**BIGDAF用户手册**

**观数科技**

**2017年8月24日**

目录

一. 插件配置 4

1. HDFS插件配置 4

2. HBASE插件配置 5

3. GATEWAY插件配置 5

二. 概览 6

三. 插件管理 7

1. HDFS插件管理 7

2. HBASE插件管理 7

3. GATEWAY插件管理 8

四. 权限管理 8

1. HDFS权限管理 8

2. HBASE权限管理 15

五. GATEWAY 21

1. Gateway权限管理 21

2. Gateway单点登录 26

3. Gateway webHdfs操作 27

六. 任务提交 29

七. 管理设置 30

八. 文件浏览 31

九. 漏洞扫描 32

十. 安全审计 33

1. HDFS日志审计 33

2. Admin日志审计 34

3. HBASE日志审计 35

4. GATEWAY日志审计 36

## **插件配置**

用户初次使用BIGDAF，需要在Admin server 对各个插件进行配置。

### HDFS插件配置

在Admin Server中点击【插件】选择【HDFS】，配置插件所需的大数据环境节点信息。

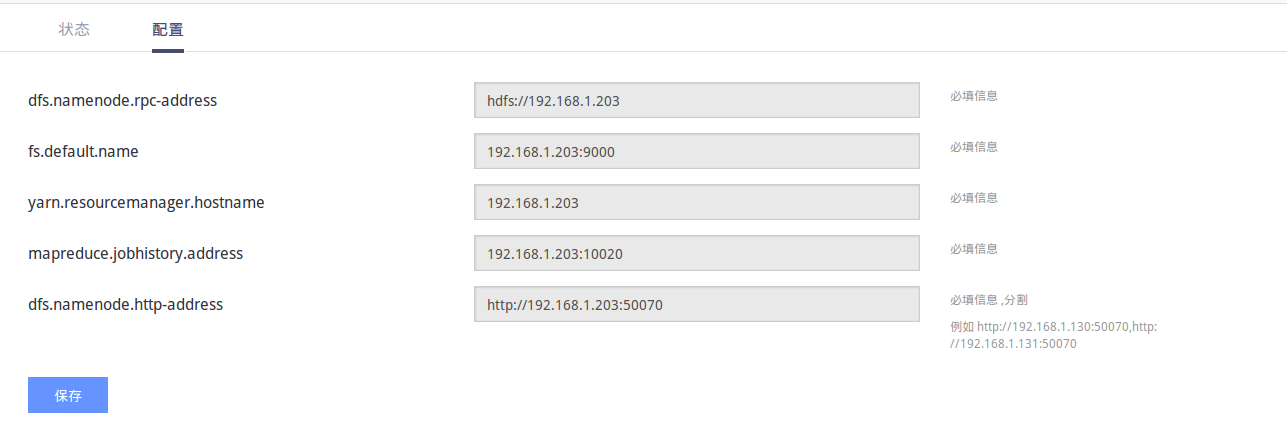


图 1 HDFS插件配置

dfs.namenode.rpc-address：配置HDFS RPC服务地址端口。

fs.default.name：配置namenode所在主机，端口号是9000。

yarn.resourcemanager.hostname： 配置resourcemanager地址。

mapreduce.jobhistory.address：配置MapReduce JobHistory Server地址。

dfs.namenode.http-address：配置HDFS web服务地址端口。

＊高可用配置两个地址中间用逗号隔开

### HBASE插件配置

在Admin Server中点击导航栏【插件】选择【HBASE】点击【配置】，配置Master及备用Master地址，多个地址用逗号隔开，配置完毕点击【保存】。



图 2HBASE插件配置

### GAteway插件配置

在Admin Server中点击导航栏【插件】选择【GATEWAY】点击【配置】，配置GATEWAY地址， 配置完毕点击【保存】。

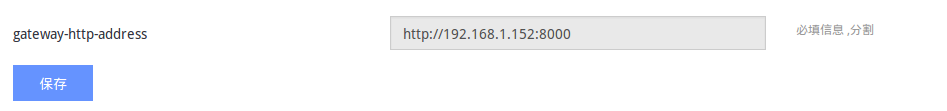


图 3GATEWAY配置

## **­­­­概览**

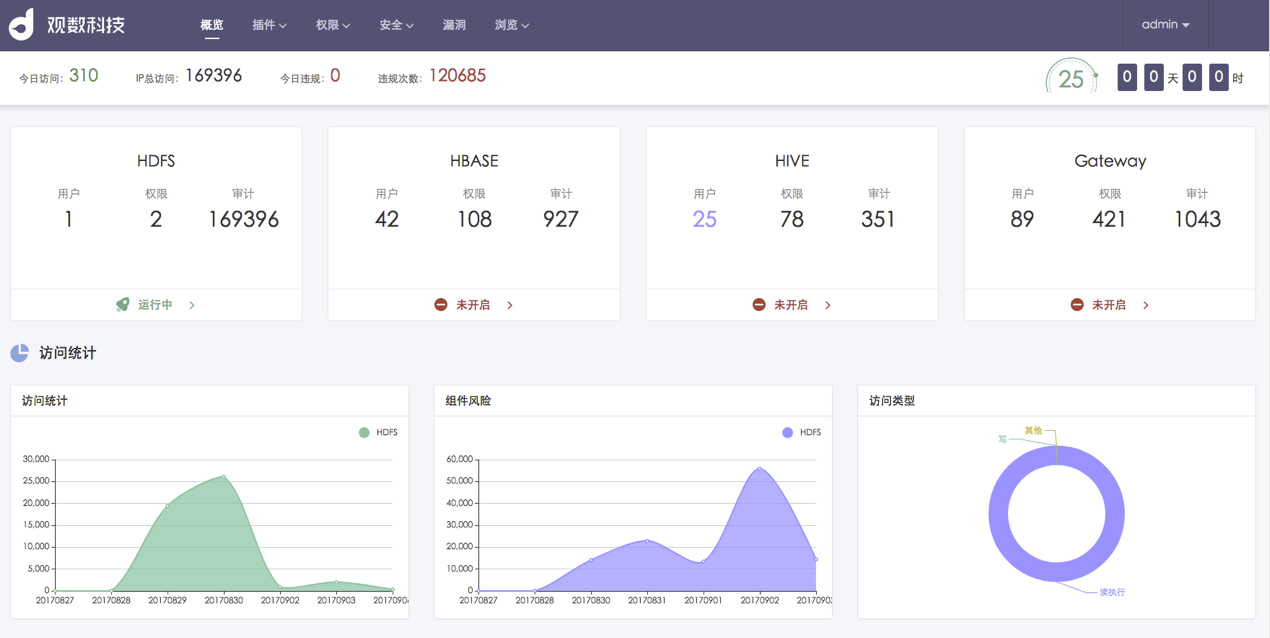


图 4 概览

**访问总览：**显示今日访问与总访问数、今日违规与总违规数，Admin server的运行时间。

**安全指数：**扫描当前大数据集群的安全状态包括基线配置、存在的漏洞数以及漏洞的危害程度予以评分，给出系统信息与系统漏洞详情。

**插件状态显示：**显示各个插件的开启、关闭与异常状态，统计插件用户、权限与已审计操作数量。

**访问统计动态图：**可监控集群的HDFS、HBASE组件的访问数量和违规数量。

## **插件管理**

### HDFS插件管理

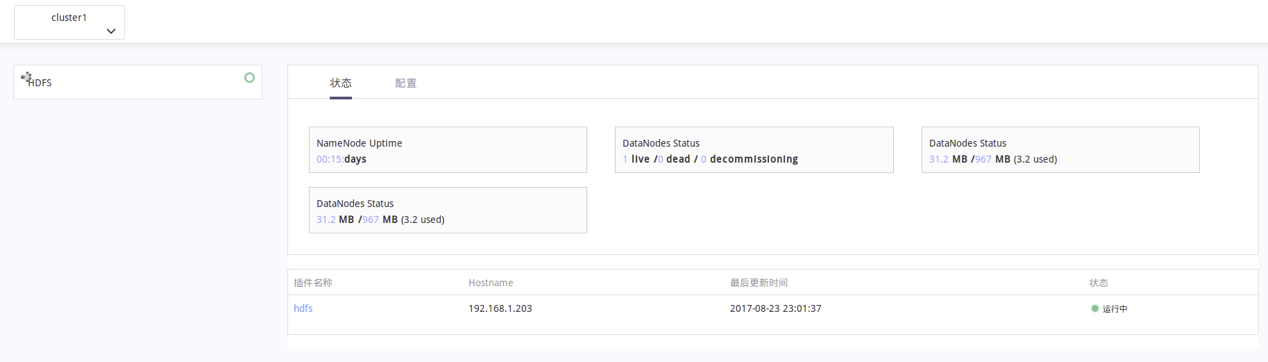


图 5HDFS插件管理

**集群状态：**查看集群Namenode、Datanode运行状态、时间以及内存使用状态。

**插件配置：**配置插件所在大数据环境参数。

**插件状态：**显示插件名称、主机名称，最后同步时间、状态。

### HBASE插件管理

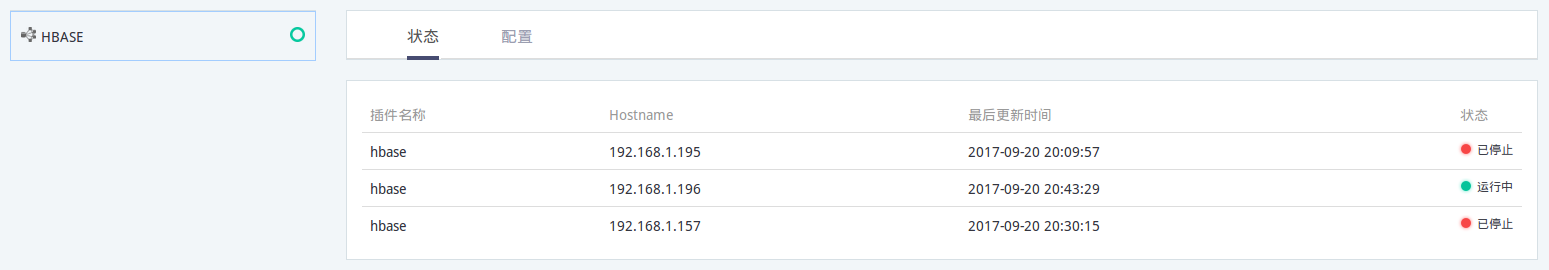


图 6HBASE插件管理

**插件配置：**配置插件所在HBASE集群的参数。

**插件状态：**显示插件名称、主机名称，最后同步时间、状态。

### GATEWAY插件管理

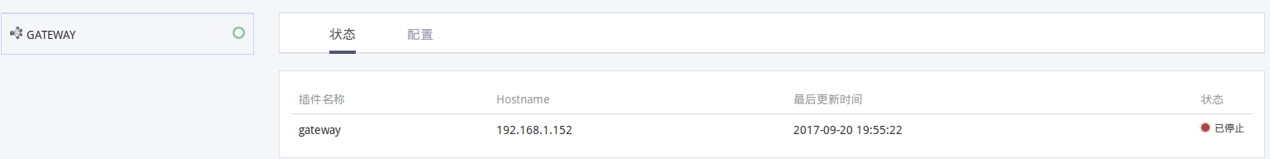


图 7 GATEWAY管理

**插件配置：**配置GATEWAY地址。

**插件状态：**显示插件名称、主机名称，最后同步时间、状态。

## **权限管理**

### HDFS权限管理

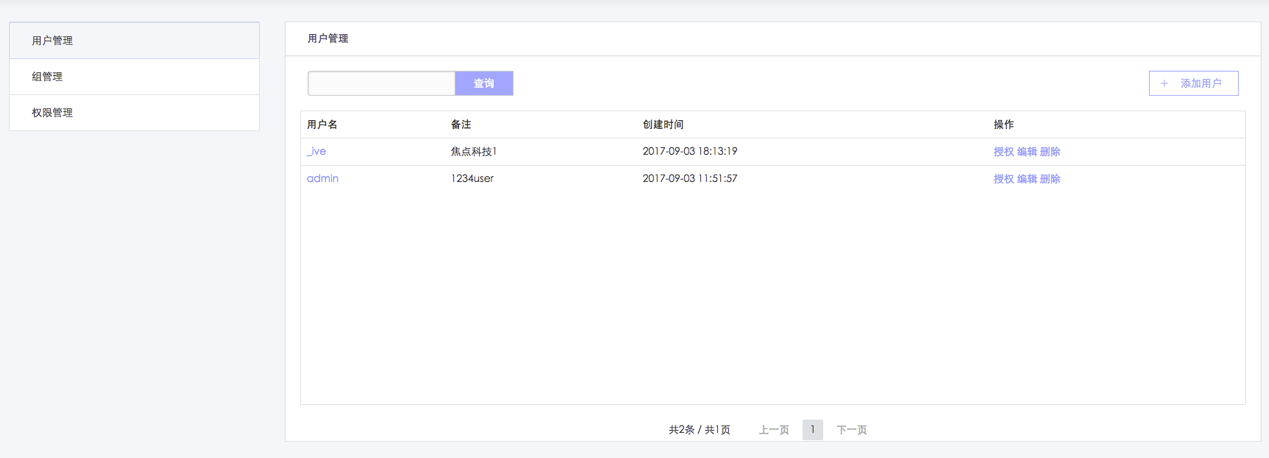


图 8 HDFS权限管理

HDFS权限管理，实现对HDFS数据资源访问权限控制。有两种用户角色配置方案，用户根据角色不同选择配置方案。

#### 大数据组件角色（HBASE、HIVE等）

* 添加用户

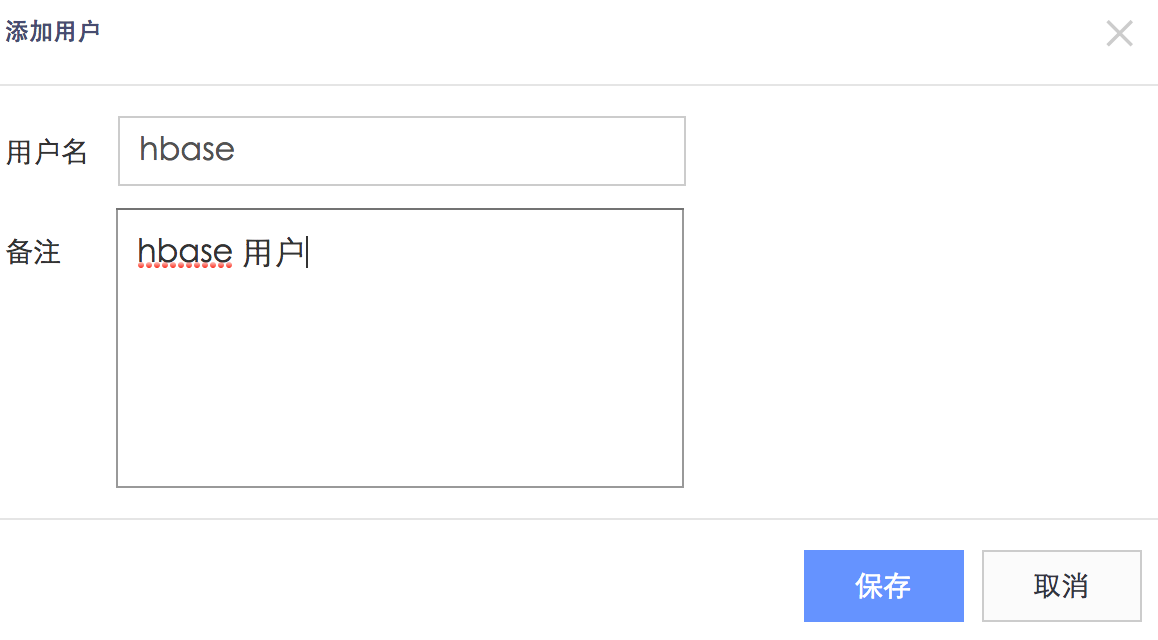
在BIGDAF的Admin Server点击【权限】选择【HDFS】。点击【添加用户】添加hbase 用户

图 9 添加用户

* 添加权限

点击【权限管理】然后【添加权限】建立hbasepri权限名

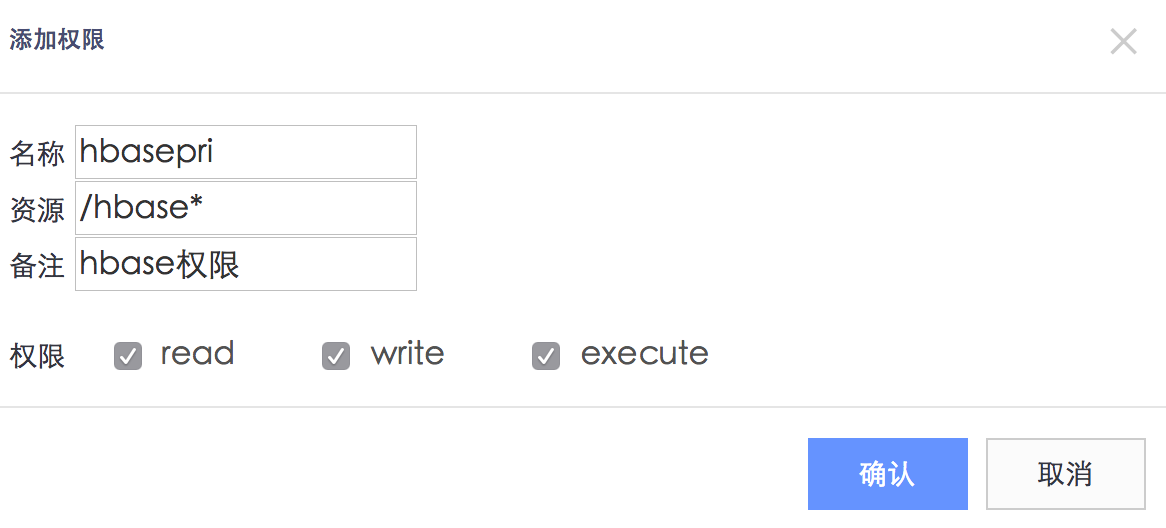


图 10 添加权限

* 授权

点击【用户管理】然后点击【授权】为用户授权hbasepri权限。

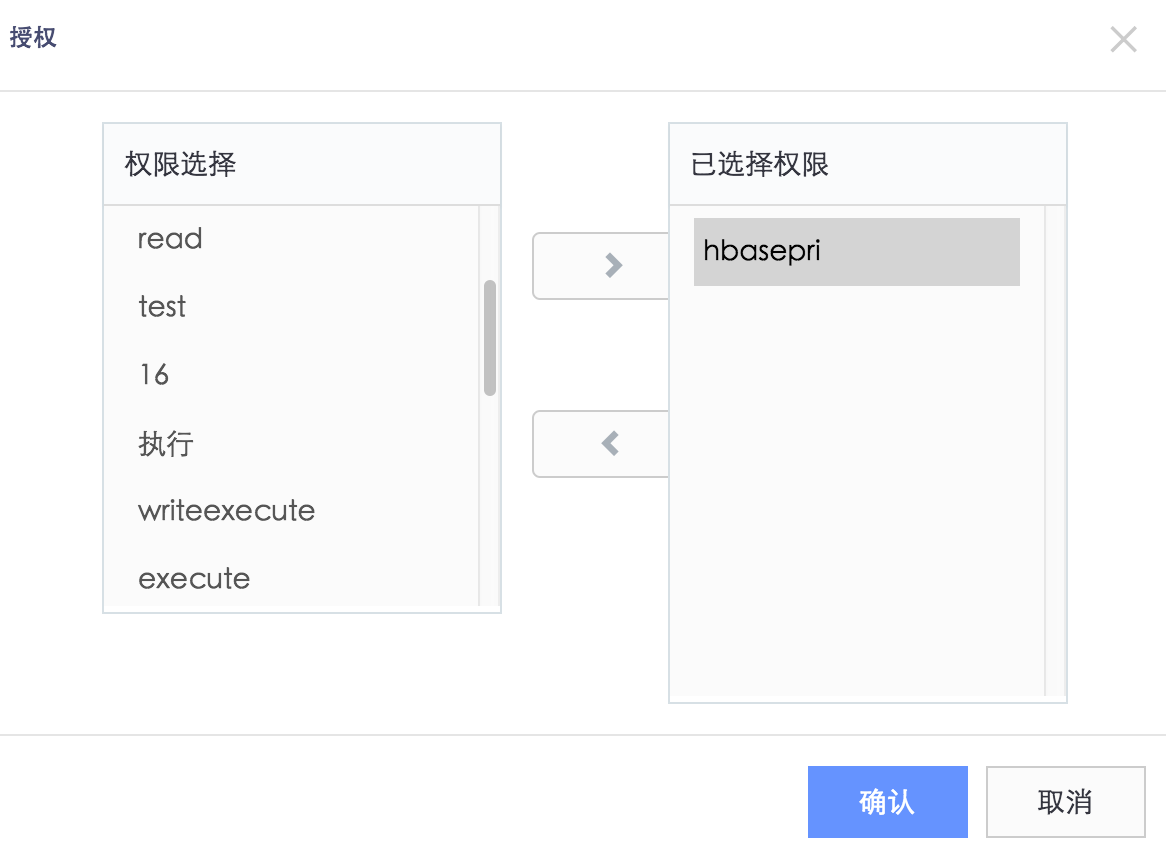


图 11 授权

* 组件配置

在hbase所有节点上，设置启动hbase账户的环境变量，编辑~/.bash\_profile追加export HADOOP\_USER\_NAME=hbase，执行source ~/.bash\_profile，完成配置（环境变量优先级高于启动用户）

#### 数据分析角色

* 添加用户

点击【用户管理】然后点击【添加用户】添加hadoop用户：



图 12 添加用户

* 添加权限

添加资源权限,点击【权限管理】然后点击【添加权限】

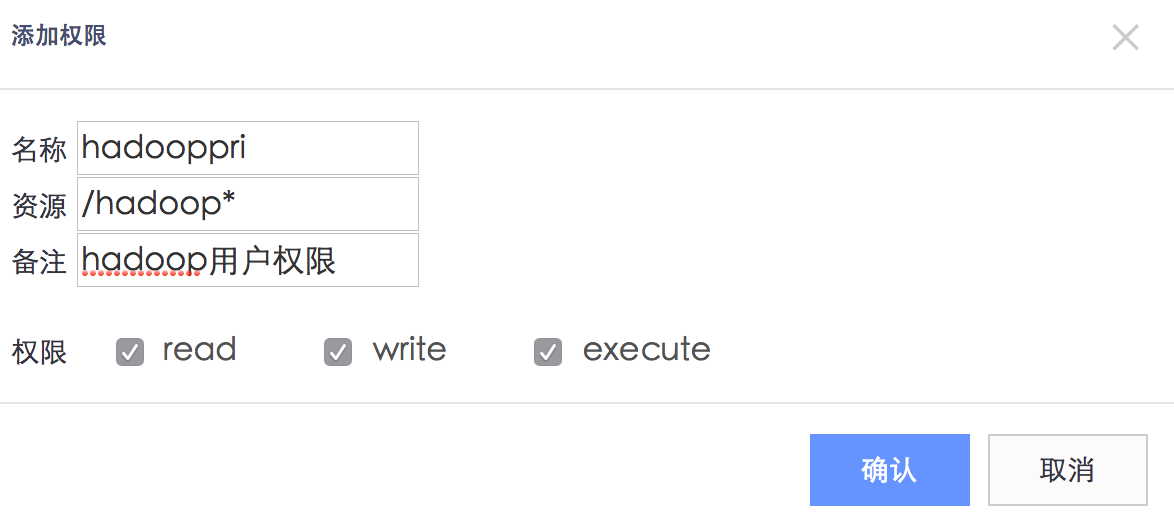


图 13 添加权限

* 授权

为hadoop用户授权，点击【用户管理】，找到hadoop用户点击后边的【授权】：



图 14 授权

* 环境配置

配置开发人员机器登录账户的环境变量，编辑~/.bash\_profile追加export HADOOP\_USER\_NAME=hadoop，执行source ~/.bash\_profile，完成配置。（环境变量优先级高于启动用户）

### HBASE权限管理

HBASE权限管理，实现对HBASE表、列簇、列进行访问权限控制 。

#### 添加用户角色并授权

* 添加权限

点击导航栏【权限】选择【HBASE】，然后点击权限管理，点击右侧的【添加权限】。

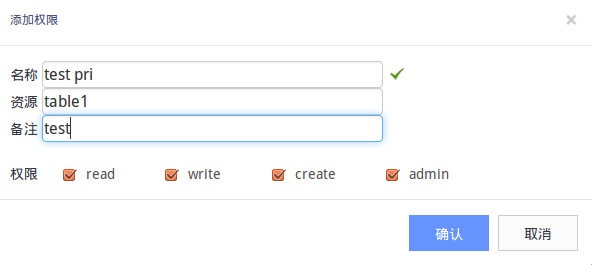


图 15 添加权限

hbase的资源配置规则如下：

【＊】：权限控制到所有表

【table】：权限控制到具体表

【table/column-family1, column-family2】 权限控制到列簇

【table/ column-family1, column-family2/ column1, column2】权限控制到列

* 添加角色并授权

点击【角色管理】选择【添加角色】，添加develop角色。

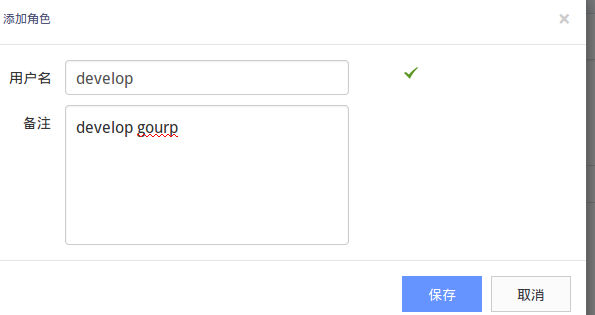


图 16 添加角色

找到develop角色，点击后边的【授权】，为develop角色授权



图 17 授权

* 添加用户并赋予角色

点击【用户管理】选择【添加用户】，添加userone用户。

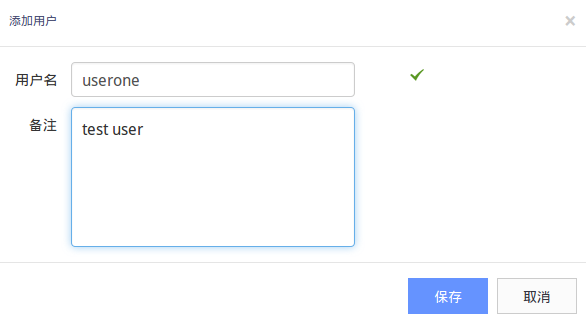


图 18 添加用户

点击userone用户后边的授权，为userone用户赋予develop角色。



图 19 用户赋予角色

#### 远程调用环境配置

方法一：远程调试时，程序里添加System.setProperty("HADOOP\_USER\_NAME", "userone")

方法二：设置程序执行主机的环境变量，编辑~/.bash\_profile追加export HADOOP\_USER\_NAME=userone，执行source ~/.bash\_profile，完成配置。

#### hbase shell client操作环境配置

方法一：在客户端shell命令行操作HBASE时，新建系统用户userone 直接切换用户su userone。

方法二：编辑~/.bash\_profile追加export HADOOP\_USER\_NAME=userone，执行source ~/.bash\_profile，完成配置。

#### storm操作环境配置

执行storm分析程序时在程序中设置：

import org.apache.storm.Config;

Config config = new Config();

Map map = new HashMap<String, String>();

map.put("HADOOP\_USER\_NAME", "userone");

config.setEnvironment(map);

## **gateway**

### Gateway权限管理

GATEWAY权限管理，实现外部用户对HDFS数据资源访问权限控制。

#### 添加用户角色并授权

* 添加权限

点击导航栏【权限】选择【GATEWAY】，然后点击权限管理，点击右侧的【添加权限】。

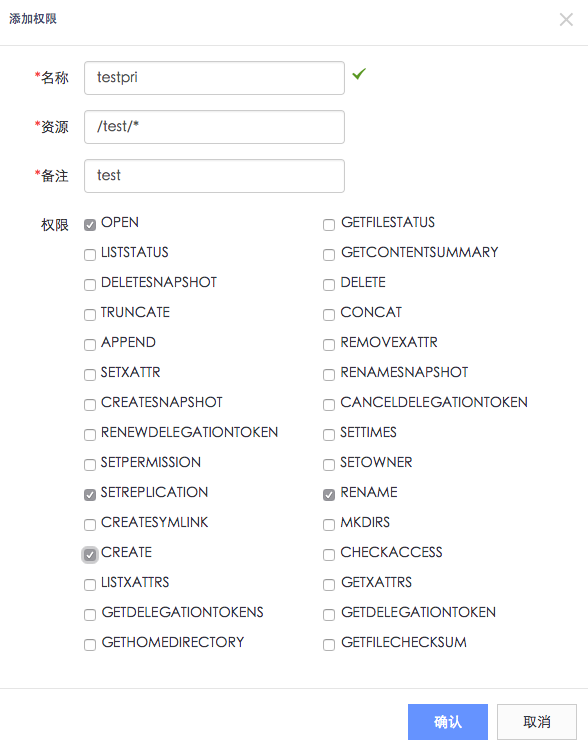


图 20 添加权限

GATEWAY的资源配置规则如下：

【＊】：代表当前目录以及子目录

* 添加角色并授权

点击【角色管理】选择【添加角色】，添加testuser角色。

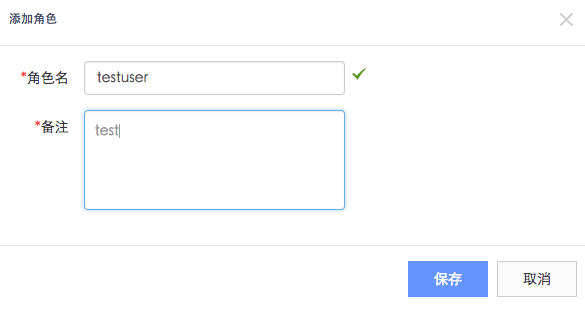


图 21添加角色

找到testuer角色，点击后边的【授权】，为testuser角色授权



图 22 授权

* 添加用户并赋予角色

点击【用户管理】选择【添加用户】，添加testname用户。



图 23添加用户

点击testname用户后边的授权，为testname用户赋予testuser角色。

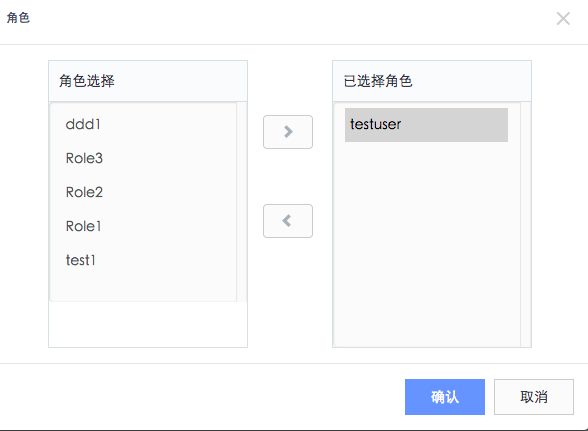


图 24 赋予角色

### Gateway单点登录

使用testname用户访问 http://{gateway服务器地址}:8000 进行单点登录,输入用户名密码并且点击不同组件的复选框，查看不同的组件页面。



图 25 单点登录

### Gateway webHdfs操作

* HTTP GET操作

curl -i -k "http://{gateway地址}:8002/webhdfs/v1/{资源路径}?op={操作}" -u 用户名:密码



图 26 操作

* HTTP PUT POST操作

curl -i –k –X ［PUT、POST］ "http://{gateway地址}:8002/webhdfs/v1/{资源路径}?op={操作}" -u 用户名:密码

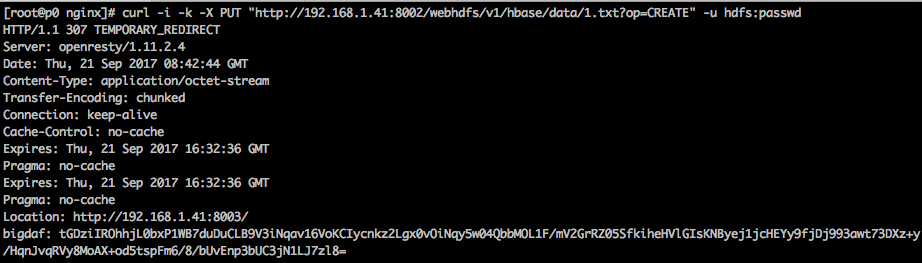


图 27 操作

将返回一个bigdaf字段秘钥，带着秘钥再次发起请求：

curl -i –k –X ［PUT、POST］ –T ｛资源｝ –H "bigdaf：秘钥" "http://{gateway地址}:8003"

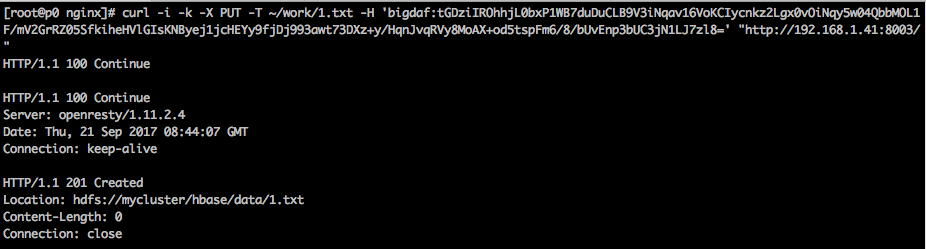


图 28 操作

## **任务提交**

可以进行任务搜索、查看任务、新建任务。用户可以通过BIGDAF平台上传执行MapReduce任务，查看任务列表，根据任务名称搜索任务。

新建任务: 输入任务名称，输入【HDFS输入目录】，填写【HDFS输出目录】，选择要上传的jar包，点击【提交】。（注意要开启jobhistoryserver）

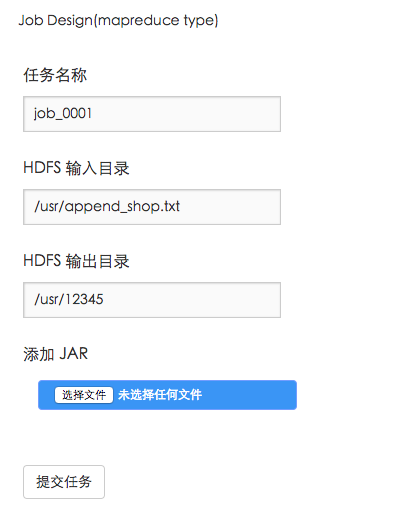


图 29 新建任务

查看任务：



图 30 任务浏览

## **管理设置**

**测试模式**：点击开启关闭BIGDAF的平台测试模式按钮，开启测试模式时，不执行访问控制策略。

**登录设置**：设置登录的最大错误次数以及错误的清零时间。



图 31 管理设置

## **文件浏览**

用户可以通过BIGDAF后台对大数据平台的文件资源进行浏览。

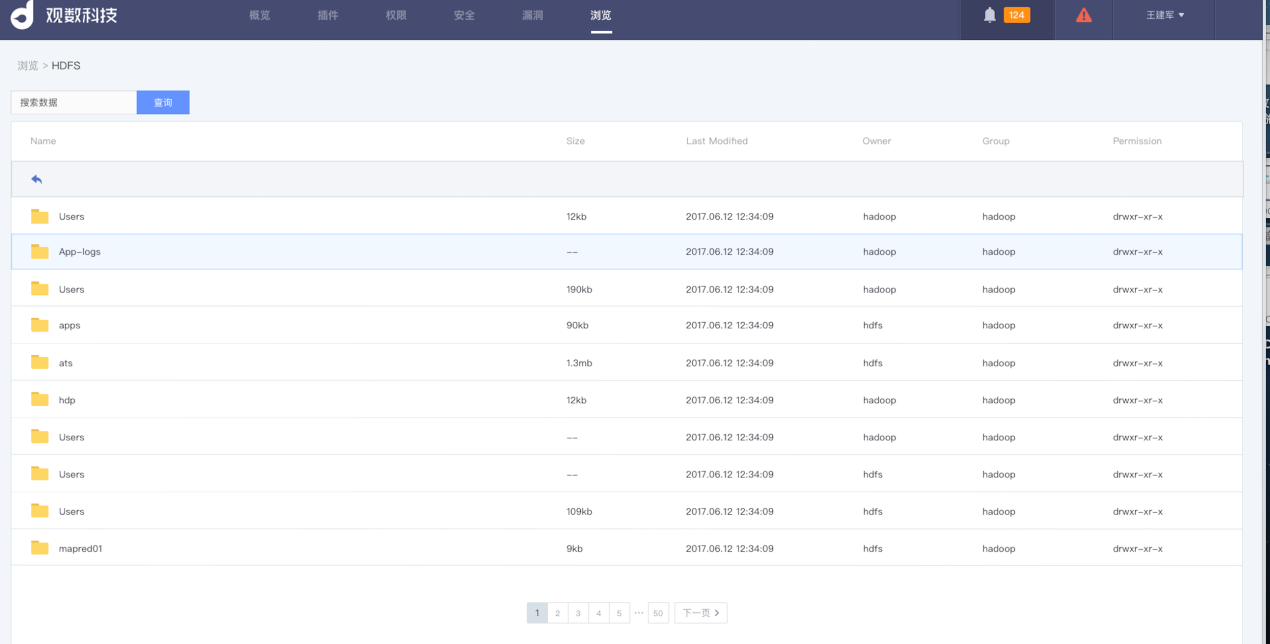


图 32 文件浏览

## **漏洞扫描**

用户点击导航栏【漏洞】可以查看大数据平台配置信息以及漏洞详细信息，点击概览页面的安全指数可以对大数据平台进行安全扫描。



图 33 漏洞扫描

## **安全审计**

登出安全管理员账户，用审计员账户登录，安全审计支持对大数据平台中HDFS、HBASE、GATEWAY组件，对被用户访问时所产生的日志数据进行统计、分析、查询及分析挖掘。

### HDFS日志审计

**HDFS日志审计：**可详细展示访问Hadoop的用户名、IP、资源、访问次数、访问的客体列表（包括被访问资源名、访问的操作行为、访问的最终结果、操作时间），可以针对用户名、日期、授权结果进行条件查询。

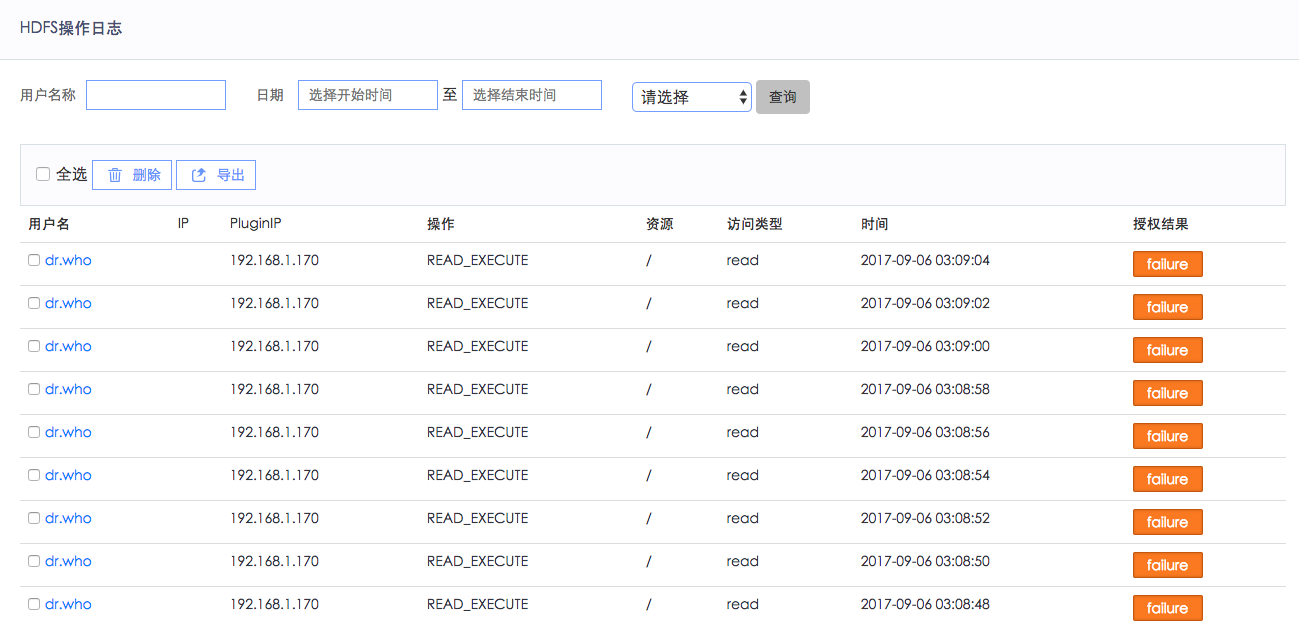


图 34 HDFS日志

### Admin日志审计

**Admin操作日志：**可以详细展示用户行为，包括用户名、操作、时间、信息。

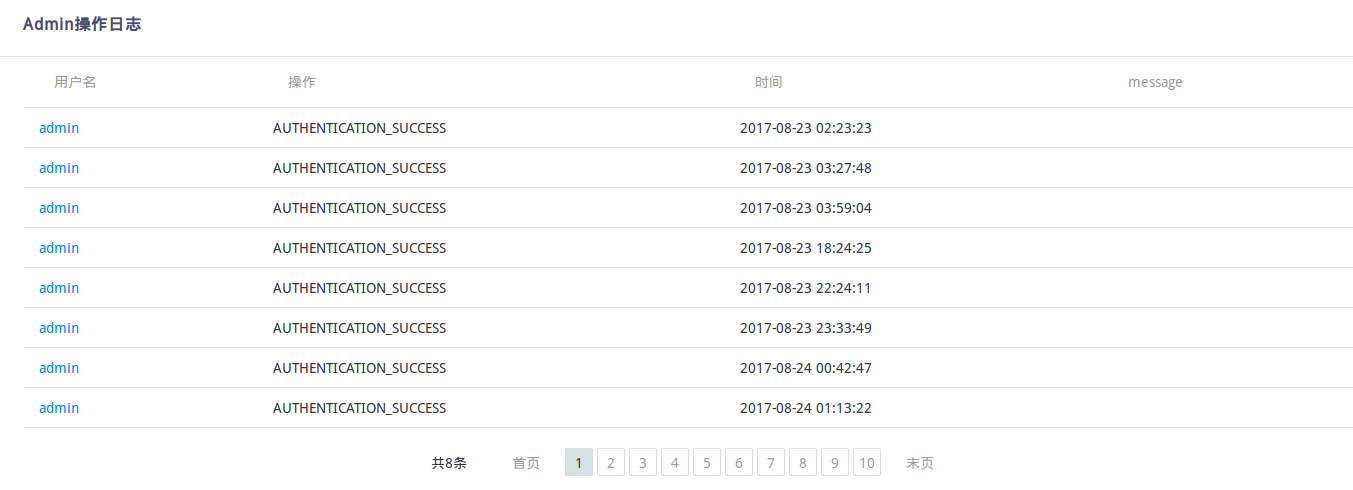


图 35 Admin日志

### HBASE日志审计

**HBASE日志审计：**详细展示访问的用户名、IP、插件IP、操作、资源、访问类型、时间、授权结果，可以针对用户名、日期、授权结果进行条件查询。

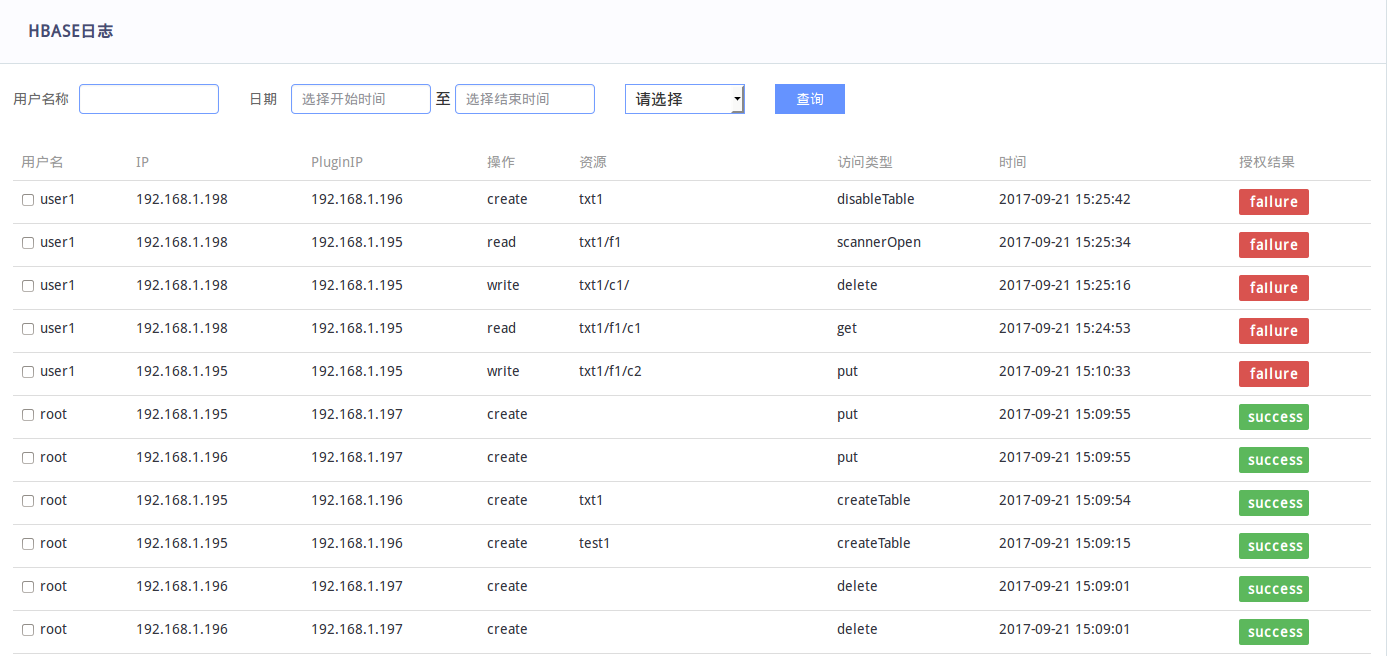


图 36 HBASE日志

### GATEway日志审计

**GATEWAY日志审计：**详细展示访问的用户名、IP、插件IP、操作、资源、访问类型、时间、授权结果，可以针对用户名、日期、授权结果进行条件查询。

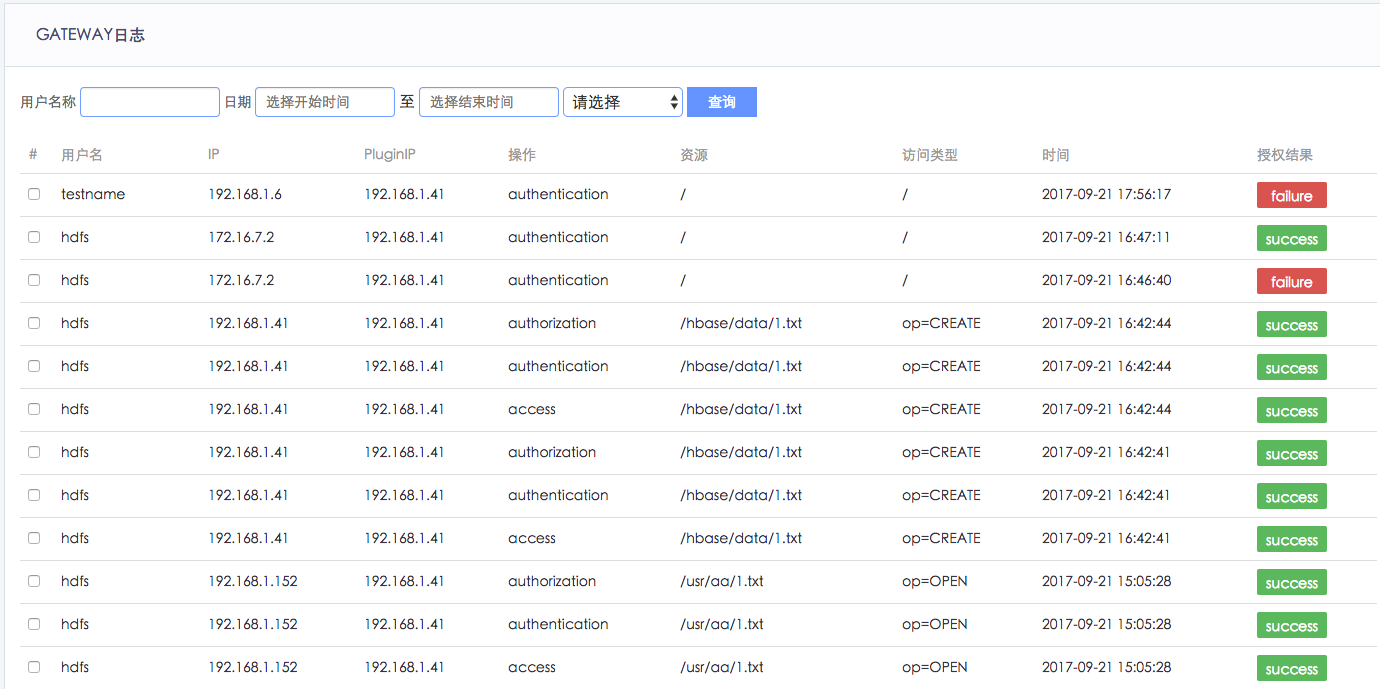


图 37 GATEWAY日志