ПАК ViPNet Coordinator HW. Система защиты от сбоев

Руководство администратора

ViPNet Virtual Private Network

infotecs

ФРКЕ.00065-08 32 02, Версия 2.6

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 документе

Для кого предназначен документ

Данный документ предназначен для администраторов, отвечающих за настройку и поддержку кластера горячего резервирования, организованного на базе ПАК ViPNet Coordinator HW1000 или HW-VPNM. В нем описаны назначение и принципы работы системы защиты от сбоев, обеспечивающей устойчивость к сбоям как одиночного ПАК, так и кластера горячего резервирования.

Описание системы защиты от сбоев, функционирующей на одиночном ПАК, приведено в документе «ПАК ViPNet Coordinator HW. Руководство администратора». Данный документ содержит подробное описание системы защиты от сбоев при функционировании в режиме кластера горячего резервирования. В документе приведена типовая схема организации кластера и пример настройки параметров для этой схемы, команды для настройки и управления кластером, а также описаны особенности обновления ПО на кластере.

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).

1

Общие сведения

Назначение системы защиты от сбоев

Система защиты от сбоев предназначена для создания отказоустойчивого решения на базе ПАК ViPNet Coordinator HW. Данная система имеет два режима функционирования:

1. Одиночный режим (режим одиночного ПАК).
2. Режим кластера (режим кластера горячего резервирования ПАК).

Внимание! Кластер горячего резервирования можно организовать только на базе ПАК ViPNet Coordinator HW1000 и HW-VPNM. ПАК ViPNet Coordinator HW100 можно использовать только как одиночный ПАК, поэтому на этом ПАК система защиты от сбоев всегда функционирует в одиночном режиме.

При работе в одиночном режиме, который устанавливается автоматически при установке ПО ПАК ViPNet Coordinator HW, система защиты от сбоев выполняет функции, обеспечивающие постоянную работоспособность основных служб, входящих в состав ПО:

- постоянный контроль состояния служб и ведение статистики использования системных ресурсов;
- обнаружение факта сбоя службы и осуществление последующих попыток восстановления работоспособности сбойного приложения;
- предотвращение внутренних сбоев в работе самой системы защиты от сбоев.

Режим кластера горячего резервирования обеспечивает передачу функций вышедшего из строя ПАК другому (резервному) ПАК. Кластер горячего резервирования состоит из двух взаимосвязанных ПАК, один из которых (активный ПАК) выполняет функции Координатора сети ViPNet, а другой ПАК (пассивный) находится в режиме ожидания. В случае сбоев, критичных для работоспособности ПО ViPNet на активном ПАК, пассивный ПАК переключается в активный режим для выполнения функций сбойного ПАК. При этом сбойный ПАК перезагружается и становится пассивным.

При работе в режиме кластера система защиты от сбоев также выполняет функции одиночного режима, т.е. обеспечивает постоянную работоспособность основных служб, входящих в состав ПО ПАК ViPNet Coordinator HW.

Внимание! Для поддержки режима кластера горячего резервирования узел, который будет разворачиваться на ПАК кластера, необходимо **зарегистрировать в прикладной задаче «ViPNet Failover»** (дополнительно к регистрации в прикладной задаче «Координатор HW1000» или «Координатор HW-VPNM»). Регистрация сетевых узлов в прикладных задачах осуществляется в Центре управления сетью (в ЦУСе) в процессе формирования сети ViPNet.

Принципы работы системы защиты от сбоев в одиночном режиме

В одиночном режиме работы система защиты от сбоев выполняет функционал, связанный с обеспечением работоспособного состояния основных служб ПО ПАК ViPNet Coordinator HW. Данный функционал обеспечивается совместной работой драйвера watchdog и программы-демона failoverd, работающей в фоновом режиме. Драйвер watchdog работает на очень низком уровне и в большинстве случаев сохраняет работоспособность даже в случаях, когда система уже не реагирует на внешние события. При соответствующей настройке (см. параметр `reboot` в секции `[misc]`) программа-демон failoverd при запуске регистрируется в драйвере и периодически опрашивает его, подтверждая работоспособность системы. Если по истечении заданного промежутка времени драйвер обнаруживает, что опроса не было, то он перезагружает систему. Перед этим он делает попытку записать на диск кэш-буферы системы, чтобы не возникло ошибок в файловой системе, однако это не всегда возможно. При корректной остановке программы-демона (например, для изменения настроек системы защиты от сбоев) она сообщает драйверу об этом, и драйвер перестает следить за временем опроса, так что система не будет перезагружена. Такой механизм обеспечивает предотвращение внутренних сбоев в демоне failoverd.

Демон failoverd осуществляет постоянный контроль за работоспособностью следующих служб ПО ViPNet:

- управляющий демон ViPNet (iplircfg);
- транспортный модуль MFTP (mftpd).

При старте ОС демон системы защиты от сбоев failoverd осуществляет старт подконтрольных служб, а также дальнейшее слежение за ними. Контроль работы этих служб осуществляется путем их регистрации в системе защиты от сбоев в момент старта с установкой периода оповещения. В процессе работы контролируемая служба (приложение) периодически определяет свое состояние и оповещает о нем систему слежения. Если контролируемое приложение в течение периода оповещения не сообщило о своем состоянии или сообщило о внутреннем сбое, то система защиты от сбоев идентифицирует сбой приложения и инициирует процедуру восстановления работоспособности этого приложения. Для этого сначала делается попытка корректной остановки сбойного приложения. Если эта попытка оказывается неудачной, то осуществляется принудительная «некорректная» остановка приложения. После этого система защита от сбоев перезапускает остановленное приложение.

В процессе работы демон защиты от сбоев failoverd ведет статистику сбоев для каждого контролируемого приложения, в том числе и для самого себя. Если обнаруживается, что для какого-либо из приложений произошло 5 сбоев подряд, т.е. в течение 5-и попыток восстановления работоспособности приложение не смогло корректно стартовать, то делается вывод о полной неработоспособности приложения. В этом случае, в зависимости от настроек системы защиты от сбоев (см. «Секция [misc]» на стр. 25), производится либо перезагрузка ОС, либо остановка сбойного приложения и прекращение слежения за ним.

Если контролируемое приложение было корректно остановлено администратором системы с помощью соответствующей команды (`iplir stop` или `mftp stop`), то оно производит дерегистрацию в системе защиты от сбоев, слежение за ним отключается. В этом случае для дальнейшей работы администратор должен вручную запустить приложение (соответственно командой `iplir start` или `mftp start`).

Если при запуске демона failoverd выясняется, что какие-либо из подконтрольных демонов были остановлены вручную, то об этом формируется предупреждение в системный журнал syslog. Предупреждение формируется также в случае, если в течение 10-и проверок подряд одного демона он находится в режиме ручной остановки. Чтобы предупреждения попадали в системный журнал syslog, необходимо настроить удаленное протоколирование на основе протокола syslog. Описание настройки удаленного протоколирования см. в документе «ПАК ViPNet Coordinator HW. Руководство администратора».

Принципы работы системы защиты от сбоев в режиме кластера горячего резервирования

Весь кластер, с точки зрения других компьютеров сети, имеет один IP-адрес на каждом из своих сетевых интерфейсов. Этим адресом обладает сервер (ПАК), находящийся в данный момент в активном режиме. Сервер, находящийся в пассивном режиме, имеет другой IP-адрес, который не используется другими компьютерами для связи с кластером. В отличие от адресов активного режима, в пассивном режиме каждый из серверов имеет свой собственный адрес на каждом из интерфейсов, эти адреса для двух серверов не совпадают.

Стек IP на каждом из серверов настраивается администратором таким образом, чтобы после перезагрузки сервер получал свои адреса пассивного режима. При загрузке запускается демон системы защиты от сбоев failoverd, который стартует в пассивном режиме. В этом режиме пассивный сервер периодически посылает в сеть запросы на поиск IP-адресов активного сервера. Если все адреса активного сервера недоступны в течение заданного времени (следовательно, активного сервера нет в сети), то пассивный сервер переходит в активный режим. При этом он устанавливает себе на всех интерфейсах соответствующие адреса активного сервера (адреса, под которыми кластер известен другим компьютерам сети) и входит в цикл проверки своих сетевых интерфейсов.

Активный сервер периодически проверяет работоспособность сети на каждом заданном в настройках интерфейсе следующим образом. Периодически, по истечении заданного в настройках временного интервала анализируется входящий и исходящий сетевой трафик, прошедший через интерфейс. Если разница в количестве пакетов между началом и концом интервала положительна, то считается, что интерфейс функционирует нормально и счетчик отказов для этого интерфейса сбрасывается. Если в течение данного интервала не было послано и принято ни одного пакета, то включается дополнительный механизм проверки, заключающийся в посылке эхо-запросов до стабильных объектов сети. Данный механизм можно использовать не только как дополнительный, но и вместо основного, это настраивается конфигурацией системы защиты от сбоев (см. «Секция [channel]» на стр. 18). Если на какой-либо из интерфейсов в заданное время не приходят ответы на эхо-запросы, счетчик отказов для этого интерфейса увеличивается на единицу. При достижении счетчиком определенного значения фиксируется полный отказ интерфейса. При возникновении полного отказа одного из интерфейсов активный сервер перезагружается. В момент перезагрузки (она занимает, как правило, около 30 секунд)

все адреса активного сервера становятся недоступны, что служит сигналом для пассивного сервера на переход в активный режим. После перезагрузки сервер, как описано выше, переходит в пассивный режим, и при работоспособном втором сервере из пары, который работает теперь как активный, остается в нем.

Внимание! При установке на каком-либо интерфейсе ПАК 1-го режима безопасности блокируется любой открытый (в том числе служебный) трафик на этом интерфейсе. Вследствие этого при проверке работоспособности интерфейсов, находящихся в 1-ом режиме безопасности, с использованием **открытых** объектов сети (см. параметр `testip` в секции `[channel]`) всегда будет фиксироваться отказ этих интерфейсов, что повлечет за собой циклическую перезагрузку серверов кластера.

Чтобы поддерживать конфигурационные файлы и журналы ViPNet на обоих серверах в актуальном состоянии, между серверами создается резервный канал, по которому с активного сервера на пассивный периодически передаются необходимые файлы. Этот канал используется только для передачи файлов с целью резервирования, и его проверка по общей схеме не выполняется. Резервный канал представляет собой соединенные кросс-кабелем адаптеры Ethernet.

Система защиты от сбоев также выполняет резервирование MFTP-конвертов, чтобы обеспечить хранение копий принятых и готовых к отправке конвертов на пассивном сервере. Передача конвертов осуществляется активным сервером по резервному каналу. При переключении пассивного сервера в активный режим сохраненные копии обрабатываются, что практически исключает потерю данных.

Внимание! В файле конфигурации для интерфейса, используемого в качестве резервного канала, необходимо установить режим безопасности 5 (драйвер ViPNet отключен).

Отключение драйвера ViPNet на интерфейсе резервного канала требуется потому, что оба сервера в кластере имеют одни и те же ключи и поэтому не могут общаться между собой по защищенному протоколу. Обмен данными по резервному каналу идет открытым трафиком. Именно поэтому при использовании в качестве резервного канала адаптеров Ethernet не следует подключать их в общую сеть, а следует соединить кросс-кабелем.

Оба сервера в используемой схеме абсолютно равноправны. При начальном запуске кластера активным станет тот сервер, который будет запущен раньше. Однако, поскольку переключение серверов из одного режима в другой занимает некоторое время, то при практически одновременном старте серверов может случиться, что они оба перейдут сначала в пассивный режим, а затем в активный. Для предотвращения такой ситуации серверы постоянно обмениваются по резервному каналу пакетами синхронизации,

содержащими информацию о режиме работы. Если обнаруживается, что оба сервера находятся в активном режиме, то запускается специальная схема выборов, которая однозначно определяет тот сервер, который должен перезагрузиться и перейти в пассивный режим.

2

Настройка системы защиты от сбоев

Общие принципы настройки

Настройка параметров работы системы защиты от сбоев осуществляется путем редактирования файла конфигурации. Для редактирования файла конфигурации используется команда `failover config edit` (см. «Команды группы failover config» на стр. 43).

Файл конфигурации системы защиты от сбоев состоит из нескольких секций. Каждая секция начинается со строки, содержащей имя секции в квадратных скобках. Каждая секция содержит несколько параметров. Строка с параметром начинается с имени параметра, затем идет знак «=» и пробел, затем значение этого параметра. Имена секций и параметров могут повторяться.

Секция [channel]

Каждый сетевой интерфейс, работоспособность которого должна проверять система защиты от сбоев при работе в активном режиме кластера горячего резервирования, описывается секцией `[channel]`.

Секция `[channel]` содержит следующие параметры:

- `device` – имя сетевого интерфейса (eth0, eth1 и т.д.), который описывает эта секция.
- `activeip` – IP-адрес, который данный интерфейс будет иметь в активном режиме.

  В качестве необязательного значения в параметре может указываться маска подсети в нотации CIDR (число значащих бит) или в обычной прямой нотации. Значение IP-адреса должно отделяться от значения маски прямым слэшем «/». Например:

  `activeip= 192.168.201.1/24` – маска задана в CIDR-нотации.

  `activeip= 68.21.12.34/255.255.252.0` – маска задана в прямой нотации.

  Если маска не указана, то будет использовано значение маски, установленное в системе. Независимо от того, в какой нотации была задана маска сети, после перезаписи файла конфигурации `failover.ini` в процессе старта демона failoverd маска будет переведена в CIDR-нотацию и сохранена в файле в таком виде.

Примечание. Явное указание значения маски подсети используется при организации схемы кластера горячего резервирования в условиях ограничений по выделению IP-адресов (см. «Схема организации кластера горячего резервирования в условиях ограничений по выделению IP-адресов» на стр. 35).

- `passiveip` – IP-адрес, который данный интерфейс будет иметь в пассивном режиме.

  В качестве необязательного значения в параметре может указываться маска сети. Требования к формату задания маски аналогичны параметру `activeip`.

- `testip` – IP-адрес маршрутизатора или другого стабильного объекта сети, которому будут посылаться эхо-запросы для проверки работоспособности этого интерфейса. Можно указывать несколько параметров `testip`, в этом случае будут посылаться эхо-запросы на все указанные адреса, и сбоем интерфейса будет считаться ситуация, когда ни от одного из адресов не получен ответ.
- `ident` – текстовая строка, идентифицирующая данный интерфейс.

- `checkonlyidle` – указывает, нужно ли проверять только неактивные интерфейсы. Может принимать значение `yes` или `no`. Если параметр установлен в `yes`, то активный сервер посылает эхо-запросы до адресов, указанных в параметрах `testip`, только в том случае, если за период опроса IP-адресов (параметр `checktime` в секции `[network]`) на данном интерфейсе не было входящих или исходящих пакетов. Если параметр установлен в `no`, то эхо-запросы посылаются всегда. По умолчанию значение параметра `yes`.

Примечание. Все параметры секций `[channel]` интерпретируются только при работе в режиме кластера горячего резервирования.

Чтобы отключить слежение за работоспособностью какого-либо интерфейса, необходимо удалить из файла конфигурации секцию `[channel]`, описывающую этот интерфейс.

Секция [network]

Секция `[network]` описывает различные параметры работы системы защиты от сбоев, относящиеся к посылке пакетов в сеть в режиме кластера горячего резервирования.

Секция `[network]` содержит следующие параметры:

- `checktime` – период опроса IP-адресов (в секундах). На активном сервере проверка работоспособности интерфейса будет проводиться с интервалом `checktime`. На пассивном сервере с интервалом `checktime` будут посылаться запросы на поиск IP-адресов активного сервера.

- `timeout` – время ожидания (в секундах) ответа на запрос (эхо-запрос или запрос IP-адресов), по истечении которого делается вывод о том, что результат запроса отрицательный.

- `channelretries` – число полученных подряд отрицательных результатов, на основании которых делается вывод о неработоспособности интерфейса на активном сервере.

- `activeretries` – число полученных подряд отрицательных результатов, на основании которых на пассивном сервере делается вывод об отсутствии в сети данного IP-адреса активного сервера.

- `synctime` – период времени (в секундах) между посылками пакетов синхронизации по резервному каналу.

- `fastdown` – указывает, нужно ли принудительно останавливать сетевые интерфейсы перед перезагрузкой сервера. Может принимать значение `yes` или `no`. Установка этого параметра в `yes` позволяет быстрее устранить присутствие сервера в сети и дать возможность второму серверу переключиться в активный режим, однако при этом завершение работы работающих сетевых сервисов происходит уже при отключенных интерфейсах и может быть некорректным.

- `afterifconf` – параметр, содержащий команды, выполняемые непосредственно после конфигурирования всех интерфейсов при смене режима. Является необязательным параметром и по умолчанию отсутствует в файле конфигурации.

- `beforeifconf` – параметр, содержащий команды, выполняемые перед конфигурированием всех интерфейсов при смене режима. Является необязательным параметром и по умолчанию отсутствует в файле конфигурации.

Последние два параметра используются для организации схемы кластера горячего резервирования в условиях ограничений по выделению IP-адресов (см. «Схема организации кластера горячего резервирования в условиях ограничений по выделению IP-адресов» на стр. 35).

Примечание. Все параметры секции `[network]` интерпретируются только при работе в режиме кластера горячего резервирования.

Все параметры секции `[network]` рекомендуется делать одинаковыми на обоих ПАК кластера.

Секция [sendconfig]

В секции `[sendconfig]` задаются параметры, контролирующие пересылку файлов с активного сервера на пассивный сервер (с целью резервирования).

Секция `[sendconfig]` содержит следующие параметры:

- `activeip` – адрес, который имеет на резервном канале второй сервер кластера, находящийся в противоположном режиме. Каждый сервер должен иметь в этом поле адрес резервного канала другого сервера.
- `sendtime` – период резервирования (в секундах), т.е. период между попытками переслать файлы.
- `config` – включение/отключение резервирования группы файлов конфигурации (см. ниже).
- `keys` – включение/отключение резервирования группы файлов ключей и справочников (см. ниже).
- `journals` – включение/отключение резервирования группы файлов журналов ПО ViPNet (см. ниже).
- `file` – произвольный файл для резервирования.
- `device` – системное имя интерфейса, который используется для организации резервного канала.
- `port` – номер порта, на котором данный сервер в активном режиме ожидает соединения на резервном канале от пассивного сервера кластера для передачи ему заданных файлов. Значение по умолчанию `10090`.
- `connectport` – номер порта, который данный сервер в пассивном режиме выбирает для соединения на резервном канале с активным сервером кластера для приема запрошенных файлов. Данный параметр может отсутствовать в конфигурационном файле. В этом случае его значение по умолчанию равно значению параметра `port`. Если параметр `port` также не указан, то значение параметра `connectport` равно `10090`.

Примечание. Все параметры секции `[sendconfig]` интерпретируются только при работе в режиме кластера горячего резервирования серверов.

Параметры `config`, `keys` и `journals` могут принимать значение `yes` или `no`. Значение `no` означает отключение резервирования соответствующей группы. По умолчанию эти параметры установлены в значение `yes`.

Внимание! Не рекомендуется отключать резервирование групп `config` и `keys`, т.к. это может привести к некорректной работе ПО ViPNet.

В группу `config` входят следующие файлы конфигурации:

- `iplir.conf` – основной файл конфигурации управляющего демона iplircfg;
- `iplir.conf-<имя интерфейса>` – файлы конфигурации сетевых интерфейсов (кроме интерфейса резервного канала);
- `firewall.conf` – файл конфигурации правил работы с открытой сетью;
- `mftp.conf` – файл конфигурации транспортного модуля MFTP;
- ряд служебных файлов конфигурации;
- файлы *.crg, содержащие контрольные суммы файлов конфигурации.

Примечание. Файл конфигурации интерфейса, используемого для организации резервного канала, не передается, поскольку для этого интерфейса всегда должен быть установлен режим 5, и никаких других настроек для него делать не нужно.

В группу `keys` входит список служебных файлов, относящихся к ключевым базам и справочникам ПО ViPNet. Список файлов может динамически меняться в процессе работы, что отслеживается демоном failoverd автоматически.

В группу `journals` входят следующие файлы:

- журналы пакетов сетевых интерфейсов (кроме интерфейса резервного канала);
- журнал конвертов транспортного модуля MFTP;
- ряд других служебных файлов журналов (список этих файлов не приводится, так как они являются вспомогательными и могут отсутствовать в ряде конфигураций ПО ViPNet).

Перечень файлов, входящих в группы `config`, `keys` и `journals`, определяется демоном failoverd автоматически на активном сервере. Пассивный сервер на каждом цикле резервирования запрашивает состав файлов, входящих в каждую из групп, для которых включено резервирование, и после этого запрашивает передачу файлов.

Внимание! Резервирование файлов, входящих в группы `config` и `keys`, производится только при запущенном на активном сервере управляющем демоне iplircfg. Резервирование файлов `mftp.conf` и `policy.conf` производится только при запущенном на активном сервере демоне `mftpd`. Указанные ограничения позволяют предотвратить передачу на пассивный сервер неправильно отредактированных файлов конфигурации.

Параметры `file` описывают резервирование файлов, не являющихся файлами конфигурации или другими служебными файлами ПО ViPNet, то есть параметры `file` могут содержать только сторонние файлы, не входящие в вышеперечисленные группы, если резервирование этих групп включено.

Примечание. Если какой-либо из файлов, заданных параметром `file`, входит в одну из перечисленных выше групп, для которой включено резервирование, он удаляется из файла конфигурации `failover.ini` демоном failoverd с выводом соответствующего предупреждения в системный журнал.

Можно задавать любое количество параметров `file`, однако следует иметь в виду, что используемый протокол передачи файлов оптимизирован для передачи коротких файлов – как правило, файлов конфигурации, и передача через систему резервирования больших файлов не рекомендуется (максимальный рекомендуемый размер составляет примерно 1 Мбайт). Кроме того, размеры файлов должны быть согласованы с параметром `sendtime` таким образом, чтобы указанного в параметре `sendtime` времени хватило на пересылку файлов.

Если имя файла начинается с символа «/», то оно трактуется как абсолютное, если с другого символа, то оно воспринимается как имя относительно каталога, где находятся базы ViPNet.

Как и в случае групп, пересылка файлов, заданных параметрами `file`, производится по запросу пассивной стороны. Однако, в отличие от передачи групп, активный сервер не формирует никаких списков, передача происходит по запросу на каждый файл, то есть в этом случае список файлов в виде параметров `file` определяется настройками пассивного сервера.

Секция [misc]

Секция `[misc]` содержит вспомогательные параметры как для режима кластера горячего резервирования серверов, так и для одиночного режима работы системы защиты от сбоев:

- `activeconfig` – путь к файлу конфигурации управляющего демона, который будет использоваться в активном режиме горячего резервирования.
- `passiveconfig` – путь к файлу конфигурации управляющего демона, который будет использоваться в пассивном режиме горячего резервирования.
- `maxjournal` – максимальное количество дней, за которое необходимо хранить записи в журнале переключений (см. «Принципы работы системы защиты от сбоев в режиме кластера горячего резервирования» на стр. 13). Является необязательным параметром. Значение параметра по умолчанию `30`.
- `reboot` – указывает, должен ли демон failoverd включать механизм регистрации в драйвере watchdog и должна ли производиться перезагрузка ОС в случае, если какое-либо из контролируемых приложений не может восстановить свою работоспособность (см. «Принципы работы системы защиты от сбоев в одиночном режиме» на стр. 11). Может принимать значение `yes` или `no`. Значение `yes` включает механизм регистрации демона failoverd и перезагрузки системы, `no` – выключает. Параметр является обязательным и интерпретируется независимо от режима работы системы защиты от сбоев.

Примечание. Параметры `activeconfig`, `passiveconfig` и `maxjournal` интерпретируются только при работе в режиме кластера горячего резервирования.

Архитектура системы защиты от сбоев подразумевает использование одной и той же конфигурации ViPNet в активном и пассивном режимах, другие возможности не поддерживаются. Поэтому в параметрах `activeconfig` и `passiveconfig` нужно указывать один и тот же файл – `/etc/iplirpsw`.

Секция [debug]

Секция `[debug]` определяет параметры ведения журнала устранения неполадок демона failoverd (подробнее о журнале устранения неполадок см. документ «ПАК ViPNet Coordinator HW. Руководство администратора»).

Секция `[debug]` содержит следующие параметры:

- `debuglevel` – уровень протоколирования, число от -1 до 5. Для модификаций ПАК с жестким диском значение по умолчанию 3, для модификаций ПАК без жесткого диска значение по умолчанию -1. Значение параметра -1 отключает ведение журнала.

- `debuglogfile` – место хранения журнала, заданное в виде `syslog:<facility.level>`. По умолчанию значение параметра устанавливается в `syslog:daemon.debug`.

3

Схемы организации кластера горячего резервирования

Типовая схема организации кластера горячего резервирования

Пример типовой схемы организации кластера горячего резервирования приведен ниже.

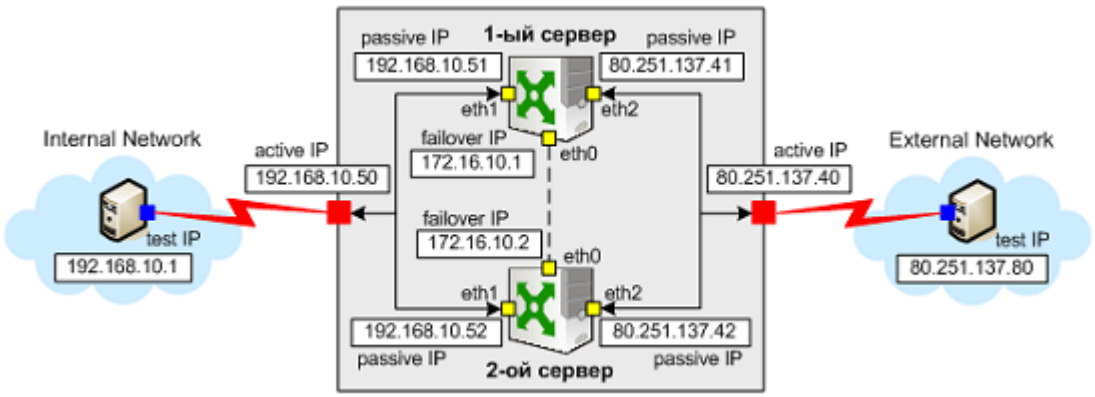

Рисунок 1: Типовая схема организации кластера горячего резервирования

В случае использования типовой схемы адреса, указанные в параметрах `activeip` и `passiveip` (см. «Секция [channel]» на стр. 18), должны **обязательно** находиться в одной подсети. При этом указание значения маски сети является необязательным.

При настройке секций `[channel]` для внутреннего (на схеме eth1) и внешнего (на схеме eth2) интерфейсов параметры `device`, `activeip` и `testip` будут одинаковыми на обоих серверах кластера, а параметры `passiveip` должны быть разными. Таким образом, в типовой схеме в каждой из сетей, в которые включены контролируемые интерфейсы кластера, должны быть выделены три IP-адреса: один для `activeip` и два для `passiveip`. IP-адрес, указанный в параметре `passiveip`, должен совпадать с адресом, который установлен для данного интерфейса командой `inet ifconfig` (описание команды см. в документе «ПАК ViPNet Coordinator HW. Руководство администратора»).

Для интерфейсов, подключенных в одинаковые сети, параметры `ident` должны совпадать на обоих серверах кластера – именно по этим параметрам система защиты от сбоев определяет интерфейсы, которые выполняют одинаковые функции на серверах кластера.

Таблица, приведенная ниже, содержит пример настройки параметров системы защиты от сбоев для типовой схемы организации кластера, представленной на схеме.

Таблица 2. Пример настройки параметров системы защиты от сбоев для типовой схемы организации кластера горячего резервирования

Настройки на первом сервере	Настройки на втором сервере
[channel]	**[channel]**
`device= eth1`	`device= eth1`
`activeip= 192.168.10.50`	`activeip= 192.168.10.50`
`passiveip= 192.168.10.51`	`passiveip= 192.168.10.52`
`testip= 192.168.10.1`	`testip= 192.168.10.1`
`ident= if-1`	`ident= if-1`
`checkonlyidle= yes`	`checkonlyidle= yes`
[channel]	**[channel]**
`device= eth2`	`device= eth2`
`activeip= 80.251.137.40`	`activeip= 80.251.137.40`
`passiveip= 80.251.137.41`	`passiveip= 80.251.137.42`
`testip= 80.251.137.80`	`testip= 80.251.137.80`
`ident= if-2`	`ident= if-2`
`checkonlyidle= yes`	`checkonlyidle= yes`
[network]	**[network]**
`checktime= 10`	`checktime= 10`
`timeout= 2`	`timeout= 2`
`activeretries= 3`	`activeretries= 3`
`channelretries= 3`	`channelretries= 3`
`synctime= 5`	`synctime= 5`
`fastdown= yes`	`fastdown= yes`
[sendconfig]	**[sendconfig]**
`device= eth0`	`device= eth0`
`activeip= 172.16.10.2` (соответствует `failover IP` второго сервера на схеме (см. Рисунок 1 на стр. 28))	`activeip= 172.16.10.1` (соответствует `failover IP` первого сервера на схеме (см. рисунок на стр. 28))

Алгоритм работы на активном сервере следующий. Через каждые `checktime` секунд проводится проверка работоспособности каждого из приведенных в конфигурации

интерфейсов. Если параметр `checkonlyidle` выставлен в `yes`, то анализируется входящий и исходящий сетевой трафик, прошедший через интерфейс. Если разница в количестве пакетов между началом и концом интервала положительна, то считается, что интерфейс функционирует нормально и счетчик отказов для этого интерфейса сбрасывается. Если в течение данного интервала не было послано и принято ни одного пакета, то включается дополнительный механизм проверки, заключающийся в посылке эхо-запросов до ближайших маршрутизаторов. Если параметр `checkonlyidle` выставлен в `no`, то механизм дополнительной проверки используется вместо основного, т.е. каждые `checktime` секунд посылаются пакеты до адресов `testip`. Затем в течение времени `timeout` ожидаются ответы. Если на каком-либо интерфейсе ответа нет ни от одного адреса `testip`, то его счетчик сбоев увеличивается на единицу. Если хотя бы на одном интерфейсе счетчик сбоев не равен нулю, то немедленно посылаются новые пакеты до всех `testip` и ожидается ответ в течение `timeout`. Если в процессе новых посылок на интерфейсе, счетчик сбоев которого не равен нулю, приходит ответ, его счетчик сбоев обнуляется. Если после какой-либо посылки счетчики сбоев на всех интерфейсах становятся равны нулю, то происходит возврат в основной цикл, новое ожидание в течение `checktime` и т.д. Если же после какого-то числа новых посылок счетчик сбоев хотя бы одного интерфейса достигнет значения `channelretries`, то фиксируется полный отказ интерфейса и начинается перезагрузка системы.

Таким образом, максимальное время неработоспособности интерфейса до того, как система защиты от сбоев сделает вывод об этом, равно `checktime + (timeout * channelretries)`.

На пассивном сервере алгоритм немного отличается. Раз в `checktime` секунд производится удаление записей в системной ARP-таблице для всех `activeip`. Затем посылаются UDP-запросы со всех интерфейсов на адреса `activeip`, в результате чего система сначала посылает ARP-запрос и только в случае получения ответа посылает UDP-запрос. После окончания интервала ожидания ответа `timeout` проверяется наличие ARP-записи для каждого `activeip` в системной ARP-таблице, по наличию которой делается вывод о работоспособности соответствующего интерфейса на активном сервере. Если ни от одного интерфейса не было получено ответа, то счетчик сбоев (он один на все интерфейсы) увеличивается. Если хотя бы от одного интерфейса ответ был получен, счетчик сбоев обнуляется. Если счетчик сбоев достигает значения `activeretries`, то производится переключение в активный режим. Максимальное время, проходящее от перезагрузки активного сервера до обнаружения пассивным этого факта, равно `checktime + (timeout * activeretries)`.

Общее время неработоспособности системы при сбое может быть немного больше, чем `checktime * 2 + timeout * (channelretries + activeretries)`. Это связано с тем, что после начала перезагрузки сбойного сервера система переводит его интерфейсы в нерабочее состояние не сразу, а через некоторое время, после остановки других подсистем. Поэтому, например, если проверяются два интерфейса и только на одном произошел сбой, то адрес второго интерфейса будет доступен еще некоторое время, в

течение которого пассивный сервер будет получать от него ответы. Обычно время от начала перезагрузки до выключения интерфейсов не превышает 30 секунд, однако оно может сильно зависеть от быстродействия компьютера и количества работающих на нем сервисов.

Схема организации кластера на базе ПАК HW-VPNM

Кластер горячего резервирования на базе ПАК ViPNet Coordinator HW-VPNM можно организовать только при установке на маршрутизаторах Huawei Secoway USG обоих ПАК режима `transparent`. В этом режиме разрешено прохождение широковещательного трафика между внутренними интерфейсами двух ПАК, которое требуется для корректной работы кластера. При работе маршрутизаторов в режиме `router` прохождение такого трафика невозможно.

Внимание! При установке на маршрутизаторах режима `router` невозможна корректная работа кластера горячего резервирования!

Ниже представлена схема организации кластера на базе ПАК ViPNet Coordinator HW-VPNM. На схеме рассмотрен пример автономной работы ПАК (без использования межсетевого экрана).

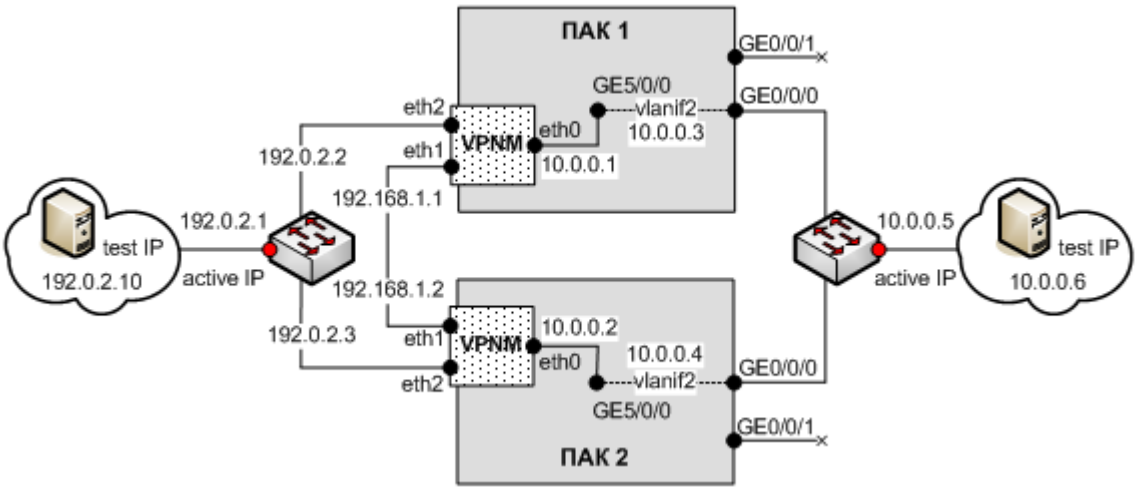

Рисунок 2: Схема организации кластера на базе ПАК ViPNet Coordinator HW-VPNM

Интерфейсы `eth1` модулей VPNM, соединенные кросс-кабелем, используются для организации резервного канала.

Для приведенной схемы кластера необходимо выполнить следующие настройки:

1 Сконфигурировать маршрутизаторы Huawei Secoway USG для работы в режиме `transparent`.

Подробное описание установки этого режима и его настройки приведено в документе «ПАК ViPNet Coordinator HW. Руководство администратора».

Примечание. На обоих маршрутизаторах должна быть создана одна и та же виртуальная сеть, но IP-адреса виртуальных интерфейсов должны быть разными. Согласно примеру на схеме, на ПАК1 следует установить IP-адрес виртуального интерфейса равным 10.0.0.3, на ПАК 2 — 10.0.0.4.

2 На каждом ПАК в файле `failover.ini` задать параметры, приведенные в таблице ниже.

Таблица 3. Пример настройки параметров системы защиты от сбоев для кластера на базе ПАК ViPNet Coordinator HW-VPNM

Настройки на ПАК 1	Настройки на ПАК 2
[channel]	**[channel]**
`device= eth0`	`device= eth0`
`activeip= 10.0.0.5`	`activeip= 10.0.0.5`
`passiveip= 10.0.0.1`	`passiveip= 10.0.0.2`
`testip= 10.0.0.6`	`testip= 10.0.0.6`
`ident= if-0`	`ident= if-0`
`checkonlyidle= yes`	`checkonlyidle= yes`
[channel]	**[channel]**
`device= eth2`	`device= eth2`
`activeip= 192.0.2.1`	`activeip= 192.0.2.1`
`passiveip= 192.0.2.2`	`passiveip= 192.0.2.3`
`testip= 192.0.2.10`	`testip= 192.0.2.10`
`ident= if-2`	`ident= if-2`
`checkonlyidle= yes`	`checkonlyidle= yes`
[network]	**[network]**
`checktime= 10`	`checktime= 10`

Настройки на ПАК 1	Настройки на ПАК 2
timeout= 2	timeout= 2
activeretries= 3	activeretries= 3
channelretries= 3	channelretries= 3
synctime= 5	synctime= 5
fastdown= yes	fastdown= yes
[sendconfig]	**[sendconfig]**
device= eth1	device= eth1
activeip= 192.168.1.2	activeip= 192.168.1.1

Схема организации кластера горячего резервирования в условиях ограничений по выделению IP-адресов

В некоторых случаях, когда выделение трех IP-адресов в одной сети для организации типовой схемы не представляется возможным (использование реальных интернет-адресов, ограничения адресного пространства сети и т.д.), можно использовать схему организации кластера, в которой требуется выделить лишь один IP-адрес для активного режима работы кластера. Пример такой схемы организации кластера приведен ниже.

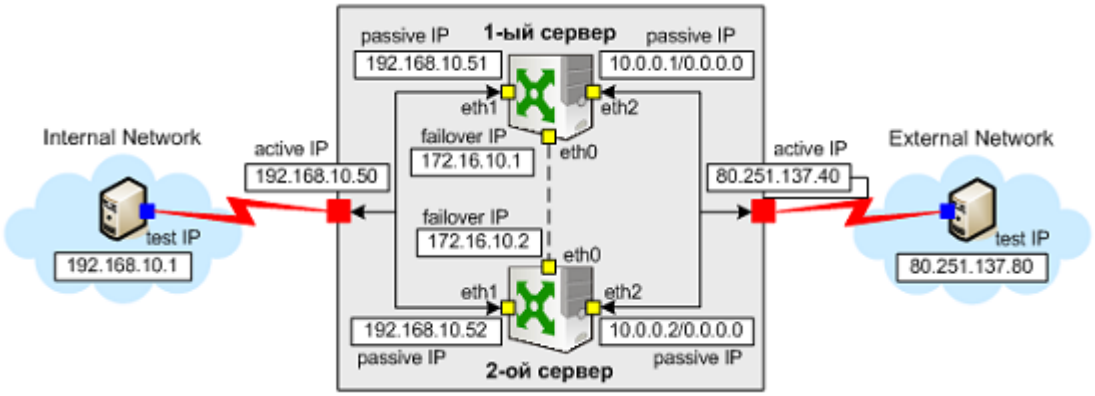

Рисунок 3: Схема включения кластера горячего резервирования в условиях ограничений по выделению IP-адресов

Из схемы видно, что, в отличие от типовой схемы включения, для внешней сети (на схеме External Network, интерфейсы eth2) выделен только один реальный IP-адрес (для активного режима) вместо трех реальных адресов в случае использования типовой схемы. Пассивные адреса выбраны из диапазона частной сети. Подключение к внутренней сети (на схеме Internal Network, интерфейсы eth1) выполнено по типовой схеме.

Общий принцип работы состоит в том, чтобы использовать на пассивном сервере адреса из другой подсети — например, из диапазона частных адресов. Чтобы пассивный сервер мог проверить наличие в сети адресов активного, на пассивном сервере устанавливается

на соответствующих интерфейсах маска подсети 0.0.0.0 и широковещательный адрес 255.255.255.255.

Такая конфигурация интерфейса заставляет пассивный сервер для любого пакета, проходящего через такой интерфейс, пытаться отправить пакет напрямую, запросив в сети MAC-адрес получателя. Таким образом, если пассивный сервер попытается послать пакет активному серверу и маршрутизация на адрес активного будет настроена через интерфейс с маской 0.0.0.0, то пассивный сервер всегда запросит MAC-адрес активного путем посылки ARP-запроса — независимо от того, к каким подсетям принадлежат адреса активного и пассивного серверов, и затем пошлет пакет на этот MAC-адрес. Такой механизм позволяет осуществлять пассивному серверу контроль работоспособности интерфейсов активного по алгоритму, описанному выше, то есть путем проверки наличия ответов на ARP-запросы. При этом важно, чтобы маршрутизация через интерфейсы с маской подсети 0.0.0.0 была настроена только на адреса активного сервера, принадлежащие соответствующим интерфейсам, чтобы такая конфигурация не нарушала работу других интерфейсов.

Примечание. Важным условием при настройке схемы, использующей только один реальный IP-адрес, является явное задание масок сети в файле конфигурации `failover.ini` для параметров `activeip` и `passiveip`. Причем для `activeip` необходимо использовать реальную маску подсети, а для `passiveip` – нулевую маску подсети.

Также с помощью соответствующих команд интерпретатора `inet ifconfig` в качестве основных параметров сетевых интерфейсов необходимо задать IP-адреса пассивного режима с маской 0.0.0.0.

При задании статических маршрутов и шлюза по умолчанию для пассивного сервера в условиях ограничения по IP адресам эти настройки будут сохранены в системе, но не будут применены немедленно, о чем выдается соответствующее предупреждение. Данные настройки будут применены только при переходе сервера в активный режим.

Для настройки правильной маршрутизации при использовании описанной схемы нужно использовать специальный сценарий (bash-скрипт), который будет задавать правильную маршрутизацию в системе как в активном, так и в пассивном режиме. Такой сценарий входит в комплект поставки ViPNet Coordinator HW и называется `change_route.sh`. При инсталляции этот скрипт устанавливается в каталог `/sbin`. Для настройки описываемой схемы, помимо задания IP-адресов для пассивного режима, необходимо в файле конфигурации `failover.ini` прописать вызов данного скрипта для следующих параметров:

- В секции `[network]` в качестве значения параметра `afterifconf`:

```
afterifconf= /sbin/change_route.sh after
```

В этом случае скрипт задания маршрутов будет вызван после конфигурации сетевых интерфейсов демоном failoverd. Для пассивного режима данный скрипт будет устанавливать в системе маршруты на адреса активного сервера.

- В секции `[network]` в качестве значения параметра `beforeifconf`:

  ```
  beforeifconf= /sbin/change_route.sh before
  ```

  В этом случае скрипт задания маршрутов будет вызван до конфигурации сетевых интерфейсов демоном failoverd. Для активного режима данный скрипт будет удалять в системе маршруты, которые были установлены в пассивном режиме при вызове `/sbin/change_route.sh after`.

Передача скрипту необходимой служебной информации производится через набор переменных окружения.

Ниже приведен пример настройки параметров интерфейсов кластера горячего резервирования, соответствующий приведенной выше схеме.

Таблица 4. Пример настройки параметров системы защиты от сбоев для схемы организации кластера в условиях ограничений по выделению IP-адресов

Настройки на первом сервере	Настройки на втором сервере
[channel]	**[channel]**
`device= eth1`	`device= eth1`
`activeip= 192.168.10.50`	`activeip= 192.168.10.50`
`passiveip= 192.168.10.51`	`passiveip= 192.168.10.52`
`testip= 192.168.10.1`	`testip= 192.168.10.1`
`ident= if-1`	`ident= if-1`
`checkonlyidle= yes`	`checkonlyidle= yes`
[channel]	**[channel]**
`device= eth2`	`device= eth2`
`activeip= 80.251.137.40/24`	`activeip= 80.251.137.40/24`
`passiveip= 10.0.0.1/0.0.0.0`	`passiveip= 10.0.0.2/0.0.0.0`
`testip= 80.251.137.80`	`testip= 80.251.137.80`
`ident= if-2`	`ident= if-2`
`checkonlyidle= yes`	`checkonlyidle= yes`
[network]	**[network]**

Настройки на первом сервере	Настройки на втором сервере
`checktime= 10`	`checktime= 10`
`timeout= 2`	`timeout= 2`
`activeretries= 3`	`activeretries= 3`
`channelretries= 3`	`channelretries= 3`
`synctime= 5`	`synctime= 5`
`fastdown= yes`	`fastdown= yes`
`afterifconf= /sbin/change_route.sh after`	`afterifconf= /sbin/change_route.sh after`
`beforeifconf= /sbin/change_route.sh before`	`beforeifconf= /sbin/change_route.sh before`
[sendconfig]	**[sendconfig]**
`device= eth0`	`device= eth0`
`activeip= 172.16.10.2` (соответствует `failover IP` второго сервера на схеме (см. Рисунок 3 на стр. 35))	`activeip= 172.16.10.1` (соответствует `failover IP` первого сервера на схеме (см. рисунок на стр. 35))

Команды управления и настройки системы защиты от сбоев

О командном интерпретаторе

Все операции по управлению и настройке системы защиты от сбоев выполняются с помощью командного интерпретатора ViPNet. Командный интерпретатор может быть запущен как локально с консоли ПАК (COM-консоли или обычной консоли), так и удаленно с других узлов сети ViPNet, связанных с ПАК. Для удаленного подключения к ПАК используется протокол SSH.

Командный интерпретатор может находиться в одном из двух режимов: в режиме пользователя или в режиме администратора. В режиме пользователя недоступны некоторые команды, требующие прав администратора. Подробное описание работы с командным интерпретатором содержится в документе «ПАК ViPNet Coordinator HW. Руководство администратора».

Команды, используемые для администрирования системы защиты от сбоев, разбиты на группы. При описании команд красным цветом выделены команды, доступные только в режиме администратора. Параметры команд указаны в угловых скобках, необязательные параметры заключены в квадратные скобки.

Команды группы failover

- `failover start [<active | passive>]` – запуск демона failoverd. Необязательный параметр `<active | passive>` можно указать только при работе в режиме кластера горячего резервирования, при работе в одиночном режиме ввод параметра невозможен. Если параметр не указан, то демон failoverd запускается в том режиме, в котором он находился до остановки.

  Параметр `<active | passive>` применяется для принудительного переключения демона failoverd в активный (`active`) либо пассивный (`passive`) режим. Возможность принудительного переключения режима должна использоваться с осторожностью.

Внимание! Перед выполнением команды принудительного переключения режима необходимо обязательно убедиться в том, что второй ПАК кластера находится в режиме, противоположном режиму данного ПАК. Следует помнить, что запуск обоих ПАК кластера в активном режиме вызовет конфликт IP-адресов и другие неприятные последствия.

- `failover stop` – остановка демона failoverd.
- `failover view -b <DD.MM.YYYY[.hh.mm.ss]> -e <DD.MM.YYYY[.hh.mm.ss]>` – просмотр журнала переключений кластера горячего резервирования за указанный интервал времени. Первый параметр команды задает начало интервала, второй параметр задает конец интервала.

Примечание. Команда `failover view` доступна только при работе в режиме кластера горячего резервирования.

Команды группы failover show

- `failover show info` – просмотр текущей информации о состоянии системы защиты от сбоев. Выводится следующая информация:
  - версия продукта ПАК ViPNet Coordinator HW;
  - версия демона failoverd;
  - идентификатор и имя ПАК (как узла сети ViPNet);
  - режим работы системы защиты от сбоев (одиночный или режим кластера);
  - локальное время на узле;
  - текущая информация о состоянии управляющего демона, демонов mftpd и failoverd.
- `failover show config` – просмотр файла конфигурации системы защиты от сбоев.

Примечание. Для завершения просмотра файла конфигурации нажмите клавишу «q».

Команды группы failover config

- `failover config mode <single | cluster>` – установка режима работы системы защиты от сбоев в одиночный режим (`single`) либо в режим кластера (`cluster`).

  

  Внимание! Команда `failover config mode` не обеспечивает перезапуск всех служб ViPNet в соответствии с заданным режимом.

  При переключении в одиночный режим появляется предупреждение о том, что все службы ViPNet будут остановлены, и запрашивается подтверждение на выполнение команды. Для дальнейшей работы в одиночном режиме необходимо выполнить команду `failover start`, в результате выполнения которой будет запущен демон failoverd и все остальные службы ViPNet.

  При переключении в режим кластера проверяется текущее состояние локального DHCP-сервера. Если DHCP-сервер запущен и (или) в настройках включен автоматический запуск DHCP-сервера, то появляется предупреждение о необходимости остановить DHCP-сервер и (или) выключить его автоматический запуск, команда не выполняется.

  После переключения в режим кластера необходимо перезапустить демон failoverd последовательным выполнением команд `failover stop` и `failover start`. После перезапуска демона failoverd система защиты от сбоев запустится в пассивном режиме.

- `failover config edit` – редактирование конфигурации системы защиты от сбоев. Запускается текстовый редактор и в него загружается файл конфигурации системы защиты от сбоев. При сохранении файла конфигурации проверяется, был ли он изменен. Если файл изменен, то появляется сообщение о том, что изменения вступят в силу только после перезапуска демона failoverd.

Обновление версии ПО ViPNet Coordinator HW на кластере

В процессе эксплуатации ПАК ViPNet Coordinator HW периодически возникает необходимость обновления версии ПО на более новую. Обновление ПО может быть выполнено удаленно из ЦУСа (путем рассылки обновлений на сетевые узлы) или локально на самом ПАК. Удаленное обновление выполняется на ПАК автоматически и не требует вмешательства администратора. Локальное обновление производится с помощью команды `admin upgrade software usb` с использованием USB-флэш. Выполнение локального обновления ПО при работе в одиночном режиме описано в документе «ПАК ViPNet Coordinator HW. Руководство администратора». Локальное обновление в режиме кластера горячего резервирования имеет ряд особенностей, порядок его выполнения приведен ниже.

Примечание. Так как кластер горячего резервирования может состоять только из ПАК ViPNet Coordinator HW1000 или HW-VPNM, описанный порядок локального обновления ПО при работе в режиме кластера относится только к этим модификациям ПАК.

При работе в режиме кластера горячего резервирования локальное обновление ПО ViPNet Coordinator HW должно выполняться в следующей последовательности:

1. Выключите интерфейс резервного канала с помощью команды `inet ifconfig <интерфейс> down` и отсоедините кросс-кабель от компьютеров.

2. Обновите ПО на пассивном ПАК с помощью команды `admin upgrade software usb` (так же, как при работе в одиночном режиме). Информацию о текущем режиме ПАК можно получить с помощью команды `failover show info` (см. «Команды группы failover show» на стр. 42).

3. После успешного обновления перезагрузите пассивный ПАК (выполните команду `machine reboot`) и убедитесь в его стабильной работе:

   - Проверьте текущее состояние служб ViPNet с помощью команды `failover show info`. Все службы должны быть запущены, система защиты от сбоев должна работать в режиме кластера.
   - В течение некоторого времени (около 15 минут) последите за работой пассивного ПАК и убедитесь, что он не перезагружается.

4. Перезагрузите активный ПАК (выполните команду `machine reboot`). В результате пассивный ПАК (с обновленным ПО) перейдет в активный режим, а ПАК со старой версией ПО окажется в пассивном режиме.

5. Обновите ПО на пассивном ПАК (выполните команду `admin upgrade software usb`).

6. После успешного обновления перезагрузите пассивный ПАК и убедитесь в его стабильной работе (как на шаге 3).

7. Соедините компьютеры кросс-кабелем и включите интерфейс резервного канала с помощью команды `inet ifconfig <интерфейс> up`.

8. Убедитесь, что резервный канал функционирует нормально. Для этого измените какую-либо настройку в файле конфигурации на активном ПАК (например, в файле `mftp.conf`) и через некоторое время проверьте, что эти же изменения появились на пассивном ПАК. Чтобы изменения попали на пассивный ПАК, необходимо включить резервирование группы файлов конфигурации.

6

Просмотр информации о работе системы защиты от сбоев

Текущее состояние системы защиты от сбоев

Для просмотра информации о текущем состоянии системы защиты от сбоев используется команда `failover show info`.

Информация о текущем состоянии системы защиты от сбоев включает в себя:

- версию ПО ViPNet в составе ПАК ViPNet Coordinator HW1000 (или HW-VPNM) и версию демона failoverd;
- идентификатор и имя сервера (как узла сети ViPNet);
- режим работы системы защиты от сбоев (одиночный или режим кластера горячего резервирования);
- локальное время на сервере;
- текущую информацию о состоянии управляющего демона, демонов mftpd и failoverd.

Если демон failoverd остановлен, то выводится только сообщение о режиме работы:

```
Failover is in <single|cluster> mode
```

Если демон failoverd запущен, то при работе в одиночном режиме выводится следующая информация:

```
Versions: ViPNet 3.6.0 (475), daemon 1.4 (9)
Workstation configured for ID 29A0022 (Coordinator_HW)
The workstation works in a single mode of protection against failures
Workstation time (utc: 1204719868) Thu Mar 25 13:07:10 2010
```

`failover mode   * single` – режим работы системы защиты от сбоев;

`failover uptime * 6d  0:23` – время работы демона failoverd;

`total cpu       * 100%` – общая загрузка CPU в системе;

`failover state  * works` – состояние демона failoverd;

```
failover cpu    * 0%          – загрузка CPU демоном failoverd;
iplir state     * works       – состояние управляющего демона;
iplir cpu       * 46%         – загрузка CPU управляющим демоном;
mftp state      * works       – состояние демона mftpd;
mftp cpu        * 40%         – загрузка CPU демоном mftpd.
```

Если демон failoverd запущен, то при работе в режиме кластера выводится следующая информация:

```
Versions: ViPNet 3.6.0 (475), daemon 1.4 (9)
Workstation configured for ID 29A0022 (Coordinator_HW)
Workstation works in a cluster mode of protection against failures
Workstation time (utc: 1204638024) Mon Mar 29 17:35:30 2010

                * local       * remote
failover mode   * active      * passive
failover uptime * 3d  5:26    * 0d  0:00
total cpu       * 80%         * 0%
failover state  * works       * unknown
failover cpu    * 7%          * 0%
iplir state     * works       * unknown
iplir cpu       * 0%          * 0%
mftp state      * works       * unknown
mftp cpu        * 66%         * 0%
```

Значения столбцов таблицы в этом случае аналогичны значениям, выводимым для одиночного режима. Отличие состоит в том, что данные выводятся для обоих ПАК кластера. Обозначения `local` и `remote` соответствуют локальному ПАК (с которого был произведен запрос информации) и второму компоненту кластера. При работе в режиме кластера команду `failover show info` можно выполнять как на активном, так и на пассивном ПАК.

При выводе информации используются следующие обозначения режимов:

- `single` – одиночный режим работы;
- `active` – активный режим кластера горячего резервирования;

- `passive` – пассивный режим кластера горячего резервирования.

Используемые обозначения состояний:

- `works` – приложение работает корректно (с точки зрения системы защиты от сбоев);
- `stopped` – приложение остановлено пользователем;
- `unknown` – состояние приложения неизвестно. Данное состояние может быть установлено в случае, если был идентифицирован сбой контролируемого приложения, попытка его перезапуска, но данных о его корректном старте пока нет.

Журнал переключений

В журнале переключений фиксируются события, происходящие в системе защиты от сбоев при ее работе в режиме кластера горячего резервирования серверов. Для просмотра записей из журнала переключений необходимо выполнить команду `failover view`, задав в параметрах нужный интервал времени:

```
failover view -b <DD.MM.YYYY[.hh.mm.ss]> -e <DD.MM.YYYY[.hh.mm.ss]>
```

где

`-b <DD.MM.YYYY[.hh.mm.ss]>` задает начало временного интервала,

`-e <DD.MM.YYYY[.hh.mm.ss]>` задает конец временного интервала.

В результате выполнения данной команды на текущую консоль выводится следующая информация:

- версия ПО ViPNet Coordinator Linux и демона failoverd;
- идентификатор и имя сервера в сети ViPNet;
- режим работы системы защиты от сбоев (всегда режим кластера горячего резервирования);
- локальное время на сервере;
- список записей из журнала переключений, попадающих в заданный интервал времени.

Информация выводится в следующем формате:

```
Veiw journal of failover switching
Versions: ViPNet 3.6.0 (475), daemon 1.4 (9)
Workstation configured for ID 29A0022 (Coordinator_HW)
The workstation works in a cluster mode of protection against failures
Workstation time (utc: 1174916969) Mon Mar 29 17:49:29 2010

09 Mar 2010 12:51:42  <P_START> Start demon failover in passive mode
22 Mar 2010 12:27:27  <A_START> Start demon failover in active mode
22 Mar 2010 14:10:35  <A_START> Start demon failover in active mode
```

```
22 Mar 2010 15:30:46  <BOOT> Boot the system
23 Mar 2010 11:09:07  <SWITCH> Switch server from passive mode to active
mode
```

Первый столбец содержит время и дату события, а второй столбец – идентификатор и полное наименование события.

Если в заданный интервал времени не попало ни одного события, то выводится сообщение:

```
There are no records in journal of switchings
```

При выводе информации используются следующие обозначения событий:

`<BOOT> Boot the system` – загрузка ОС;

`<P_START> Start demon failover in passive mode` – старт в пассивном режиме;

`<A_START> Start demon failover in active mode` – старт в активном режиме;

`<SWITCH> Switch server from passive mode to active mode` – переключение серверов.

Команда `failover view` доступна только в случае работы системы защиты от сбоев в режиме кластера горячего резервирования серверов. Команда доступна на обоих серверах кластера.

Работа кластера горячего резервирования совместно с коммутационным оборудованием

На практике часто встречаются схемы подключения ПАК, объединенных в кластер горячего резервирования, к различному коммутационному оборудованию. Это могут быть коммутаторы (switch), маршрутизаторы (router) и другое оборудование. Конфигурация данного оборудования может напрямую влиять на корректную работу механизмов кластера горячего резервирования. В частности, на коммутационном оборудовании администратором могут быть заданы настройки, запрещающие прохождение тех или иных сетевых пакетов, среди которых могут оказаться служебные пакеты, необходимые для правильного функционирования ПО ViPNet в режиме кластера горячего резервирования. В связи с этим при организации схем включения кластера горячего резервирования необходимо проверить соответствующие настройки сетевого коммутационного оборудования:

- Должны пропускаться ICMP эхо-запросы с IP-адресов активного ПАК до всех заданных IP-адресов `testip` (см. «Секция [channel]» на стр. 18) и ответы на них.
- Должны пропускаться ARP-запросы с IP-адресов пассивного ПАК для IP-адресов активного ПАК и ответы на них.

Указанные правила касаются всех контролируемых сетевых интерфейсов (для которых существует секция `[channel]` в файле `failover.ini`) в схеме кластера горячего резервирования .