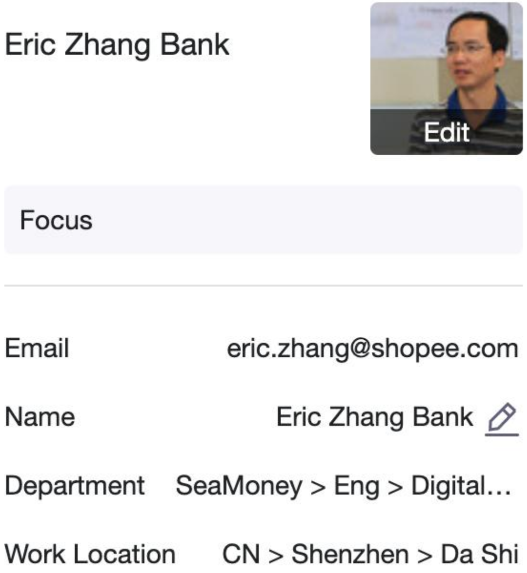
TE{HADEMY TE{HADEMY

Technology risk prevention and control in Digital Bank

eric.zhang@shopee.com

Self Introduction



Eric Zhang Bank

Focus

Email	eric.zhang@shopee.com
Name	Eric Zhang Bank
Department	SeaMoney > Eng > Digital…
Work Location	CN > Shenzhen > Da Shi

ICBC 中国工商银行

阿里巴巴 Alibaba.com

蚂蚁集团 ANT GROUP

Shopee

seaMoney

Agenda

1. **Technology Risk Background and Objectives**
    a. Technology risk background
    b. Technology risk prevent and control objectives

2. **Data consistency risk prevention and control**
    a. Cross database consistency risk(跨库一致性风险)
    b. Cross system consistency risk(跨系统一致性风险)
    c. Cross datacenter consistency risk(跨机房一致性风险)

3. **Business continuity risk prevention and control**
    a. Daily development and operational risk
    b. DR Switching Risk

4. **Q&A**

Technology Risk Background and Objectives

技术风险背景

近期，金融信息系统频繁出现中断，技术风险防控的重要性凸显。

2023.11

DBS(星展银行)

新加坡金管局强制实施 六个月暂停 星展银行的非必要活动（2023 年星展银行银行服务的 5 项严重中断）

2023.03

Shopee Indonesia Bank

Shopee Indonesia Bank core database hardware failure, the app cannot be logged in, and portal/payment services are unavailable,the incident lasted for 0.5 hours;

2021.11

DBS(星展银行)

DBS Bank's online banking service was down due to daily service upgrades and thousands of customers complained; the service was interrupted for nearly 48 hours

2019.08

CCB(建设银行)

China Construction Bank's mobile banking is out of order, and inter-bank transfer transactions cannot be credited in real time; the outage lasts for 1.5 hours

2016.01

HSBC(汇丰银行)

HSBC's online banking failed and 17 million personal and business accounts were unable to log in normally for 9 hours

2015.12

Ant Group(蚂蚁集团)

Ant Financial system malfunctioned, Yu'e Bao earnings were repeatedly distributed, and the financial loss was more than 100 million.

技术风险定义：

Any adverse situation caused by the use of computer hardware, software, and networks（计算机硬件、软件、网络所引发的不利情况）, including program errors, system downtime, software defects, operating errors, hardware failures, insufficient capacity, network vulnerabilities, etc. [Worldwide standards for banking]

技术风险特征：

隐藏性（隐蔽性）。技术风险就像病毒一样，长期潜伏在人体内。一般情况下，不会影响日常运营。但随着内外部环境的发展变化，如果不采取风险缓释措施，可能会发展成为风险事件。

突然性（突发性）。技术风险事件往往伴随着自然环境的变化或人为主观失误而发生，如地震、火灾、网络攻击等，具有随机性，难以预测。一旦发生，它们可能会失控并迅速蔓延。

惨重（灾难性）。一些全球重大科技风险事件往往会造成服务中断、财务损失、客户流失，甚至可能导致机构倒闭等严重后果。

技术风险防控目标：

Data security（数据安全性）。That is to ensure the confidentiality, integrity and availability of data. In layman's terms, data "cannot be lost"(数据"不能丢")
Business continuity（业务连续性）。That is to ensure that the information system can provide services stably and continuously. In layman's terms, the system "cannot be interrupted"（系统"不能断"）

Analysis of technical risks in different stages of Digital Bank

opening stage(开业期)	rapid development stage(快速发展期)	stable stage(稳定期)
● 代码中使用的中间件客户端版本多样，依赖冲突；使用有问题的客户端；配置不合理； ● 缺乏灰色能力；服务关闭和释放； ● 缺乏监控能力；接口耗时、接口成功率等服务接口监控数据缺失，难以定位问题；	● Data consistency issues between systems lead to financial losses; ● The business is growing rapidly, the number of systems has increased by one times compared to the opening of the bank, and the risk of DR switching has increased; ● Improper service dependence; for example, lower-layer services depend on upper-layer services;	● Data storage capacity risk (mysql/ceph/es) ● Risk culture(建立风险文化，风险前置) ● Risk handling efficiency (通过平台工具或算法,提升问题识别/处理的效率)

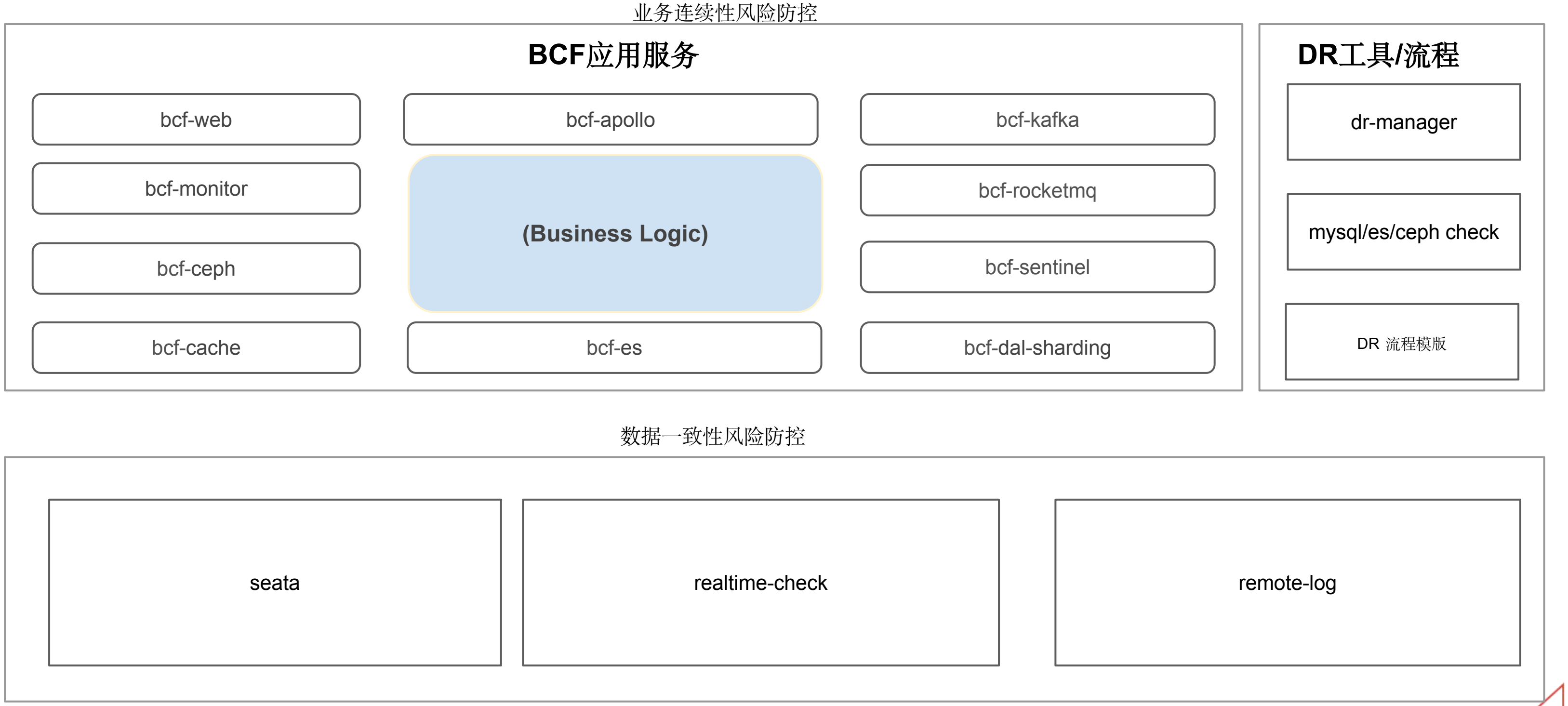
Digital Bank technology risk prevention and control objectives

Based on the problems encountered at different stages of Digital Bank development and the priority of each technical risk treatment, combined with the CAP principle of distributed systems, we set ourselves the following objectives(根据数字银行发展的不同阶段遇到的问题及各个技术风险处理的优先级，结合CAP原理，我们给自己设定如下目标):

Technical risk prevention and control objectives **(技术风险防控目标)**	**import and urgent** **(重要且紧急)**	**import and not urgent** **(重要不紧急)**
Data consistency risk **(数据一致性风险)**	**cross database consistency risk(跨库数据一致性风险)** ● The business system database is split, and the same transaction may across different databases. Using technical means to ensure **cross database consistency** and **prevent financial loss.** **cross system consistency risk(跨系统数据一致性风险)** ● Business systems are driven by RPC or messages, and data inconsistencies between systems are caused by network and other reasons; **Discovering data inconsistencies between systems** through technical means and providing early warning to prevent risk expansion；	**cross datacenter consistency risk(跨机房数据一致性风险)** ● The mysql database uses a semi-synchronous mechanism for cross datacenter disaster recovery; there is a risk that data in transit is not synchronized to the DR datacenter; **Assessing the total risk funds of data in transit** through technical means for business decision-making, and prevent risky account transactions ,thereby preventing financial loss；
Business continuity risk **(业务连续性风险)**	**daily development and operational risk(日常开发和运行风险)** ● Manage and control the dependencies and configuration of middleware through the **development framework**, and standardize the configuration and use of middleware during development. ● Use technical means to solve service release issues and prevent and control change risks; ● Monitor service interface quality and dependencies, and promote interface optimization and service governance ● Prevent and control development risk through development guidelines and development process inspections;	**dr switchingrisk(DR切换风险)** ● Through tool or process optimization, ensure that DR switching does not lose data, RPO=0; ● Through tool or process optimization, ensure that the DR datacenter can be switched,RTO < 4 hours;

Digital Bank technology risk prevention and control system

Preliminarily establish Digital bank technology risk prevention and control system; we try to have no or less intrusion into the business; let the market team focus on business logic development（过去三年我们横向团队初步建立起数字银行技术风险防控体系；对业务尽量无侵入或少侵入；让市场研发团队专注于业务逻辑开发。）



业务连续性风险防控

BCF应用服务

bcf-web

bcf-monitor

bcf-ceph

bcf-cache

bcf-apollo

(Business Logic)

bcf-es

bcf-kafka

bcf-rocketmq

bcf-sentinel

bcf-dal-sharding

DR工具/流程

dr-manager

mysql/es/ceph check

DR 流程模版

数据一致性风险防控

seata

realtime-check

remote-log

Part 1: Data consistency risk prevention and control

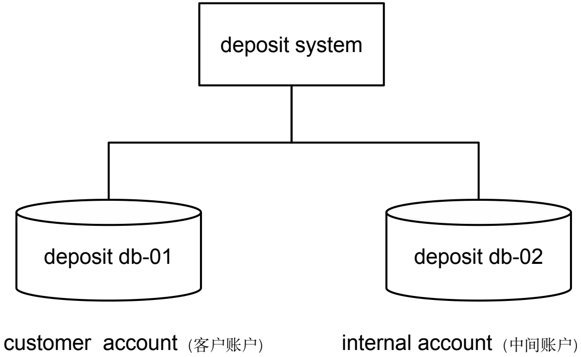
1.Cross database consistency risk(跨库一致性风险)

2.Cross system consistency risk(跨系统一致性风险)

3.Cross datacenter consistency risk(跨机房一致性风险)

Cross database consistency risk (跨库一致性风险)

01 Situation



Distributed Transaction:
1.customer account unfreese 100
2.customer account - 100
3.internal account + 100;

Distributed Transaction Rollback:
1.internal account - 100;
2.customer account + 100
3.customer account freese 100

ID bank 2022.07.20 live issue

Normal processing(正常处理):

- Freeze customer funds 100 yuan;
- Recharge 100 yuan to wallet balance;
- Accept ack from wallet
- Unfreeze customer funds and debit 100 yuan;
- Credit internal account 100 yuan;
- The customer account and internal account are in different database , and the transaction is distributed;

Exception rollback(异常回滚):

- The deposit system failed to credit internal account due to mysql lock competition;
- The deposit system rolled back the transaction;
- however, it only rollbacked the customer's funds and did not freeze the customer's funds;
- As a result, the customer had 100 yuan available and continued to transfer funds out and funds lost;

02 Target

The business system database is split, and the same transaction may across different databases. Using technical means to ensure cross database consistency and prevent financial loss.

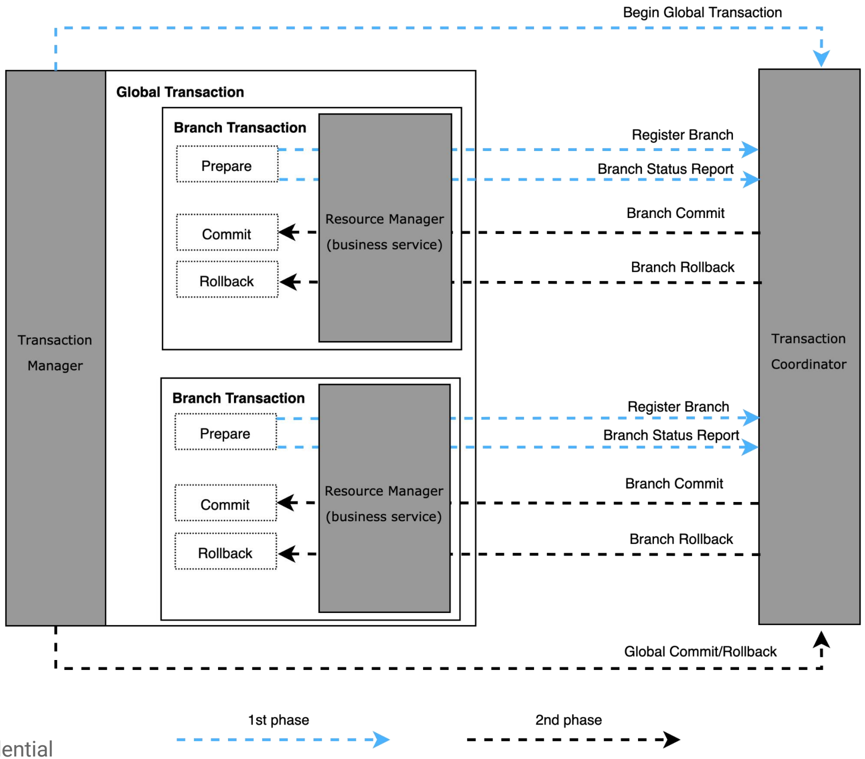
Cross database consistency risk solution compare

03 Action

	Mysql XA	JTA	TCC	SAGA	Transaction Message	Local Message Table
Data Consistency	⭐⭐⭐	⭐⭐⭐	⭐⭐	⭐⭐	⭐	⭐
High Availability	⭐	⭐	⭐⭐	⭐⭐	⭐⭐	⭐⭐
Business intrusion(业务侵入性)	⭐⭐	⭐⭐	⭐	⭐⭐⭐	⭐⭐	⭐⭐⭐
Industry usage rate	⭐	⭐	⭐⭐⭐	⭐	⭐	⭐⭐
Heterogeneous data source(是否支持异构数据源)	✅	✅	❌	✅	❌	❌
Usability(易用性)	⭐⭐	⭐⭐	⭐⭐⭐	⭐	⭐⭐	⭐

Cross database consistency risk solution selection: TCC

After comparing several distributed transaction solutions and weighing code controllability and ecological maturity, we decided to adopt Ant Group’s open source TCC solution Seata(对比几种分布式事务解决方案，权衡代码可控度、生态成熟度之后，我们决定采用蚂蚁开源的TCC解决方案Seata)。



Advantage:

- Github popular
- Nearly 150 companies use this solution;
- The source code and documentation are complete and easy to control;

☆ Star 24.2k

Disadvantage:
1. There are more than 10 bugs to be fixed; the code needs to be completely analyzed and repaired;
2. Code analysis and testing of abnormal scenarios are required to ensure that the functions are correct and complete;

Part 1: Data consistency risk prevention and control

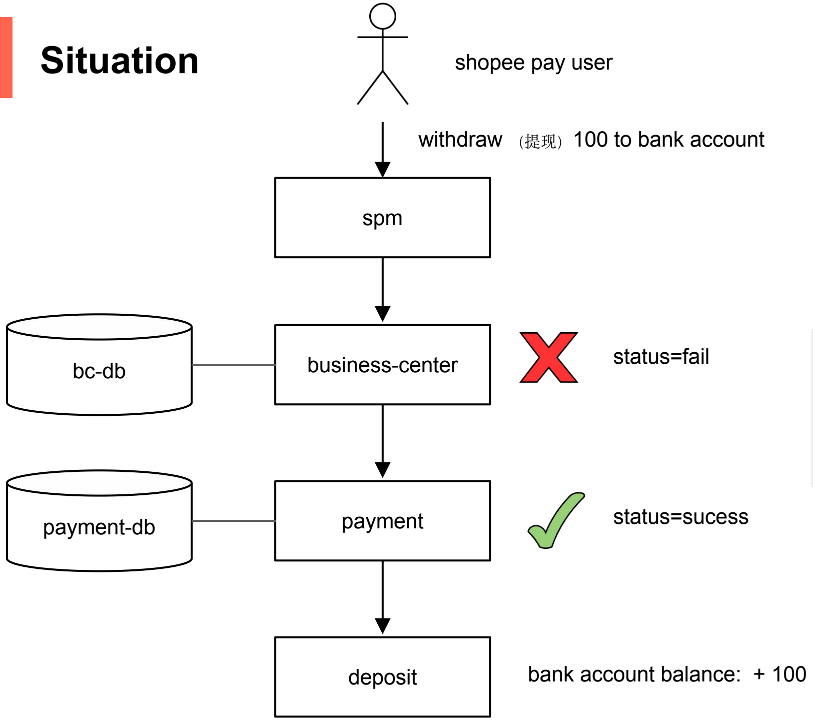
1.Cross database consistency risk(跨库一致性风险)

2.Cross system consistency risk(跨系统一致性风险)

3.Cross datacenter consistency risk(跨机房一致性风险)

Cross system consistency risk(跨系统一致性风险)

01 Situation



ID bank 2022.06.25 live issue

- shopee pay account : freeze 100
- if get success resut,account -100 ;
- if get fail result ,unfreeze 100;

- business-center encountered a network timeout when calling payment; however, the payment has been processed successfully,
- business-center retried, payment return failed result, error code: repeated request

02 Target

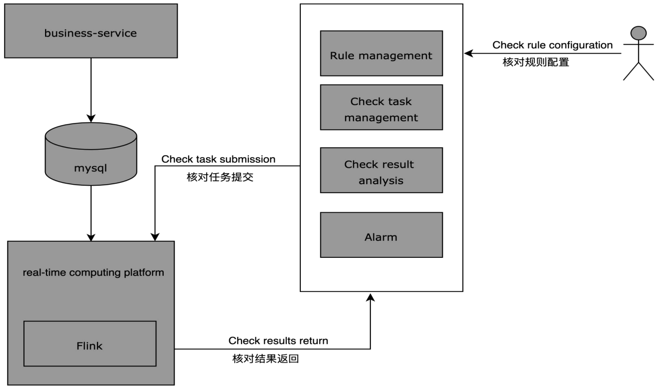
Business systems are driven by RPC or messages, and data inconsistencies between systems are caused by network and other reasons;
Discovering data inconsistencies between systems through technical means and providing early warning to prevent risk expansion;

Cross system consistency risk solution compare

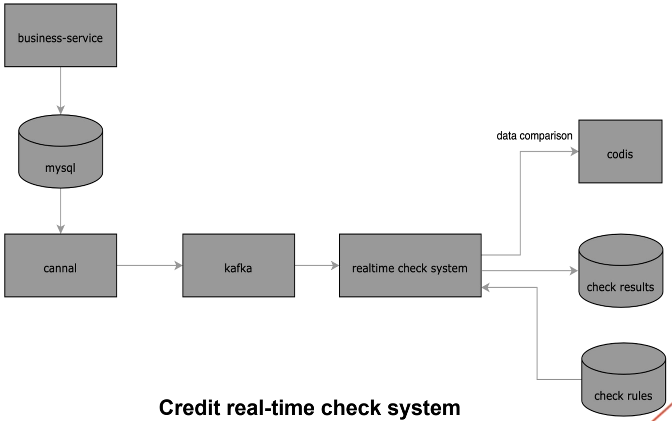
03 Action

Considering that the Credit real-time check system has been running stably online for more than 1 year, in order to quickly launch the real-time check system in digital banks and reduce the risk of financial loss caused by data inconsistency, our team decided to adopt the credit solution and continue to iterate based on the credit code branch(考虑到Credit实时核对系统已经在线上稳定运行1年以上，为了快速在数字银行上线实时核对系统，降低数据不一致引起的资损风险，我们团队决定采用credit的方案，并在credit代码分支基础上继续迭代)；

	Anti Group realtime-check	Credit realtime-check
Performance	N s check complete, high throughput	N s check complete, high throughput
Development Cost	2 人月	0
Technology stack	Java	Go



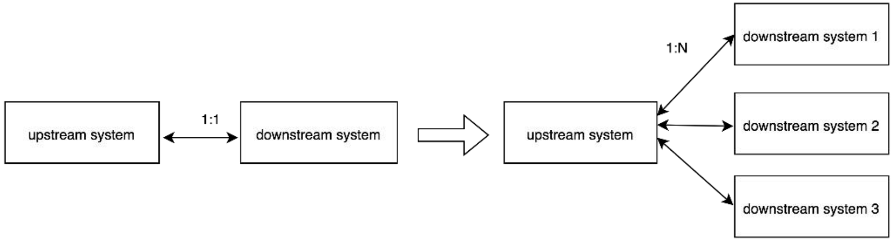
Ant Group real-time check system
(蚂蚁实时核对系统)

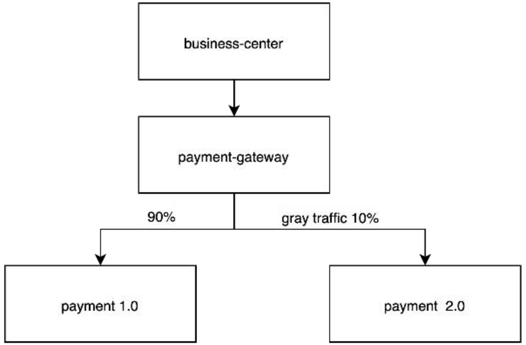


Credit real-time check system
(Credit实时核对系统)

Cross system consistency risk: Expansion based credit solution

a) parent-child rule (父子规则)





rule_id	upstream_db	upstream_tb	downstream_db	downstream_tb	parent_rule_id
rule_id_a	db_a	tb_a	db_b	tb_b	null
rule_id_b	db_a	tb_a	db_c	tb_c	rule_id_a

1. One business-center order only corresponds to one payment order. Whether it corresponds to 1.0 or 2.0 is unknown; downstream differences are shielded through parent-child rules; so that one business-center order only hits the parent rule and ignores the child rules;

2. payment1.0 and payment2.0 only hit 1 rule;

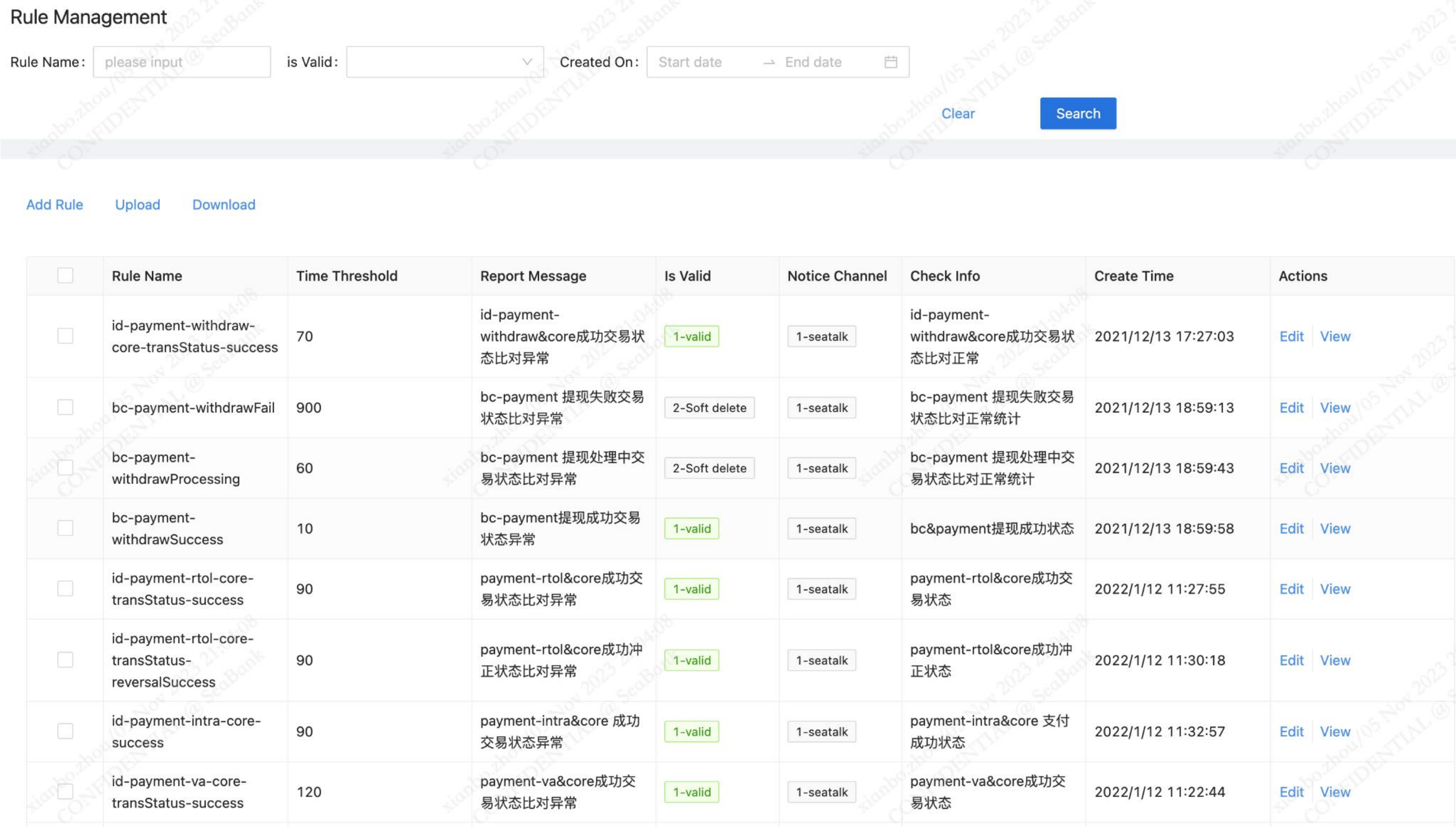
b) add matching syntax(增加匹配语法)

Match symbols	description	example	remark
=	equal	appId=cashLoan	
!	not equal	status!1	

add 6 matching syntax

Match symbols	description	example	remark
%	similar to sql like	uniCode%BBW	
<len>	character length	passage_id<len>7:7	the length of passage_id is between 7 and 7, which is equal to 7
<in>	similar to sql in	tran_status<in>S:N	tran_status is S or N
<not>	similar to sql not in	tran_status<not>S:N	tran_status not S AND N
,	similar to sql and	status!1,uniCode%BBW	status !=1 and uniCode contains bbw
|	similar to sql or	appId=cashLoan|status!1	When AND and OR coexist, analyze the OR logic first, and then analyze the AND logic.

Cross system consistency risk: Configuration Console



Rule Management

Rule Name: please input   is Valid: Created On: Start date → End date

Clear   Search

Add Rule   Upload   Download

□	Rule Name	Time Threshold	Report Message	Is Valid	Notice Channel	Check Info	Create Time	Actions
□	id-payment-withdraw-core-transStatus-success	70	id-payment-withdraw&core成功交易状态比对异常	1-valid	1-seatalk	id-payment-withdraw&core成功交易状态比对正常	2021/12/13 17:27:03	Edit | View
□	bc-payment-withdrawFail	900	bc-payment 提现失败交易状态比对异常	2-Soft delete	1-seatalk	bc-payment 提现失败交易状态比对正常统计	2021/12/13 18:59:13	Edit | View
□	bc-payment-withdrawProcessing	60	bc-payment 提现处理中交易状态比对异常	2-Soft delete	1-seatalk	bc-payment 提现处理中交易状态比对正常统计	2021/12/13 18:59:43	Edit | View
□	bc-payment-withdrawSuccess	10	bc-payment提现成功交易状态异常	1-valid	1-seatalk	bc&payment提现成功状态	2021/12/13 18:59:58	Edit | View
□	id-payment-rtol-core-transStatus-success	90	payment-rtol&core成功交易状态比对异常	1-valid	1-seatalk	payment-rtol&core成功交易状态	2022/1/12 11:27:55	Edit | View
□	id-payment-rtol-core-transStatus-reversalSuccess	90	payment-rtol&core成功冲正状态比对异常	1-valid	1-seatalk	payment-rtol&core成功冲正状态	2022/1/12 11:30:18	Edit | View
□	id-payment-intra-core-success	90	payment-intra&core 成功交易状态异常	1-valid	1-seatalk	payment-intra&core 支付成功状态	2022/1/12 11:32:57	Edit | View
□	id-payment-va-core-transStatus-success	120	payment-va&core成功交易状态比对异常	1-valid	1-seatalk	payment-va&core成功交易状态	2022/1/12 11:22:44	Edit | View

Part 1: Data consistency risk prevention and control

1.Cross database consistency risk(跨库一致性风险)

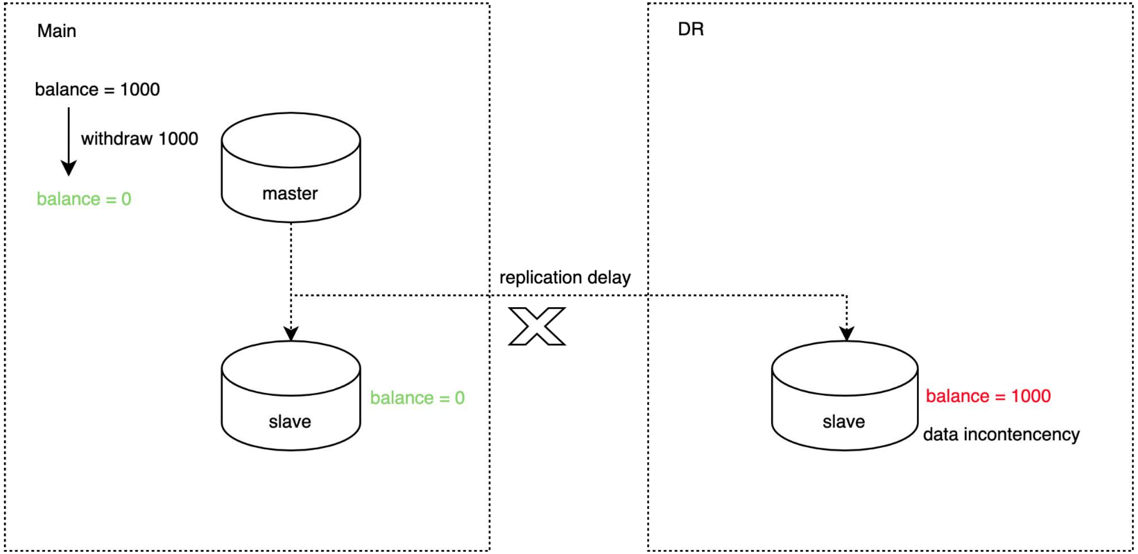
2.Cross system consistency risk(跨系统一致性风险)

3.Cross datacenter consistency risk(跨机房一致性风险)

Cross datacenter consistency risk background(跨机房一致性风险)

01 Situation

MySQL database cross datacenter disaster recovery uses a semi-synchronous mechanism to replicate data; due to network delays and other reasons, MySQL cannot guarantee the data consistency between the primary node and the backup node resulting in financial loss in serious cases.



02 Target

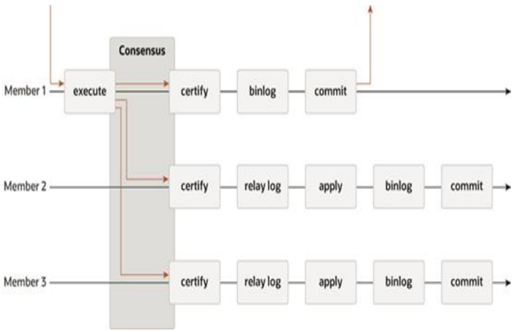
The mysql database uses a semi-synchronous mechanism for cross datacenter disaster recovery; there is a risk that data in transit is not synchronized to the DR datacenter; Assessing the total risk funds of account in transit(评估在途账户风险资金总额) through technical means for business decision-making, and prevent risky account transactions(阻止风险账户发起交易) ,thereby preventing financial loss;

Cross datacenter consistency risk solution compare

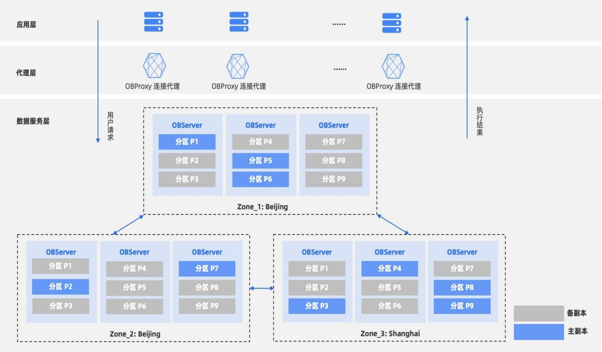
03 Action

对比行业通用解决方案（通过数据库系统保障RPO=0），考虑技术自主可控，机房及维护成本，权衡利弊后我们决定放弃数据库多节点强一致的方案（RPO=0）；从评估业务影响范围的角度考虑，采取远程日志方案（RPO>0）。

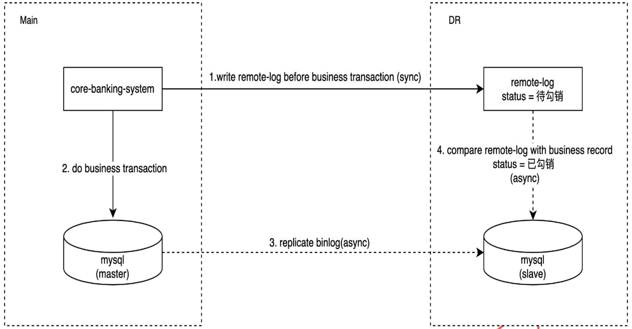
	mysql mgr	oceanbase	remote-log
RPO	0	0	> 0
RTO	unknow, 37unfixed bugs until Sep 2023	8s	4 hours
Datacenter Cost	N/A	multi datacenter,at least 3millions $	3 datacenter，the 3rd datacenter low cost, $ 100 K
Maintenance Cost	N/A	high	low
Autonomous and controllable(自主可控)	N/A	✗	✓
Other	N/A	business competition(商业竞争)	N/A



mysql mgr（组复制）



oceanbase

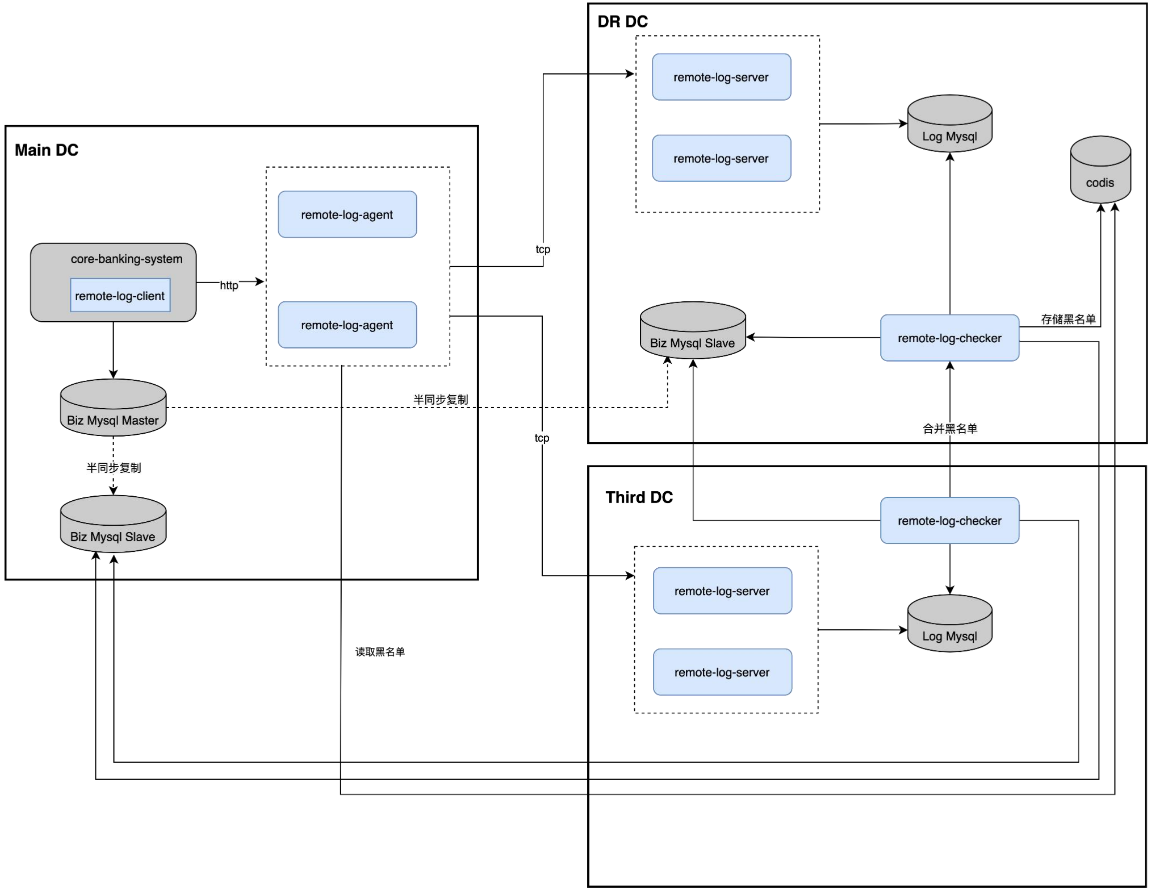

Main
core-banking-system
2. do business transaction
mysql
(master)
1.write remote-log before business transaction (sync)
3. replicate binlog(async)
DR
remote-log
status = 待勾销
4. compare remote-log with business record
status = 已勾销
(async)
mysql
(slave)

remote-log

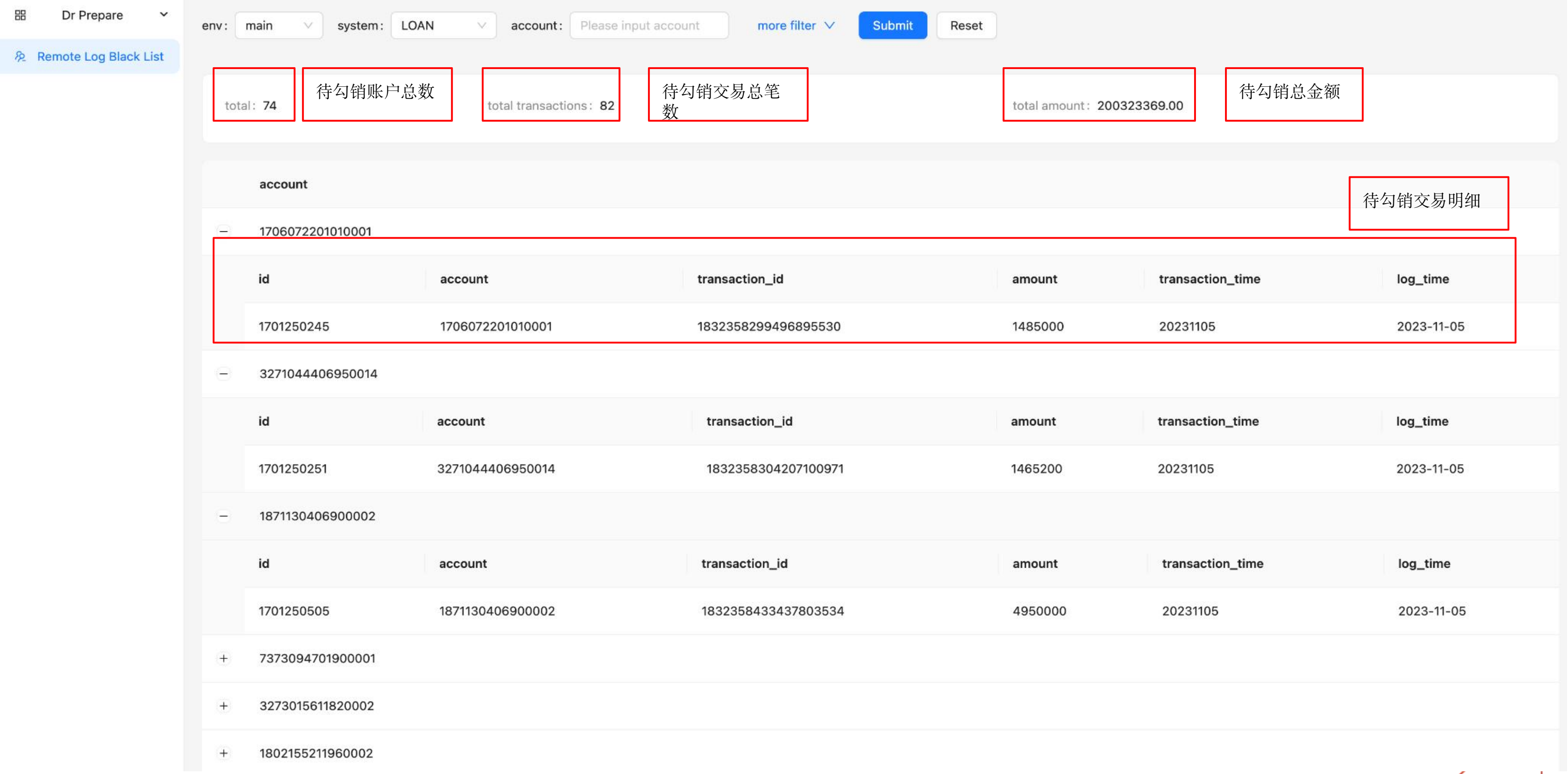
Cross datacenter consistency risk solution: remote-log

remote-log system

- remote-log-client
- remote-log-agent
- remote-log-server
- remote-log-checker



Cross datacenter consistency risk solution: console



env: main system: LOAN account: Please input account

total: 74

待勾销账户总数

total transactions: 82

待勾销交易总笔数

total amount: 200323369.00

待勾销总金额

account

待勾销交易明细

1706072201010001

id	account	transaction_id	amount	transaction_time	log_time
1701250245	1706072201010001	1832358299496895530	1485000	20231105	2023-11-05

3271044406950014

id	account	transaction_id	amount	transaction_time	log_time
1701250251	3271044406950014	1832358304207100971	1465200	20231105	2023-11-05

1871130406900002

id	account	transaction_id	amount	transaction_time	log_time
1701250505	1871130406900002	1832358433437803534	4950000	20231105	2023-11-05

+ 7373094701900001
+ 3273015611820002
+ 1802155211960002

Data consistency risk prevention and control achievements

04 Result

1. Cross database risk prevention and control

Seata replace Saga, applied in deposit productization(在存款产品化中通过Seata取代供应商的Saga方案，解决存款核心跨库数据一致性问题)

2. Cross system risk prevention and control

- Production application(生产应用)：2022.06.09 Real-time check alarms reveals 1 financial loss incidents and avoid further expansion of risks(实时核对告警发现资损问题，及时止损避免风险扩大)
- Market Coverage(市场覆盖情况)：Covers three market fund processing scenarios of ID/PH/SG; coverage scenarios are 51/31/59 respectively; business scenarios coverage 100%；

3. Cross datacenter risk prevention and control:remote logs

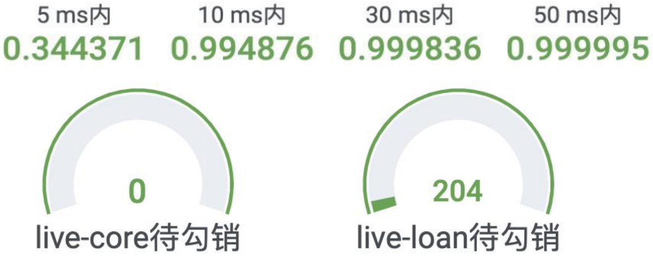
a) Production application(生产应用)

- 2023/03/27 core banking database failure we assesses business impact scope through remote logs(核心银行数据库故障我们通过远程日志评估业务影响范围)

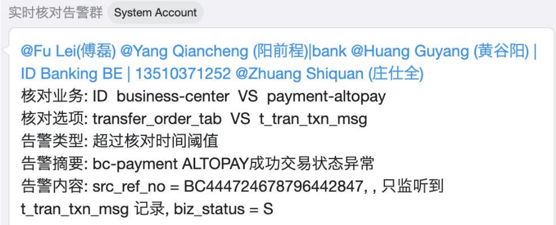
b) Market Coverage(市场覆盖情况)

- ID: Deposit/Loan/Payment Acquisition/Payment Clearing/Payment Channel,5 types of businesses; synchronization mode, coverage 100%
- PH: Deposit/Loan/Payment Acquisition/Payment Clearing/Payment Channel,5 types of businesses; synchronization mode, coverage 100%
- SG:Investment/Payment Acquisition/Payment Settlement/Payment channel/Loan,5 types of businesses; asynchronous mode,coverage 100%

c) Online operation status(线上运行情况)



5 ms内	10 ms内	30 ms内	50 ms内
0.344371	0.994876	0.999836	0.999995



实时核对告警群 System Account

@Fu Lei(傅磊) @Yang Qiancheng (阳前程)|bank @Huang Guyang (黄谷阳) | ID Banking BE | 13510371252 @Zhuang Shiquan (庄仕全)
核对业务: ID business-center VS payment-altopay
核对选项: transfer_order_tab VS t_tran_txn_msg
告警类型: 超过核对时间阈值
告警摘要: bc-payment ALTOPAY成功交易状态异常
告警内容: src_ref_no = BC444724678796442847, , 只监听到 t_tran_txn_msg 记录, biz_status = S

Private & confidential

Data consistency risk prevention and control objectives comparison

1、**Cross database consistency risk(跨库一致性风险)**
The business system database is split, and the same transaction may across different databases. Using technical means to ensure **cross database consistency** and **prevent financial loss.**

Ensure cross database data consistency through the distributed transaction framework seata(通过分布式事务框架seata保障跨库数据一致性)

2、**Cross system consistency risk(跨系统一致性风险)**
Business systems are driven by RPC or messages, and data inconsistencies between systems are caused by network and other reasons; **Discovering data inconsistencies between systems** through technical means and providing early warning to prevent risk expansion;

Use real-time check to detect data inconsistencies between systems and provide early alarms （使用实时核对发现系统间数据不一致并进行预警）

3、**Cross datacenter consistency risk(跨机房一致性风险)**
The mysql database uses a semi-synchronous mechanism for cross datacenter disaster recovery; there is a risk that data in transit is not synchronized to the DR datacenter; **Assessing the total risk funds of account in transit** through technical means for business decision-making, and prevent risky account transactions ,thereby preventing financial loss;

- Transaction logs are written to the remote log system synchronously(交易日志同步写入远程日志系统)
- remote-log asynchronous reconcile; evaluate the amount of un-reconciled accounts and form a blacklist to prevent dynamic transactions of blacklisted accounts(远程日志异步勾销；评估未勾销账户金额并形成黑名单，阻止黑名单账户动账交易)

Part 2: Business continuity risk prevention and control

1.Daily development and operational risk

2.DR Switching Risk

Daily development and operational risk

01 Situation

1.New technology team (more than 90% members work in the team less than 1 year in 2021), the business system is built on open source middleware, and improper use of middleware in daily development causes live issues.

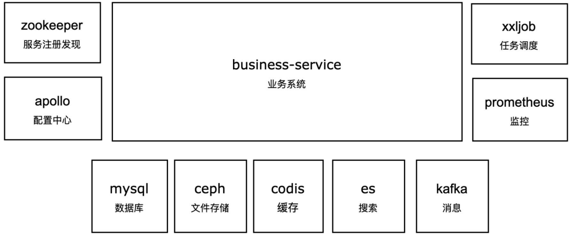
● many kinds of middleware clients	[5 codis-client/kafka-client,3 zk-client,dependency conflicts]
● improper use of middleware	[2021.07.01 Loan codis distributed lock connection not released, transaction fell 0]
● parameter configuration incorrect	[2021.08.30 Payment gateway OOM, payment service is unavailable]
● middleware client version incompatible	[2022.04.22 Mobile banking zk client used a higher version of the client, resulting in data nodes stacking, which in turn affected mobile banking service discovery]

2. Daily changes cause live issues

- **Code change** typical case**:** In the first half of 2021,the ID Bank system was shut down for release(停机发布); in order to reduce the impact on customers, it chose to release in the early morning;
- **Configuration chang** typical case: 2023.06.07 PH Bank App certificate configuration change error causes the entire bank app to become unavailable
- **SQL change** typical case: 2023.09.07ID bank payment database executes online DDL resulting in payment transaction falling to 0

3.With the rapid development of business, the number of self-developed services is growing rapidly (50+ -> 75+ self-developed services), the technical structure has gradually become complex, and there are risks in online operation(随着业务快速发展，自研服务数量快速增长（50+ ->75+），技术架构逐步复杂化，线上运行存在风险)

- The service interface design is unreasonable and the app frequently times out, affecting customer use(服务接口设计不合理，具体表现为app端超时，影响客户使用)
- Services grow wildly, boundaries are unclear, and dependencies between services are unreasonable(服务野蛮生长，边界不清，服务之间依赖关系不合理)



zookeeper 服务注册发现

apollo 配置中心

business-service 业务系统

xxljob 任务调度

prometheus 监控

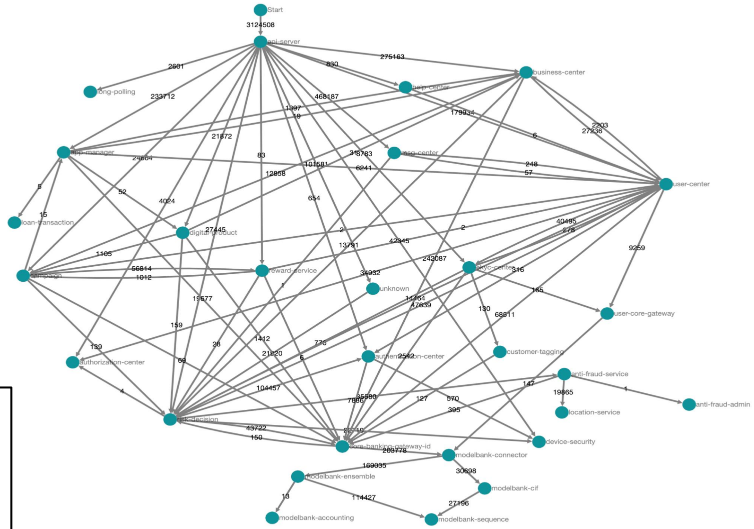
mysql 数据库

ceph 文件存储

codis 缓存

es 搜索

kafka 消息



02 Target

- Manage and control the dependencies and configuration of middleware through the development framework, and standardize the configuration and use of middleware during development.
- Use technical means to solve service release issues and prevent and control change risks;
- Monitor service interface quality and dependencies, and promote interface optimization and service governance
- Prevent and control devlopment risk through development guidelines and development process inspections;

Daily development and operational risk solution compare

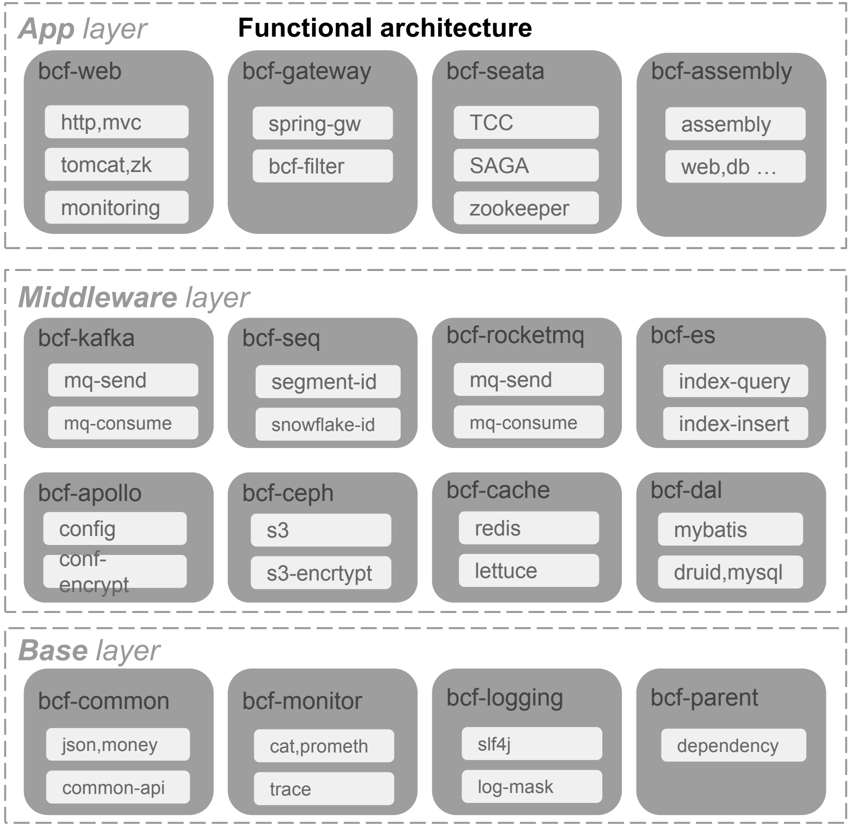
03

Action

	Elements(要素)	Spring Cloud	Dubbo
Effect (使用效果)	Function (功能丰富度)	★★★★	★★
	Scalability (可扩展性)	★★★	★★
	Observability (可观测性)	★★★	★★
Cost (使用成本)	Application integration costs (应用集成容易程度)	★★★★	★★★
	Maintainability (可维护性)	★★★★	★★
Ecology (生态)	Maturity (成熟程度)	★★★★	★★★
	Industry trends (业界流行情况)	★★★★	★★★
Others (其他)	Team factors (团队接受容易程度)	★★★	★★

Daily development and operational risk solution selection:BCF

BCF（Banking Cloud Framework）：Function customization and capability expansion based on spring cloud



Functional architecture

App layer

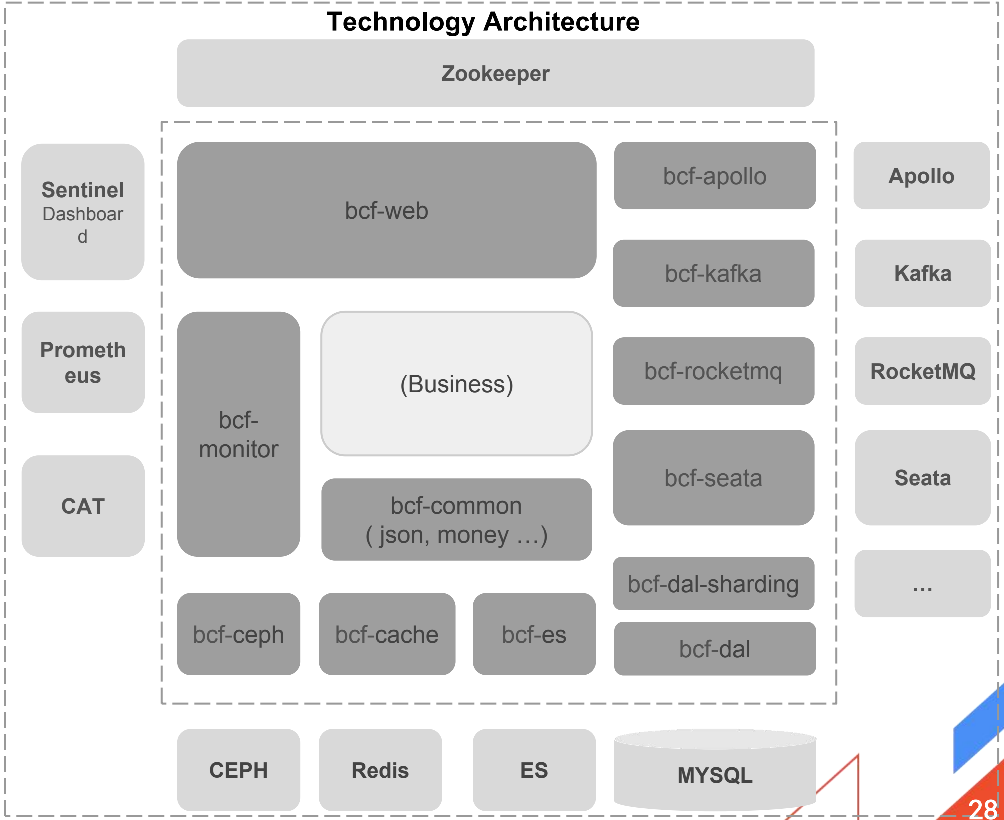
- bcf-web: http,mvc; tomcat,zk; monitoring
- bcf-gateway: spring-gw; bcf-filter
- bcf-seata: TCC; SAGA; zookeeper
- bcf-assembly: assembly; web,db …

Middleware layer

- bcf-kafka: mq-send; mq-consume
- bcf-seq: segment-id; snowflake-id
- bcf-rocketmq: mq-send; mq-consume
- bcf-es: index-query; index-insert
- bcf-apollo: config; conf-encrypt
- bcf-ceph: s3; s3-encrtypt
- bcf-cache: redis; lettuce
- bcf-dal: mybatis; druid,mysql

Base layer

- bcf-common: json,money; common-api
- bcf-monitor: cat,prometh; trace
- bcf-logging: slf4j; log-mask
- bcf-parent: dependency



Technology Architecture

Zookeeper

Sentinel Dashboard

Prometheus

CAT

bcf-web

bcf-monitor

(Business)

bcf-common (json, money …)

bcf-ceph

bcf-cache

bcf-es

bcf-apollo

bcf-kafka

bcf-rocketmq

bcf-seata

bcf-dal-sharding

bcf-dal

Apollo

Kafka

RocketMQ

Seata

...

CEPH

Redis

ES

MYSQL

Business continuity risk prevention and control result 1: BCF

04 Result

Easy integrate:

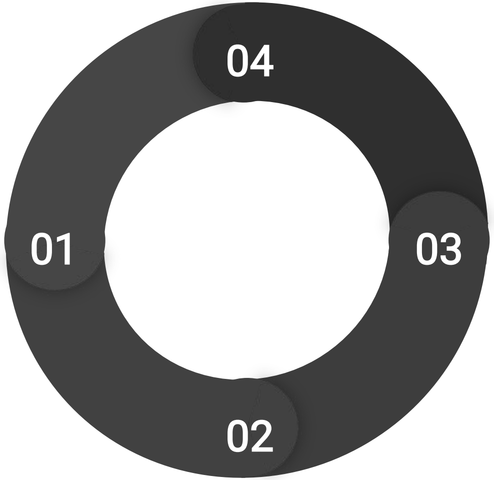
1.1 BCF One-click integration(一键集成):

```
mvn archetype:generate -
DarchetypeGroupId=com.shopee.bank -
DarchetypeArtifactId=bank-project-archetype
-DgroupId=com.shopee.banking -DartifactId=appname -
Dpackage=com.shopee.banking.appname -Dbasedir=. -
DbcfGroupId=com.shopee.bankingcommonframework -
DbcfVersion=2.7.2-RELEASE
```

1.2 BCF manual integration(手工集成):

```
<parent>
    <artifactId>bcf-parent</artifactId>
    <groupId>com.shopee.bankingcommonframework</groupId>
    <version>2.7.2-RELEASE</version>
</parent>

<dependency>
    <groupId>com.shopee.bankingcommonframework</groupId>
    <artifactId>bcf-starter-assembly</artifactId>
    <version>2.7.2-RELEASE</version>
</dependency>
```



P0/P1 issues:

0 P0 incident, 4 P1 incidents, the incidents are not caused by BE Service.

	2021	2022	2023
ID	0	0	2P1 (硬件故障, 前端故障)
PH	N/A	1P1 (发布顺序)	1P1 (业务备付金账户余额不足)
SG	N/A	N/A	0

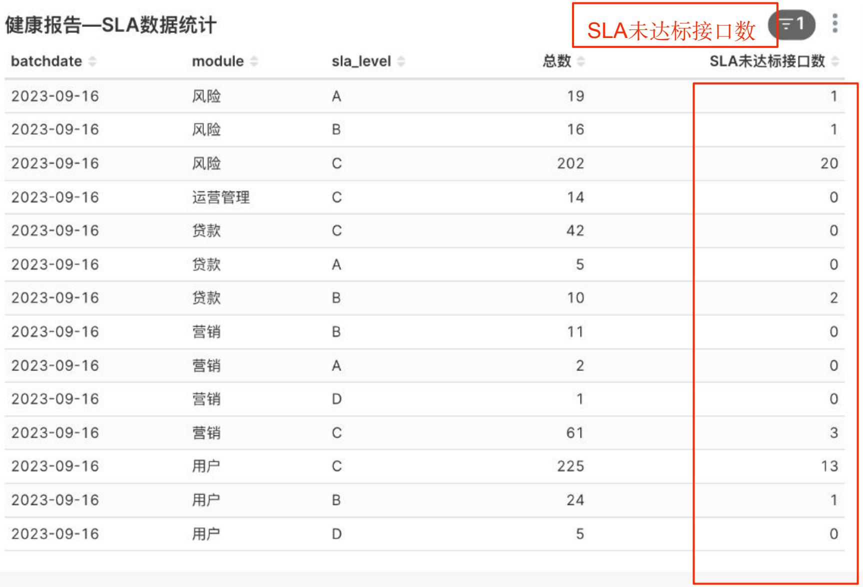
Core System availability:

ID/PH/SG bank core system availability
99.97/99.95/99.99

BCF Market Coverage(市场覆盖情况):

- ID: 71/75 BCF services,1738 APIs, coverage 95%
- PH: 74/74 BCF services,1019 APIs, coverage 100%
- SG: 57/69 BCF services,1042 APIs, coverage 83%

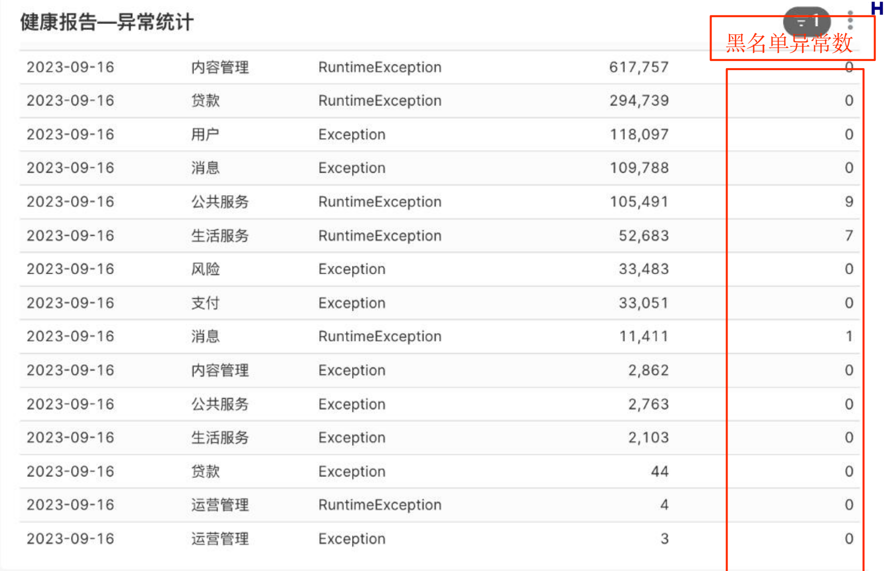
Business continuity risk prevention and control result 2:service health report



健康报告—SLA数据统计

SLA未达标接口数

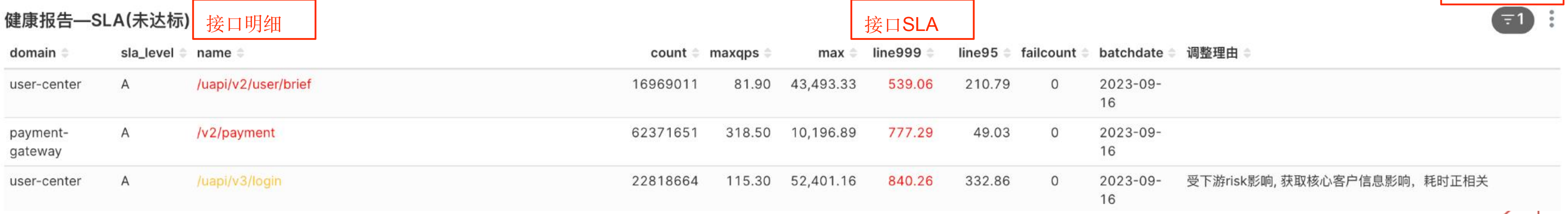
batchdate	module	sla_level	总数	SLA未达标接口数
2023-09-16	风险	A	19	1
2023-09-16	风险	B	16	1
2023-09-16	风险	C	202	20
2023-09-16	运营管理	C	14	0
2023-09-16	贷款	C	42	0
2023-09-16	贷款	A	5	0
2023-09-16	贷款	B	10	2
2023-09-16	营销	B	11	0
2023-09-16	营销	A	2	0
2023-09-16	营销	D	1	0
2023-09-16	营销	C	61	3
2023-09-16	用户	C	225	13
2023-09-16	用户	B	24	1
2023-09-16	用户	D	5	0



健康报告—异常统计

黑名单异常数

2023-09-16	内容管理	RuntimeException	617,757	0
2023-09-16	贷款	RuntimeException	294,739	0
2023-09-16	用户	Exception	118,097	0
2023-09-16	消息	Exception	109,788	0
2023-09-16	公共服务	RuntimeException	105,491	9
2023-09-16	生活服务	RuntimeException	52,683	7
2023-09-16	风险	Exception	33,483	0
2023-09-16	支付	Exception	33,051	0
2023-09-16	消息	RuntimeException	11,411	1
2023-09-16	内容管理	Exception	2,862	0
2023-09-16	公共服务	Exception	2,763	0
2023-09-16	生活服务	Exception	2,103	0
2023-09-16	贷款	Exception	44	0
2023-09-16	运营管理	RuntimeException	4	0
2023-09-16	运营管理	Exception	3	0



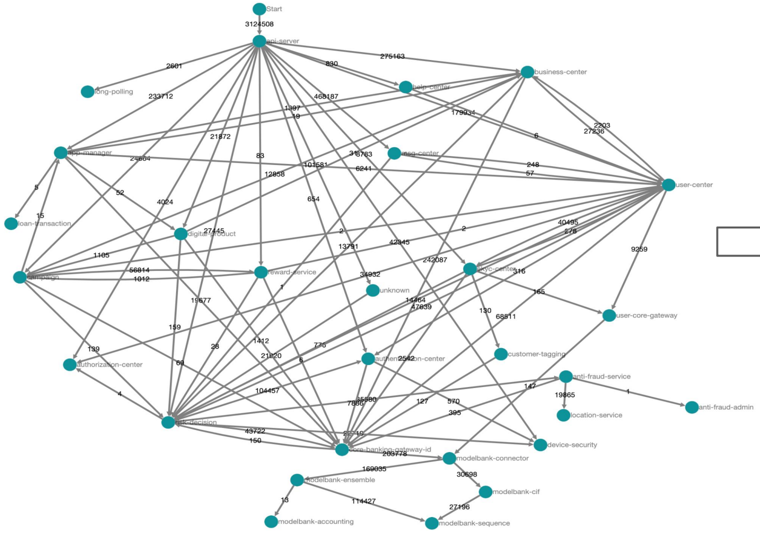
健康报告—SLA(未达标)

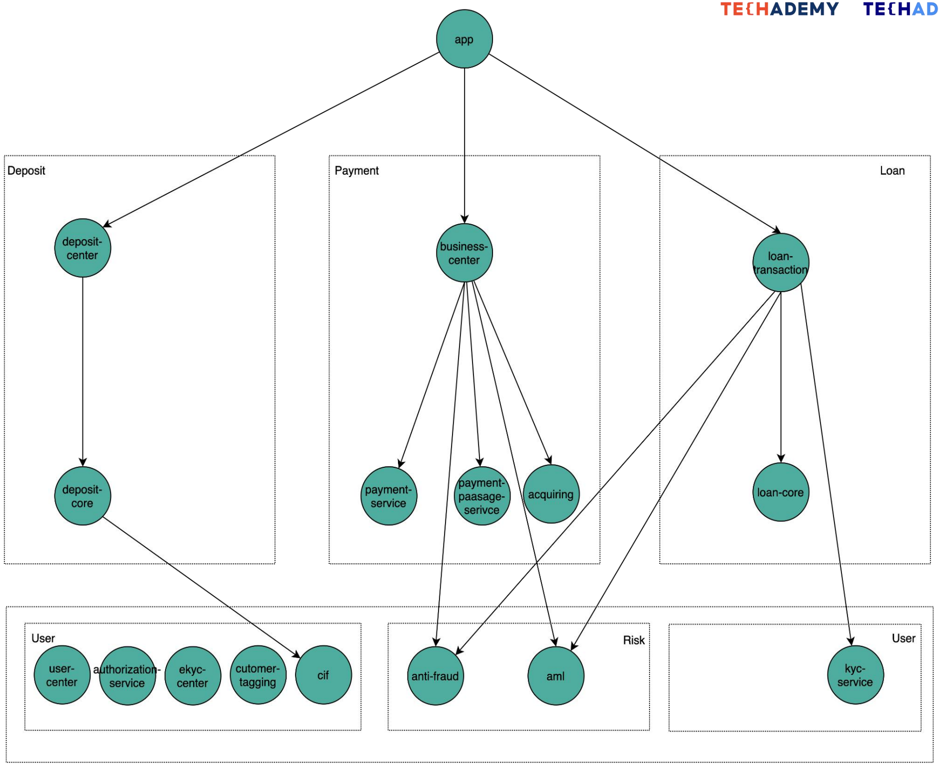
接口明细

接口SLA

domain	sla_level	name	count	maxqps	max	line999	line95	failcount	batchdate	调整理由
user-center	A	/uapi/v2/user/brief	16969011	81.90	43,493.33	539.06	210.79	0	2023-09-16	
payment-gateway	A	/v2/payment	62371651	318.50	10,196.89	777.29	49.03	0	2023-09-16	
user-center	A	/uapi/v3/login	22818664	115.30	52,401.16	840.26	332.86	0	2023-09-16	受下游risk影响，获取核心客户信息影响，耗时正相关

Business continuity risk prevention and control result 3:service dependency report





Promote application architecture optimization, net architecture -> vertical architecture（推动应用架构持续治理，网状架构->垂直化架构）

Part 2: Business continuity risk prevention and control

1.Daily development and operational risk

2.DR Switching Risk

DR Switching risk background:dr switch

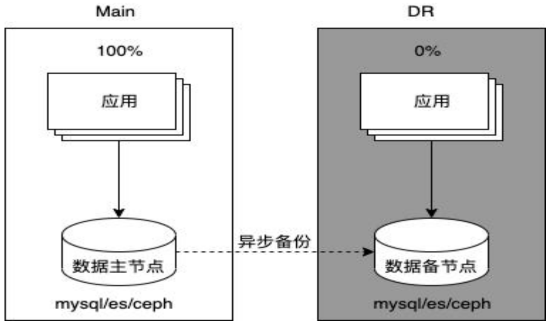
01 Situation

1. Regulatory requirements(监管要求)

Trials are carried out on the Disaster Recovery Plan at least 1 (one) time in 1 (one) year for all critical systems or applications according to the results of a business impact analysis and represent all critical infrastructure and involve IT users. The RTO is 4 hours, RPO is 0.

2. DR datacenter cold backup(DR机房冷备)

- Asynchronous data backup may result in data loss, and the RPO may not meet compliance requirements(数据异步备份存在数据丢失风险，RPO可能不满足合规要求)
- DR datacenter cold backup, no online traffic is running, and whether the service is available is unknown(DR机房没有运行线上流量、服务是否可用未知,RTO可能不满



3.Project management complexity(项目管理复杂度)

The project cycle is as long as 6 months, involving about 100+ people from 10+ teams including development/QA/SRE/3rd parties/local, etc., with a total manpower investment of about 900 people/day, including tech design, risk prevention and personnel communication in all aspects of the project process. It is a very big challenge in terms of organization and coordination(项目周期长达6个月，涉及开发/QA/SRE/三方/local等10+团队约100+人，总人力投入约900人/天，项目过程中的各环节方案设计、风险防案以及人员沟通和组织协调等方面都面临非常大的挑战).

4. Operation and maintenance complexity(运维复杂度)

- 170+ services, 20+ third-party channels, 10+ types of middleware, and 180+ databases were switched to the DR datacenter, and after completing the verification of 200+ use cases, and run it in the DR datacenter for 2 days, and then switch back to the Main datacenter(170+服务、20+个第三方渠道、10+种中间件、180+个数据库都切换到DR机房，完成200+用例的验证，然后在DR机房运行2days,最后回切Main机房);

服务数/切换时间	手机银行	核心银行	数仓	公共服务	第三方服务	服务总数	技术切换时间 (min)
2021	43	35	5	12	14	**109**	**64**
2022	50	78	13	13	19	**173**	180

Number of services and DR switching time consumption of ID Bank in 2021-2022
(ID银行2021-2022年服务数量及DR切换耗时情况)

02 Target

- Through tool or process optimization, ensure that DR switching does not lose data, RPO=0;
- Through tool or process optimization, ensure that the DR datacenter can be switched,RTO < 4 hours;

DR Switching risk solution: division of responsibilities of project

03 Action

角色	职责
市场pic	1、DR切换第一责任人。　2、协调资源完成技术方案落地
横向pic	1、DR切换主要责任人，配合市场PIC完成DR切换； 2、输出整体DR切换方案和时序,DR切换技术风险分析和预案设计 3、制定DR目标文件并牵头DR项目管理 4、沉淀DR切换提效工具 5、check pic 输出的方案正确性和完整度 6、组织DR切换复盘，总结DR经验，推广各个市场。
各个模块pic	1、根据DR切换手册指引完成对应模块的切换方案梳理。 2、根据DR切换目标文件完成对应的task。 3、确保负责模块DR切换的顺利完成。
SRE	1、完成DR 网络重建 2、协调硬件、应用厂商、关联方的等切换运维人员 3、ops端切换方案 4、负责切换方案脚本整理
QA	1、输出测试用例 2、负责DR 切换/回切后的内部验证 3、记录各个步骤的实际开始时间、完成时间
DBA	1、完成数据备份　2、完成数据库切换
中间件SRE	1、负责对应中间件切换　2、负责对应中间件数据同步一致
PM	1、配合DR切换协调关联方停流方案
Local 业务人员	1、负责提供演练公告方案　2、负责流量放开前的业务验证 3、负责协调DR切换各个关联方
第三方服务支持人员(硬件、应用厂商、关联方)	1、配合DR切换，处理DR切换中对应应用发生的问题

DR Switching risk solution: RPO=0

Mysql

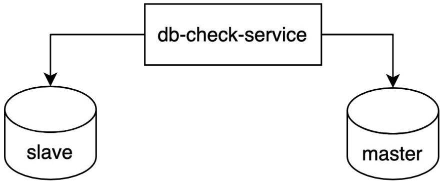
Application

Compare the data consistency of key business slave nodes and master nodes(比较关键业务数据库从节点和主节点数据一致性)

1. Table structure full database full table scan(表结构全库全表扫描)

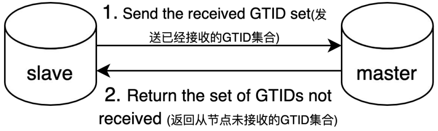
2. Unique ID full database full table scan(唯一id全库全表扫描)

3.Specify time period scanning for core fields, such as account balance, payment status, distributed sequence, etc(核心字段指定时间段扫描，例如账户余额，支付状态，分布式sequence等)



Mysql

Compare whether the GTID of the master and slave nodes are consistent(比较主从节点GTID是否一致)


slave
master
1. Send the received GTID set(发送已经接收的GTID集合)
2. Return the set of GTIDs not received (返回从节点未接收的GTID集合)

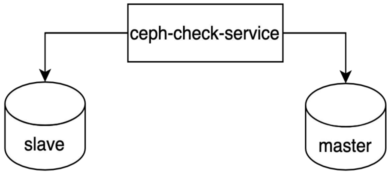
Ceph

Application

Taking the master node as the benchmark, compare the data consistency between the slave node and the master node(以主节点为基准,比较从节点和主节点数据一致性)

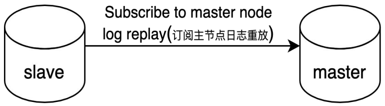
1. Full scan by bucket (paged query) to compare object consistency(按bucket全量扫描(分页查询）比较object一致性)

2. Compare object consistency by lastmodify incremental scan(按lastmodify增量扫描比较object一致性)



Ceph

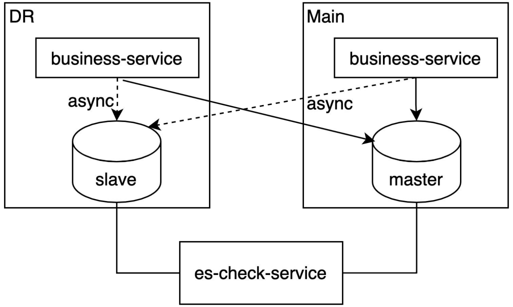
Compare the number of documents in the bucket to see if they are consistent(比较bucket内文档数量是否一致)



ES

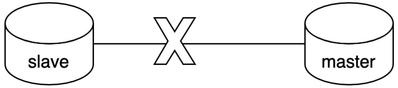
Application

Using the Main cluster as the benchmark, scan the es index according to the full/incremental strategy and compare document by document(以Main集群为基准按全量/增量策略扫描es索引逐个document比较)；



ES

No guarantee is provided; the officially provided data replication plan across datacenter requires payment(未提供保障；官方提供的数据跨机房复制方案需要付费)；



DR Switching risk solution: RTO < 4hours

1.**Process guarantee** (流程保障)

1

切换方案按模块梳理

1. 各模块PIC分别负责整理各自的方案
2. 项目组评审方案保障方案正确性

2

DR nonlive演练（3轮）

1. 验证SRE/DBA执行脚本的有效性.
2. 验证整个DR切换操作序列的配合默契程度

3

DR 环境验证（3轮）

1. 做到100%核心业务场景的覆盖，保证DR切换前DR环境的可用性
2. 验证Local对环境和测试用例验证流程熟悉程度

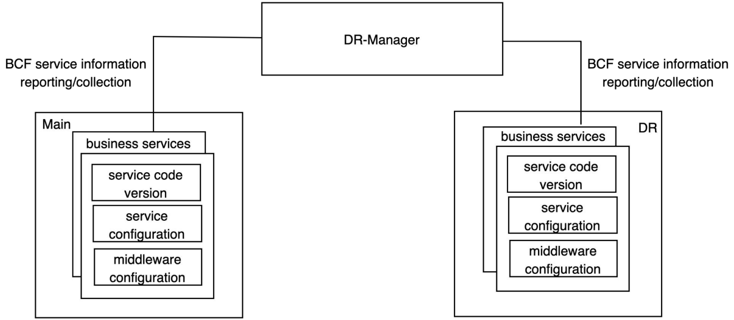
4

项目周会

1.通过周会及时跟进项目进度和风险
2. 通过周报同步信息到各干系人

2.**Tool guarantee** (工具保障)

Automatically compare the consistency of Live/DR services and configurations(自动比较Live/DR服务及配置的一致性)



DR-Manager

BCF service information reporting/collection

BCF service information reporting/collection

Main

business services

service code version

service configuration

middleware configuration

DR

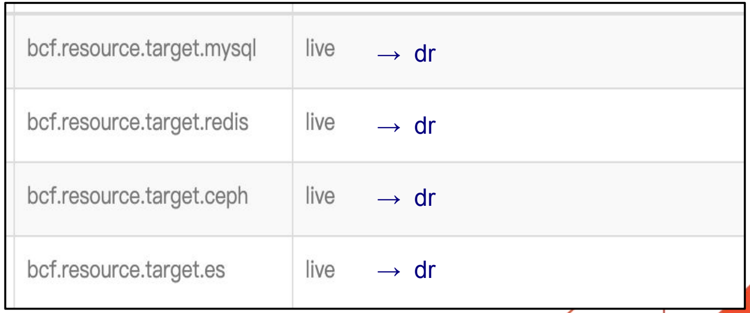
business services

service code version

service configuration

middleware configuration

Switch network connections with one click without restarting the service(连接一键切换，不重启服务)



bcf.resource.target.mysql	live	→ dr
bcf.resource.target.redis	live	→ dr
bcf.resource.target.ceph	live	→ dr
bcf.resource.target.es	live	→ dr

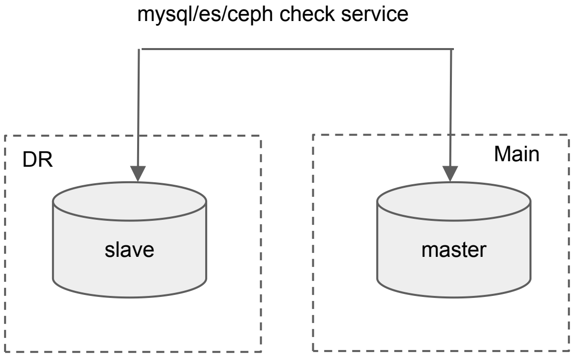
DR Switching risk prevention and control results

04 Result

RPO/RTO

- 2023 PH DR switching(PH银行2023DR切换)
  RPO: 0
  Technical RTO: 1 hour and 26 minutes (objective 1.5 hours)
  Compliance RTO: 2 hours and 43 minutes (objective 4 hours)
- 2023 ID/SG DR switching successfully achieved compliance & technical objectives(2023 DR切换顺利达成合规&技术目标)

Tool



Process

- 开发DR梳理模版
- SRE梳理模版
- QA梳理模版
- 第三方依赖梳理模版
- DR项目管理模版
- DR环境重建时序模版
- DR切换checklist
- DR切换时序模版

Business continuity risk prevention and control objectives comparison

Daily development and operational risk(日常开发和运行风险)

- Manage and control the dependencies and configuration of middleware through the **development framework**, and standardize the configuration and use of middleware during development.
- Use technical means to solve service release issues and prevent and control change risks;
- Monitor service interface quality and dependencies, and promote interface optimization and service governance
- Prevent and control code risks through development guidelines and development process inspections;

1）Prevent daily development and online operation risks through **BCF**
(通过BCF防范日常开发和线上运行风险)
1.1 Middleware versions and dependencies are unified into the framework; middleware public configurations are uniformly provided by the framework(中间件版本和依赖统一到框架中；中间件公共配置由框架统一提供)；
1.2 Prevent and control code change risks through gray release and elegant start and stop(通过灰度发布、优雅启停防控代码变更风险)
1.3 Service interface quality monitoring report, service dependency monitoring report(服务接口质量监控报告, 跨领域调用监控报告)
1.4 **Development guideline and process inspections**：Tech Design Guideline、Coding Guideline , Code Review Guideline , Java Project Structure Guideline , Unit Test Guideline , Monitoring and Alerting Guideline, Tech Design Check , Tech Design Virtual Team,Code review

DR Switching risk(DR切换风险)

- Through tool or process optimization, ensure that DR switching does not lose data, RPO=0;
- Through tool or process optimization, ensure that the DR datacenter can be switched,RTO < 4 hours;

2）2023 ID/PH/SG DR switching successfully achieved compliance & technical objectives(2023 DR切换顺利达成合规&技术目标)
2.1 2023 ID DR switching(ID银行2023DR切换)
RPO: 0
Technical RTO: 1 hour and 26 minutes (objective 1.5 hours)
Compliance RTO: 2 hours and 43 minutes (objective 4 hours)
2.2 Process template accumulation
2.3 Tool accumulation: db-check-serivce, es-check-service, ceph-check-service

Q & A

Thank you