кроме того, существует дополнительный канал **Local** (локальный). При связи по **каналу Local** исходящие конверты складываются в каталог, указанный в настройках этого канала. В качестве каталога локального канала может использоваться как каталог на локальном диске, так и смонтированная удаленная файловая система. В частности, можно организовать локальный канал между Координаторами, работающими под разными операционными системами (см. Настройка канала Local между Координаторами Windows и Linux (на стр. 33)). Входящие конверты забираются из каталога, указанного в конфигурации транспортного модуля.

Транспортный модуль взаимодействует только с Клиентами (узлами с установленным ПО ViPNet Client), зарегистрированными в ЦУСе на данном Координаторе, и с другими Координаторами, связь с которыми определяется исходя из таблиц маршрутизации, задаваемых в ЦУСе. Передача конвертов осуществляется в соответствии с маршрутами,

жестко заданными в этих таблицах. Если конверт имеет несколько адресатов, он расщепляется на части, соответствующие адресам. При поступлении конверта, в зависимости от настроек, транспортный модуль либо начинает устанавливать соединение с другим Координатором или со своим Клиентом, либо ожидает, когда с ним установит соединение другая сторона. В настройках транспортного модуля может быть задан период опроса других узлов независимо от наличия для них конвертов.

Транспортный модуль функционирует в виде программы-демона mftpd, работающей в фоновом режиме. Кроме того, для выполнения обмена по каналу SMTP/POP3 используется внешний модуль MailTrans, функционирующий в виде программы mailtrans.

Алгоритм работы транспортного модуля

В данном разделе приведены правила, определяющие поведение транспортного модуля при обмене конвертами.

Прием конвертов

Конверты, принятые по любому из поддерживаемых типов каналов, помещаются в очередь на обработку. При нахождении ошибки в структуре конверта, а также других ошибок конверт помещается в специальный каталог для поврежденных конвертов `in_path/invalid`, где `in_path` – каталог входящих конвертов, задаваемый в секции `[transport]` файла конфигурации транспортного модуля (см. «Секция [transport]» на стр. 19). При разрыве соединения или другой ошибке в процессе приема конвертов продолжение передачи возлагается на передающую сторону. Конверты, адресованные данному узлу, подвергаются соответствующей обработке. Конверты, адресованные другим узлам, передаются в соответствии с таблицей маршрутизации.

При приеме конвертов, содержащих управляющую информацию по обновлению адресных справочников данного узла и/или его ключевых баз, а также содержащих обновление ПО ViPNet Coordinator Linux или обновление политики безопасности, транспортный модуль помещает файлы обновления в каталог, указанный в секции `[upgrade]` его конфигурационного файла (см. «Секция [upgrade]» на стр. 20). Перед проведением обновления в зависимости от настроек транспортного модуля производится автоматическое сохранение текущей конфигурации ViPNet (см. документ «ViPNet Coordinator Linux. Руководство администратора»).

Для обновления адресных справочников и/или ключевых баз, а также политики безопасности производится перезапуск управляющего демона iplircfg, который непосредственно проводит обновление.

Для обновления ПО ViPNet Coordinator Linux вызывается специальный исполняемый файл сценария, поставляемый вместе с файлами обновления, который останавливает все службы ViPNet и производит попытку выгрузки драйверов ViPNet. В случае успеха он производит обновление ПО, а затем загружает обновленные версии используемых драйверов и служб ViPNet.

При работе Координатора в составе кластера горячего резервирования алгоритм обновления ПО ViPNet Coordinator Linux отличается от описанного выше (см. документ «ViPNet Coordinator Linux. Система защиты от сбоев. Руководство администратора»). Конверт с обновлением ПО принимается «активным» Координатором кластера. Затем, используя специальный протокол взаимодействия, копия конверта передается на «пассивный» Координатор кластера. После успешной распаковки и обработки на обоих Координаторах осуществляется синхронный запуск сценария обновления, описанного выше. Сценарий обновления не будет запущен до тех пор, пока «пассивный» Координатор корректно не обработает все команды «активного». После завершения работы сценария службы на «пассивном» Координаторе стартуют с временной задержкой для исключения одновременного перехода Координаторов в активный режим. Завершающим этапом является обмен командами, определяющими результаты обновления, и формирование на их основе общего результата обновления ПО.

Примечание. Обновление ПО считается успешным, если оно успешно завершилось на обоих Координаторах кластера горячего резервирования.

Передача конвертов

Исходящие конверты помещаются в соответствующую очередь. При извлечении конверта из очереди осуществляется попытка его передачи, если это не запрещено настройками соответствующего канала (см. «Секция [channel]» на стр. 16). При разрыве соединения или других ошибках в процессе передачи повторная попытка передачи осуществляется через интервал, указанный в настройках транспортного модуля (см. «Секция [misc]» на стр. 24). В случае канала MFTP повторная передача информации всегда продолжается с точки разрыва, то есть передается не весь конверт, а лишь его оставшаяся часть. Полностью переданные конверты удаляются из очереди. Кроме того, если это не запрещено настройками MFTP (см. «Секция [misc]» на стр. 24), в специальном каталоге создается файл нулевой длины с именем переданного конверта. Расположение этого каталога задается путем `out_path/sent`, где `out_path` – каталог исходящих конвертов, задаваемый в секции `[transport]` файла конфигурации транспортного модуля (см. «Секция [transport]» на стр. 19).

Регулярно (раз в час) очередь исходящих конвертов просматривается на наличие устаревших конвертов, время хранения которых превысило допустимый предел, заданный в конфигурации (см. «Секция [misc]» на стр. 24). Такие конверты удаляются из очереди и помещаются в «корзину» – специальный каталог, также задаваемый в конфигурации. Из этого каталога конверт удаляется при достижении предельного времени хранения конвертов в «корзине».

Настройка транспортного модуля

Конфигурационный файл транспортного модуля

Все настройки транспортного модуля содержатся в его конфигурационном файле, который называется `mftp.conf` и расположен в подкаталоге `/user` того каталога, где хранятся ключевые базы (указывается в файле `/etc/iplirpsw`). Данный конфигурационный файл создается при первом старте MFTP-демона и содержит значения параметров по умолчанию.

Внимание! Для правильной работы транспортного модуля необходимо внести соответствующие изменения в его конфигурационный файл!

Секции конфигурационного файла транспортного модуля

Конфигурационный файл транспортного модуля состоит из секций, каждая из которых содержит ряд параметров. Имена секций заключены в прямые скобки, например `[channel]`, `[misc]`. Значения параметров отделяются от их идентификаторов знаком «=» и следующим за ним пробелом, например: `ip= 192.168.201.1`.

Для параметров, отсутствующих в секциях, используются значения по умолчанию.

Секция [channel]

Секции `[channel]` содержат настройки каналов, по которым данный Координатор может осуществлять обмен с другими узлами. Каждому каналу соответствует своя секция `[channel]`. Количество параметров в каждой секции зависит от типа выбранного канала. По умолчанию при создании файла конфигурации все типы каналов устанавливаются в значение `mftp`.

Внимание! Добавление и удаление секций `[channel]` осуществляется автоматически, поэтому не следует добавлять и удалять секции данного типа вручную!

Секции `[channel]` содержат ряд общих параметров для каналов любого типа:

- `id` – уникальный 4-байтовый идентификатор сетевого узла ViPNet, с которым устанавливается обмен по данному каналу. Идентификатор представлен в шестнадцатеричном виде, например: `id= 0x270e000a`.

  

  Примечание. Изменять параметр `id` вручную не следует!

- `name` – имя сетевого узла ViPNet. Этот параметр носит информационный характер.

- `type` – тип канала. Может принимать следующие значения: `local`, `mftp`, `smtp`. По умолчанию значение параметра `mftp` для всех узлов. Если данный параметр отсутствует, то используется значение по умолчанию.

- `off_flag` – признак отключения канала (`yes/no`). По умолчанию значение параметра `no`. Установка параметра в значение `yes` позволяет временно отключить канал. В таком случае исходящие конверты, передаваемые по этому каналу, будут оставаться в очереди до тех пор, пока канал не будет включен или инициатором соединения по данному каналу не станет удаленный Сервер-маршрутизатор (Координатор). Если инициатором соединения в данном случае станет удаленный Клиент, то предназначенные ему конверты не отправляются, а этому Клиенту передается специальная команда, которая выключает соответствующий канал в настройках его транспортного модуля. Если данный параметр отсутствует, то используется значение по умолчанию.

- `call_flag` – признак немедленной передачи конвертов по каналам MFTP и SMTP (`yes/no`). По умолчанию значение параметра `yes`. При установке значения параметра в `yes` попытка передачи конверта по данному каналу будет производиться немедленно. В противном случае конверт будет оставаться в очереди до тех пор, пока инициатором соединения по данному каналу не станет удаленный узел (в случае MFTP-канала) или не будет вызван модуль MailTrans (в случае SMTP-канала). Если данный параметр отсутствует, то используется значение по умолчанию.

Для каждого из типов каналов существуют специфические параметры.

Специфические параметры для канала MFTP

Для канала MFTP в секции `[channel]` дополнительно задаются следующие параметры:

- `ip` – IP-адрес удаленного сетевого узла. Значение данного параметра запрашивается у управляющего демона. Если оно по каким-либо причинам не было сообщено (равно 0.0.0.0), то его можно задать вручную, а затем перезапустить транспортный модуль. Данный параметр может изменяться в процессе работы, поэтому корректировать его вручную не рекомендуется.

- `call_timeout` – интервал опроса (в секундах) соответствующего удаленного сетевого узла. Время следующего опроса отсчитывается от момента разрыва последнего соединения с этим узлом.

  При значении параметра `-1` опрос не производится. По умолчанию значение параметра `-1` для всех узлов. Если данный параметр отсутствует, то используется значение по умолчанию.

- `last_port` – значение порта, по которому осуществлялось последнее удачное MFTP-соединение. Это значение будет использоваться при следующей попытке соединения с этим узлом.

Внимание! Менять параметр `last_port` вручную не следует!

- `last_call` – время последней попытки опроса данного канала.

Внимание! Менять параметр `last_call` вручную не следует!

- `last_err` – время, когда произошла последняя ошибка при попытке соединения или в процессе передачи данных.

Внимание! Менять параметр `last_err` вручную не следует!

Специфические параметры для канала Local

Для канала Local в секции `[channel]` дополнительно задаются следующие параметры:

- `path` – полный путь (относительно корневого каталога) к каталогу, в который помещаются исходящие конверты для данного канала. Этот параметр задает лишь основной каталог. В процессе работы транспортный модуль создает в этом каталоге подкаталог `local`, именно в этот подкаталог помещаются исходящие конверты.

  Пример настройки этого параметра см. в приложении Настройка канала Local между Координаторами Windows и Linux (на стр. 33).

- `last_err` – время, когда произошла последняя ошибка при попытке соединения или в процессе передачи данных.

Внимание! Менять параметр `last_err` вручную не следует!

Специфические параметры для канала SMTP

Для канала SMTP в секции `[channel]` дополнительно задаются следующие параметры:

- `reportaddress` – адрес ящика электронной почты, в который будут отправляться исходящие конверты. Адрес задается в соответствии со следующим правилом:

  ```
  reportaddress= <username>@<servername>.<domain>
  ```

- `version` – версия протокола инкапсуляции конверта MFTP в почтовый конверт RFC-822, передаваемый по каналу SMTP. Возможные значения параметра: `1.0` и `2.0`. В случае использования протокола `1.0` MFTP-конверт полностью инкапсулируется в SMTP-конверт для передачи. Версия протокола `2.0` позволяет передать MFTP-конверт в виде нескольких SMTP-конвертов. Это удобно в случае использования ограничений на размер писем SMTP/POP3-серверами. При отправке MFTP-конверт разбивается на несколько SMTP-конвертов, размер каждого из которых не превышает заданный параметром `maxsize` (см. ниже). Принимающая сторона собирает все SMTP-фрагменты в единый MFTP-конверт.

  По умолчанию данный параметр отсутствует в секциях [channel]. В случае отсутствия параметра в секции [channel] используется версия протокола 1.0.

Примечание. По умолчанию используется протокол `1.0`, так как предыдущие версии транспортного модуля несовместимы с протоколом `2.0`.

Также с версией 2.0 несовместим транспортный модуль продуктов линейки CUSTOM VPN Windows.

- `maxsize` – максимальный размер почтового SMTP-конверта при отправке (в килобайтах). Используется в случае, если установлена версия протокола `2.0` (см. параметр `version`). Значение `0` означает, что ограничение на размер SMTP-конвертов отсутствует. Допустимые значения данного параметра: от 100 до 2048000 (2 ГБ). По умолчанию данный параметр отсутствует в секциях `[channel]`. Если параметр `version` в секции задан и имеет версию 2.0, то обязательно необходимо задать значение параметра `maxsize`.

Секция [transport]

Данная секция содержит ряд параметров, определяющих пути к транспортным каталогам, то есть к каталогам, участвующим в обмене конвертами, их обработке и т.п. Эти параметры задают лишь основные каталоги. Вспомогательные каталоги создаются транспортным модулем в процессе работы как подкаталоги основных. При первом создании конфигурационного файла значения параметров этой секции определены по умолчанию относительно каталога ключевых баз.

Примечание. Транспортный модуль при каждом запуске проверяет существование каталогов, заданных этими параметрами, и при необходимости создает их.

Секция `[transport]` содержит следующие параметры:

- `in_path` – полный путь к каталогу, в который помещаются полностью принятые конверты. По умолчанию значение параметра `basedir/in`, где `basedir` – полный путь к каталогу ключевых баз.
- `out_path` – полный путь к каталогу, в который внешние приложения помещают сформированные конверты для отправки. По умолчанию значение параметра `basedir/out`.
- `trash_path` – полный путь к каталогу, в который помещаются устаревшие конверты из исходящей очереди – так называемая «корзина». По умолчанию значение параметра `basedir/trash`.
- `local_path` – полный путь к каталогу, в который другие сетевые узлы помещают входящие конверты, передаваемые по локальному каналу. По умолчанию значение параметра `basedir/local`.

Секция [upgrade]

В данной секции присутствуют параметры, которые определяют поведение транспортного модуля при приеме обновления. Секция `[upgrade]` содержит следующие параметры:

- `upgrade_path` – полный путь к каталогу, в который помещаются файлы обновления после распаковки соответствующих конвертов. По умолчанию значение параметра `basedir/ccc`, где `basedir` – полный путь к каталогу ключевых баз.
- `upgrade_ini` – имя файла конфигурации для процесса обновления. По умолчанию значение параметра `basedir/user/upgrade.conf`.
- `upgrade_for_kc_path` – полный путь к каталогу, в который внешние приложения помещают файлы с запросами сертификатов `*.sok`. По умолчанию значение параметра `basedir/ccc/for_kc`.
- `upgrade_checktimeout` – интервал (в секундах) периодической проверки транспортного каталога, заданного параметром `upgrade_path`, на наличие файлов обновления. В случае соответствия файлов обновления условиям обновления (время

обновления и т.д.) происходит вызов модуля обновления. По умолчанию значение параметра `300` (секунд).

- `confsave` – тип сохраняемой конфигурации при автосохранении перед проведением обновления. Может принимать следующие значения: `full`, `partial` и `off`. При значении параметра `full` производится автосохранение полной конфигурации, при значении `partial` – частичной конфигурации. При значении параметра `off` автосохранение не производится. По умолчанию значение параметра `partial`.

- `maxautosaves` – количество автосохраненных конфигураций в базе. Перед очередным автосохранением конфигурации проверяется число автосохраненных конфигураций. Если это число больше или равно значению `maxautosaves`, то из базы удаляются самые старые автосохраненные конфигурации в таком количестве, чтобы осталось `maxautosaves-1`, после чего сохраняется текущая конфигурация. При этом в системный журнал syslog выводится соответствующее сообщение. Текущая версия транспортного модуля имеет ограничение на максимальное количество автосохраненных конфигураций – не более 10, поэтому значение параметра `maxautosaves` не может превышать 10. При попытке установки большего значения оно принудительно устанавливается равным максимально допустимому значению.

Секция [mailtrans]

В данной секции присутствуют параметры, которые определяют взаимодействие транспортного модуля с модулем почтового обмена MailTrans. Секция `[mailtrans]` содержит следующие параметры:

- `mailtrans_bin` – полный путь к исполняемому файлу модуля почтового обмена. По умолчанию значение параметра `/sbin/mailtrans`.

- `inputmailbox` – адрес почтового ящика, из которого модуль почтового обмена будет забирать конверты по протоколу POP3. Адрес задается в соответствии со следующим правилом:

  ```
  inputmailbox= <username>:<password>@<IP-адрес POP3-сервера>
  ```

- `outputmailbox` – IP-адрес SMTP-сервера, на который модуль почтового обмена будет отправлять конверты по протоколу SMTP.

- `frommailbox` – почтовый адрес отправителя SMTP-конвертов. Адрес задается в соответствии со следующим правилом:

  ```
  frommailbox= <username>@<servername>.<domain>
  ```

- `mail_in_path` – полный путь к каталогу, в который модуль почтового обмена помещает принятые конверты. По умолчанию значение параметра `basedir/smtpin`.

- `mail_in_chunks_path` – полный путь к каталогу, в который модуль почтового обмена помещает принятые фрагменты SMTP-конвертов в случае использования протокола `2.0`. По умолчанию значение параметра `basedir/smtpin/chunks`.

- `mail_out_path` – полный путь к каталогу, в котором транспортный модуль формирует заголовочные файлы на отправляемые конверты. По умолчанию значение параметра `basedir/smtpout`.

- `mail_call_timeout` – интервал (в секундах) периодического вызова модуля почтового обмена, то есть период опроса почтового ящика входящих конвертов и отправки исходящих конвертов по каналу SMTP. При значении параметра `-1` периодический вызов не производится. Однако при наличии в очереди исходящих конвертов, предназначенных для отправки по каналу SMTP, вызов будет производиться, если это не запрещено параметром `call_flag` соответствующего канала. По умолчанию значение параметра `-1`.

- `maxsmtpsize` – максимальный размер конверта, передаваемого по каналу SMTP, (в мегабайтах). По умолчанию данный параметр отсутствует. Отсутствие данного параметра означает, что ограничение на размер передаваемого конверта по каналу SMTP отсутствует. Если размер конверта, передаваемого по SMTP-каналу, превышает размер, заданный данным параметром, то конверт удаляется из очереди. При этом отправителю конверта будет отправлена транспортная квитанция о невозможности отправки конверта получателю.

Секция [journal]

Секция `[journal]` содержит параметры настройки журнала конвертов, обрабатываемых транспортным модулем MFTP. В процессе работы транспортный модуль осуществляет запись информации об обработанных конвертах в специальную базу данных, называемую журналом конвертов. В журнал заносится информация:

- о полностью принятых конвертах;

- об отправленных конвертах;

- об удаленных конвертах;

- о поврежденных конвертах.

База данных журнала конвертов ведется в виде бинарного файла `mftpenv.db`, который находится в подкаталоге `basedir/user`, где `basedir` – полный путь к каталогу ключевых баз.

Секция `[journal]` содержит следующие параметры:

- `use_journal` – включение/выключение ведения журнала в текущем сеансе работы транспортного модуля (`yes/no`). По умолчанию значение параметра yes. Если данный параметр отсутствует, то используется значение по умолчанию.

- `max_size` – максимальный размер (в мегабайтах) файла журнала конвертов. При превышении указанного размера осуществляется запись поверх самых старых записей. При изменении максимального размера журнала в процессе работы происходит реконструкция файла. В случае уменьшения размера по сравнению с предыдущим из файла удаляются записи с наиболее старыми датами. По умолчанию значение параметра `1` (мегабайт). Если данный параметр отсутствует, то используется значение по умолчанию.

- `dump_filename` – префиксная часть имени текстового файла, в который осуществляется регулярный дамп информации из журнала конвертов. По умолчанию значение параметра `/var/log/mftpenv.log`. Постфиксная часть имени файла определяется текущей датой и зависит от интервала дампа, заданного параметром `dump_interval`. Например, файл дампа может иметь имя `/var/log/mftpenv.log.2009.09.23`.

Внимание! Менять параметр `dump_filename` вручную не следует!

- `dump_interval` – интервал создания (в днях) файлов дампа информации из журнала конвертов. В процессе работы транспортный модуль выводит информацию об обработанных конвертах в текущий файл дампа. По истечении интервала, заданного данным параметром, создается новый файл дампа, постфиксная часть которого определяется текущей датой. По умолчанию значение параметра `1` (день). Если данный параметр отсутствует, то используется значение по умолчанию.

- `last_dump` – время создания текущего файла дампа.

Внимание! Менять параметр `last_dump` вручную не следует!

Секция [misc]

Секция `[misc]` содержит различные параметры, определяющие работу транспортного модуля в целом:

- `port` – порт, на котором демон mftpd ожидает соединения по каналу MFTP от удаленных сетевых узлов. По умолчанию значение параметра `5000`.

- `max_listen_ports` – диапазон значений перебора портов для соединений по каналу MFTP с удаленным узлом в случае неудачи. Транспортный модуль циклично перебирает порты в диапазоне от `port` до `port+max_listen_ports-1`. Для ожидания входящих соединений транспортный модуль прослушивает все порты из указанного диапазона. По умолчанию значение параметра `3`.

- `num_attempts` – количество последовательных попыток соединения, после которых устанавливается тайм-аут, если соединиться так и не удалось. По умолчанию значение параметра `3`.

- `max_connections` – максимальное количество входящих и исходящих соединений по каналам MFTP. По умолчанию значение параметра `100`.

- `send_buff_size` – размер буфера передачи (в байтах). Минимально допустимое значение `1024` (байт), значение по умолчанию `65500` (байт).

- `recv_buff_size` – размер буфера приема (в байтах). Минимально допустимое значение `1024` (байт), значение по умолчанию `65500` (байт).

  Во многих случаях значение `65500` параметров `send_buff_size` и `recv_buff_size` является оптимальным для обеспечения максимальной скорости приема/передачи конвертов транспортным модулем.

- `pingpong` –включение/выключение режима обмена конвертами по каналу MFTP (`yes/no`). По умолчанию значение параметра `yes`.

  Если значение параметра `pingpong` установлено в `yes`, это означает, что сторона, передавшая конверт, позволяет передать конверт другой стороне, то есть узлы обмениваются конвертами поочередно. Если же значение установлено в `no`, то сторона, начавшая передавать конверты, будет их передавать, пока они не закончатся, и только после этого позволит передавать конверты другой стороне.

- `connect_timeout` – интервал (в секундах), в течение которого Координатор будет пытаться установить соединение с удаленным узлом по каналу MFTP. Если по истечении этого интервала соединение не было установлено, то повторные попытки будут происходить через интервал `outenv_timeout` (см. ниже). По умолчанию значение параметра `2` (секунды).

- `wait_timeout` – интервал (в секундах) ожидания активности установленного MFTP-соединения. Если в течение этого интервала узлы, установившие соединение, не обменялись никакой информацией, то данное соединение закрывается. Если в процессе обмена исходящие конверты для удаленного узла были переданы не полностью, то повторные попытки соединения будут происходить через интервал `outenv_timeout` (см. ниже). По умолчанию значение параметра `300` (секунд).

- `outenv_timeout` – интервал (в секундах), в течение которого исходящие конверты для канала, на котором произошла ошибка передачи, не могут быть повторно отправлены. Если на каком-либо канале произошла ошибка передачи (разрыв соединения и т.п.) и для этого канала существуют исходящие конверты, то следующая попытка передачи произойдет через `outenv_timeout` секунд. По умолчанию значение параметра `300` (секунд).

- `ttl_ctl` – время жизни конвертов, содержащих управляющие запросы, в исходящей очереди (в днях). Если по истечении времени `ttl_ctl` конверт не удалось отправить, то он удаляется из очереди и помещается в корзину. По умолчанию значение параметра `10` (дней).

- `ttl_out` – время жизни прикладных конвертов в исходящей очереди (в днях). Если по истечении времени `ttl_out` конверт не удалось отправить, то он удаляется из очереди и помещается в корзину. По умолчанию значение параметра `30` (дней).

- `ttl_trash` – максимальное время хранения конвертов в корзине (в днях). Если время хранения конверта в корзине превышает `ttl_trash`, то конверт удаляется. По умолчанию значение параметра `90` (дней).

- `save_sent` – включение/выключение хранения имен отправленных прикладных конвертов (`yes/no`). По умолчанию значение параметра `no`. Если значение параметра установлено в `yes`, то при успешной отправке конверта в каталоге `out_path/sent` создается файл нулевой длины с именем, идентичным имени отправленного конверта.

Секция [reserv]

Секция `[reserv]` содержит параметры настройки транспортного модуля на Координаторе, работающем в составе кластера горячего резервирования (см. документ «ViPNet Coordinator Linux. Система защиты от сбоев. Руководство администратора»):

- `cmd_port` – номер порта, на котором демон mftpd, находящийся на «пассивном» Координаторе кластера, ожидает соединений от «активного» Координатора по резервному каналу для приема управляющих команд. Данный параметр должен иметь одинаковое значение в файлах конфигурации транспортного модуля на

«активном» и «пассивном» Координаторах. По умолчанию значение параметра `6084`.

- `unpack_timeout` – интервал времени (в секундах), в течение которого «активный» Координатор будет ожидать ответы на команды со стороны «пассивного» Координатора, и в случае отсутствия ответов повторять команды. Этот параметр используется системой удаленного обновления ПО. Кроме того, данный параметр определяет интервал сканирования каталога, заданного параметром `upgrade_path` секции `[upgrade]` (см. «Секция [upgrade]» на стр. 20), для анализа состояния процесса обновления ПО. По умолчанию значение параметра `60` (секунд).

- `transfer_timeout` – интервал времени (в секундах), в течение которого «активный» Координатор будет осуществлять попытки передачи копии MFTP-конверта на «пассивный» Координатор в случае неполного дублирования данного конверта. В течение данного интервала обработка конверта на «активном» Координаторе полностью блокируется. Если по завершении этого интервала конверт не будет передан на «пассивный» Координатор, то продолжится его дальнейшая обработка. По умолчанию значение параметра `60` (секунд).

- `use_reserv` – параметр отвечающий за принудительное включение или отключение режима резервирования конвертов в кластере горячего резервирования. Параметр может принимать значения yes (резервирование на пассивный сервер производится) и no (резервирование на пассивный сервер не производится). Если `use_reserv=no`, резервирование конвертов не производится, независимо от того, в каком режиме запущен демон mftpd (пассивный или активный).

  При отключении резервирования конвертов исходящая очередь конвертов на серверах кластера может быть рассинхронизированна. В этом случае выполнять синхронизацию обоих серверов кластера необходимо будет вручную. Также при выключенном резервировании конвертов на пассивном сервере пришедшее на кластер удаленное обновление ПО применится только активным сервером кластера, пассивный сервер нужно будет обновлять вручную.

  Для корректной работы кластера горячего резервирования с выключенным резервированием конвертов настройки серверов кластера должны выполняться симметрично на обоих серверах кластера.

Секция [debug]

Секция `[debug]` содержит параметры ведения журнала устранения неполадок транспортного модуля (см. документ «ViPNet Coordinator Linux. Руководство администратора»):

- `debuglevel` – уровень протоколирования, число от `-1` до `5`, по умолчанию `3`. Значение параметра `-1` отключает ведение журнала.

- `debuglogfile` – идентификатор, определяющий место хранения журнала. Формат данного идентификатора следующий: `<спецификатор протокола>:<спецификатор URL для данного протокола>`. Подробное описание возможных значений данного параметра приведено в документе «ViPNet Coordinator Linux. Руководство администратора». Значение параметра по умолчанию `file:/var/log/mftp.debug.log`, что соответствует записи журнала в указанный файл.

3

Работа с транспортным модулем

Команды управления транспортным модулем

Как уже уточнялось, транспортный модуль функционирует в качестве программы-демона mftpd в фоновом режиме. По умолчанию после установки ПО ViPNet Coordinator Linux демон mftpd прописывается в стартовых системных сценариях и при загрузке системы стартует после запуска управляющего демона iplir.

При старте и в процессе работы демон mftpd посылает информационные сообщения и сообщения об ошибках в системный журнал syslog. Обычно такие сообщения помещаются системой в файл `/var/log/messages`. Анализируя данные сообщения, можно определить причины некорректной работы транспортного модуля.

Действия, необходимые для управления транспортным модулем, могут быть выполнены с помощью сценария mftp, расположенного в каталоге `/sbin`. Возможны следующие команды:

- `mftp start` – запускает демон mftpd;
- `mftp stop` – останавливает демон mftpd;
- `mftp check` – создает конфигурационный файл `mftp.conf` транспортного модуля (если он не был создан), корректирует его параметры и, если необходимо, перезаписывает его;
- `mftp info [remote_station_address]` – выводит на стандартный вывод информацию об очереди исходящих конвертов (см. «Просмотр информации об очереди исходящих конвертов» на стр. 31);
- `mftp restart` – перезапускает демон mftpd.

Перед первым запуском демона mftpd необходимо сформировать его конфигурационный файл `mftp.conf`, который расположен в подкаталоге `/user` каталога ключевых баз. Для этого необходимо выполнить команду `mftp check`. После этого необходимо откорректировать созданный файл в соответствии с нужными настройками. После того, как соответствующие настройки произведены, можно запускать транспортный модуль командой `mftp start`. Об успешном запуске демона mftpd можно судить по соответствующим сообщениям в системном журнале syslog, а также по наличию соответствующего процесса в системе.

Если в процессе работы появилась необходимость в изменении параметров транспортного модуля, то предварительно его необходимо остановить командой `mftp stop`, а после редактирования файла `mftp.conf` запустить командой `mftp start` для того, чтобы изменения вступили в силу http://www.infotecs.ru.

Просмотр информации об очереди исходящих конвертов

В дистрибутив ПО ViPNet Coordinator Linux входит утилита `mftp_remote_info`, которая предназначена для получения информации об очереди исходящих конвертов транспортного модуля. С помощью этой утилиты можно получить информацию об отправителе, получателях, имени, размере конверта, а также другую информацию как от локального транспортного модуля (работающего на том же узле, что и утилита `mftp_remote_info`), так и от транспортного модуля, работающего на удаленном узле. Обмен информацией между транспортным модулем и утилитой `mftp_remote_info` происходит по протоколу TCP/IP.

Запуск данной утилиты осуществляется командой `mftp info`. В качестве необязательного параметра можно задавать адрес удаленного узла (это может быть IP-адрес или доменный адрес). Если параметр не задан, то адрес узла считывается из файла `/etc/iplirnetpsw` (см. документ «ViPNet Coordinator Linux. Руководство администратора»). Если в указанном файле задан адрес собственного (локального) узла, то информация об очереди исходящих конвертов на локальном узле выводится на стандартный вывод. Если адрес соответствует удаленному узлу, то проверяется присутствие пароля администратора в файле `/etc/iplirnetpsw`. Если пароль администратора отсутствует, то он запрашивается у пользователя в интерактивном режиме. Только в случае ввода правильного пароля администратора можно получить доступ к информации об очереди исходящих конвертов на удаленном узле.

Утилита `mftp_remote_info` выводит информацию об очереди исходящих конвертов в следующем формате:

```
"ID  Name  Size  [Type]  Prio Date  Time  SenderID  SenderName"
"ReceiverID  ReceiverName"
"ReceiverID  ReceiverName"
…
```

где:

- `ID` – уникальный идентификатор конверта в очереди;
- `Name` – имя конверта;
- `Size` – размер конверта в килобайтах;

- `Type` – тип конверта;
- `Prio` – приоритет конверта;
- `Date, Time` – дата и время создания конверта (первого помещения в очередь);
- `SenderID` – идентификатор узла-отправителя;
- `SenderName` – имя узла-отправителя;
- `ReceiverID` – идентификатор узла-получателя;
- `ReceiverName` – имя узла-получателя.

В случае отсутствия конвертов в очереди выводится сообщение «`queue is empty`».

Тип конверта может иметь следующие значения:

- `Mail` – прикладной конверт;
- `Control request` – конверт, содержащий управляющий запрос;
- `Control request answer` – ответ на управляющий запрос;
- `Task receipt` – прикладная квитанция;
- `Transport receipt` – транспортная квитанция.

Настройка канала Local между Координаторами Windows и Linux

Рассмотрим схему сети ViPNet, в которой задействованы два Координатора, один из которых работает под управлением ОС Windows, другой — под управлением ОС Linux. На каждом Координаторе в ЦУСе зарегистрированы Клиенты, для которых он является Сервером-маршрутизатором. Требуется организовать взаимодействие этих Координаторов по локальному каналу (Local), то есть через локальные папки. Обозначим Координатор с ОС Windows как Координатор-W, а Координатор с ОС Linux как Координатор-L.

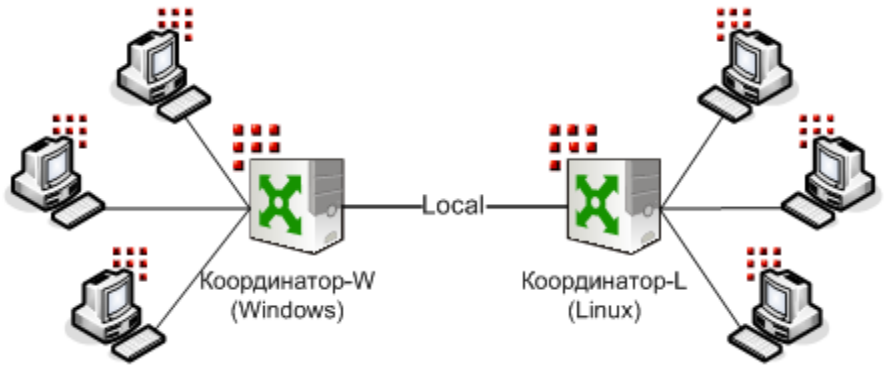

Рисунок 1: Схема к настройке канала Local между Координаторами Windows и Linux

Чтобы организовать локальный канал, надо на каждой стороне открыть доступ к нужной локальной папке (каталогу) и соответствующим образом настроить канал связи с другой стороной. На стороне Координатора-L часть настроек выполняется с помощью программы Samba, которая включена в некоторые дистрибутивы Linux. Если Samba не включена в дистрибутив, необходимо самостоятельно установить эту программу, а также программы smbfs и smbclient.

Для настройки локального канала между Координатором-W и Координатором-L выполните следующие действия:

1 На Координаторе-W стандартными средствами Windows откройте общий доступ к папке, в которую установлен его транспортный модуль, и разрешите полный доступ к этой папке.

Внимание! В качестве имени общего ресурса задайте только одно слово, иначе будет невозможно смонтировать его на Координаторе-L!

2 На Координаторе-L с помощью программы Samba смонтируйте общий ресурс Координатора-W.

Например, для монтирования в ОС Linux Debian 5.0.4 выполните следующую команду:

```
mount -t smbfs //<IP-адрес или имя компьютера Координатора-W>/<имя общего ресурса на Координаторе-W> /mnt/win
```

Примечание. Для уточнения синтаксиса команды в других ОС Linux смотрите документацию на Samba и справочные страницы (man).

3 На Координаторе-L создайте каталог обмена для локального канала (например, `/usr/share/local`) и дайте всем пользователям полные права (чтение, запись и выполнение) на этот каталог и на все вложенные каталоги и файлы с помощью следующей команды:

```
chmod –R a+rwx /usr/share/local
```

4 На Координаторе-L с помощью программы Samba откройте общий доступ к каталогу `local`.

Чтобы открыть доступ, в конфигурационном файле `/etc/smb.conf` создайте раздел (секцию) с именем, под которым будет доступен каталог, и укажите в этом разделе путь к каталогу и разрешение на чтение и запись в этот каталог. Например:

```
[mftp_local]
path = /usr/share/local
read only = no
```

Кроме того, в секции `[global]` установите параметр `security` в значение `share`:

```
[global]
security = share
```

5 На Координаторе-W стандартными средствами Windows подключите общий ресурс `mftp_local` как сетевой диск.

6 На Координаторе-W настройте локальный канал связи с Координатором-L:

- запустите транспортный модуль и нажмите в строке меню кнопку **Настройки**;
- в окне **Настройки** выберите вкладку **Каналы** и дважды щелкните строку с Координатором-L;
- выберите тип канала **Локальный**, нажмите кнопку **Обзор** и выберите подключенный диск с `mftp_local`;
- нажмите кнопку **ОК**.

7 На Координаторе-L настройте локальный канал связи с Координатором-W. Для этого в файле `mftp.conf` произведите следующие изменения:

- В секции `[channel]`, описывающей канал связи с Координатором-W:
  - задайте локальный тип канала (`type= local`);
  - в параметре `path` укажите путь к смонтированной папке транспортного модуля Координатора-W (`path= /mnt/win`);
  - удалите параметры `off_flag`, `call_flag`, `ip`, `call_timeout`, `last_port`, `last_call`.
- В секции `[transport]` укажите путь к папке, в которую Координатор-W будет помещать входящие конверты:

```
local_path= /usr/share/local/Local
```

Внимание! Последняя составляющая в значении параметра `local_path` должна быть указана с учетом регистра (`Local`).

8 Проверьте работу канала.

Для проверки отправьте какой-либо файл с Клиента, зарегистрированного на Координаторе-W, Клиенту, зарегистрированному на Координаторе-L (или

наоборот). Успешная доставка файла будет служить подтверждением того, что локальный канал между Координаторами настроен правильно и работоспособен.