Functional Specification

WAY4™ HA Cluster. Функциональная спецификация

03.51.30

13.04.2020

СОДЕРЖАНИЕ

В документации используются следующие обозначения:

- названия полей экранных форм выделяются *курсивом*;
- комбинации клавиш приводятся в угловых скобках, например, <Ctrl>+<F3>;
- названия кнопок экранных форм и вкладок приводятся в квадратных скобках, например, [Approve];
- последовательность выбора пункта в меню пользователя или контекстном меню отображается с помощью стрелок следующим образом: "Issuing → Contracts Input & Update";
- последовательность выбора пункта в системном меню отображается с помощью стрелок следующим образом: Database => Change password;
- различные переменные значения, например, имена каталогов и файлов, а также пути к файлам, варьируемые для каждой локальной машины, приводятся в угловых скобках, например, <OWS_HOME>.

Предостережения и информационные сообщения размечаются следующим образом:

Предостережения в связи с возможностью совершения неправильных действий.

Сообщения, содержащие информацию о важных особенностях, дополнительных возможностях или оптимальном использовании некоторых функций системы.

1. Используемые термины

HA – High availability – высокая доступность.

Источники операций (**Operation source)** – пользовательские приложения (DBM, WAY4M, WAY4WEB), Web-сервисы, Online и Offline каналы, Datamart и т. д.

Операции (Operations) – бизнес-транзакции.

Критичная операция – операция, требующая обеспечения высокой доступности в соответствии с бизнес-требованиями (см. "Обработка операций").

Некритичная операция – операция, не требующая обеспечения высокой доступности в соответствии с бизнес-требованиями.

Узел (**Node)** – один из экземпляров базы данных системы WAY4 (WAY4 DB).

HA-Кластер (HA Cluster) – решение по резервированию БД, включающее одну первичную базу, одну или несколько вторичных. В простейшем случае, вторичная база только одна.

Первичный узел/ база данных/БД (Primary node/database/db) – база данных, обрабатывающая любой тип операций.

Вторичный узел/ база данных/БД (Secondary node/database/db) – клон/ копия первичного узла/базы данных в HA Cluster БД.

Процесс синхронизации (Synchronisation process) – передача измененных данных из одной базы данных (БД-источник) в другую (БД-приемник).

Синхронизация (Synchronisation) – устранение различий между копиями данных БД WAY4 на узле-источнике и узле-приемнике в результате процесса синхронизации.

Недоступные изменения – часть измененных данных, которые не могут быть переданы в узел-приемник по причине недоступности узла-источника.

Транспорт (Transport) – часть процесса синхронизации, отвечающая за захват изменений данных на узле-источнике, их преобразование и доставку на другой узел кластера.

Безопасная операция (Safe operation) – операция:

- Воспроизводимая – может быть правильно воспроизведена на других узлах в результате синхронизации;
- Самодостаточная – включает в себя все необходимые элементарные шаги и является логически независимым пакетом изменений с точки зрения бизнеса;
- Бесконфликтная – для всех выполненных изменений данных существуют соответствующие процедуры разрешения конфликтов при синхронизации.

Безопасность операции определяется реализацией, а не бизнесом.

Критичные для бизнеса операции реализуются как безопасные.

Если результаты операции записываются только в журнал выполнения процессов (Process Log), то данная операция уже является безопасной.

Небезопасная операция – операция, не являющаяся безопасной. В результате доработок системы WAY4 небезопасные операции могут становиться безопасными.

In-Flight-операция – операция, начавшаяся на некоторой БД, но не завершившаяся по причине недоступности БД.

2. Введение

WAY4™ HA Cluster предназначен для обеспечения высокой доступности системы WAY4 за счет увеличения количества узлов – экземпляров БД системы WAY4.

Возможные причины недоступности системы WAY4:

- Плановые, включая обновление системы;
- Внеплановые, включая недоступность сервера и тайм-ауты.

WAY4™ HA Cluster позволяет сократить время недоступности до одной минуты в каждом случае плановой или внеплановой недоступности.

2.1 Ситуации, в которых обеспечивается высокая доступность

Для обеспечения работоспособности серверов баз данных следует учитывать возможные плановые, либо внеплановые причины простоя.

К плановым работам, требующим отключения узла или вызывающим его недоступность, относятся:

- Установка обновлений программного обеспечения (WAY4, Oracle, OS и т.д.).
- Обновление оборудования.
- Физическое перемещение оборудования.

Условия обеспечения работоспособности системы в этих случаях приведены в разделе "Проведение плановых работ".

К внеплановым причинам недоступности узла могут относиться:

- Сбои в работе узла (Computer failure).
- Сбои хранения данных (Storage failure).
- Нарушение целостности данных (Data corruption).
- Критическое снижение производительности БД Oracle (Oracle DB degradation).
- Отказы сети.
- Сбои в работе внешнего оборудования (например, отключение электропитания или неисправные системы охлаждения).
- Человеческий фактор (например, действия персонала, приводящие к неработоспособности БД/оборудования).

В таких случаях работоспособность системы обеспечивается при условии, что внеплановый сбой произошел только на одном узле, и остальные узлы кластера работают в штатном режиме.

Для обеспечения доступности серверов баз данных и прочего оборудования в случаях внеплановых простоев, необходимо организовать его размещение и подключение таким образом, чтобы свести к минимуму, а по возможности исключить риск одновременной

неработоспособности всех узлов кластера. Например, размещать узлы кластера в различных зданиях или в нескольких географически удаленных центрах обработки данных.

2.2 Обработка операций

Список **критичных операций**, для которых обеспечивается высокая доступность:

- Эквайринг:
  - Все исходящие online-транзакции с банкоматов, POS-терминалов, импринтеров, киосков самообслуживания, электронной коммерции, в том числе:
    - P2P;
    - Торговые операции (Retail); вторичные online-транзакции (отмены, Sales Completions, (Tibs) adjustments и т. д.);
  - Автоматические отмены бизнес-транзакций и отмены повторов;
  - Инкассация банкоматов;
  - Выгрузка проведенных транзакций на POS-терминалах (закрытие цикла, online, offline, получение BatchId для нового финансового цикла терминала);
  - Транзакции электронной коммерции;
  - Динамическая смена ключей;
  - Отслеживание статусов оборудования банкоматов;
  - Отслеживание ограничителей активности (только по транзакциям, входящим в список критичных функциональных возможностей);
  - Учет программы лояльности (*);
  - Запрос на получение одноразовых паролей на банкомате;
  - WS API (*);
- Эмиссия:
  - Входящие авторизации, в том числе:
    - Запросы баланса;
    - Переводы средств по постоянным платежным поручениям;
    - Вторичные входящие авторизации (reversals, adjustments, advices etc);
    - Чиповые авторизации;
    - P2P;
    - Запрос мини-выписки;
    - Формирование мини-выписки;
  - Отслеживание ограничителей транзакционной активности (только по транзакциям, входящим в список критичной функциональности);
  - Отслеживание неправильного ввода PIN;

    - SMS-нотификация;
    - Блокировка карты;
    - Поддержка клиента и поиска ошибок, как минимум, по только что совершенным транзакциям;
    - 3d-secure-транзакции (генерация и использование одноразовых паролей);
    - Учет программы лояльности (*);
    - Запросы в RBS (*);
    - Загрузка заявлений на изменение значений классификаторов;
    - Загрузка курсов валют;
    - WS API (*);
- Транзитные операции (Switch):
    - Транзитные авторизации, в том числе:
        - вторичные транзитные авторизации;
        - SAF.

Остальная функциональность считается **некритичной**, и по ней допускается меньшая степень доступности. Примеры некритичной функциональности:

- Финансовая обработка документов;
- Прием и отправка файлов, включая выгрузку, загрузку документов и заявлений;
- Ежедневные процедуры;
- Выпуск новых и повторный выпуск карт;
- Обработка заявлений. Следует помнить, что ввод нового заявления через online-каналы может являться критичной функциональностью.
- Формирование отчетов.

Список критичных операций может расширяться.

> (*) – возможность и сроки реализации критичной операции, как безопасной, должны быть исследованы для каждого конкретной поставки.

2.3 Перечень автоматизированных рабочих мест (АРМ) и приложений дистанционного банковского обслуживания (ДБО)

Решение позволяет оказывать поддержку клиентов и в случае недоступности первичного узла с использованием следующих приложений:

- GUI APM:

    - Customer Service Screen;
- Web-based APM:
    - Customer Service Workbench(**);
    - Merchant Service Workbench(**);
    - Merchant Portal (**);
- Приложения ДБО:
    - Web-banking(**)
    - Mobile-banking(**)

(**) – доступность функциональности приложения на вторичных узлах должна быть исследована для каждой конкретной поставки.

3. Описание решения HA Cluster

3.1 Архитектура

Высокая доступность системы для обработки критичных операций обеспечивается за счет использования двух и более экземпляров БД системы WAY4. Эти экземпляры называются узлами.

3.1.1 Виды узлов

Виды узлов:

- Первичный — экземпляр WAY4 DB, на котором выполняются любые операции, включая настройку конфигурации WAY4 (далее "конфигурация").
- Вторичный — экземпляр WAY4, на котором могут выполняться:
  - Все критичные операции;
  - Все операции чтения, например отчеты, выгрузки, Web-сервисы типа GET. Это позволяет снизить нагрузку на первичный узел.

3.1.2 Принципы построения решения

Основные положения:

1. В любой момент времени только одна БД в HA Cluster считается эталонной – Primary.
2. Нет отличий между операциями BackOffice и Online. Поскольку операции самообслуживания становятся все более востребованными и популярными, граница между операциями BackOffice и Online стирается. Часть операций BackOffice становятся критичными.
3. Критичные операции реализуются как безопасные. При расширении списка критичных операций в результате доработки системы так же расширяется список безопасных операций.
4. Вторичный узел (Вторичная БД) обрабатывает только безопасные операции, и любая безопасная операция может быть выполнена на вторичном узле.
5. Операции изменения данных конфигурации всегда являются небезопасными.
6. На логическом уровне данные в первичном узле и вторичных узлах одинаковые. На физическом уровне допускается различие – записи в экземплярах БД могут иметь разные идентификаторы.

3.1.3 Синхронизация данных

Способы синхронизации данных:

1. Все модификации данных, сделанные на первичном узле, воспроизводятся на вторичных узлах "как есть". Такая синхронизация называется "сырой" (Raw data synchronisation) и выполняется только в том случае, если первичный и вторичный узел имеют одну и ту же версию WAY4 DB.
2. Все операции, выполненные на вторичном узле, воспроизводятся на других узлах. Такая синхронизация называется «воспроизведением» (Reproducing synchronisation). При этом воспроизводится только side-эффект (изменения данных в системе) проведенных операций, но не проводится повторное взаимодействие с внешними системами, например, отправка SMS-нотификаций. Такая синхронизация требует, чтобы версия БД-приемника была бы не ниже версии БД-источника. Разница в версиях возможна при обновлении системы.

3.2 Варианты топологий

Возможные варианты топологий:

- Двухузловой **HA Cluster Active-Passive Basic (Basic AP)**. В штатной ситуации все операции выполняются на первичном узле, Web-сервисы также подключаются к первичному узлу. Но отчеты и «тяжелые» выгрузки могут выполняться на вторичном узле. В случае простоя обработка критичных операций и работа Web-сервисов переносится на вторичный узел. После возобновления работы обработка критичных операций и работа Web-сервисов возвращается на первичный узел. Архитектура решения поддерживает многократное переключение обработки критичных операций между узлами (без пересоздания вторичного узла).

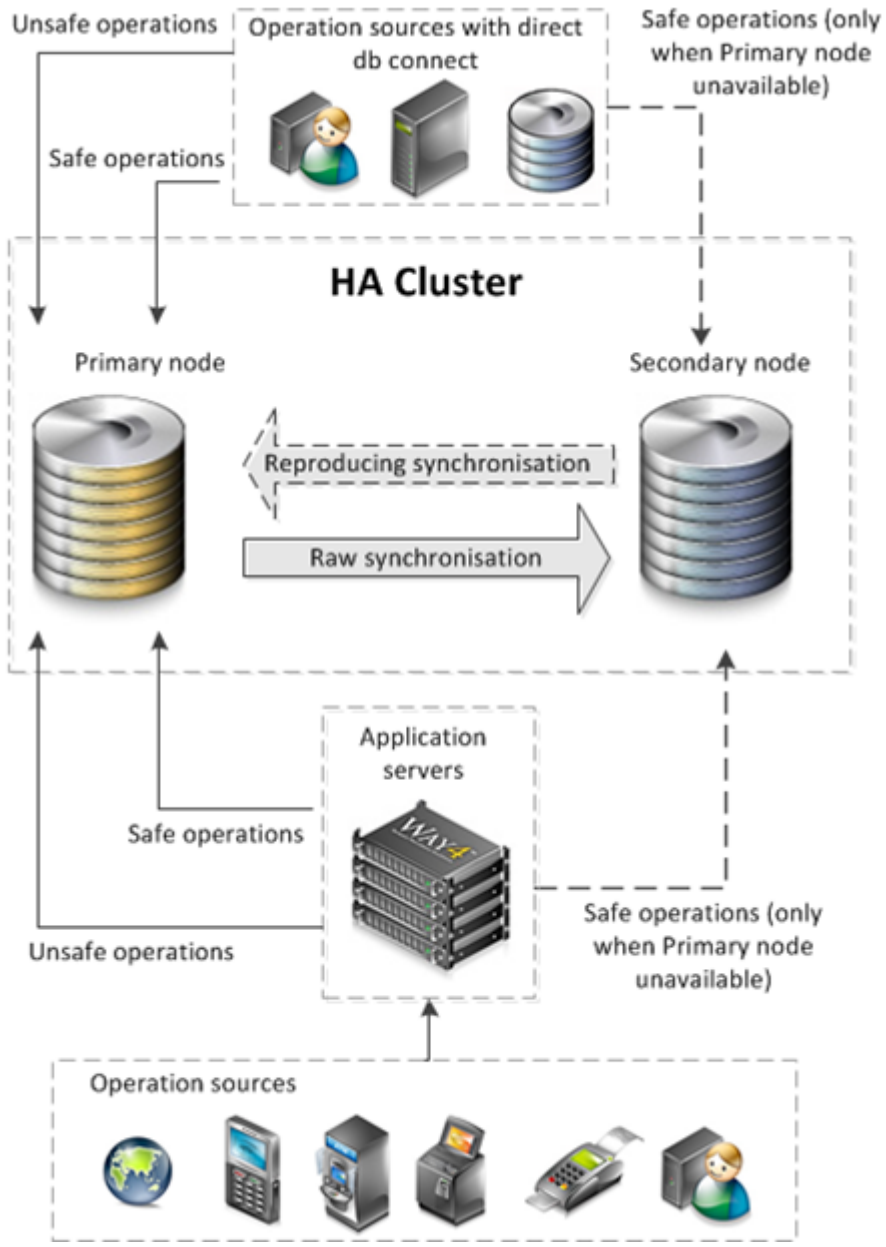

Рис. Двухузловая Basic AP топология

- Двухузловой **HA Cluster Active-Passive Split** (**Split AP**). В штатной ситуации BackOffice-операции, Issuing Online, Internet Banking выполняются на первичном узле, а Acquiring Online, Switching Online, «тяжелые» отчеты и выгрузки — на вторичном. Web-сервисы также работают на вторичном узле, однако все небезопасные операции, инициированные через Web-сервисы, выполняются на первичном узле. При недоступности одного из узлов обработка критичных операций переключается на доступный узел, а затем возвращается обратно. Архитектура решения поддерживает многократное переключение обработки критичных операций между узлами (без пересоздания вторичного узла).

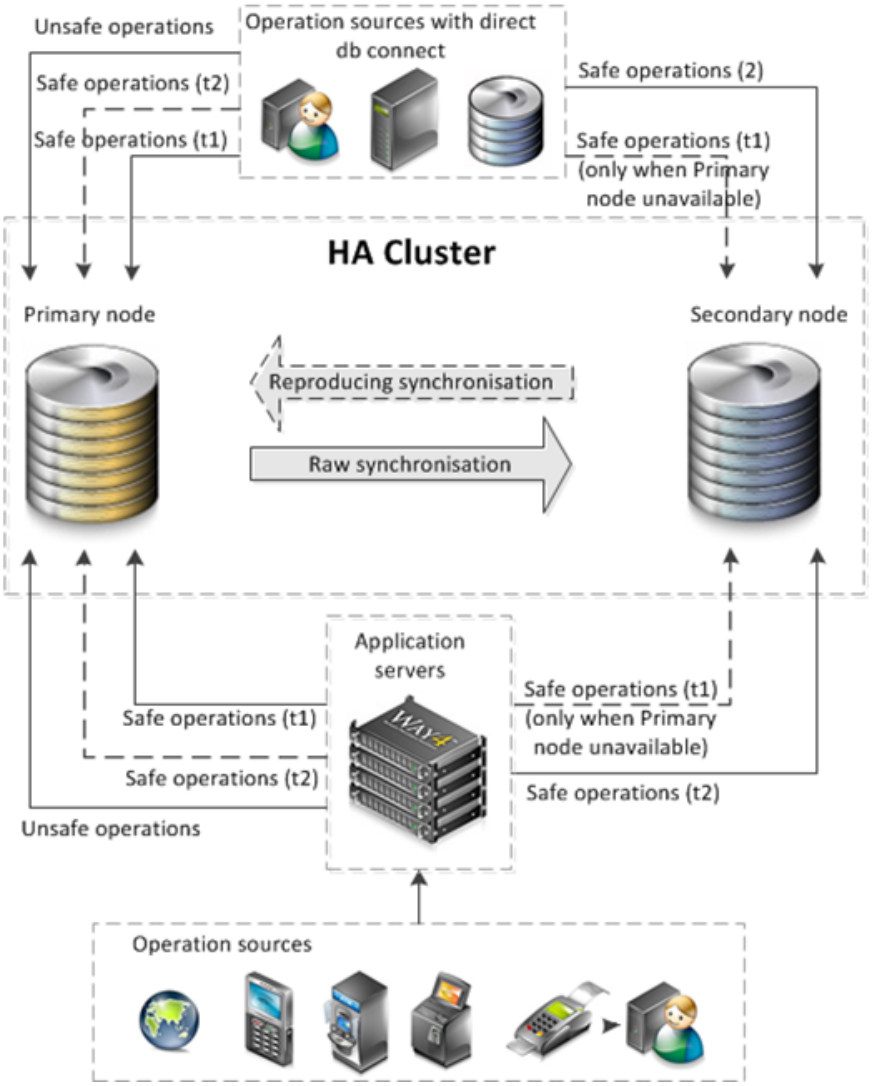

Рис. Двухузловая Split AP топология

3.3 Транспорт для синхронизации данных

Для синхронизации данных между узлами используется транспорт WAY4Replication. Описание продукта WAY4Replication приведено в функциональной спецификации "WAY4Replication. Программное решение для обеспечения синхронизации данных".

3.4 Дополнительный механизм репликации состояния узлов и сервисов

По умолчанию репликация состояния узлов и сервисов выполняться только с помощью транспорта WAY4Replication. Для повышения надежности репликации состояния узлов и сервисов может быть включен дополнительный механизм репликации состояния узлов и сервисов с помощью приложения Transaction Switch. Типовая схема репликации состояния узлов

и сервисов с помощью приложения Transaction Switch и транспорта WAY4Replication приведена на Рисунке.

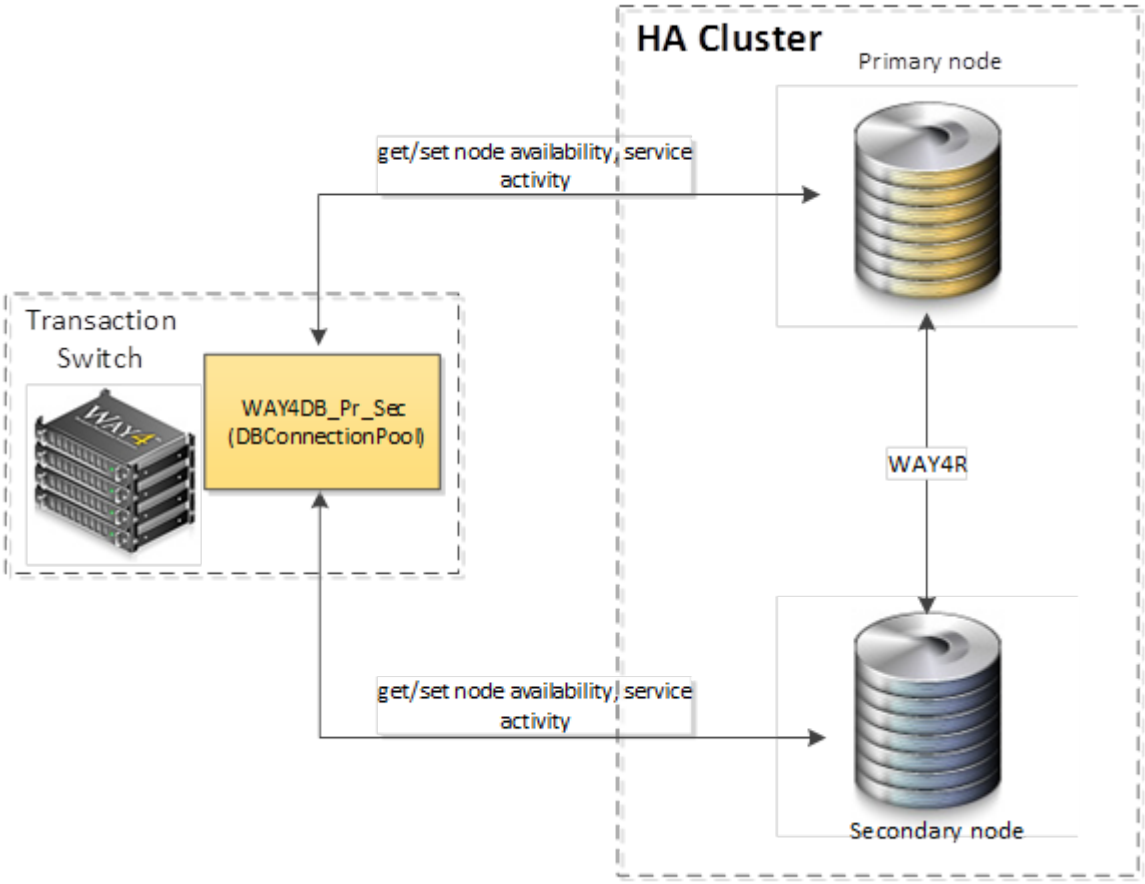

Рис. Схема репликации состояния узлов и сервисов

Используется существующие экземпляры приложения Transaction Switch.

В приложении Transaction Switch настраивается сервис WAY4DB (DBConnectionPool).

По умолчанию один раз в секунду сервис WAY4DB (DBConnectionPool) обращается к двум подключенным узлам для проверки изменения состояния узла и сервисов. При изменении состояния на одном узле отправляет изменения на другой узел. Изменения применяются только тогда, когда дата изменения больше даты, сохраненной в записи состояния узла или сервиса.

4. Варианты использования

4.1 Создание вторичного узла

База данных вторичного узла может быть создана:

- как полная копия первичного узла методом восстановления БД на определенный SCN, после чего включается процесс синхронизации с первичным узлом.
- методом выгрузки и последующей загрузки всех данных первичного узла (метод "Export All data"), после чего включается процесс синхронизации с первичным узлом.

4.2 Использование узлов для выполнения операций

Серверы приложений настраиваются таким образом, что могут работать с несколькими БД во всех топологиях.

4.3 Переключение операций между узлами

Переключение с исходного узла на альтернативный узел предполагается осуществлять как в ручном, так и в автоматическом режиме. Режим переключения (вручную или автоматический) задается при настройке решения. Обратное переключение с альтернативного узла на исходный узел всегда выполняется вручную.

4.3.1 Ручное переключение

Ручное переключение выполняется либо с помощью DB Replication Console (консоли), либо через пользовательский интерфейс DB Manager/WAY4 Manager.

После пометки узла как недоступного, автоматически выполняется переключение компонентов системы WAY4 (Access Server, Transaction Switch и т д.) на вторичные узлы.

4.3.2 Автоматическое переключение

Для автоматизации процесса обнаружения проблем на основной базе данных и своевременного переключения на резервную базу предназначен продукт Auto_Switchover.

Auto_Switchover выполняет следующие функции:

- Диагностику недоступности основной БД;
- Принятие решения о переключении БД;

- Переключение БД.

Подробное описание Auto_Switchover приведено в функциональной спецификации на продукт "WAY4™ Auto_Switchover. Автоматическое переключение между базами данных".

4.4 Восстановление первичного узла при помощи Oracle Physical StandBy

БД Oracle StandBy может использоваться в любой из вариантов HA Cluster топологий.

В штатном режиме узел Physical StandBy является полной копией первичного узла, синхронизируемой через журнальные файлы.

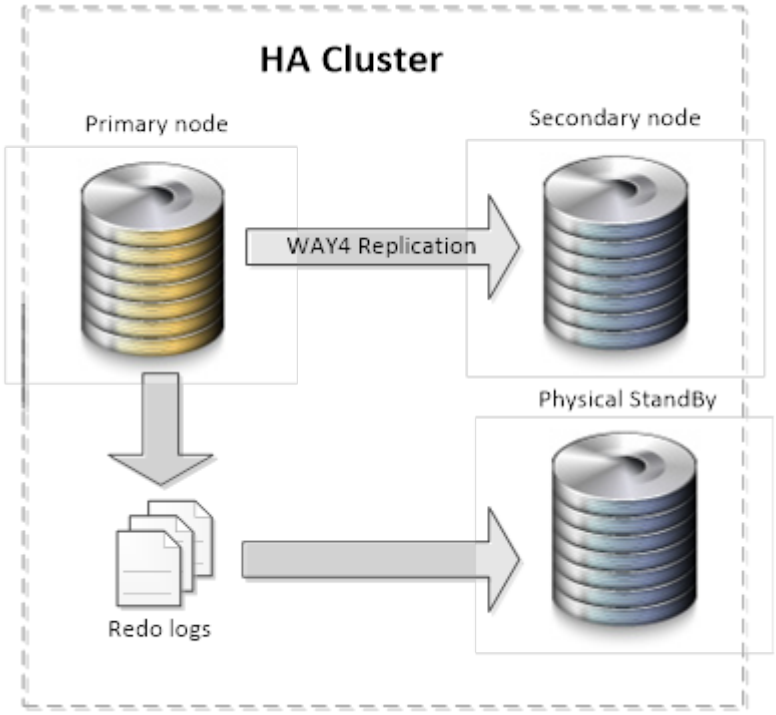

Рис. Использование Oracle Physical Standby

В случае плановой или внеплановой недоступности первичного узла выполняется синхронизация и переключение компонентов системы WAY4 с первичного на вторичный узел.

Если принимается решение о прекращении по какой-либо причине использования первичного узла (выход из строя или плановая замена), производится активация Physical StandBy, вывод из эксплуатации текущего первичного узла и объявление Physical StandBy новым первичным узлом в решении.

Затем выполняется обратная синхронизация данных со вторичного узла на новый первичный узел и обратное переключение со вторичного на новый первичный узел.

Завершающим шагом является подготовка нового Physical StandBy.

4.5 Проведение плановых работ

Для обеспечения высокой доступности системы WAY4 все плановые работы в текущий момент времени следует проводить только на одном узле при условии, что остальные узлы кластера доступны.

4.6 Частичное обновление системы (Patch)

Patch устанавливается на первичном узле, при условии того, что Patch не приводит к структурным изменениям данных. Если нужен простой, то на время простоя этого узла критичные операции выполняются на вторичных узлах.

После запуска исходного первичного узла Patch устанавливается по очереди на все вторичные узлы.

4.7 Обновление системы (Upgrade)

Upgrade проводится на первичном узле, а затем на вторичном узле. На время простоя первичного узла при upgrade критичные операции выполняются на вторичных узлах. На время простоя вторичного узла при upgrade критичные операции выполняются на первичном узле.

При проведении upgrade, в случае неудачного его выполнения на первичном узле, поддерживается возможность повторного переключения на вторичный, еще не обновлявшийся узел: после возвращения на обновленный первичный узел и обнаружения неудачно проведенного upgrade, выполнение критичных операций вновь осуществляется на вторичном узле.

Все номера карт, по которым осуществлялась попытка обработки операций с момента возвращения на первичный узел, версия системы на котором была обновлена неудачно, помещаются в специальный список. Обработка критичных операций по картам, включенным в данный список, на вторичном узле не осуществляется. В зависимости от настроек продуктов платежных систем, для определенных карт из этого списка могут быть сделаны исключения и поддержана обработка операций.

После устранения причин неудачного upgrade на первичном узле осуществляется переключение с вторичного на первичный узел.

4.8 Пересоздание вторичного узла

При необходимости вторичный узел может быть пересоздан как копия первичного узла. Для выполнения операции следует остановить процессы синхронизации и заново создать вторичный узел.

5. Ограничения

Решение имеет ряд ограничений:

1. Каждый экземпляр пользовательских приложений DB Manager и WAY4 Manager может работать только с одним узлом. Для корректной работы должны быть настроены и запущены несколько копий DBM/WAY4M, либо следует использовать Web-клиент.
2. Возможны случаи, приводящие к одновременной недоступности первичного и вторичных узлов: одновременное обесточивание; одновременное вступление в действие релизов МПС, после которых транзакции на неподготовленных узлах будут отвергаться; необходимость остановки процессинга из-за выявленной аппликационной ошибки или ошибки системного программного обеспечения, имеющей место на обоих узлах и т.д.
3. На вторичных узлах допускаются только безопасные операции, в том числе операции из списка критичных (см. "Обработка операций").
4. В решении не поддерживается блокировка карты на вторичном узле через заявления в случае использования модуля Advanced Applications R1, но операция поддерживается в случае использования модуля Advanced Applications R2.
5. Stand-In Processing (STIP) для авторизационных запросов, используемый в случаях недоступности Core Banking System, не поддерживается на вторичном узле.
6. В топологии Basic AP требуется небольшой простой для переключения. В случае планового переключения время простоя складывается из времени, необходимого для завершения In-Flight-операций (~10 секунд), времени, необходимого для синхронизации изменений между узлами (~10 секунд), и времени выполнения переключения (~3 секунды). В случае внепланового переключения ко времени планового простоя добавляется время, необходимое для обнаружения недоступности (~10 секунд при автоматическом переключении).
7. In-Flight-операции выполняются на той же БД, где они начались. При плановом переключении транзакционного потока на другой узел обработка In-Flight-операций всегда завершается на том же узле, где началась их обработка. При внеплановой недоступности узла, на котором началась обработка In-Flight-операций, по всем таким операциям произойдет технический отказ.
8. При внеплановом переключении возможно наличие изменений на основном узле, не синхронизированных с резервным узлом по причине недоступности основного узла.
9. При использовании топологии Split AP возможен неточный учет ограничителей активности уровня финансового института, если он используется одновременно как эмиссией, так и эквайрингом.
10. В топологии Basic AP использование вторичного узла для выполнения некритичных операций невозможно.
11. Для достижения высокой доступности на случай неработоспособности одной из площадок целиком, на второй площадке должен быть не только вторичный узел, но и аппликационные серверы. Внешние приложения должны автоматически выбирать доступные аппликационные серверы для подключения.

12. Вторичный узел не может использоваться как Первичный.
13. После возвращения на первичный узел, на котором выполнен структурный upgrade, повторное использование вторичных узлов без пересоздания или обновления до версии, используемой на первичном узле, недопустимо.
14. Решение HA требует дополнительной защиты первичной базы. Варианты дополнительной защиты: StandBy; GeoMirroring.
15. Начиная с версии 03.51.30 компоненты решения на платформе WAY4U не поддерживаются, компоненты должны быть переведены на платформу Transaction Switch.

6. Технические требования

В разделе приведены требования к первичному и вторичному узлам при переходе к архитектуре HA Cluster с одноузловой архитектуры.

Изменение требований к первичной БД:

	HA Cluster Active-Passive Basic	**HA Cluster Active-Passive Split**
Количество Процессоров	1,2 от исходного	без изменений
Лицензии Oracle	1,2 от исходного	без изменений
Производительность дисковой подсистемы	1,2 от исходного	без изменений

Для каждого вторичного узла требуется:

	HA Cluster Active-Passive Basic	**HA Cluster Active-Passive Split**
Количество Процессоров	1/2 от первичной БД	1 от первичной БД
Лицензия Oracle	1/2 от первичной БД	1 от первичной БД
Объем памяти	Как у первичной БД	
Объем дискового пространства	Как у первичной БД	
Производительность дисковой подсистемы	1/2 от первичной БД	

7. Воздействие на другие компоненты

При использовании данного решения следует учитывать затраты на поддержку вторичных узлов.

При выполнении доработок системы следует учитывать, что все новые критичные операции должны создаваться как безопасные.

Если для работы с внешними системами используются WAY4 аппликационные серверы, то дополнительной доработки внешних систем не требуется.

Для обеспечения высокой доступности критичных операций, обслуживаемых внешними системами, подключенными напрямую к БД системы WAY4, требуются дополнительные исследования и работы по реализации переключения этих систем на альтернативные узлы.