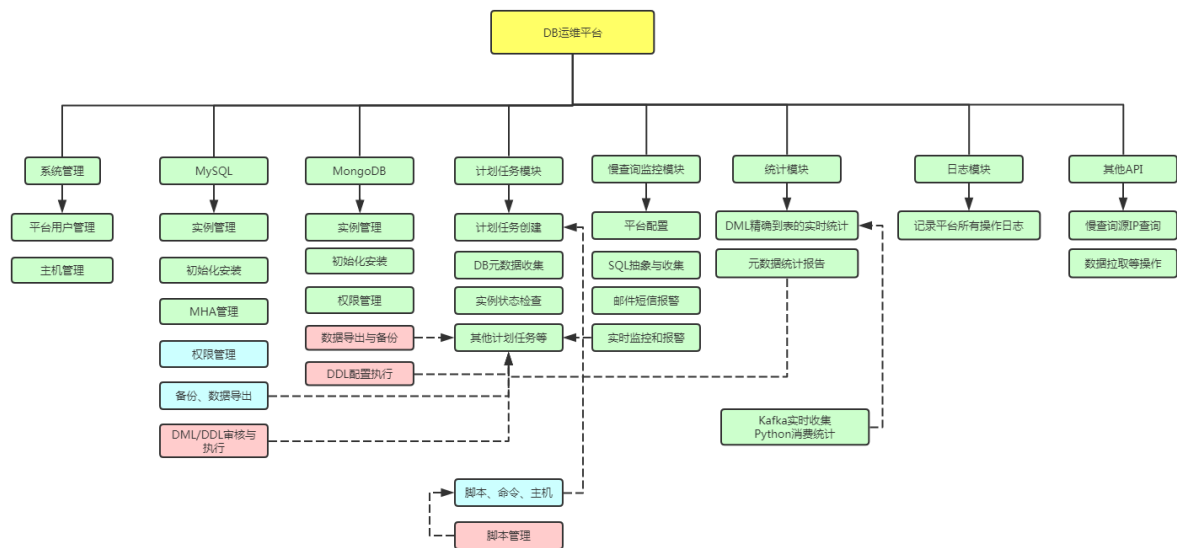


权限管理

Mysql与MongoDB的权限管理与申请

2018-08-16 自动化运维分享--张煜杰

先介绍一下目前平台的开发进度与计划，图中绿色代表已经上线正常使用，蓝色正在开发中，红色为计划开发。



系统管理：

平台用户管理：包括用户的增删改操作，和用户授权等

主机管理：查询主机的内存和磁盘用量等基本信息，其他信息去CMDB系统查询

Mysql:

实例管理界面：查询所有的实例信息，可对实例进行启停操作以及修改信息等

初始化安装：单节点mysqld的初始化部署安装

MHA管理：MHA的检查与部署搭建、启停操作和切换

权限管理：用户权限管理与授权，权限申请，权限审批等

备份：包括xtrabackup正常备份任务，以及日常的一些数据导出操作

慢查询实时报警：实时监控mysql慢日志，根据平台配置好的收件人进行邮件和短信报警

DML审核与执行：计划使用inception进行sql审核，配合计划任务定点执行DDL或DML操作

MongoDB:

实例管理界面：查询所有的实例信息，可对实例进行启停操作以及修改信息等

初始化安装：高可用集群、单节点mongod的部署安装

权限管理：用户与角色权限管理与授权，权限申请，权限审批等

备份：日常数据导出操作

慢查询实时报警：实时监控mongodb慢日志，根据平台配置好的收件人进行邮件和短信报警

DDL审核与执行：配合计划任务进行索引创建，shard分片操作等。

其他模块：

慢查询监控报警：ZMQ实时收集统计慢日志，抽象入库，计划任务根据配置好的人发送相关慢查询邮件

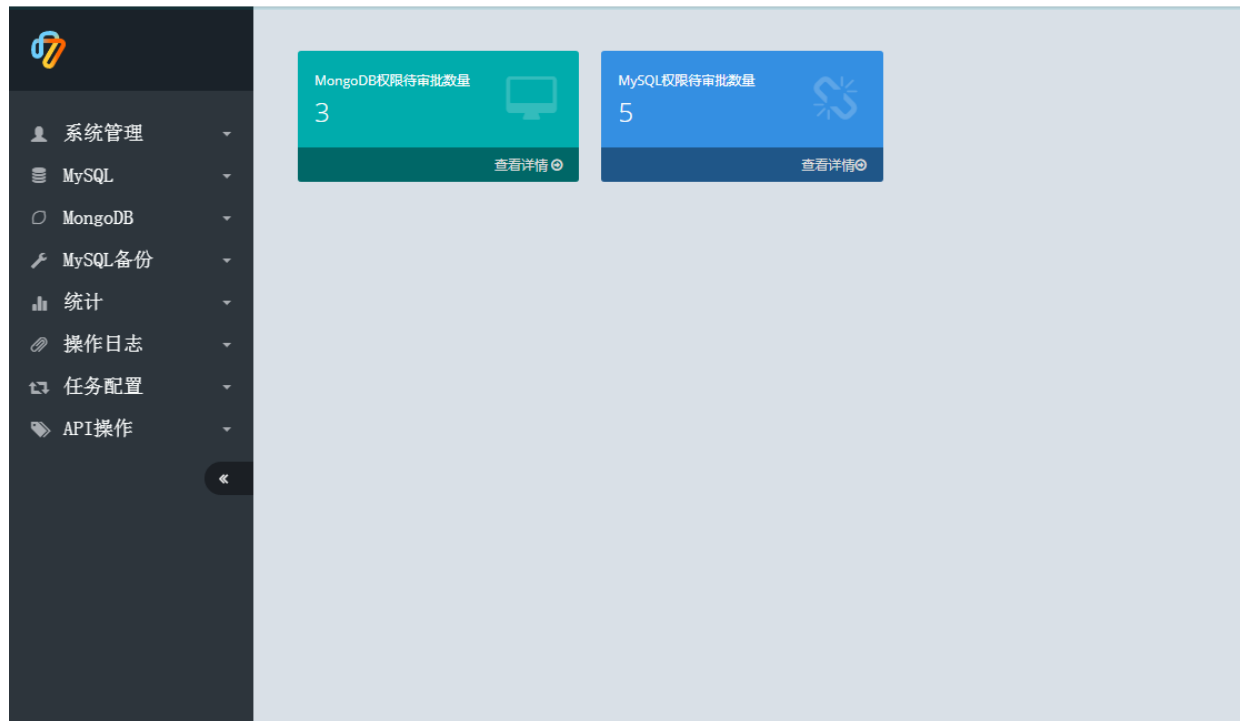
计划任务模块：各种各样的任务，数据收集，监测，备份，DDL等

统计模块：DML实时统计，需要java配合将操作写入kafka集群。元数据收集与统计，包括表数据量，数据量，索引等大小的

日志模块：记录平台所有的操作日志

其他API：慢查询源IP的查询界面等其他一些开发需求

一起作业数据库管理平台



今天我主要分享Mysql和Mongodb的权限管理这一块，前段时间搬完机房后 实在是受不了天天来找开权限，最后决定重新规划权限，规范申请流程。然后就优先开发了平台的权限管理模块。

第一版权限规划：

DBA角色：权限管理，查询，直接开通高权限用户，审批后的执行等所有操作

开发角色：权限申请

项目负责人：权限申请，权限审批

一、Mysql权限管理：

1、权限管理细化粒度：

集群名--用户名--库名--表名--访问源IP--权限详情

Mysql 权限管理

权限新开

选择集群: Mysql-DBTEST 用户名(可模糊匹配): 查询 授权日志

集群	用户	库名	表名	权限	访问源IP	业务	创建时间	操作
Mysql-DBTEST	test_user	dba2	*	SELECT INSERT UPDATE DELETE SHOW VIEW	10.200.3.2	测试	2018-08-16 19:09:53	更新备注
Mysql-DBTEST	test_user	dba	t2	SELECT INSERT UPDATE DELETE SHOW VIEW	10.200.3.2	测试	2018-08-16 19:09:53	更新备注
Mysql-DBTEST	test_user	dba3	*	SELECT INSERT UPDATE DELETE SHOW VIEW	10.200.3.2	测试	2018-08-16 19:09:53	更新备注

2、DBA角色的权限新开与查询：

Mysql 用户授权与新开！

选择集群:

Mysql-DBTEST

查看集群信息

选择库/表:

dba

☐

t

☒

t2

dba2

☐

t

☒

dba3

☐

test

选择权限:

☐ SELECT

☐ INSERT

☐ UPDATE

☐ DELETE

☐ SHOW VIEW

☐ ALTER

☐ CREATE

☐ DROP

☒ ALL

选择用户:

test_user

+ 新读写用户

+ 新只读用户

查看当前用户权限

访问源IP:

10.200.3.2
10.200.5.%

(每行一个IP，不要加其他符号)

业务说明:

测试

授权

返回

-- 库名表名，用户名元数据的显示：

- 1.直接连接从库查询，读实例中information库里的元数据信息，拿到后返回前端渲染
- 2.同时对比平台元数据库里的信息，如果不一致的话提示DBA检查，返回错误

-- 用户密码问题：

- 1.如果为新建用户，检查用户如已存在或元数据不一致，返回错误
- 2.如果开通现有用户，主机存在，则直接授权
- 3.如果开通现有用户，主机不存在，开通时使用的密码为该用户对别的某个主机的密码。

-- 授权成功后根据 集群名--用户名--库名--表名--访问源IP 来更新权限，如果没有该记录则新增

-- 所有的流程都对平台元数据记录表依赖性比较大，所以在第一次上线的时候一定要保证平台元数据表与实例中的一致

-- 日志记录：记录所有授权操作日志

Mysql 授权日志								
Show	20	entries	Search:					
库群	USER	DB	权限	IP	授权类型	授权结果	授权时间	日志详情
Mysql-DBTEST	test_user	dba2.* dba.t2 dba3.*	SELECT,INSERT,UPDATE,DELETE,SHOW VIEW	10.200.3.2	现有用户新建权限	授权成功	2018-08-16 19:09	日志详情
Mysql-DBTEST	tyfxs_my01_rw	dba.t2 dba2.* dba3.*	SELECT,INSERT,UPDATE,DELETE,SHOW VIEW	192.168.100.100	现有用户新建权限	授权成功	2018-08-16 17:11	日志详情
asdf	aaa_my01_rw	test.* cba.asddd abc.zyj	SELECT	1.1.1.1	新建用户	授权成功	2018-08-13 17:25	日志详情



二、Mongo权限的管理

1、角色Role的管理：

可以对多个用户进行授权同一个角色，管理方便

mongo的role分为自建角色和内建角色，内建例如readAnyDatabase、clusterMonitor等mongo自带的在建用户的时候可以直接授予

下面说一下自建角色的管理，粒度也是 集群名-角色名-库名-表名-权限详情 来细化管理，上几张图大家应该能看明白

MongoDB 角色授权！

选择集群:

dbatest1

查看集群信息

库名:

* 为开通所有库

表名:

* 为开通所有表

选择权限:

☐ find☐ insert☐ remove☐ update☐ listIndexes☐ listDatabases☐ listCollections☐ collStats☐ dbHash☐ createIndex☐ createCollection☐ killCursors☐ dropCollection☐ dropDatabase

选择角色:

abcd

+ 创建新角色

查看当前角色权限

角色备注:

授权

返回

MongoDB 角色管理

角色授权与创建

授权日志

选择集群:

dbatest1

角色名(可模糊匹配):

查询

集群	角色名	库名	表名	权限	业务	创建时间	更新时间	操作
dbatest1	dddd	aaaaaa	bbbbbbbb	find listIndexes createIndex	测试	2018-08-14 18:28:51	2018-08-14 18:28:51	<div>更新备注</div>
dbatest1	abcd	abc		find createIndex createCollection killCursors		2018-08-14 17:58:28	2018-08-14 17:58:28	<div>更新备注</div>

2、用户管理：

有了角色之后，用户的管理相对简单，与mysql几乎一样的逻辑：

Mongo 用户授权与新开！

选择集群:

dbatest1

查看集群信息

选择角色:

abcd

+ 创建新角色

查看角色权限

内建角色:

☒ readAnyDatabase

☐ readWriteAnyDatabase

☐ clusterMonitor

☐ root (超级用户)

选择用户:

qwrsa

+ 创建新用户

查看当前用户权限

备注:

授权

返回

MongoDB 用户管理

用户授权与创建

授权日志

选择集群:

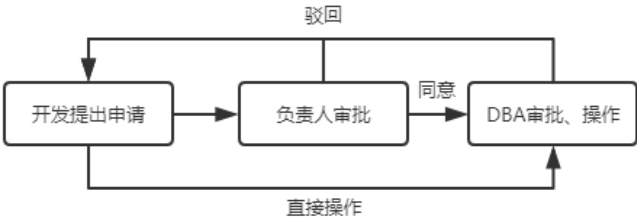
dbatest


用户名(可模糊匹配):

查询

集群	用户名	自建角色	内建角色	业务备注	创建时间	更新时间	操作
dbatest1	qwrsa	abcd dddd	readAnyDatabase		2018-08-08 14:3 7:15	2018-08-14 18:2 9:00	<div>更新备注</div>
dbatest	asdf		readAnyDatabase	333	2018-08-08 15:0 3:45	2018-08-08 15:0 3:45	<div>更新备注</div>
dbatest1	sdaafsdf		readAnyDatabase	123	2018-08-08 14:5 7:58	2018-08-08 14:5 7:58	<div>更新备注</div>

三、最后以Mongoddb为例说一下权限申请与审批：





MySQL

MongoDB

权限申请

API操作

我的申请

MongoDB 权限申请 !

申请人: ppp

部门与业务组: 小学业务 作业 + 添加新项目组

选择集群: Mongo-BgTest 查看集群信息

选择库/表:

klx_eng

☒ wy_test_000

☒ student_accuracy

☐ wy_test

☒ test

☒ col

选择权限: ☒ 只读权限 ☐ 读写权限

申请原因: 测试

提交申请 返回

流程比较简单：

- 1、部门与业务项目组的信息，负责人等需要手动来维护，或者从公司平台调接口
- 2、集群信息在平台元数据表里直接读取
- 3、选择进群后根据IP和集群模式连接实例，获取所有的库名表名，回前端渲染
- 4、权限分只读和读写两种权限
- 5、申请原因为必填项，方便以后查看记录
- 6、每个申请都会产生一个唯一的工单号
- 7、所有的申请都在数据库中通过一个申请表来管理

下面截几张申请提交后的查看界面和审批操作界面：

开发角色：

MongoDB权限申请单

Show20entries

Search:

申请工单号	部门	项目名	DB 集群名	库名,表名	权限	申请原因	申请人	下一级审批人	状态	提交时间	操作
500025	小学业务	作业	Mongo-BgTest	klx_eng.vwy_test_000 klx_eng.student_accuracy_test.*	只读	测试	ppp	yujiezhang	审批中...	2018-08-17 12:52:32	修改 驳回 流程日志
500024	小学业务	作业	Mongo-BgTest	test.* klx_eng.*	只读	qwe	ppp	yujiezhang	已驳回	2018-08-15 19:55:04	修改 流程日志
500023	小学业务	作业	Mongo-BgTest	klx_eng.* test.*	读写	kl	ppp	yujiezhang	已驳回	2018-08-15 19:53:45	修改 流程日志

Showing 1 to 3 of 3 entries

Previous1Next

负责人角色：

审批记录

MongoDB权限审批

如果审批异常后需要驳回,请从 审批记录 页面操作...

Show20entries

Search:

申请工单号	申请人	部门	项目名	DB 集群名	库名,表名	权限	申请原因	状态	提交时间	操作
500025	ppp	小学业务	作业	Mongo-BgTest	klx_eng.vwy_test_000 klx_eng.student_accuracy_test.*	只读	测试	待审批...	2018-08-17 12:52:32	同意 驳回 流程日志

Showing 1 to 1 of 1 entries

Previous1Next

DBA角色：

审批记录

MongoDB权限审批

如果审批异常后需要驳回,请从 审批记录 页面操作...

Show20entries

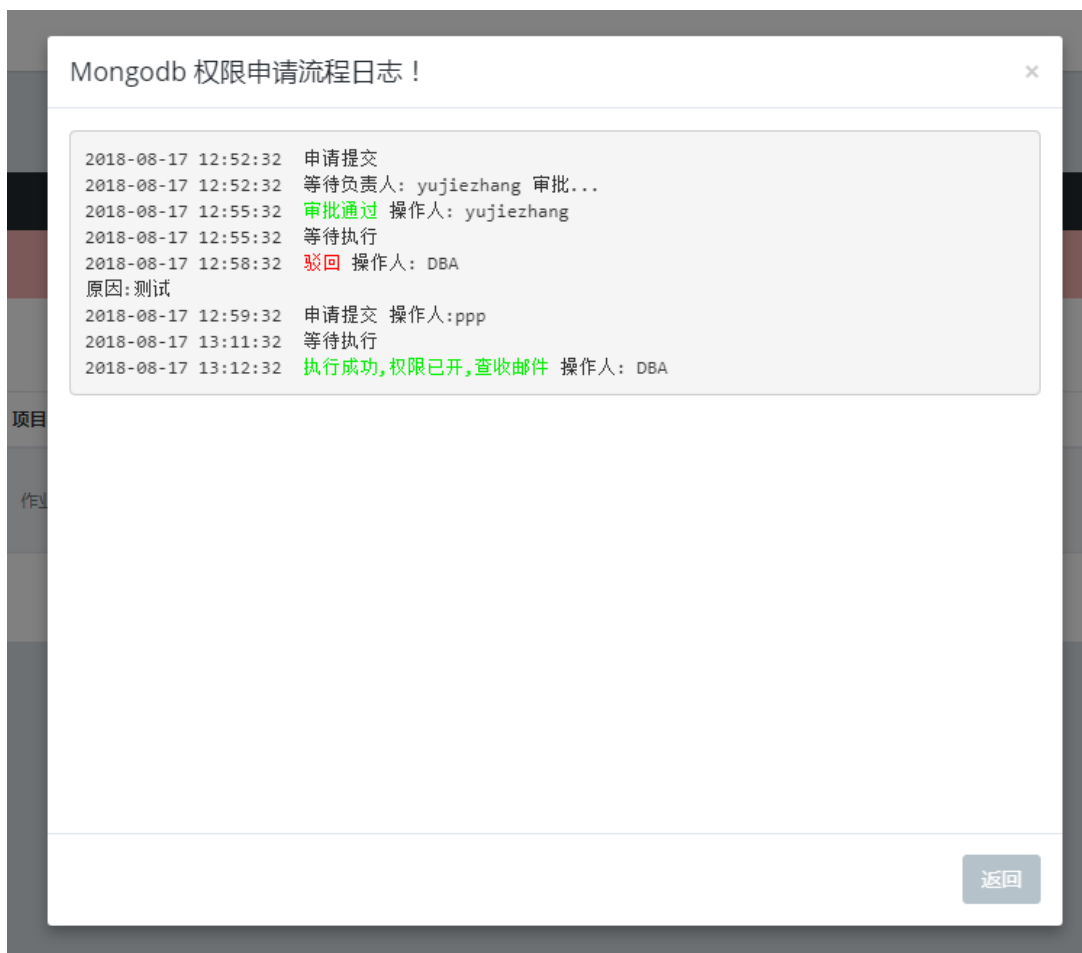
Search:

申请工单号	申请人	部门	项目名	DB 集群名	库名,表名	权限	申请原因	状态	提交时间	操作
500025	ppp	小学业务	作业	Mongo-BgTest	klx_eng.vwy_test_000 klx_eng.student_accuracy_test.*	只读	测试	审批通过 等待执行	2018-08-17 12:52:32	查看执行 驳回 流程日志

Showing 1 to 1 of 1 entries

Previous1Next

测试日志：



以上是我今天分享的东西，没有说的太细，只是讲了下大体流程，大家有兴趣或者不明白的地方可以私聊我。