|  |
| --- |
| **Проект {{ project\_name }} ПАК СКАЛА^Р {{ pac\_type }}**  **Инсталляционная карта** |
|  |
|  |
|  |

# История изменений

| **Версия** | **Дата** | **Автор изменений** | **Описание изменений** |
| --- | --- | --- | --- |
| 1.0 | {{ changes.change\_date }} | {{ changes.change\_author }} | {{ changes.change\_description }} |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Согласовано

|  |  |  |  |
| --- | --- | --- | --- |
| **ФИО** | **Должность** | **Дата** | **Подпись** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Содержание

[1 История изменений 2](#_Toc175148662)

[2 Согласовано 3](#_Toc175148663)

[3 Содержание 4](#_Toc175148664)

[4 Введение 5](#_Toc175148665)

[5 Общая модель комплекса 6](#_Toc175148666)

[6 Схема интеграционного взаимодействия 8](#_Toc175148667)

[7 Структура внутренних соединений 9](#_Toc175148668)

[8 Подключение в сеть Заказчика 10](#_Toc175148669)

[9 Предлагаемое размещение оборудования в шкафу 14](#_Toc175148670)

[10 Обеспечение отказоустойчивости, масштабируемости и эксплуатации ПАК 15](#_Toc175148671)

[11 Физическая схема развертывания 18](#_Toc175148672)

[12 Серверы ПАК СКАЛА^Р МБД.Г 19](#_Toc175148673)

[12.1 Требования к оборудованию 19](#_Toc175148674)

[12.2 Требования к ОС 19](#_Toc175148675)

[12.3 Требования к установленному ПО 19](#_Toc175148676)

[12.4 Права доступа 19](#_Toc175148677)

[12.5 Требования к дисковой подсистеме 19](#_Toc175148678)

[13 Рабочие места 22](#_Toc175148679)

[13.1 Требования к оборудованию 22](#_Toc175148680)

[13.2 Требования к установленному ПО 22](#_Toc175148681)

# Введение

В данном документе описываются принципы и требования по установке на территории Банка ВТБ (ПАО) (далее – Банк) оборудования ПАК СКАЛА^Р {{ pac\_type }} (см. таб.1) и его подключению в ЛВС Банка.

# Общая модель комплекса

Таблица 1. Спецификация ПАК СКАЛА^Р {{ pac\_type }} и поставочные реквизиты

| **Наименование** | **Кол-во, шт.** | **Комментарий** | **Год и порядковой номер поставки** | **Партийный номер модуля Скала^Р ПАК** |
| --- | --- | --- | --- | --- |
| {%tr for item in tbl1\_contents %} |  |  |  |  |
| {{ item.cols[‘spec’] }} | {{ item.cols[‘amount’] }} | {{ item.cols[‘comment’] }} | {{ item.cols[‘date’] }} | {{ item.cols[‘articul’] }} |
| {%tr endfor %} |  |  |  |  |

Таблица 2. Ресурсы хоста виртуализации, выделенные под виртуальные машины (далее - ВМ)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Имя ВМ** | **ОС** | **vCPU** | **RAM, ГБ** | **Размещение** | | **Комментарий** |
| **Объем диска, ГБ** | **Тип устройства** |
| {%tr for item in tbl2\_contents %} |  |  |  |  |  |  |
| {{ item.cols[‘name’] }} | {{ item.cols[‘OS’] }} | {{ item.cols[‘vCPU’] }} | {{ item.cols[‘RAM’] }} | {{ item.cols[‘space’] }} | {{ item.cols[‘diskType’] }} | {{ item.cols[‘comment’] }} |
| {%tr endfor %} |  |  |  |  |  |  |

# Схема интеграционного взаимодействия

Не используется. Наполнение раздела в зоне ответственности Заказчика.

# 

# Структура внутренних соединений

Таблица 3. Таблица коммутации ПАК

| **№  п.п.** | **Откуда** | | **Куда** | | **Скорость  (Гбит/c)** | **Тип** |
| --- | --- | --- | --- | --- | --- | --- |
| **Устройство** | **Порт** | **Устройство** | **Порт** |
| {%tr for item in tbl3\_contents %} |  |  |  |  |  |  |
| {{ item.cols[‘num’] }} | {{ item.cols[‘s\_name’] }} | {{ item.cols[‘s\_port’] }} | {{ item.cols[‘d\_name’] }} | {{ item.cols[‘d\_port’] }} | {{ item.cols[‘speed’] }} | {{ item.cols[‘type’] }} |
| {%tr endfor %} |  |  |  |  |  |  |

# Подключение в сеть Заказчика

Подключение ПАК к сети Банка происходит в зоне безопасности {{ segment\_name }} двумя контурами: {{ segment\_data }} (взаимодействие серверов) и {{ segment\_mgmt }} (интерфейсы управления серверами).

* Контур {{ segment\_data }} обеспечивает подключение серверов к фабрике коммутаторов. Сопряжение с сетью Банка осуществляется по схеме второго уровня MLAG посредством 4-х трансиверов (по 2 на каждый коммутатор) 100GBASE-DR1, предоставляя суммарную пропускную способность в 400 Гбит/с, соединенных оптическими патч-кордами LC-LC. Контур подключается через trunk отдельным VLAN {{ vlan\_data }} и имеет выделенную сеть {{ data\_net }}.
* Контур {{ segment\_mgmt }} обеспечивает доступ к интерфейсам управления со стороны Банка. Каждый коммутатор управления подключается к одному коммутатору Банка посредством интерфейса 1000-BASE-T. Контур подключается через trunk одним VLAN {{ vlan\_mgmt }} (интерфейсы iBMC и интерфейсы управления коммутаторами) с сетью {{ ipmi\_net }}.

В коммутаторе управления ПАК предусмотрены «сервисные порты», предназначенные для физического подключения инженеров и обслуживающего персонала. См. **Таблица 6. Сервисные порты ПАК**

{{ img1 }}

Рисунок 1. Схема ПАК сетевая структурная

{{ img2 }}

Рисунок 2. Схема ПАК сетевая логическая

Таблица 4. Адреса интерфейсов серверного оборудования и ВМ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№** | **Имя хоста \ ВМ** | **Роль \ Имя ВМ** | **IP DATA**  **{{ data\_net }}** | **IP IPMI**  **{{ ipmi\_net }}** | **IP MON Vision**  **{{ vision\_net }}** | **Год и порядковый номер поставки** |
|  | {%tr for item in tbl4\_contents %} |  |  |  |  |  |
| {{ item.cols[‘num’] }} | {{ item.cols[‘name’] }} | {{ item.cols[‘role’] }} | {{ item.cols[‘ip\_d’] }} | {{ item.cols[‘ip\_m’] }} | {{ item.cols[‘ip\_v’] }} | {{ item.cols[‘date’] }} |
|  | {%tr endfor %} |  |  |  |  |  |

Таблица 5. Адреса интерфейсов коммутаторов ПАК

| **№** | **Имя коммутатора** | **Тип** | **IP MGMT**  **{{ mgmt\_net }}** | **Год и порядковый номер поставки** |
| --- | --- | --- | --- | --- |
|  | {%tr for item in tbl5\_contents %} |  |  |  |
| {{ item.cols[‘num’] }} | {{ item.cols[‘name’] }} | {{ item.cols[‘type’] }} | {{ item.cols[‘ip\_m’] }} | {{ item.cols[‘date’] }} |
|  | {%tr endfor %} |  |  |  |

Таблица 6. Сервисные порты ПАК

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Размещение** | | | **Роль** | **DNS-имя** | **Порт** | **VLAN** |
| **ЦОД** | **Стойка** | **Unit** |
|  |  |  |  | {%tr for item in tbl6\_contents %} |  |  |
| {{ item.cols[‘dc’] }} | {{ item.cols[‘rack’] }} | {{ item.cols[‘unit’] }} | {{ item.cols[‘role’] }} | {{ item.cols[‘name’] }} | {{ item.cols[‘port’] }} | {{ item.cols[‘vlan’] }} |
|  |  |  |  | {%tr endfor %} |  |  |

# Предлагаемое размещение оборудования в шкафу

{{ img3 }}

# Обеспечение отказоустойчивости, масштабируемости и эксплуатации ПАК

**Масштабируемость** системы обеспечивается за счет возможности горизонтальной масштабируемости сегмент-серверов СУБД ADB.

СУБД ADB имеет в основе распределенную массивно-параллельную архитектуру на основе PostgreSQL и реализует концепцию «Shared Nothing» - когда узлы кластера, которые взаимодействуют для выполнения вычислительных операций, не разделяют ресурсы: каждый из них имеет собственную память, операционную систему и жесткие диски. За счет этого ADB реализует принцип горизонтальной масштабируемости: разбиение системы на отдельные структурные компоненты с независимыми физическими машинами, параллельно выполняющих запросы. Таким образом, добавление к системе новых узлов позволяет горизонтально масштабировать общую производительность.

**Отказоустойчивость** системы обеспечивается за счет следующих элементов:

1. Резервный (Standby) мастер-сервер.

В кластере ADB имеются 2 мастер-сервера (основной и резервный), расположенные на разных серверах. Резервный мастер-сервер синхронизируется с основным мастер-сервером с помощью используемой в СУБД PostgreSQL технологии опережающей записи (Wright Ahead Log, WAL – все изменения таблиц и индексов записываются в файл только после их занесения в журнал). Переключение мастер-сервером осуществляется в ручном режиме с помощью соответствующих команд. Failover клиентских подключений возможно реализовать несколькими способами:

* использовать Failover connection string. Например, jdbc:postgresql://master-1-ip:5432,master-2-ip:5432/adb&USER=etl\_user;
* настроить виртуальный IP-адрес для всех клиентов и использовать балансер для переключения коннекта с мастера на запасной мастер;
* использовать DNS-имя сервера для подключения клиентов. В случае выхода из строя мастер сервера, прописывать в DNS ip-адрес запасного сервера;
* использовать pgbouncer.

1. Зеркалирование сегментов с данными.

Данные в кластере ADB хранятся на сегмент-серверах, каждый из которых состоит из нескольких сегментов (инстансов) Greenplum Database PostgreSQL. Резервирование сегмент-серверов осуществляется при помощи создания копии-зеркала сегмент-инстанса, который хранится на другом сегмент-сервере. В случае отказа одного или нескольких сегментов они помечаются как сбойные и вместо них автоматически запускаются их зеркальные сегменты. Репликация данных для зеркальных сегментов происходит с помощью используемой в СУБД PostgreSQL технологии опережающей записи (Wright Ahead Log, WAL – все изменения таблиц и индексов записываются в файл только после их занесения в журнал).

1. Использование нескольких интерконнектов.

Позволяет повысить пропускную способность канала взаимодействия сегментов между собой и обеспечить отказоустойчивость кластера за счет перераспределения трафика. Распределение сегментов по сетевым интерфейсам выбирается индивидуально и может подстраиваться под задачи кластера – так, например, все основные сегменты можно заставить использовать один сетевой интерфейс, резервные сегменты же будет использовать второй.

1. Аппаратный RAID.

Дисковые массивы с данными на сегмент-серверах объединены в RAID10 для повышения производительности и обеспечения дополнительной отказоустойчивости в случае выхода из строя одного из дисков.

**Виртуализация ПО СКАЛА-Р Управление** -система серверной виртуализации ПО СКАЛА-Р Управление является гипервизором, реализованным на базе KVM.

Виртуальные среды — это общее наименование виртуальных машин и контейнеров виртуализации в ПО СКАЛА-Р Управление. Виртуальные среды размещают на хостах и используют их физические ресурсы для своей работы.

Масштабируемость на уровне хоста виртуализации обеспечивается:

* Возможностью добавления дисковых ресурсов в сервер с обеспечение отказоустойчивости на уровне организации аппаратного RAID;
* Возможностью добавления памяти RAM в сервер.

Масштабируемость виртуальных сред обеспечивается следующим встроенным функционалом СКАЛА-Р управления:

* Динамическое назначение ресурсов для виртуальной среды в процессе ее работы: ЦПУ, память, диски, сетевые интерфейсы;
* Предоставление виртуальным средам большей памяти, чем доступно физически, за счет динамического перераспределения памяти между виртуальными средами и освобождения неиспользуемой памяти;
* Исчерпывающий набор функций управления жизненным циклом виртуальных машин.

Отказоустойчивость виртуальных сред обеспечивается:

* Созданием резервных копий, снимков и клонов виртуальных сред с последующим хранением на внешнем устройстве через подключенный к среде виртуализации NFS каталог[[1]](#footnote-1).

**ПО СКАЛА^Р Геном. Управление ПАК** -система производства и управления жизненным циклом Машин Скала^р.

Система снижает влияние человеческого фактора при обслуживании и эксплуатации, сокращает время проведения процедур эксплуатации, упрощает процесс обновления компонентов Машины.

Система обеспечивает:

* Обновление компонентов ОС и прикладного ПО Машины;
* Управление картами IP-адресации Машин;
* Поддержание в актуальном состоянии прошивок аппаратной части Машины;
* Актуализация документов, сопровождающих Машину.

**ПО СКАЛА^Р Визион. Мониторинг ПАК** –система мониторинга Машин Скала^р.

Система осуществляет процесс мониторинга программных компонент ПАК, осуществляет сбор информации о количестве и составе управляемых объектов, метрик, выполняет построение отчетов по данным мониторинга, обеспечивает оповещение при сбоях в работе.

Система обеспечивает:

* Обеспечивает мониторинг компонентов Машин Скала^р как системного уровня, так и уровня ПО ADB;
* Обеспечивает эффективный сбор, хранение и анализ метрик компонентов Машин Скала^р;
* Помогает в принятии решений при нетиповых ситуациях. Актуализация документов, сопровождающих Машину

# Физическая схема развертывания

В данном разделе описывается распределение компонент по физическому оборудованию, а также указываются коммутационные требования к сетевому взаимодействию между компонентами ПАК.

{{ img4 }}

Рисунок 3. Схема физических подключений ПАК

# Серверы ПАК СКАЛА^Р МБД.Г

## Требования к оборудованию

Перечень оборудования приведен в разделе 5. Дополнительных требований не предъявляется.

## Требования к ОС

* ОС для всех физических узлов кластера – {{ OS\_version }};
* ОС для всех служебных ВМ кластера – {{ OS\_version }}.

## Требования к установленному ПО

Требования к ПО не предъявляются, т.к. все необходимое ПО содержится в комплекте поставки ПАК.

## Права доступа

Требования к правам доступа будут проработаны в рамках согласования архитектуры ИБ и связанных артефактов.

## Требования к дисковой подсистеме

Дисковая подсистема каждого из серверов укомплектована при поставке ПАК. Расширение дисковой подсистемы не предусматривается. Масштабирование емкости кластера без падения уровня производительности достигается добавление дополнительных сегмент-узлов в ПАК однотипной аппаратной конфигурации.

Таблица 7. Параметры дисковой подсистемы по ролям узлов ПАК

| **№** | **Роль** | **Спецификация дисковой подсистемы сервера ПАК** | **Кол-во дисков \ Тип RAID \ Назначение группы (например - ОС)** | **RAID-группа \ Тип раздела \ Раздел, Гб (объем) \тип FS \ точка монтирования (по необходимости).** | **Точка монтирования - параметры** |
| --- | --- | --- | --- | --- | --- |
|  | {%tr for item in tbl7\_contents %} |  |  |  |  |
| {{ item.cols[‘num’] }} | {{ item.cols[‘type’] }} | {{ item.cols[‘spec’] }} | {{ item.cols[‘raid’] }} | {{ item.cols[‘mount’] }} | {{ item.cols[‘params’] }} |
|  | {%tr endfor %} |  |  |  |  |

Таблица 8. Физическая структура дисковой подсистемы на уровне ОС Segment-узлов

|  |  |  |  |
| --- | --- | --- | --- |
| **NAME** | **SIZE** | **TYPE** | **MOUNTPOINT** |
| {%tr for item in tbl8\_contents %} |  |  |  |
| {{ item.cols[‘name’] }} | {{ item.cols[‘size’] }} | {{ item.cols[‘type’] }} | {{ item.cols[‘mount’] }} |
| {%tr endfor %} |  |  |  |

Таблица 9. Физическая структура дисковой подсистемы на уровне ОС Master-узлов

|  |  |  |  |
| --- | --- | --- | --- |
| **NAME** | **SIZE** | **TYPE** | **MOUNTPOINT** |
| {%tr for item in tbl9\_contents %} |  |  |  |
| {{ item.cols[‘name’] }} | {{ item.cols[‘size’] }} | {{ item.cols[‘type’] }} | {{ item.cols[‘mount’] }} |
| {%tr endfor %} |  |  |  |

Таблица 10. Физическая структура дисковой подсистемы на уровне ОС ADCC-узлов

|  |  |  |  |
| --- | --- | --- | --- |
| **NAME** | **SIZE** | **TYPE** | **MOUNTPOINT** |
| {%tr for item in tbl10\_contents %} |  |  |  |
| {{ item.cols[‘name’] }} | {{ item.cols[‘size’] }} | {{ item.cols[‘type’] }} | {{ item.cols[‘mount’] }} |
| {%tr endfor %} |  |  |  |

# Рабочие места

## Требования к оборудованию

* LAN соединение до всех компонентов, присутствующих на схемах;
* Соединение должно поддерживать протоколы: HTTP/HTTPS, sql\*net, ssh, sftp, jdbc;
* Минимальные системные требования ограничиваются минимальными системными требованиями к ОС (Windows 10).

## Требования к установленному ПО

Таблица 10. Пакеты ПО, установленные на узлы кластера ADB

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 1 | chrony | 16 | netcat | 31 | nfs-common |
| 2 | astra-updat | 17 | fio | 32 | dnsutils |
| 3 | cron | 18 | lsof | 33 | openjdk-11-jdk[[2]](#footnote-2) |
| 4 | sosreport | 19 | psmisc |  |  |
| 5 | net-tools | 20 | pigz |  |  |
| 6 | telnet | 21 | strace |  |  |
| 7 | unzip | 22 | tcpdump |  |  |
| 8 | tar | 23 | ipmitool |  |  |
| 9 | curl | 24 | gdb |  |  |
| 10 | wget | 25 | pciutils |  |  |
| 11 | htop | 26 | lshw |  |  |
| 12 | atop | 27 | hwinfo |  |  |
| 13 | nmon | 28 | dmidecode |  |  |
| 14 | iftop | 29 | sysstat |  |  |
| 15 | iperf | 30 | python3 |  |  |

1. Подробное описание режима резервного копирования виртуальных сред приведено в артефакте проекта «Руководство администратора ИС» [↑](#footnote-ref-1)
2. OpenJDK 11 можно взять из extended repo Астры [↑](#footnote-ref-2)