скала^р

Машина виртуализации рабочих мест Скала^р МВ.ВРМ

Машина виртуализации
рабочих мест

Технический обзор

skala-r.ru info@skala-r.ru

ОГЛАВЛЕНИЕ

1. Предисловие....3
2. Введение....4
3. Отличительные черты....19
4. Состав решения....20
5. Высокая доступность и защита данных....27
6. Информационная безопасность....30
7. Гарантированное качество....31
8. Требования к размещению решения....32
9. Техническая поддержка....33
О компании....35

1. ПРЕДИСЛОВИЕ

Описание документа

Этот технический обзор дает концептуальный и архитектурный обзоры **Машины виртуальных рабочих мест Скала^р MB.BPM**

Брошюра описывает то, как оптимизированные программно-аппаратные комплексы отвечают современным вызовам, и фокусируется на **Машине виртуальных рабочих мест Скала^р** как одном из лидирующих решений в этом сегменте.

Аудитория

Эта брошюра предназначена для сотрудников компании Скала^р, партнеров и заказчиков, перед которыми ставятся задачи разработки решения, закупки, управления или эксплуатации **Машины виртуальных рабочих мест Скала^р MB.BPM**.

Ревизии

Перечень ревизий документа представлен ниже (Таблица 1).

Таблица 1. Ревизии

Дата	Описание
Январь 2023	Создание

Обратная связь

Скала^р и авторы этого документа будут рады обратной связи по нему.

Свяжитесь с командой Скала^р по электронной почте MV@skala-r.ru.

2. ВВЕДЕНИЕ

Удаленная работа на инфраструктуре виртуальных рабочих мест и терминальных серверов

В настоящий момент многие организации испытывают потребность организовать инфраструктуру для удаленной работы сотрудников, или быть готовым начать её массово предоставлять.

Притом, в современных реалиях для России можно выделить несколько трендов.

Во-первых, двуединое понятие «инфраструктуры удаленных рабочих мест». Всё чаще это одновременно две технологии, в какой-то пропорции делящие между собой доли пользователей. Эти технологии — BPM, виртуальные рабочие места (VDI, Virtual Desktop Infrastructure), и терминальные серверы (включая публикацию отдельных приложений).

Интересно что редко, но регулярно, пользуется спросом третий вариант — подключение к физическим ПК, в рамках единой системы.

Во-вторых, строгий курс на Linux, во всех элементах решений. Windows-инфраструктуры, часто, по прежнему используются, но даже если так — новые фермы виртуализации рабочих мест строятся на Linux-инфраструктуре.

Машина **Скала^р MB.BPM** учитывает эти тренды, в решении реализованы возможности использования и Windows-, и Linux-операционных систем. Притом, и в варианте BPM, и в варианте терминальных серверов.

Примечательно, что такая инфраструктура обеспечивает ряд преимуществ, даже если пользователи с ней взаимодействуют не удаленно, а из офиса организации.

Обычно, можно выделить следующие преимущества.

Безопасность

Когда пользователь работает на удаленном рабочем месте, это рабочее место расположено в ЦОД организации. Все данные пользователя хранятся на нем. Доступ к прочим системам разрешен только с этого безопасного рабочего места, а не с устройства пользователя.

Кроме того, можно разрешить доступ не только определенным пользователям, но и только с определенных устройств. Каждое подключение попадает в журнал, доступный для аудита.

Таким образом, контроль за данными и безопасностью усиливается. Ограничение доступа к системам и данным извне организации реализуется во многом уже самой архитектурой такой системы.

Совместимость

Удаленные рабочие места очень сильно типизируются. Одинаковые ресурсы, одинаковые операционные системы и их версии, одинаковое окружение. Притом, таких «типов» может быть несколько даже для одного пользователя.

Такие возможности приводят к тому, что задача массового запуска ПО с теми или иными требованиями совместимости с окружением решается путем запуска его в удаленных\виртуальных рабочих местах. ПО не запускается на устройствах пользователей, для которых, обычно, характерен разброс в характеристиках, версиях и окружении.

Такие конфигурации могут быть востребованы как на постоянной основе, так и на время миграции прикладного ПО на целевую платформу.

Оптимизация

Удаленные рабочие места очень сильно типизируются. Одинаковые ресурсы, одинаковые операционные системы и их версии, одинаковое окружение. Это минимизирует количество инцидентов, требующих внимания администраторов и специалистов поддержки пользователей.

Обслуживание, т.е. такие операции как установка обновлений на ОС, на ПО, изменение состава типового ПО рабочего места отлично автоматизируются, что приводит к тому, что трудозатрат на обслуживание большого числа рабочих мест требуется немного. А некоторые операции, такие как массовое быстрое добавление ресурсов к рабочему месту, в принципе доступно для рабочих мест только когда они виртуальные.

Машина виртуальных рабочих мест Скала^р МВ.ВРМ

Машина **Скала^р МВ.ВРМ** призвана быть гибким строительным блоком для инфраструктуры удаленных\виртуальных рабочих мест. В зависимости от бизнес-требований или фаз проекта, Машина может быть установлена в той или иной конфигурации. Например, стартовый модуль Машины позволит реализовать первую фазу решения для 400 пользователей. Затем, имеющиеся ресурсы могут быть расширены под требуемое количество пользователей второй фазы добавлением модулей расширения. На следующей фазе проекта может быть добавлена ещё одна Машина в другом ЦОД для реализации катастрофоустойчивости инфраструктуры виртуальных рабочих мест.

Целесообразность использования **Скала^р МВ.ВРМ** начинается примерно с 400 пользователей. Протестированный максимум — 16 000 пользователей. В проработке находятся инфраструктуры свыше чем на 25 000 пользователей.

Машина **Скала^р МВ.ВРМ** использует в качестве фундамента гиперконвергентную Машину виртуализации **Скала^р МВ.С**, и программное решение **Базис.WorkPlace** (также известное как «Скала-р ВРМ (Виртуальное рабочее место)».

Базис.WorkPlace является зрелым продуктом, одним из ведущих Российских решений виртуализации рабочих мест, с большим количеством функций.

(В тексте термины **Базис.WorkPlace** и ВРМ взаимозаменяемы. Например, «клиент **Базис.WorkPlace**» и «клиент ВРМ» означают одно и то же.)

Преимущества Машины Скала^р МВ.ВРМ

- Создание, настройка и управление пулами виртуальных рабочих столов разного назначения: от набора рабочих столов, которые настраиваются индивидуально под нужды каждого пользователя (например, руководителя или уникального специалиста) до набора типовых рабочих мест госслужащего или пула виртуальных машин, создаваемых по мере необходимости сроком на одну пользовательскую сессию.
- Кроме виртуальных рабочих мест и терминальных серверов, поддерживается управление доступом пользователей к отдельным приложениям, опубликованным на терминальных серверах, а также подключение пользователей к физическим компьютерам.
- Поддержка как Windows, так и Linux.

- Множество настроек безопасности, таких как поддержка смарт-карт и двухфакторной авторизации, авторизация пользовательских устройств.
- Поддержка т.н. «связанных клонов», режима старта множества виртуальных рабочих мест из единого «мастер-образа».
- Все функции ВРМ доступны через программные интерфейсы (API), за счет чего возможна дополнительная автоматизация операций над инфраструктурой.
- Нечувствительность к единичным отказам, как на уровне платформы виртуализации, так и на уровне компонентов ВРМ-инфраструктуры. Возможность создания катастрофоустойчивых решений.
- Гиперконвергентная архитектура уровня виртуализации упрощает масштабирование решения и обеспечивает надежную и производительную работу при больших нагрузках. Гиперконвергентная система хранения поддерживает масштабирование производительности как вертикально (выбором более быстрых накопителей), так и горизонтально — выбором большего числа накопителей/серверов. Кроме того, такая система состоит из большого числа равнозначных узлов и архитектурно не имеет единственного компонента, который мог бы стать узким местом.
- Гарантия совместимости — Скала^р проводит R&D работы по выбору и валидации оборудования вместе с используемым программным обеспечением. Серверы, контроллеры, накопители, сетевые коммутаторы, программное обеспечение виртуализации, управления, виртуальных рабочих мест — тестируются и аттестуются именно в той комбинации, которая будет поставляться.
- Серийное производство позволяет создать тиражируемое решение с регламентными сроками доступности. Оборудование из состава Машины является не только технически валидированным, но и массово доступным для заказа. В том числе, за счет сотрудничества с несколькими поставщиками оборудования, кроме собственного производства серверов марки Скала^р.
- Собственная служба поддержи позволяет обеспечить поддержку из одного окна — по всем составляющим комплекса. Инциденты, даже на стыке аппаратных и программных компонентов, будут разбираться службой поддержки Скала^р, которые, при необходимости, уже сами обратятся в поддержку производителя конкретного компонента.

Сценарии использования Машины ВРМ

Машину может быть целесообразно использовать в разных сценариях. Как правило, они отличаются масштабами и комплексностью.

Масштаб удобно оценивать в количестве пользователей (хотя эта характеристика и не является всеобъемлющей и однозначной, но она позволяет быстро получить оценку).

Комплексность зависит от числа и состава компонентов, входящих в состав решения или интегрирующихся с ним. Например, если конкретном случае решение будет предоставлять только виртуальные рабочие места, то комплексность решения ниже, чем если ещё и доступ к сессиям терминальных серверов.

«Инфраструктура филиала»

Характерным примером является сценарий построения ВРМ-инфраструктуры для относительно небольшого числа пользователей (Рис. 1). Хотя мы и назвали этот сценарий «инфраструктура филиалов», но подобная инфраструктура вполне может быть

востребована и внутри центрального ЦОД, например, для особенной категории пользователей.

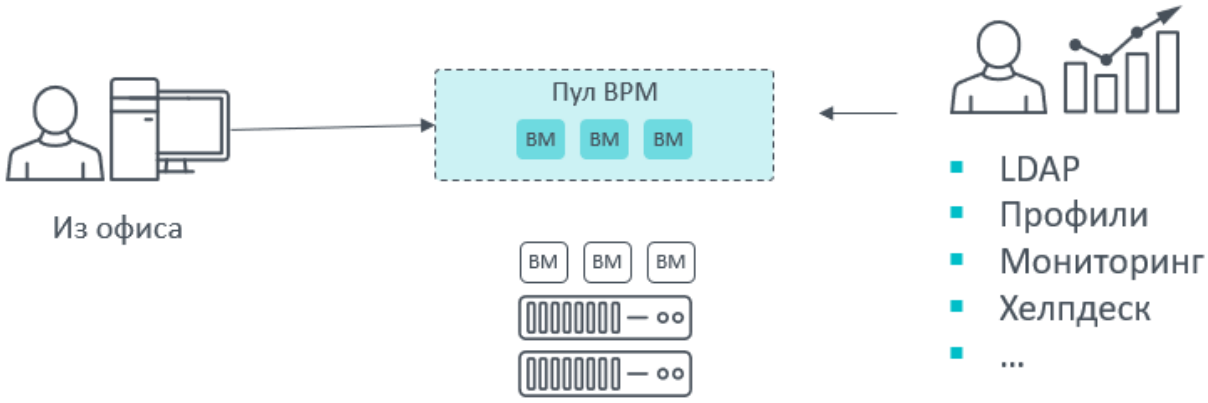


Рис. 1. Схема «Инфраструктуры филиала»

В этом сценарии, как правило, отличительными особенностями инфраструктуры будут:

- одна Машина, минимальной конфигурации;
- допустимо отсутствие балансировщика нагрузки — клиент ВРМ позволяет указать адреса пары диспетчеров подключений, и в нем реализована логика обращения ко второму если первый не ответил. Это позволяет реализовать сценарий резервирования диспетчеров подключений без балансировщика нагрузки;
- отсутствие катастрофоустойчивости.

Какое же число пользователей является «небольшим»?

В случае Машины **Скала^р МВ.ВРМ** — это примерно 400, для существенно меньшего количества теряется целесообразность построения выделенной под ВРМ инфраструктуры.

(Но в этом случае следует рассмотреть **Машину серверной виртуализации Скала^р МВ.С**, дополнив её лицензиями на ВРМ. Такая комбинация позволит получить инфраструктуру серверной виртуализации, и часть её ресурсов выделить для ВРМ).

Сценарий импортозамещения

В этом сценарии перед организацией стоит задача создать крупную инфраструктуру ВРМ с нуля (Рис. 2). Притом, это может быть как первая такая инфраструктура, так и инфраструктура на замену таким решениям, как Citrix XenDesktop, VMware Horizon и др.

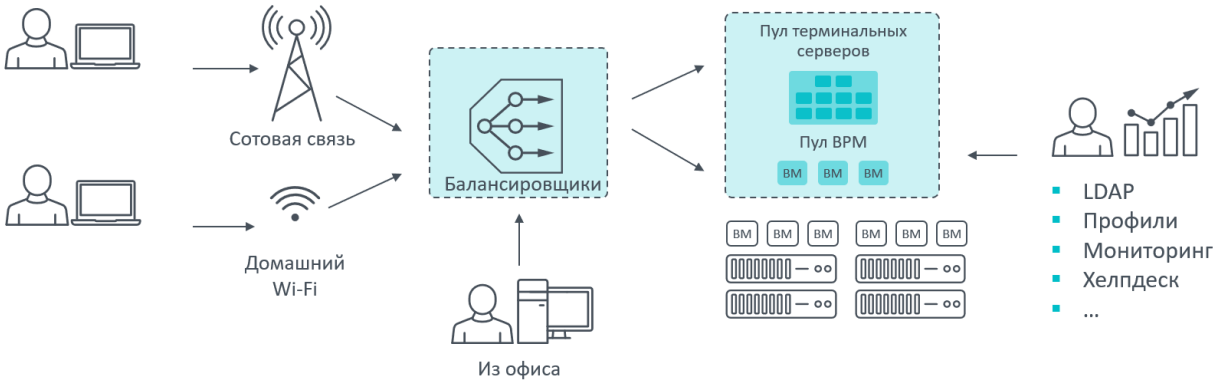


Рис. 2. Схема сценария импортозамещения

Вилка количества пользователей очень большая — начиная с нескольких сотен, продолжая несколькими тысячами, и даже несколькими десятками тысяч пользователей.

Отличительными особенностями такой инфраструктуры являются комплексность и задействование максимума функционала решения:

- в первую очередь, это комбинация выделенных виртуальных машин BPM и сессий терминальных серверов;
- неоднородный доступ — одни пользователи подключаются изнутри корпоративной сети, другие — «снаружи». И для тех, и для других потребуются масштабируемая и отказоустойчивая инсталляция диспетчеров подключения BPM. И такая же — балансировщиков нагрузки;
- использование Linux-операционных систем как на стороне виртуальных рабочих мест и терминальных серверов, так и на стороне пользовательских устройств;
- использование периферийных устройств;
- требования по управляемости такой инфраструктуры часто многократно выше. Приоритет функций по хелпдеску, отчетности, мониторингу, средствам автоматизации повышается.

Архитектурные варианты Машины BPM

В этом разделе будут описаны основные компоненты решения (Рис. 3) и наиболее часто встречающиеся варианты их реализации.

Обратите внимание — в составе Машины **Скала^р MB.BPM** одновременно присутствуют и платформа виртуальных рабочих мест, и платформа серверной виртуализации. Здесь будут приведены основные архитектурные особенности этой платформы, но если вам потребуется больше деталей, то обратитесь к техническому обзору Машины **Скала^р MB.C**.

Виртуальные рабочие места — это очень комплексное решение, и не все его компоненты могут войти в состав Машины. В первую очередь, речь про такие компоненты как гостевые операционные системы виртуальных рабочих мест, службы управления профилями пользователей, и др.

Эти компоненты специфичны для каждого проекта, их лицензирование, планирование и эксплуатация не покрывается в данном документе.

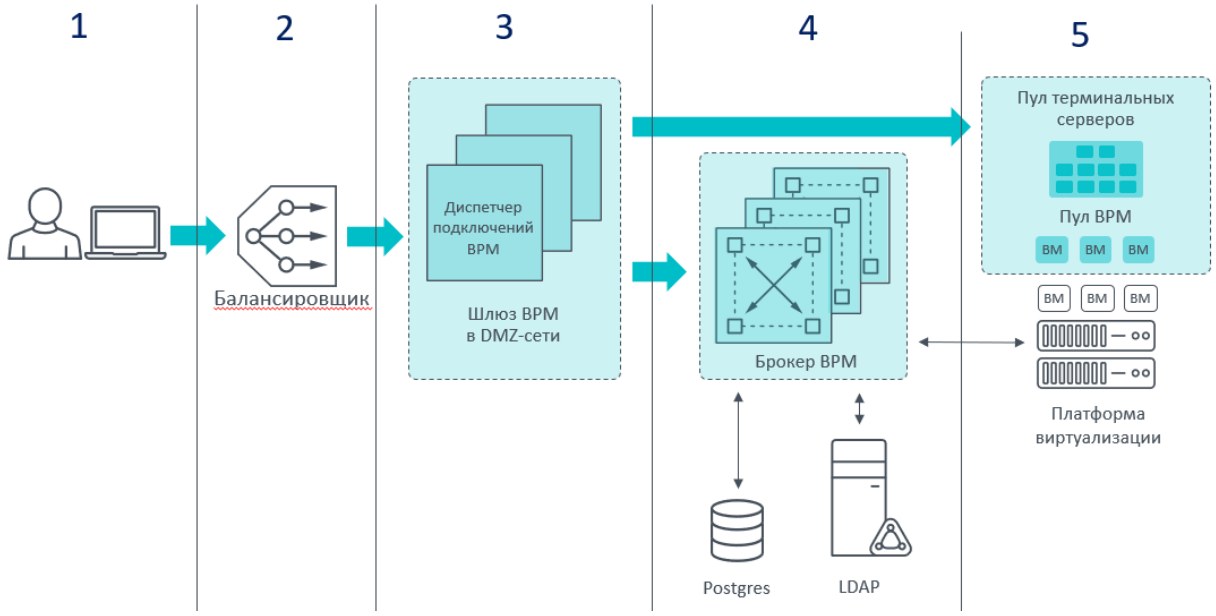


Рис. 3. Основные компоненты решения Скала^р MB.BPM

1. Устройство доступа пользователя и клиент Базис WorkPlace

Может быть компьютером с Windows- или Linux-операционной системой, а также «тонким клиентом». Основное требование — на нем должен быть установлено программное обеспечение «клиент **Базис.WorkPlace**», которое реализует подключение к рабочему месту.

Это приложение выполняет ряд задач, кроме собственно подключения:

- Формирование hardware ID (HWID) для авторизации устройства доступа. При подключении к Диспетчеру подключений клиент передает HWID и информацию об устройстве. Если настроена соответствующая политика, то Брокер BPM производит авторизацию устройства по hardware ID.
- Взаимодействие со смарт-картой при авторизации по сертификату.
- Смена пароля пользователя. Если во время авторизации оказалось, что пароль пользователя просрочен, клиент отображает экран смены пароля. Важная функция для пользователей, у которых VDI является единственным окном в корпоративную сеть.
- Настройка и запуск протокола доставки рабочего стола. Клиент **Базис.WorkPlace** позволяет пользователю настроить проброс принтеров, смарт-карт, локальных дисковых ресурсов, выбрать монитор и режим отображения удаленного рабочего стола и т.д. Для настройки некоторых параметров требуется разрешение администратора. Когда настает момент подключения к виртуальному рабочему столу, клиент формирует параметры запуска используемого протокола и запускает его.

2. Балансировщик нагрузки

Опциональный (в небольших масштабах внедрения) компонент решения. Обеспечивает балансировку нагрузки между диспетчерами подключений, и отказоустойчивость (перенаправляя обращения на работающие диспетчеры вместо отказавших).

Альтернативой является штатная функция клиента **Базис.WorkPlace** использовать список адресов диспетчеров подключений, с последовательным обращением к каждому адресу из этого списка.

3. Диспетчер подключений Базис.WorkPlace

Виртуальная машина с установленным серверным ПО с ролью «Диспетчер подключений». Этот сервер:

1. принимает подключения пользователей;
2. передает их на сервер с ролью «Брокер BPM» для авторизации;
3. после успешной авторизации открывает подключение к удаленному рабочему месту или терминальному серверу.

Обратите внимание, что подключение к рабочему столу всегда осуществляется «сквозь» диспетчер подключений. Таким образом, диспетчер подключений является единственным компонентом решения, который должен быть напрямую доступен с устройства пользователя.

Обычно, это означает, что именно виртуальные машины с этой ролью доступны «извне» сетевого сегмента BPM, что они работают в DMZ, и доступ к ним и их состояние наиболее важно контролировать с точки зрения ИБ.

Диспетчер подключений пересылает запросы пользователей на тот или иной из доступных брокеров BPM, а после успешной авторизации — открывает «сквозь себя» подключение к виртуальному рабочему месту. Каждый диспетчер способен обслужить, обычно, до 1500-2000 пользовательских сессий.

4. Брокер BPM

Виртуальная машина с установленным серверным ПО, с ролью «Брокер BPM». Этот сервер является ядром BPM-инфраструктуры, хранит и обслуживает конфигурацию, интегрируется со сторонними компонентами.

На схеме на Рис. 4 проиллюстрировано, что брокер:

- принимает обращения пользователей, и взаимодействует с LDAP-каталогом для их авторизации;
- общается с базой данных, выделенной под BPM, где хранит конфигурацию;
- обращается на платформу виртуализации для выполнения операций над виртуальными машинами.

В зависимости от числа пользователей (и, как следствие, нагрузки) брокеров может быть несколько экземпляров, и даже более того — на отдельные виртуальные машины могут быть вынесены некоторые компоненты брокера.

Каждый брокер способен обслужить до различное число пользователей в зависимости от конфигурации своей виртуальной машины.

5. Виртуальные рабочие места и терминальные серверы

Администратор BPM указывает параметры пулов виртуальных рабочих мест, такие как число виртуальных машин в пуле, образ из которого их следует создавать, должны ли это быть полные виртуальные машины или связанные клоны (linked clones).

Кроме того, администратору доступно создание пулов терминальных серверов с указанием соответствующих параметров.

Брокер BPM обеспечивает эти конфигурации, развертывая соответствующие виртуальные машины на платформе виртуализации из указанных шаблонов.

Типовая схема

В архитектурной схеме присутствуют как специфичные для **Скала^р МВ.BPM** компоненты, так и неспецифичные.

Ко вторым относятся каталог LDAP, гостевые ОС, инструменты управления профилями пользователей, системы информационной безопасности и т.п. Они останутся за рамками данного документа.

Начнем со специфичных для **Скала^р МВ.BPM** компонентах (Рис. 4).

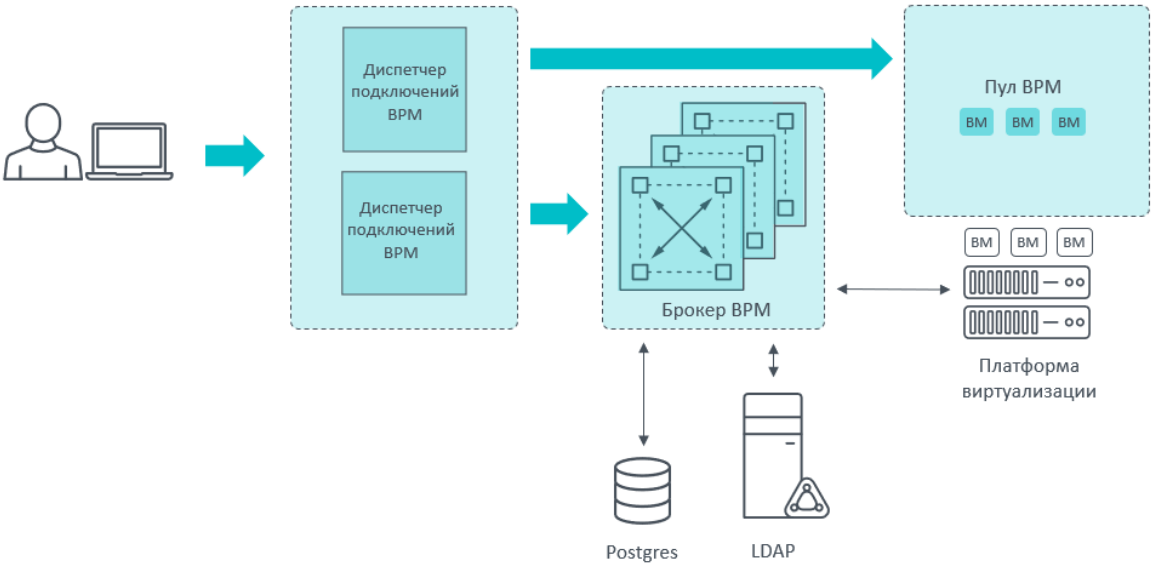


Рис. 4. Типовая схема

База данных Postgres может быть развернута в виртуальной машине на самой Машине **Скала^р МВ.BPM**.

В типовой схеме развертывается пара диспетчеров подключений BPM. Один экземпляр способен обслужить 1500-2000 пользователей, чего часто достаточно. Но для реализации высокой доступности этого компонента следует добавить второй экземпляр.

Адреса этих диспетчеров следует указать в настройках клиента BPM, который должен быть установлен у каждого пользователя инфраструктуры BPM. При указании больше одного адреса клиент будет подключаться к ним последовательно. Таким образом, даже если один из них будет временно недоступен, подключение всё равно произойдет.

Брокер BPM обычно развертывается в отказоустойчивой конфигурации из трех экземпляров.

Работоспособность BPM-инфраструктуры напрямую зависит от работоспособности платформы виртуализации. Далее будет описана её типовая архитектура для BPM-решения.

В платформе виртуализации можно выделить три основных компонента: сервер управления, программная система хранения и конфигурация кластера гипервизоров.

Так как для работоспособности BPM критически важен сервер управления платформой виртуализации, то его следует установить в отказоустойчивой конфигурации и настроить резервное копирование.

Типичная конфигурация для программной системы хранения — по умолчанию. Основная переменная величина — политика резервирования данных для разных компонентов. Для критичных виртуальных машин, как правило, целесообразно выбрать политику обеспечивающую потерю двух компонентов. К критичным относятся серверные компоненты BPM, сервер управления платформой виртуализации, прочие виртуальные машины, относящиеся к важным для BPM функциям (серверы LDAP, файловые серверы, серверы баз данных и др.).

Для некритичных виртуальных машин может быть политика хранения с меньшим резервированием, вплоть до его отсутствия. Последнее может быть целесообразно для типовых рабочих мест (обычно, «связанных клонов»), внутри которых не предполагается хранения данных пользователей. Как следствие, при отказе, например, накопителя и выходе из строя тех виртуальных машин что были на нем частично расположены — могут быть развернуты дополнительные новые копии. Целесообразность подобного подхода следует оценивать в каждом случае независимо.

Для кластера гипервизоров стандартным подходом является настройка функций высокой доступности и балансировки нагрузки (DRS). Кроме того, для тех компонентов решения, что развернуты в кластерной конфигурации на нескольких виртуальных машин (это брокер BPM, диспетчер подключений, сервер управления платформой виртуализации, в первую очередь) следует настроить правила anti-affinity. Это важно для того, чтобы исключить вероятность что они окажутся на одном сервере и откажут одновременно в случае его сбоя.

Варианты установки компонентов

В этом разделе будет указаны самые важные варианты развертывания компонентов Машины **Скала^р МВ.BPM**.

1. Устройство доступа пользователя

Устройства доступа могут быть разными, на них могут быть установлены разные ОС. Но ключевая характеристика — на нём должен быть установлен (или интегрирован в ОС тонкого клиента) клиент BPM.

Обратите внимание, что решение поддерживает клиентские устройства, построенные на процессорах Байкал и Эльбрус.

Кроме того, реализована поддержка **Базис.WorkPlace** для тонких клиентов с **KasperskyOS**, и тонких клиентов GETMOBIT.

2. Балансировщик нагрузки

В некоторых случаях в решение целесообразно добавить балансировщик нагрузки, задачи которого:

- предоставлять единый адрес для подключений пользователей;
- обеспечивать высокую доступность диспетчеров подключений;
- балансировать нагрузку между диспетчерами подключений.

При использовании балансировщика нагрузки важно обеспечить его собственную высокую доступность.

3. Диспетчер подключений ВРМ

Для диспетчеров подключений можно выделить три критерия, влияющие на архитектуру.

Первое — производительность. В среднем, один экземпляр диспетчера подключений способен обслужить 1500-2000 пользователей. Если в конкретном проекте есть основания предполагать нехарактерную нагрузку, целесообразно провести тестирование для подтверждения этой оценки. Если одномоментных подключений пользователей предполагается больше, чем способен обработать один диспетчер — следует развернуть дополнительные экземпляры.

Второе — высокая доступность. Диспетчеры подключений могут становится недоступны, планово или аварийно. Следует заложить дополнительные экземпляры диспетчеров подключений, по схеме N+X, где N — это требуемое число экземпляров диспетчеров с точки зрения производительности, а X — дополнительные экземпляры на случай отказа.

Третье — подключение к ВРМ-инфраструктуре может быть востребовано из разных сетевых сегментов. Например, из офисной сети и через интернет для удаленных сотрудников. В некоторых случаях регламенты информационной безопасности потребуют использования независимых групп диспетчеров подключений для этих сегментов. Тогда выбор числа диспетчеров для каждого сегмента производится независимо, по вышеописанным соображениям.

4. Брокер ВРМ

Брокер ВРМ является сердцем Машины **Скала^р МВ.ВРМ**. При его недоступности ВРМ перестает функционировать. Поэтому для промышленных сценариев брокер должен быть развернут в отказоустойчивой конфигурации на трех виртуальных машинах.

Для инфраструктур на многие тысячи пользователей брокер ВРМ может быть целесообразно развернуть на большем количестве машин, если есть основания считать, что производительности трех будет недостаточно в пиковые часы.

Для самых масштабных инфраструктур на отдельные виртуальные машины может быть выделен компонент «Redis» для дополнительного повышения производительности компонента «Брокер ВРМ». Если Redis выносится отдельно, то это дополнительные 3+ виртуальные машины с этим компонентом.

5. Виртуальные рабочие места и терминальные серверы

Для виртуальных рабочих мест целесообразно использовать архитектуру связанных клонов всегда, когда только возможно. Она обеспечивает быстрое развертывание и переразвертывание виртуальных рабочих мест (что важно при обновлении ОС и ПО на них), экономит место на системе хранения, и значительно упрощает администрирование.

Архитектура связанных клонов предполагает наличие виртуальной машины с предустановленной ОС и ПО, которая выступает мастер-образом (или «золотым» образом).

Её образ используется «только на чтение» множеством виртуальных машин одного «пула виртуальных рабочих мест», все они стартуют с этого единого образа (Рис. 5).

Затем каждая из этих виртуальных машин использует для записи своих уже уникальных данных небольшой диск «дельту».

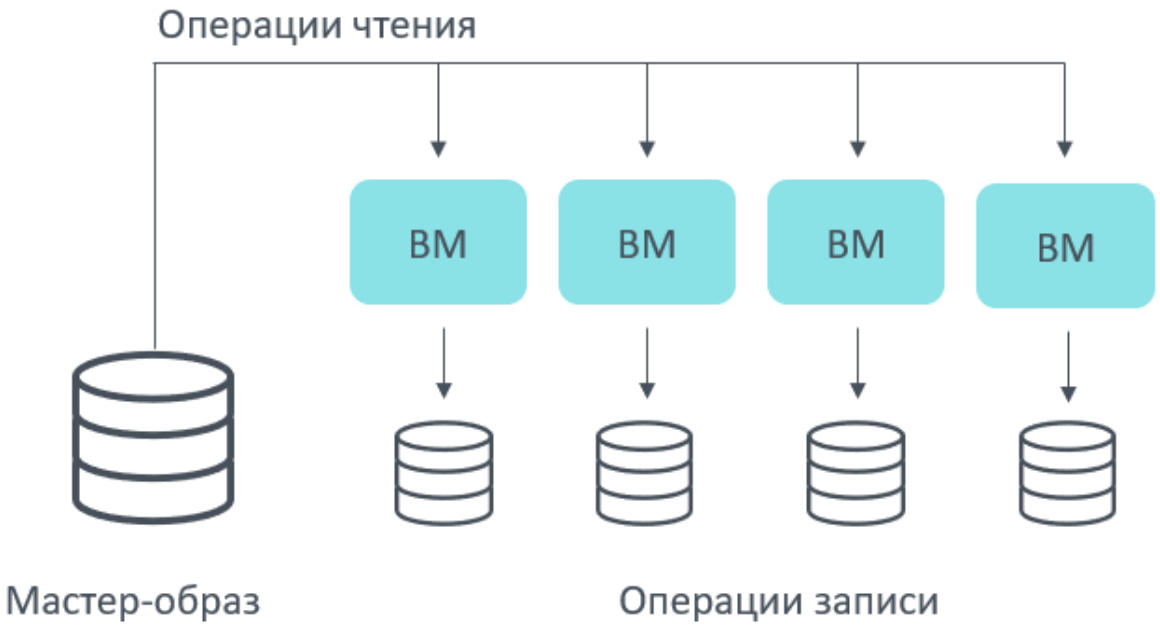


Рис. 5. Архитектура связанных клонов

Предполагается, что этот дельта-диск будет периодически обнуляться, и состояние виртуальной машины будет «откатываться» на мастер-образ. Уникальность каждой виртуальной машины будет обеспечена (если это востребовано) данными из перемещаемого профиля пользователя, который должен быть обеспечен сторонними инструментами.

6. Протокол доступа к виртуальному рабочему месту

В решении виртуальных рабочих мест могут быть использованы разные протоколы. В первую очередь, это RDP и RX@Etersoft. Выбор конкретного протокола следует осуществить в зависимости от требований к решению и возможностей протоколов.

Возможности протоколов указаны в актуальной документации.

Сайзинг

Ниже описаны пределы масштабирования для Машины (Таблица 2).

Таблица 2. Пределы масштабирования Скала^р MB.BPM

Параметр	Значение
Макс. количество площадок (ЦОД) на одну инсталляцию BPM	1
Рекомендуемый максимум одновременных соединений на одну инсталляцию Скала^р BPM	Рекомендовано: 10 000 Протестированный максимум: 16 000

Рекомендуемый максимум Диспетчеров подключений на одну инсталляцию Скала^р BPM	10
Рекомендуемый максимум одновременных соединений на Диспетчер подключений	2000
Рекомендуемый максимум Брокер-менеджеров на одну инсталляцию Скала^р BPM	7
Протестированный максимум одновременных соединений на 1 ядро CPU Брокер-менеджера	320

Возможности Базис.WorkPlace

Создание пулов рабочих столов

Пул рабочих столов — это логическое объединение виртуальных рабочих столов для какой-то одной группы или категории пользователей. Один пул может содержать как набор одинаковых рабочих столов, созданных для использования группой пользователей, так и набор разных рабочих столов, каждый из которых предназначен для конкретного пользователя.

Использование пула рабочих столов как единицы управления позволяет реализовать такие функции как:

- автоматизация создания и публикации рабочих столов для конечных пользователей за счет использования шаблонов предустановленных виртуальных машин;
- возможность настройки общих параметров при создании рабочих столов в пуле;
- автоматическая регистрация виртуальных рабочих столов в Active Directory (с добавлением в заданное организационное подразделение) при развертывании пула. Это упрощает администрирование и применение групповых политик. В зависимости от использованного сервиса LDAP может быть верно и для отличных от Active Directory решений;
- возможность разграничения доступа пользователей (групп пользователей) не только на уровне отдельных рабочих столов, но и их пулов, что драматически упрощает администрирование разграничения прав;
- упрощение мониторинга большого количества виртуальных рабочих мест: их работоспособности, использования ресурсов, подключения пользователей, распределения по хостам виртуализации и т.п.;
- возможность ограничения пула виртуальных рабочих столов по доступным ресурсам среды виртуализации: CPU, RAM, Disk;
- возможность развертывания пула виртуальных рабочих столов на нескольких хостах виртуализации с автоматическим распределением виртуальных машин пула по хостам;
- поддержка нескольких виртуальных сетей для пула рабочих столов, т.е. возможность размещать рабочие столы пула в разных виртуальных сетях.

По степени автоматизации жизненного цикла предусмотрено три типа пулов рабочих столов:

- Пул сессионных рабочих столов. Все виртуальные машины стартуют из единого мастер образа, все изменения, что пользователь внес в рабочий стол, удаляются (немедленно или с какой-то периодичностью). Пользователь подключается на любую свободную виртуальную машину из пула. Если для работы пользователя необходимы данные из его перемещаемого профиля — в решении должен быть предусмотрен соответствующий компонент.
- Полуавтоматический пул рабочих столов. В этом случае все виртуальные машины пула будут развертываться из единого мастер-образа, но каждая будет закреплена за каким-то одним пользователем. Все изменения что пользователь внесет в свою виртуальную машину сохранятся.
- Пул персонализированных рабочих столов. Минимальная автоматизация жизненного цикла, каждый рабочий стол уникален и даже может быть развернут из собственного шаблона.

Для пулов сессионных рабочих столов имеется возможность смены мастер-образа с последующим переразвертыванием пула. Поддерживается как принудительное обновление (когда все рабочие столы пула удаляются и развертываются заново), так и обновление только рабочих столов, не назначенных пользователям. С целью ускорения развертывания пула столы горячего резерва создаются параллельно. По умолчанию, одновременно могут подготавливаться 15 рабочих столов.

Управление пулами рабочих столов

Администратору **Базис.WorkPlace** доступен выбор многих рабочих столов пула для выполнения массовых операций. Доступна фильтрация выбора по таким параметрам, как:

- принадлежащие одному пулу;
- назначенные на конкретного пользователя;
- находящиеся в определенном статусе;
- с активными подключениями пользователей;
- размещенные на определенном хосте виртуализации.

Функций управления рабочими столами множество. Полный список доступен в документации. Здесь будут указаны самые важные функции, выделяющие **Скала^р МВ.ВРМ**:

- контроль версий агентов рабочих столов и их обновление как в отдельном рабочем столе, так и в выбранной группе или пуле рабочих столов;
- перевод рабочего стола в режим обслуживания;
- перенос рабочего стола в другой пул РС того же или другого типа (без потери привязки пользователя);
- завершение сеанса пользователя, принудительное отключение пользователя, отвязка пользователя от рабочего стола;
- отправка сообщения подключенным пользователям;
- подключение администратора в сессию пользователя для удаленной поддержки;

- предоставление доступа одному пользователю к нескольким рабочим столам из разных пулов, как сессионных, так и персонализированных;
- подключение одновременно к нескольким виртуальным рабочим столам с одного устройства доступа.

Управление пулами терминальных серверов

Терминальные серверы дополняют виртуальные рабочие места, предоставляя большую эффективность использования ресурсов ценой меньшей изоляции пользователей друг от друга. В случае терминального сервера пользователь получает одну из многих сессий на нем вместо выделенной под себя виртуальной машины.

Такая комплементарность приводит к тому, что в инфраструктурах ВРМ на большое число пользователей часто можно встретить одновременно и терминальные серверы, и виртуальные рабочие места.

При работе с пулами терминальных серверов администратору доступны инструменты автоматизации, которые позволяют массово разворачивать терминальные серверы из заранее подготовленного шаблона. Распределение пользователей между серверами пула происходит автоматически. С точки зрения пользователя нет никакой разницы, подключился ли он к терминальному серверу или к виртуальному рабочему месту.

Администратору доступны следующие функции работы с терминальными серверами и их пулами:

- создание, редактирование и удаление пулов терминальных серверов;
- редактирование параметров, выключение/запуск, перезагрузка и удаление терминального сервера;
- управление виртуальной средой терминального сервера;
- управление сессиями пользователей терминального сервера;
- отправка сообщений подключенным пользователям.

Одной из важных возможностей **Базис.WorkPlace** является функция «публикации приложения», или предоставление пользователю доступа к окну отдельного приложения с терминального сервера. Поддерживается доставка приложений, разработанных как для ОС семейства Windows, так и для Linux.

Для терминальных приложений не имеет значения, какая ОС установлена на устройстве доступа. Благодаря этому пользователь может на своем компьютере:

- работать с приложениями, несовместимыми с его ОС, например, с Windows-приложениями на ОС Linux;
- использовать несколько приложений, которые не могут быть одновременно установлены на одном ПК, например, разные версии одного и того же офисного пакета.

Управление пулами физических рабочих столов

Иногда наравне с виртуальными рабочими местами и терминальными серверами возникает необходимость обеспечить доступ некоторых пользователей до своего физического компьютера. В этом случае **Базис.WorkPlace** позволяет решить задачу при помощи пула физических рабочих столов.

Для физических рабочих столов обеспечиваются те же возможности централизованного управления доступом пользователей и уровень безопасности подключения, что и для виртуальных.

Создание такого пула в значительной степени автоматизировано:

1. Чтобы инициировать процесс, достаточно установить на офисный ПК сотрудника агент **Базис.WorkPlace** и указать в его настройках адрес Брокера ВРМ.
2. При запуске Агента он автоматически передает Брокеру информацию об этом ПК, на основании чего последний включается в каталог физических ПК.
3. Теперь он доступен администратору для добавления в пул физических рабочих столов.

3. ОТЛИЧИТЕЛЬНЫЕ ЧЕРТЫ

Отличительными чертами **Машины виртуальных рабочих мест Скала^р МВ.ВРМ** являются поставка модульного программно-аппаратного комплекса «под ключ», ориентированного на высокую надежность и высокую производительность.

Протестированный максимум в 16 000 единовременных подключений, отсутствие бутылочного горлышка.

Высокая надежность реализована в нескольких аспектах.

Во-первых, ВРМ-решение, гипервизор и программно-определяемая система хранения создавались и развиваются с упором на надежность. Для нас критично не допускать потерь данных из-за отказов хранилища. Резервирование данных настраивается — для особо критичных виртуальных машин можно повысить резервирование данных со стандартной «второй копии» до требуемых значений.

Высокая доступность компонентов ВРМ-решения обеспечивается штатной горизонтальной масштабируемостью каждого компонента, включая сервер управления платформой виртуализации.

Кроме того, для этих и других виртуальных машин доступен кластер высокой доступности платформы виртуализации, минимизирующий время простоя при отказах серверов. Он обеспечивает высокую доступность также и виртуальных рабочих мест.

Во-вторых — выбор и валидация оборудования на этапе R&D. Конфигурация Машины предусматривает резервирование всех потенциальных единых точек отказа оборудования. Это не только серверы и накопители, но и сетевые контроллеры и коммутаторы из состава Машины.

В-третьих — отсев брака оборудования на производстве.

Кроме того, высокий уровень автоматизации производства Машины гарантирует повторяемый результат и точную конфигурацию устанавливаемых программных компонентов.

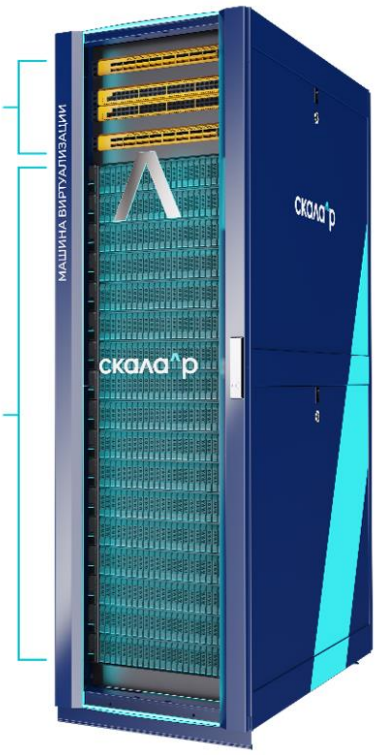
Последнее по порядку, но не по значению — служба поддержки из одного окна Скала^р.

4. СОСТАВ РЕШЕНИЯ

Машина виртуализации состоит из следующих блоков:

Коммутационный блок

Блок вычисления и хранения



Коммутационный блок обеспечивает сетевую связность несколькими сетевыми фабриками.

Блок вычисления и хранения обеспечивает вычислительные ресурсы и ресурсы хранения, на серверах этого блока выполняются программные компоненты Машины.

Коммутационный блок

Коммутационный блок представляет собой 2 или 3 набора коммутаторов для организации сетей для задач:

- интерконнекта — техническая сеть Машины для трафика программного хранилища;
- доступа — сеть для виртуальных машин;
- управления — сеть для доступа к IPMI-контроллерам серверов из состава Машины.

Типовые конфигурации коммутационного блока — 2+2+1 или 2+1 коммутатора.

Конфигурация 2+2+1

В этой конфигурации первая пара коммутаторов обеспечивает сеть доступа, вторая пара — коммутации. Еще один коммутатор обеспечивает сеть для контролеров управления IPMI.

В последнем случае коммутатор не дублирован в силу невозможности подключения контролеров IPMI более чем одним сетевым интерфейсом.

Конфигурация 2+1

В этой конфигурации одна пара коммутаторов обеспечивает и сеть интерконнекта, и сеть доступа. Разделение сетей достигается за счет их изоляции через VLAN. Сеть управления IPMI реализуется так же, как в первом варианте.

Выбор того, какую конфигурацию использовать, зависит от сайзинга, в частности, ожидаемой нагрузки на сети доступа и интерконнекта.

Кроме того, в зависимости от ряда факторов могут быть выбраны коммутаторы с портами 25, 40 или 100 Гбит/с. (Коммутатор для сети управления IPMI всегда с портами 1 Гбит/с).

Блок вычисления и хранения

Блок вычисления и хранения компонуется по модульному принципу. В зависимости от требуемых ресурсов изменяется количество модулей или конфигурация узлов в модулях.

Узлы вычисления Скала^р МВ.ВРМ

Машина виртуализации Скала^р МВ.ВРМ построена, как правило, на базе узлов собственного бренда Скала^р. Но, для гарантии удовлетворения требований заказчиков (в том числе по срокам поставок), поддерживаются партнерские отношения с некоторыми другими поставщиками серверного оборудования.

Выбор конкретного производителя обуславливается целесообразностью в конкретном проекте, в зависимости от таких факторов, как требования наличия Машины в реестре российской радиоэлектронной продукции, возможности поставки по оптимальной стоимости, и других факторов, позволяющих подобрать максимально подходящее решение в каждом конкретном случае.

В общем случае это универсальные серверы общего назначения в стоечном исполнении с конструктивом, достаточным для размещения не менее 4 дисков (обычно 12—24).

Минимальное число узлов (серверов) в составе одной Машины — 4. Максимальное число, технически, многие десятки и сотни, но оно обуславливается не ограничением на поддерживаемое число, а целесообразностью. Целесообразность определяется исходя из таких факторов, как, например, обеспечение сетевой связности (межстоечные сети доступа и/или интерконнекта), архитектурой отказоустойчивости (несколько кластеров / программных хранилищ среднего размера обычно предпочтительнее одного, но огромного).

Программные компоненты Машины виртуальных рабочих мест

Программная часть **Скала^р МВ.ВРМ** реализована с помощью компонентов, перечисленных ниже (Таблица 3).

Таблица 3. Компоненты Машины виртуализации Скала^р МВ.ВРМ

Наименование ПО	Назначение

ПО Базис.WorkPlace («Скала^р BPM (Виртуальное рабочее место)»)	Брокер подключений и организация инфраструктуры виртуальных рабочих мест.
ПО «Скала^р Управление»	Сервер управления платформой виртуализации. Управляет гипервизорами, кластерами высокой доступности и балансировки нагрузки, виртуальными машинами и проч.
ПО «Скала^р Управление — Система серверной виртуализации»	Гипервизор. Обеспечивает разделение ресурсов сервера между виртуальными машинами.
ПО «Скала^р Управление — Программно-определяемое хранилище»	Программно-определяемое хранилище. Обеспечивает распределенный дисковый массив.

Базис.WorkPlace

Ключевым программным компонентом Машины **Скала^р MB.BPM** является продукт для организации инфраструктуры виртуальных рабочих мест — **Базис.WorkPlace**, также известный как «Скала^р BPM (Виртуальное рабочее место)».

Инфраструктура виртуальных рабочих мест предполагает набор программного обеспечения, который решает следующие задачи:

- интеграция с системой виртуализации для развертывания из шаблона и управления жизненным циклом непосредственно виртуальных машин — рабочих мест;
- брокер соединений, обеспечивающий подключение пользователей к своим виртуальным рабочим места и терминальным серверам;
- обеспечение протокола доставки удаленных рабочих столов и отдельных приложений.

Скала^р Управление

Сервер управления платформой виртуализации размещается в одной или нескольких виртуальных машинах на серверах комплекса, а его агенты устанавливаются на всех физических серверах.

Серверы из состава Машины объединяются в одну или несколько групп (кластеров), для которых включается функция высокой доступности. Так как данные с используемого распределенного дискового хранилища доступны сразу всем серверам кластера, то при отказе сервера те виртуальные машины, которые выполнялись на нем в момент отказа, будут перезапущены на прочих серверах кластера.

Скала^р Управление — Система серверной виртуализации

Гипервизор, программное обеспечение виртуализации, устанавливается на каждом физическом сервере.

ПО Скала^р Управление — Система серверной виртуализации является классическим гипервизором на базе open-source решения KVM. Основные свойства:

- поддержка основных операционных систем, включая российские;
- полноценное управление жизненным циклом виртуальных машин;
- добавление устройств к виртуальной среде в процессе работы: ЦПУ, память, диски, сетевые интерфейсы;
- динамическое перераспределение памяти между виртуальными средами для увеличения физически доступной памяти (за счет освобождения неиспользуемой);
- резервное копирование виртуальных сред.

Скала^р Управление — Программно-определяемое хранилище

Также на каждом сервере устанавливается программное обеспечение распределенного дискового хранилища. Это ПО позволяет объединить все накопители, установленные в серверах Машины, в единое дисковое пространство. Оно используется любой из виртуальных машин этой Машины виртуализации и может быть использовано внешним потребителем (по iSCSI). Для данных на этом хранилище доступно резервирование, за счет чего обеспечивается высокая доступность данных и устойчивость к сбоям хранилища при единичных отказах серверов и накопителей.

Основные функции и свойства:

- алгоритмы обеспечения избыточности данных: хранение двух и более реплик данных на накопителях разных хостов комплекса **Скала^р МВ.ВРМ** или хранение блоков четности/избыточности (Erasure Coding). Немного упрощая, поддерживаются алгоритмы, логически похожие на RAID 1, RAID 6;
- поддержка накопителей HDD и SSD с интерфейсами SATA, SAS для получения характеристик, наиболее полно отвечающих вашим требованиям;
- гибкие возможности модернизации и обслуживания серверов без прерывания работы;
- настройка до 4-х уровней хранения (tier). Файлы-диски виртуальных машин привязываются к одному из уровней хранения, с определенным типом накопителей.

Лицензирование Машины

В Машине **Скала^р МВ.ВРМ** лицензированию подлежат следующие компоненты (Таблица 4).

Таблица 4. Лицензирование компонентов

Наименование ПО	Назначение	Единица лицензирования
Базис.WorkPlace (он же «Скала^р ВРМ (Виртуальное рабочее место)», оба названия актуальны)	Система виртуализации рабочих мест	Именованные пользователи или конкурентные сессии

Скала^р Управление — Система серверной виртуализации	Обеспечение виртуализации серверных систем (сервер управления входит в эту лицензию)	Процессор (сокет)
Скала^р Управление — Программно-определяемое хранилище	Реализация распределенного дискового массива	Тб полезной ёмкости

К каждому компоненту обязательно приобретение сертификата технической поддержки на 1 год минимум.

Кроме того, часть ПО доступна в разных редакциях. Таким образом, для лицензирования Машины следует определиться с редакцией и количеством лицензий.

Правила лицензирования Базис.WorkPlace

Для лицензирования BPM следует учесть следующие правила:

1. Доступна единственная редакция.
2. Подключения к виртуальным рабочим местам и к терминальным серверам лицензируются независимо. Для терминальных серверов доступно лицензирование только по конкурентным сессиям, для подключений к виртуальным рабочим местам доступен выбор между двумя вариантами лицензирования:
    a. именованный пользователь;
    б. конкурентная сессия.
3. Должно быть определено требуемое число лицензий каждого вида.
4. Следует выбрать наиболее подходящий под задачу протокол. Такой протокол как RX@Etersoft потребует дополнительной лицензии.
5. Приобретение технической поддержки обязательно.
6. Дополнительные лицензии рассчитываются отдельно по собственным правилам:
    a. виртуализация (описано в этом документе) — входит в состав Машины;
    б. лицензии на **гостевые ОС** для брокеров, диспетчеров и прочих сервисных виртуальных машин основного ПО Машины — предоставляются в рамках лицензий ПО Виртуализации и BPM;
    в. лицензии на гостевые ОС в терминальных серверах, на сами терминальные серверы, для пользовательских виртуальных машин — не входят в состав Машины.

Правила лицензирования гипервизора

В зависимости от максимального количества вычислительных узлов в машине виртуализации и дополнительных функций доступны три вида редакции гипервизора:

- базовая;
- корпоративная;
- расширенная.

Редакции различаются по максимальному количеству серверов, используемых в решении, и желаемой функциональности. Сравнительная таблица с количественными и функциональными возможностями редакций лицензий приведена ниже (Таблица 5).

Таблица 5. Сравнение редакций лицензий

Возможности продукта	Базовая	Корпоративная	Расширенная
Максимальное количество физических процессоров в 1 комплексе	8	32	256
Максимальный размер полезного хранилища в 1 комплексе, ТБ	50	1000	не ограничено
Пакеты технической поддержки	9x5	9x5, 24x7	9x5, 24x7
Режим высокой доступности	●	●	●
Мгновенные снимки (snapshot)	●	●	●
Живая миграция виртуальных машин	●	●	●
Управление пулами ресурсов	●	●	●
Ролевая модель администрирования	●	●	●
Встроенная система резервного копирования и восстановления	●	●	●
Интеграция со сторонними средствами обеспечения безопасности	●	●	●
Создание многоуровневого хранилища (tiering)*	●	●	●
Модули сбора данных о системе	●	●	●
Система мониторинга производительности и работоспособности	●	●	●
Интеллектуальные оповещения администраторам	●	●	●
Поддержка внешних систем резервного копирования и восстановления		●	●
Управление несколькими кластерами из единого центра		●	●
Динамическая миграция виртуальных машин между узлами в зависимости от		●	●

Возможности продукта	Базовая	Корпоративная	Расширенная
нагрузки с автоматической балансировкой узлов (DRS)			
Правила размещения виртуальных машин между хостами (affinity|antiaffinity rules)		•	•

Правила лицензирования программно-определяемого хранилища

Приобретение лицензий на данное ПО является обязательным на каждый Тбайт (двоичный, с точки зрения ОС) полезного пользовательского пространства, которое вычисляется по следующей формуле для каждого уровня (tier) ресурсов. Уровень хранения должен собираться на носителях одного и того же типа и номинала.

Формула для расчёта лицензируемой полезной ёмкости выглядит следующим образом:

*<Емкость накопителя десятичный ТБ> * <Количество накопителей> / <Фактор репликации> * 0.84,*

где:

- <Емкость накопителя> — емкость одного накопителя, используемого в распределенном дисковом массиве для хранения данных пользователей, в единицах, указанных на маркировке накопителя;
- <Количество накопителей> — общее количество накопителей, установленных в вычислительных узлах Скала^р МВ и используемых в распределенном дисковом массиве для хранения данных пользователей;
- <Фактор репликации> — параметр резервирования данных, влияющий на отношение сырой ёмкости дискового массива к полезной ёмкости. Например, при использовании типовой настройки репликации 3:2 <Фактор репликации> = 3;
- 0.84 — коэффициент перевода заводской ёмкости дисков в видимый ОС платформы объём.

Служебные диски по ОС, под службу MDS (см. ниже), под кэши записи не включаются в расчет.

Общая лицензируемая, она же полезная, ёмкость определяется как сумма всех расчетов по каждому уровню (tier). Дроби округляются до целого, в большую сторону.

5. ВЫСОКАЯ ДОСТУПНОСТЬ И ЗАЩИТА ДАННЫХ

Инфраструктура виртуальных рабочих мест реализуется прикладным ПО на платформе виртуализации. Высокая доступность компонентов **Базис.WorkPlace** реализована архитектурно возможностью развертывать их в кластерной конфигурации. Высокая доступность виртуальных рабочих мест обеспечивается, как правило, средствами платформы виртуализации.

Кроме того, важно обеспечить высокую доступность данных ВРМ (дисков виртуальных машин, данных профилей пользователей), а также «внешних» относительно ВРМ компонентов, таких как база данных ВРМ, сервис каталогов и пр.

Высокая доступность компонентов Базис.WorkPlace

Брокер ВРМ развертывается в трех экземплярах, образующих отказоустойчивый кластер.

По соображения сайзинга число экземпляров может быть увеличено, протестированным максимумом является 7.

Диспетчер подключений развертывается в нескольких экземплярах. Каждый из них самодостаточен и взаимозаменяем, поэтому в случае отказа какого-то из них достаточно чтобы пользователи обращались на другой диспетчер подключений. Это реализуется или соответствующей настройкой балансировщика нагрузки или, если использование балансировщика нагрузки было признано нецелесообразным, указанием списка адресов диспетчеров подключений в настройках клиента ВРМ.

Высокая доступность виртуальных рабочих мест

Высокая доступность виртуальных рабочих мест обеспечивается функционалом кластера высокой доступности платформы виртуализации. Если произошел отказ какого-то из серверов, и отказали работающие на нем виртуальные машины — они будут перезапущены на прочих серверах Машины.

Высокая доступность данных

Программно-определяемая подсистема хранения из состава Машины **Скала^р МВ.ВРМ** хранит данные с настраиваемой избыточностью. Поддерживается два алгоритма:

- создание реплик, полных копий данных;
- избыточное кодирование (Erasure Coding).

В первом случае для каждого «блока» данных создается указанное число копий, притом никакие копии этого блока не будут расположены на одном и том же сервере (Рис. 6).

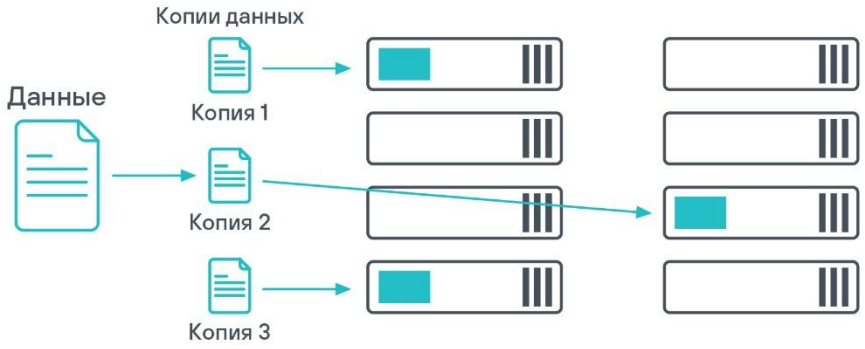


Рис. 6. Создание реплик, полных копий данных

За счет этого в случае отказа серверов или накопителей в них данные виртуальной машины продолжат оставаться доступными.

Обычно используется политика хранения в 2 или 3 копиях.

Во втором случае резервирование обеспечивается добавлением блоков четности/избыточности. Могут использоваться следующие варианты (данные + четность), в зависимости от желаемого уровня доступности и количества хостов в системе: 3 + 2, 5 + 2, 7 + 2, 17 + 3. Схема реализации технологии избыточного кодирования для случая 5 + 2 приведена ниже (Рис. 7).

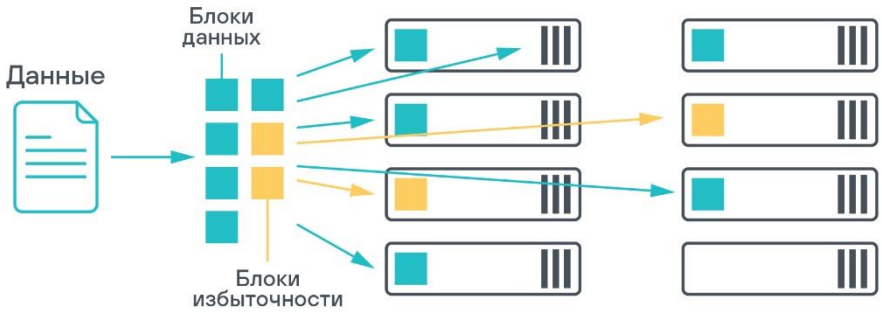


Рис. 7. Избыточное кодирование

Преимущества и ограничения этих вариантов

Преимущества реализации избыточности данных репликами:

- высокая производительность дисковой подсистемы;
- быстрое восстановление недостающих копий данных при отказе одного или двух серверов;
- процесс восстановления недостающих реплик практически не влияет на общую производительность дискового хранилища;
- чаще целесообразен для небольших комплексов.

К недостаткам режима создания реплик можно отнести высокие накладные расходы на хранение данных.

Режим избыточного кодирования позволяет более эффективно использовать дисковое пространство, но у него имеются следующие ограничения:

- для достижения целевой производительности может потребоваться больше накопителей / выбор более быстрых накопителей в некоторых сценариях;
- более низкая скорость восстановления недостающих копий данных (rebuild) при потере одного или двух серверов;
- дополнительная загрузка процессоров;
- для его использования требуется пять серверов и больше.

Какой вариант целесообразно выбрать для тех или иных пулов виртуальных рабочих мест зависит от их критичности.

В ряде сценариев целесообразно хранить данные профилей пользователей не «внутри» виртуальных рабочих мест, а на отдельном хранилище перемещаемых профилей.

В таком случае высокая доступность данных профилей должна быть обеспечена выбранным хранилищем (не входит в состав Машины).

Катастрофоустойчивость

Существуют два варианта организации катастрофоустойчивой инфраструктуры.

В простом случае может быть целесообразно реализовать «растянутый кластер» средствами платформы виртуализации и программно-определяемой системы хранения.

В другом случае строится две независимые инфраструктуры BPM на своей площадке каждая. Идентичность виртуальных рабочих мест (версии ОС, наборы ПО и т.п.) обеспечивается администраторами. Потребуется реализовать катастрофоустойчивость перемещаемых профилей на каком-то хранилище (не входит в состав Машины).

В обоих вариантах потребуется реализовать «переключение» между площадками на «точке входа» пользователей в BPM, обычно ею выступает балансировщик нагрузки.

Реализация катастрофоустойчивой инфраструктуры содержит в себе много нюансов, описание которых выходит за рамки данного документа. В случае интереса к катастрофоустойчивой конфигурации Машины следует обратиться за консультацией к представителю Скала^р или сертифицированного партнера.

Резервное копирование

Резервное копирование инфраструктуры BPM сводится, в основном, к резервной копии содержимого базы данных BPM и к копии компонента «deploy», с помощью которого можно переразвернуть компоненты BPM.

Резервное копирование виртуальных машин (таких как «золотые образы») можно осуществлять встроенным в сервер управления виртуальной платформы инструментом.

6. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Информационная безопасность **Скала^р МВ.ВРМ** обеспечивается за счет использования комплекса мер:

- Идентификация и аутентификация пользователей, включая двухфакторную. Поддерживаются следующие токены и смарт-карты:
  - ESMART Token ГОСТ;
  - Рутокен ЭЦП 2.0;
  - eToken;
  - JaCarta.
- Идентификация и авторизация пользовательских устройств доступа.
- Встроенная настраиваемая политика паролей и поддержка парольных политик подключаемых внешних LDAP-каталогов.
- Подключение к виртуальным рабочим местам через единую точку входа в ВРМ — Диспетчер подключений. Прямой доступ невозможен.
- Автоматическое блокирование учетных записей, устройств доступа, IP-адресов при многократном вводе неправильного логина/пароля.
- Ролевая модель доступа, при которой пользователю ВРМ доступны только действия, определенные назначенной ему ролью.
- Разграничение прав доступа из корпоративной и из внешней сетей.
- Сессионное подключение пользователей к виртуальным ресурсам: для каждого подключения каждого пользователя создается индивидуальная сессия и подготавливается к работе только выбранный им рабочий стол. После завершения сеанса пользователя сессия завершается, как и работа виртуального рабочего стола.
- Регулярный автоматический контроль целостности компонентов системы.

Машина виртуальных рабочих мест может быть использована в информационных системах с дополнительными требованиями согласно нормативной документации.

Те или иные версии ПО из состава Машины виртуализации получали сертификат ФСТЭК. Кроме того, Машина совместима с рядом аппаратных и программных наложенных средств обеспечения информационной безопасности.

Для получения текущего статуса сертификации или возможности использования наложенных средств следует обратиться к представителю Скала^р.

Таким образом, Машина виртуализации может быть использована:

- в государственных информационных системах (ГИС) вплоть до 1 класса;
- информационных системах персональных данных до 1 уровня защищенности;
- в системах, где к актуальным отнесены угрозы 1-го и 2-го типа.

Однако каждый такой проект требует отдельной проработки. Для консультации по этому вопросу рекомендуется обратиться к профильному системному интегратору или представителю Скала^р.

7. ГАРАНТИРОВАННОЕ КАЧЕСТВО

Качественные показатели Машины виртуальных рабочих мест **Скала^р МВ.ВРМ** обеспечиваются её соответствием проверенному стандартному варианту, соблюдением установленных норм и требований по формированию, реализацией работ высококвалифицированными специалистами на всех этапах жизненного цикла.

Производство (комплектование и развёртывание ПО)

- При производстве используются высококачественные комплектующие.
- Сборка продукции осуществляется строго в соответствии с утверждённым планом размещения компонентов.
- Первичное развертывание ПО осуществляется в автоматическом режиме.
- Дополнительные настройки ПО осуществляются в соответствии с утверждённой методикой и пошаговой инструкцией.
- Осуществляется функциональное тестирование сформированной Машины.
- Отклонения от типового решения **Скала^р МВ.ВРМ** исключены.

Передача в эксплуатацию

- **Скала^р МВ.ВРМ** полностью сформирована, протестирована, готова к размещению в сети заказчика и размещению прикладного ПО.
- В комплекте со **Скала^р МВ.ВРМ** передаются паспорт решения, сертификат на поддержку.
- Проводится обучение специалистов заказчика работе со **Скала^р МВ.ВРМ** (по запросу).

Дополнительные требования

Возможна реализация дополнительных требований по модернизации или развитию **Скала^р МВ.ВРМ** (по запросу), в том числе:

- аппаратная модернизация решения;
- горизонтальное или вертикальное масштабирование нового или имеющегося решения;
- изменение функциональности компонентов дистрибутивов ПО, их доработка;
- тестирование приложений, производительности приложений или иное другое запрошенное тестирование.

Работы выполняются с участием архитекторов и инженеров, разработчиков Машины и ПО **Скала^р МВ.ВРМ**.

8. ТРЕБОВАНИЯ К РАЗМЕЩЕНИЮ РЕШЕНИЯ

Решение представляет собой серверный монтажный шкаф 19”, высота 42U, с дальнейшей возможностью модульной расширяемости до 14 стоек.

Наполнение шкафа оборудованием и совокупный вес зависят от выбранного варианта решения и могут составлять от 400 до 800 кг.

Для подключения шкафа к системе электроснабжения должны быть предусмотрены два независимых входа электропитания.

Расчётная потребляемая мощность шкафа составляет от 6 до 11 кВт.

В месте установки должны быть предусмотрены соответствующие мощности по отводу тепла.

Требования для подключения Машины к локальной сети заказчика определяются на этапе формирования спецификации Машины.

При развёртывании решения на нём будут выполнены настройки сетевых адресов в соответствии со структурой сети заказчика. Заказчик должен предоставить необходимые данные в соответствии с номенклатурой компонентов решения.

В сети заказчика должны быть настроены соответствующие маршруты и права доступа.

Дальнейшие мероприятия по вводу в эксплуатацию осуществляются заказчиком путём настройки прикладных программных систем.

9. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Поставка **Скала^р МВ.ВРМ** осуществляется с предварительными сборкой, тестированием и настройкой оборудования согласно требованиям заказчика. Качественная поддержка **Скала^р МВ.ВРМ** обеспечивается едиными стандартами гарантийного и постгарантийного технического обслуживания:

- Пакет услуг по технической поддержке на первый год включен в поставку.
- Заказчик может выбирать пакет в базовом режиме 9x5 или в расширенном режиме 24x7 (опция для критической функциональности).
- Срок начально приобретаемой технической поддержки может быть увеличен до 3 и 5 лет, также доступна пролонгация поддержки.
- Возможно включение в состав стандартных пакетов дополнительных опций и услуг.

Состав типовых пакетов услуг по технической поддержке представлен в таблице ниже (Таблица 6).

Таблица 6. Пакеты услуг по технической поддержке Скала^р МВ.С

Услуга	Пакет «9x5»	Пакет «24x7»
Режим «Обслуживание комплекса Скала^р МВ.ВРМ в режиме 9x5» (в рабочее время по рабочим дням)	+	—
Режим «Обслуживание комплекса Скала^р МВ.ВРМ в режиме 24x7» (круглосуточно)	—	+
Предоставление доступа к системе регистрации запросов/инцидентов Service Desk	+	+
Предоставление доступа к базе знаний по продуктам Скала^р	+	+
Предоставление обновлений лицензионного ПО Скала^р	+	+
Диагностика, анализ и устранение проблем в работе комплекса Скала^р МВ.ВРМ, включая: ▪ устранение аппаратных неисправностей; ▪ техническое сопровождение ПО.	+	+
Консультации по работе комплекса Скала^р МВ.ВРМ	+	+

Услуга	Пакет «9x5»	Пакет «24x7»
«Защита конфиденциальной информации» (неисправные носители информации не возвращаются Заказчиком)	Опция	Опция
Замена и ремонт оборудования по месту установки	+	+
Доставка оборудования на замену за счет производителя	+	+
Расширенные опции обслуживания	—	+
Времена реагирования и отклика, не более:		
Время регистрации обращений	30 минут, рабочие часы (9x5)	30 минут, круглосуточно (24x7)
Подключение специалиста к решению инцидентов критичного и высокого уровней	В течение 1 рабочего часа (9x5)	В течение 1 часа (24x7)

Примечание к срокам ремонта оборудования: комплекс **Скала^р МВ.ВРМ** архитектурно является устойчивым к выходу из строя отдельных компонентов и даже узлов, поэтому нет необходимости в обеспечении дорогостоящего сервиса срочного восстановления оборудования в течение суток и менее. В комплексе предусмотрено, как минимум, двойное резервирование основных компонентов, позволяющее сохранять данные и работоспособность даже при выходе из строя нескольких дисков и/или серверов.

Полное описание услуг поддержки доступно на сайте www.skala-r.ru.

О КОМПАНИИ

Компания Скала^р — разработчик и производитель модульной платформы для высоконагруженных корпоративных и государственных информационных систем.

Машины Скала^р являются серийно выпускаемыми преднастроенными комплексами и позволяют осуществлять быстрое развёртывание и ввод в эксплуатацию.

Модульный принцип обеспечивает интеграцию разнородных компонентов ИТ-инфраструктуры в единую платформу предприятий, корпораций и ведомств.

Единые поддержка и сервисное обслуживание для всех продуктов линейки Скала^р от производителя обеспечивают оперативное разрешение инцидентов на стыке технологий.

Дополнительная информация — на сайте www.skala-r.ru.