

# AWS资源池管理设计（平台管理员功能）

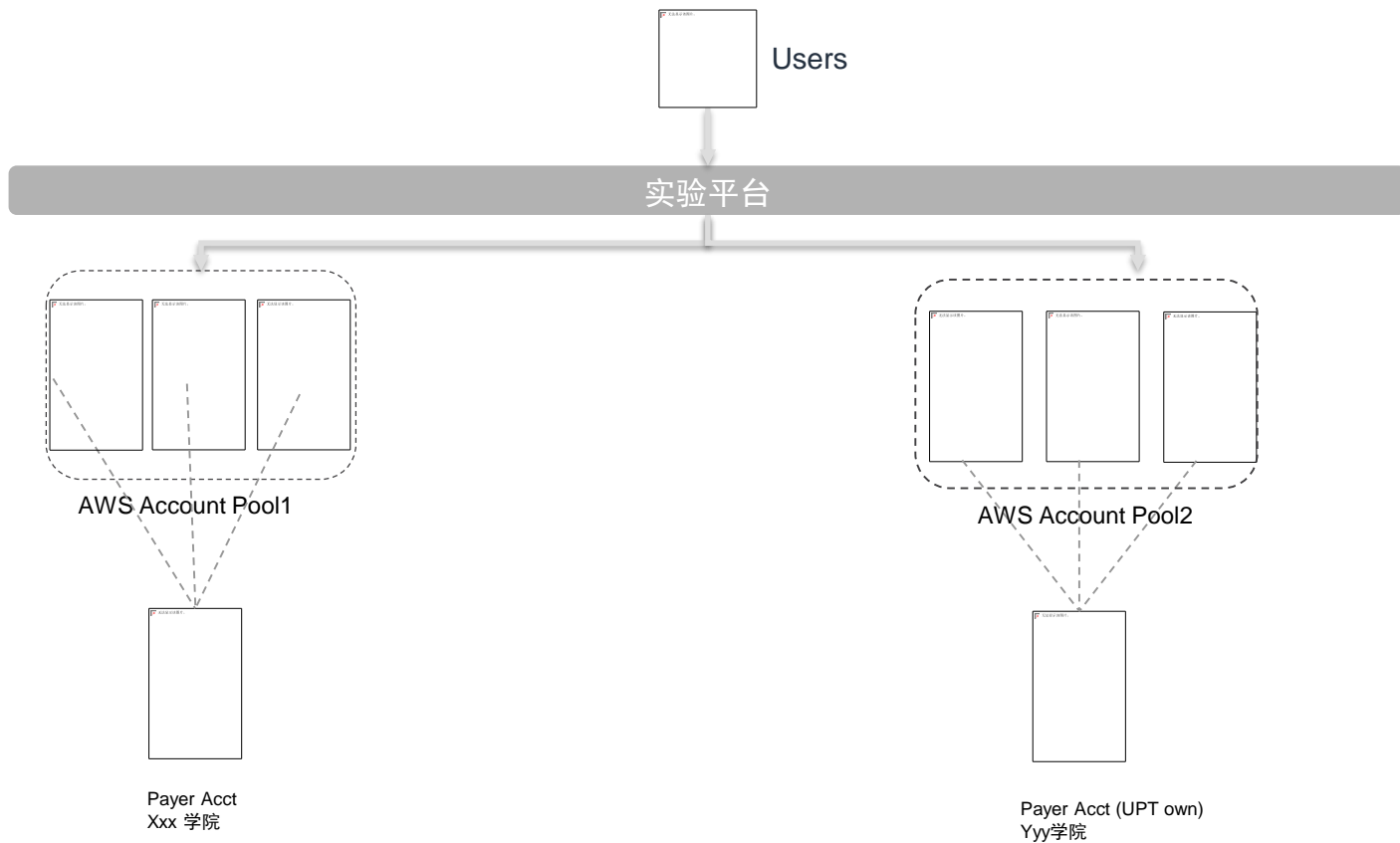


修改为

- AWS资源池管理
  - 平台AWS账号池
  - 院系AWS账号池

说明：

1. 平台AWS账号池，用于管理接入UPT平台的AWS Payer Account和院系 AWS Account的对应关系。
2. 院系AWS账号池，用于管理各个院系所使用的AWS账号



# 平台AWS账号池主页面（平台管理员）



平台AWS账号列表

新增

激活/注销

删除

修改

批量导入

选择	付款账号名称	Account ID	是否UPT 所有	IAM User	AK	SK	加入时间	状态
<input type="checkbox"/>	UPT-泰豪学院	354235235232	是	354235235232	ASDFA58765875	asdff4a746aasdf7	2018-02-25 11:58:37	激活
<input type="checkbox"/>	河北工业大学	234512412121	否	354235235232	aserDFA58765875	as6a4sasdfaa54s7	2018-08-28 09:42:39	激活
<input checked="" type="checkbox"/>	UPT-云普教研	747463525252	是	354235235232	ASDFA58765875	6a4sdf4a746a54s7	2018-08-28 09:42:39	注销
<input type="checkbox"/>	南方科技大学	938512724121	否	354235235232	asdfasf5986876asd	asdfa6543563afs6	2018-08-28 09:42:39	激活
<input type="checkbox"/>	AWS Hackthon	234523452234	否	354235235232	afas75d4fa6s4dfas	fasdfas76df4asdfa	2018-08-28 09:42:39	激活

首页

前一页

1

后一页

尾页

说明：

1. 【平台AWS账号】作为payer account 用于关联院系所有的实验账号；
2. 【平台AWS账号】有两类，UPT所有的，和非UPT所有的（院系自己付款的账号），将来做付款统计或账单区分；
3. 每个【平台AWS账号】要有一个IAM User用于系统提取账单。

# 院系AWS账号池主页面（平台管理员功能）



院系列表

关联AWS账号池

- 新增
- 激活/注销
- 删除
- 修改
- 批量导入

- 江西科技大学
- 南方科技大学
- 江西泰豪学院
- 云普教研室
- 深度学习开放课程
- AWS Hackthon

选择	使用类型	Account ID	是否付款账号	关联付款账号	付款账号名称	加入时间	状态	试验中
<input type="checkbox"/>	不登陆AWS	123456789012	否	354235235232	UPT-泰豪学院	2018-06-25 11:58:37	激活	是
<input type="checkbox"/>	登陆AWS	234523523523	否	354235235232	UPT-泰豪学院	2018-08-28 09:42:39	激活	是
<input checked="" type="checkbox"/>	登陆AWS	756745745456	否	354235235232	UPT-泰豪学院	2018-08-28 09:42:39	注销	否
<input type="checkbox"/>	登陆AWS	234523523555	否	354235235232	UPT-泰豪学院	2018-08-28 09:42:39	激活	否
<input type="checkbox"/>	登陆AWS	352412412412	否	354235235232 zhichi	UPT-泰豪学院	2018-08-28 09:42:39	激活	是

## IAM User 管理

IAM用途	IAM user	Password	PK	SK	当前使用者	操作
IAM - 管理	UPTadmin	Skfj_8923	fjkgfkg25235	Gkjgh2kjg2k		<div>激活（注销）</div> <div>修改</div>
IAM - 实验	UPTstu	Lklaks_34	hgk2jgh4412	kjhg1kj2gkg	王飞扬-14计算机	<div>激活（注销）</div> <div>修改</div>

说明二：

1.

选择【关联AWS账号池】中的1个账号时，在下方的【IAM User 管理】中显示该账号的IAM信息；
2.

每个用于实验的AWS账号必须有2个IAM User，【IAM – 管理】这个IAM User在【新增】院系关联账号的时候手动输入，【IAM – 实验】这个IAM User可以在增加实验账号调用API创建（需要确认API是否支持\*\*）；
3.

必须在【关联AWS账号】和【IAM-管理】和【IAM-实验】都是有效激活状态的情况下，才能被作为可以用的实验账号；
4.

【AM – 管理】和【IAM-实验】的用户名和密码修改后，系统在进行实验的时候要用新的用户名和密码；
5.

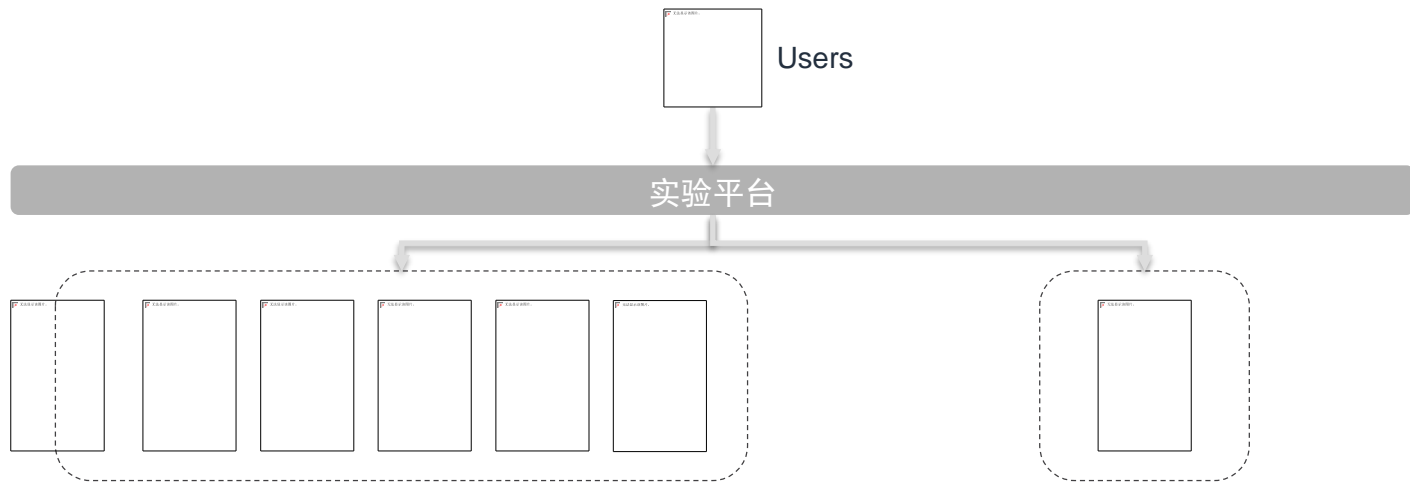
实验结束后后台释放AWS账号在实验过程中创建的资源后，系统在后台自动修改【IAM】为【默认IAM实验密码】，改密码可以在平台的配置界面中进行设置，界面待定；
6.

【当前使用者】会根据后台自动分配实验时轮空的AWS 账号的使用者。

说明一：

- 1.【使用类型】：登录AWS Console，不登录AWS Console；
- 2.每个院系只能有一个不登陆AWS Console的AWS Account，用于只使用计算类资源且不需操作AWS Console的实验；
- 3.选择左侧【院系列表】后，右侧显示对应该院系的【关联账号池】；
- 4.【关联账号池】的标题栏点选后，可以根据该列排序；
- 5.AWS account的创建需要走线下流程单独申请，不在本平台中创建；
- 6.【修改】操作只能在选择一个条目的情况下进行；
- 7.【激活/注销】会改变当前的账号使用状态，需要检查该账号是否有实验进行中，如果有则提前结束实验，清理资源，收回IAM权限；
- 8.【院系列表】的增删改在原【机构管理】中进行；
- 9.【批量导入】用Excel表格把事先创建好的Account ID以及对应的IAM User导入，导入过程中需要查重、验证信息是否正确

# AWS Account （技术参考）



登console的实验多个AWS Account

- 临时/短时实验，学生需登录Console进行操作；
- 分配IAM User，不直接分配root user；
- 基本策略：自动打Tag，禁止创建User.....
- 教师设计实验template时临时取用（需Attach新的role）；

不登console的实验每个学员只有1个 AWS account

- 长期试验，仅提供EC2、RDS等资源的访问权限，不提供console登录；
- 平台层提供基于实验名称打标签的能力；
- 实验平台运维人员掌握Credential

注：因不同实验所需权限不同，应准备不同的IAM role，根据实验内容关联给IAM User

# Resource Release（Console类实验-技术参考）

Lab lifetime

## Initialization

## Execution

## Termination



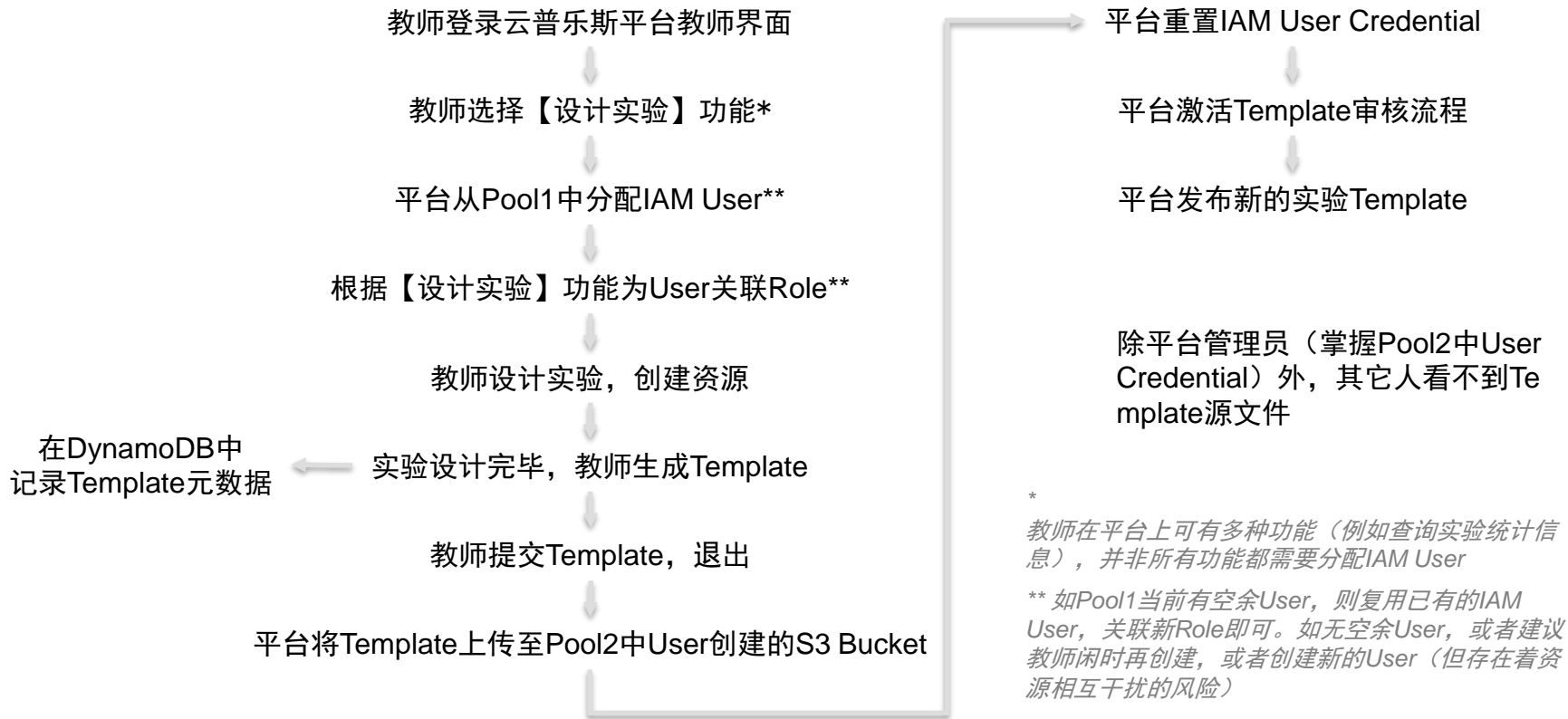
\* Template保存在Pool2

User的Bucket中，仅在初始化实验环境时为Bucket关联Pool1中User的访问权限

\*\* 可参考Auto Tag的blog，对不能打tag的资源（例如：Key-Pair）通过Name记录

\*\*\* 根据Tag删除资源，先删除自建资源，再删除Stack，避免资源关联的依赖

# Lab Design Process（技术参考）



# 学生登录界面参考（仅供参考）

