И. И. Зензин

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ОТКРЫТЫХ РАСПРЕДЕЛЕННЫХ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ НА ОСНОВЕ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ «ГОРЯЧЕГО» РЕЗЕРВИРОВАНИЯ СЕРВЕРОВ[1]

Введение

Распределенные вычислительные системы все больше завоевывают популярность в России и во всем мире. Их широкое распространение и глобализация связей увеличивают спрос на непрерывный уровень обслуживания. От стабильного и постоянного предоставления сервиса начинает зависеть все большее число пользователей. Даже короткий перерыв или сбой в работе может быть чреват финансовыми потерями или ущербом для деловой репутации компании, атаки на такие компании чаще всего бывают заранее подготовлены и связаны с атаками типа «Отказ в обслуживании».

На сегодняшний день существует целый ряд технологий, реализующих процесс «горячего» резервирования серверов безопасности. Ввиду многообразия этих технологий перед администратором безопасности стоит нетривиальная задача выбора той технологии, которая соответствовала бы довольно значительному набору требований, предъявляемых при реализации автоматизированных систем различного назначения. Статья посвящена анализу двух из существующих технологий «горячего» резервирования серверов безопасности.

1. Защита распределенной вычислительной системы с применением отказоустойчивой конфигурации Cisco

Для повышения отказоустойчивости брандмауэров, защищающих сеть от атак, компания Cisco предлагает использовать технологию Failover. По этой технологии возможно объединить два идентичных межсетевых экрана PIX, которые будут работать в паре в режимах Active/Standby Failover или Active/Active Failover. Режим Active/Standby Failover представляет собой отказоустойчивое решение, при котором второстепенный межсетевой экран берет на себя всю нагрузку в случае серьезных атак с отказом доступа на активный межсетевой экран, вследствие которых брандмауэр может уйти в режим перезагрузки.

Active/Active Failover режим позволяет балансировать нагрузку на брандмауэры, что делает их устойчивее к различным атакам на компьютерную сеть организации.

Комплексы Cisco ASA 5500 поддерживают Failover-технологию. Кроме того, ASA 5500 позволяет реализовать технологию VPN-кластеризации [1]. С ее помощью несколько комплексов объединяются в единый виртуальный VPN-кластер с балансировкой нагрузки между комплексами в кластере. Крушение одного из комплексов не приведет к остановке VPN-сервисов, следующий комплекс продолжит предоставлять сервис без каких-либо последствий для клиентов.

Основной и второстепенный межсетевые экраны соединяются друг с другом по Failover-каналу, по которому происходит обмен сообщениями о состоянии работы межсетевых экранов и синхронизация конфигурации. В комплексе ASA 5500 для канала задействуются по одному Ethernet-интерфейсу. Межсетевые экраны PIX также позволяют не занимать Ethernet-интерфейсы для Failover-канала, а использовать для этого Serial-интерфейсы, соединенные друг с другом Serial Failover кабелем.

Межсетевые экраны PIX (или комплексы ASA 5500) возможно дополнительно объединить Stateful Failover каналом, по которому передаются состояния соединений (ARP, NAT, IPSec и

[1] Статья написана в рамках НИР «Обеспечение безопасности информации в открытых распределенных вычислительных системах», заданной Государственным контрактом № П2397 в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 годы.

GTP таблицы, состояния TCP, UDP и HTTP соединений) с основного межсетевого экрана второстепенному [2]. В случае сбоя основного брандмауэра второстепенный переходит в активное состояние с восстановлением всех соединений, находящихся на основном брандмауэре до сбоя. Так как для Stateful Failover канала задействуется по одному Ethernet-интерфейсу, на каждом оборудовании межсетевые экраны PIX должны иметь в своем составе не менее трех Ethernet-интерфейсов.

2. Технология «горячего» резервирования серверов ViPNet Failover

Режим кластера «горячего» резервирования предназначен для «горячей» замены функций одного из серверов с ПО ViPNet другим сервером в случае сбоя первого. Кластер «горячего» резервирования серверов состоит из двух компьютеров, один из которых («активный») выполняет функции сервера (координатора) ViPNet, а другой находится в режиме ожидания («пассивный»). В случае сбоев, критичных для работоспособности ПО ViPNet на «активном» координаторе, «пассивный» переключается в «активный» режим, выполняя функции сбойного сервера. При работе в режиме кластера «горячего» резервирования система защиты от сбоев также выполняет и функционал одиночного режима работы, т. е. обеспечивает постоянную работоспособность основных служб, входящих в состав ПО ViPNet Coordinator Linux.

Весь кластер, с точки зрения других компьютеров сети, имеет один IP-адрес на каждом из своих сетевых интерфейсов. Этим адресом обладает сервер, 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 [3].

В случае использования типовой схемы организации кластера «горячего» резервирования серверов все используемые IP-адреса (один общий адрес для «активного» режима, два адреса для «пассивного» режима) должны находиться в одном адресном пространстве (сети). В случае, если возможности по выделению адресов ограничены, может применяться схема, рассчитанная на выделение только одного реального IP-адреса на интерфейс для активного режима. Стек IP на каждом из серверов настраивается 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 (и, значит, 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 [3]. 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 ближайших маршрутизаторов. Если на каком-либо из интерфейсов в заданное время не приходит ответ от маршрутизатора, 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, становится в «пассивный» режим и при работоспособном втором сервере из пары, который работает теперь как активный, остается в нем.

События, связанные с работой режима «горячего» резервирования серверов, записываются демоном failoverd в базу данных, которая называется «журнал переключений». В нее попадают следующие типы событий [3]:

- Загрузка системы. Это событие записывается при старте демона failoverd при загрузке ОС;
- Старт в «пассивном» режиме. Это событие записывается при старте демона failoverd вручную в «пассивном» режиме;
- Старт в «активном» режиме. Это событие записывается при старте демона failoverd вручную в «активном» режиме;
- Переключение серверов. Это событие записывается при переключении сервера из «пассивного» режима в «активный».

Журнал переключений ведется на каждом из серверов кластера. С активного сервера журнал периодически передается на пассивный сервер, заменяя его журнал. При нормальной работе кластера журнал будет содержать только события переключения режима, так как события старта сервера в «пассивном» режиме будут теряться при получении журнала с активного сервера. Если сервер стартует в «пассивном» режиме, а затем, не получив журнал переключений от активного сервера, сам становится активным, то журнал будет содержать события старта в «пассивном» режиме либо загрузки системы, из чего можно заключить, что второй сервер кластера неработоспособен (завис или отключен).

Для того чтобы поддерживать конфигурационные файлы и базы 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 системой резервирования, и его проверка по общей схеме не выполняется. Резервный канал может представлять собой соединенные кросс-кабелем платы Ethernet (это предпочтительно) или нуль-модем [3]. Кроме того, система защиты от сбоев при каждом своем запуске включает режим резервирования MFTP-конвертов демона mftpd. Система резервирования MFTP-конвертов обеспечивает хранение копий принятых и готовых к отправке конвертов на пассивном сервере. Передача конвертов осуществляется активным сервером по резервному каналу. При переключении данного сервера в «активный» режим сохраненные копии обрабатываются, что практически исключает потерю данных. Включение системы резервирования MFTP-конвертов обеспечивается посредством запуска демона mftpd с соответствующими ключами для каждого из режимов. Если используется поддержка SNMP, то при запуске на активном сервере демона ViPNet на компьютер, который указан в файле конфигурации SNMP как Trap sink, посылается соответствующее событие (Trap). Эта возможность может быть использована администратором для оповещения о сбое одного из серверов.

Оба сервера в используемой схеме абсолютно равноправны. При начальном запуске кластера активным станет тот сервер, который будет запущен раньше. Однако поскольку переключение сервера из одного режима в другой занимает некоторое время, то при практически одновременном старте серверов может случиться, что оба они 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 сервера. Если обнаруживается, что оба сервера находятся в «активном» режиме, то запускается специальная схема выборов, которая однозначно определяет один из серверов, который должен перезагрузиться и перейти в «пассивный» режим.

Заключение

Предложенное в работе описание двух технологий «горячего» резервирования серверов безопасности позволит администраторам открытых распределенных вычислительных систем детальным образом понять возможности по резервированию серверов одним из двух рассмотренных способов. Использование технологий «горячего» резервирования серверов, расположенных на границах открытых распределенных систем, даст возможность улучшить показатели отказоустойчивости, избежать длительной недоступности системы, подверженной атакам вида «отказ в обслуживании». Применение технологий «горячего» резервирования позволит специалистам, администрирующим открытые распределенные вычислительные системы, добиться высокого уровня доступности сервисов, функционирующих в подобных системах.

Изложенные результаты получены в рамках реализации ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009—2013 годы.

СПИСОК ЛИТЕРАТУРЫ:

1. The Cisco ASA 5500 as a Superior Firewall Solution. 2006 г. URL: http://cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/prod_white_paper0900aecd8058ec85.pdf.
2. How Failover Works on the Cisco Secure PIX Firewall. 2006 г. URL: http://www.cisco.com/application/pdf/paws/5220/failover.pdf.
3. ViPNet Coordinator Linux. Система защиты от сбоев / ОАО ИнфоТеКС. М., 2010. — 28 с.